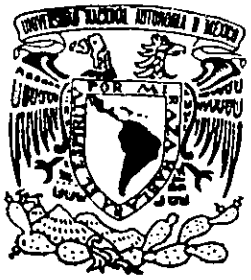
85



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

METODOLOGIA PARA EL ANALISIS DEL RIESGO EN SISTEMAS DE INFORMACION

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A

ANGELICA ZAMORA GONZALEZ

DIRECTOR: ING. RAFAEL ENRIQUEZ VAZQUEZ

CODIRECTOR:

ING. GABRIEL CASTILLO HERNANDEZ

MEXICO, D.F. NOVIEMBRE DE 2000

A DIOS

Por regalarme la oportunidad de vivir
Porque sin su infinita presencia
Mis sueños no serían realidad.
Gracias Siempre Gracias.

A Mis Padres: Aída y Francisco

Por su lucha inquebrantable
Para impulsarnos a seguir adelante
Por transmitirme la vida
Y hacerme parte de la suya.
Gracias! Los Quiero Muchísimo.

A Mis Hermanos:
José Antonio, Francisco, Jeanette y Verónica

Por su apoyo constante,
Porque este logro es parte de ustedes también
Por su paciencia
Por todos esos momentos de alegría que hemos compartido.
Gracias! Son mi mejor ejemplo.

A Mi Tía Raquel

Por haberme dejado compartir una vida contigo
Por ese gran ejemplo de fortaleza
Y amor que nos regalaste
Sé que estarás siempre a mi lado... Te extraño!

A Mi Alma Matter

Gracias a la Facultad de Ingeniería,
A la Universidad Nacional Autónoma de México
Por permitirme llevar su nombre con gran orgullo.

A Gabriel Castillo y Rafael Enríquez

Por brindarme su apoyo,
Compartir conmigo sus conocimientos,
Por su paciencia infinita
Sobretodo Gracias por su Amistad!

Especialmente a todas aquellas personas
Que compartieron conmigo su tiempo,
Sus conocimientos, su amistad
Y apoyo en todo momento:

Rubén Valle: Gracias por creer en mí y ser parte de este sueño que hoy es una realidad

A mis compañeros de Bancomer, en especial a los de Seguridad y Continuidad del Negocio

A mis compañeros y amigos de la Facultad de Ingeniería por todo lo compartido.

Angélica Zamora González

"Atreverse sigue siendo la mejor manera de alcanzar el éxito"

ANÓNIMO

ÍNDICE

CAPITULO IV
SERVICIOS DE SEGURIDAD

CAPÍTULO V
PLAN DE RECUPERACION

CAPÍTULO VI
METODOLOGIA PARA EL ANALISIS DEL RIESGO EN SISTEMAS DE INFORMACION

CONCLUSIONES

APENDICE A
RESEÑA SOBREEL ATLAS NACIONAL DE RIESGOS

GLOSARIO

BIBLIOGRAFIA

Introducción

Hoy en día el énfasis en la seguridad de los sistemas informáticos ha ido incrementado día con día, la sociedad cada vez más hace uso exhaustivo de la información, por pequeña que sea su necesidad. Para todos es sabido que la necesidad de información se ha convertido en uno de los elementos más importantes de una organización, cualquiera que sea su dimensión y su función.

La evolución de la tecnología nos ha facilitado las condiciones para una elaboración, difusión y rápida recepción de información a través de diversos medios como Internet, bases de datos, computadoras portátiles, modems de alta velocidad, satélites, redes, etc. La importancia del envío y recepción de la información radica principalmente en el significado que tenga para nuestra organización. Esta información generalmente incluye datos de cómo funciona nuestra empresa, resultados de investigaciones, nuevos productos y/o servicios, estadísticas, planes estratégicos, procesos e innovaciones entre otras.

En algunas ocasiones la información llega a ser, para una empresa, uno de sus activos más importantes ya que de ésta depende la operación y continuidad de la misma. Sin embargo todos sus demás activos conviven en un ambiente vulnerable a sufrir algún tipo de daño, la identificación, el análisis, la priorización, la corrección y costo de estos es tarea de un análisis del riesgo.

Como se puede suponer no es tarea fácil realizar este análisis, sin embargo el no realizar el esfuerzo podrá, en un dado caso, costarle a la organización la supervivencia en el mercado. En el presente trabajo se presentará una metodología con el fin de realizar el análisis del riesgo de una forma práctica y aplicable para cualquier tipo de organización.

Contenido

En el capítulo I de la presente tesis se describirá los aspectos básicos y fundamentales de la seguridad de los sistemas informáticos y todos aquellos tópicos relacionados para poder conocer e identificar los aspectos más importantes de la metodología que se desarrollará para el análisis del riesgo. Estos conceptos nos permitirán identificar los aspectos más relevantes que deberemos analizar en la práctica de esta metodología.

El objetivo del capítulo II es el plantear la importancia y los fundamentos teóricos a fin de realizar un análisis del riesgo tanto de la organización, como de los sistemas, aplicaciones e infraestructura que engloban la actividad diaria de una empresa, a fin de identificar vulnerabilidades y puntos vitales para nuestra organización.

El capítulo III hace uso del capítulo anterior con el fin de darle una estructura práctica a los conceptos e importancia del análisis del riesgo enfocando éste a la administración y control adecuado de los puntos vitales de una organización disminuyendo así la posibilidad de amenazas e intrusiones de nuestros sistemas sin la cual sería difícil asegurar su funcionalidad.

El capítulo IV tiene como intención presentar la importancia de contar con servicios de seguridad, identificados por el análisis de riesgo, adecuados a cada sistema y/o aplicación en la medida que se tornan vitales para la integración e interacción de la empresa con sus clientes. Este tipo de sistemas y/o aplicaciones se convierten así en criticas y demandan de disponibilidad, confidencialidad e integridad en la información y manejo de datos y transacciones.

En el capítulo V se presentará bajo toda la estructura presentada en los capítulos anteriores el aseguramiento de la continuidad del negocio a través de planes de recuperación basados en el análisis del riesgo de toda nuestra organización.

Finalmente en el capítulo VI se presentará la Metodología para realizar un Análisis del Riesgo, y el caso práctico de un Grupo Financiero junto con los resultados generales obtenidos de su aplicación.

El presente trabajo de tesis es el resultado de la experiencia obtenida dentro del área de Seguridad y Continuidad del Negocio, del análisis y desarrollo de sistemas de información, de soportes a proyectos como "Año 2000", "Contingencia", entre muchos otros dentro del Grupo Financiero Bancomer.

Objetivo

Desarrollar una metodología capaz de analizar y determinar los principales riesgos a los que un sistema de cómputo se enfrenta a fin de que, en la medida de lo posible, sean controlados y podamos contar con sistemas de cómputo seguros.

Capítulo I

Fundamentos de Seguridad en Sistemas Informáticos

Origen de la seguridad en los sistemas información

La protección de la información no es nueva, durante el transcurso de la historia han existido diversos métodos para almacenar, transmitir y proteger la información. En varias áreas en las cuales se desempeña el ser humano como es la economía, política, comercio, etc., la información representa un gran valor. Las decisiones derivadas de esta adquieren un carácter vital así como la rapidez y seguridad con que se maneje. Como es de suponerse esta clasificación de la información tuvo origen en el campo militar y diplomático, a continuación se describe una breve historia de lo que considero son los orígenes de la seguridad de la información.

El origen de la seguridad en los sistemas informáticos se hace presente ante la necesidad de proteger los sistemas operativos con el fin de incrementar y al mismo tiempo facilitar el nivel de servicio de estos. Posteriormente por la necesidad de trabajar diferentes personas al mismo tiempo en un sistema hizo más clara la importancia de asegurar el servicio y proteger a los usuarios de si mismos, es decir se debía de asegurar que no fuera alterado el trabajo de un usuario por otra persona de tal manera que se llegará a alterar un mismo dato por dos personas al mismo tiempo, siendo esta actividad intencional o accidental.

La protección de la paginación del sistema a través de llaves y los mecanismos de manejo de memoria virtual fueron algunas de las soluciones que se generaron ante esta necesidad. Sin embargo una de las tendencias que surgieron fue la generación de sistemas operativos más complejos, respecto a lo que se refiere al manejo de memoria principalmente a fin de que se evitaran alteraciones no deseadas a las áreas de memoria que manejan los sistemas operativos. A pesar de esta primera medida la seguridad se complicó más al contrario de lo que se hubiera esperado.

Uno de los primeros obstáculos con que se encontraron las organizaciones fueron principalmente la falta de difusión de la importancia de la seguridad en los sistemas además de lo costoso que resultaba adquirir o desarrollar métodos y sistemas que protegieran la información. El concepto que se tenía acerca de la seguridad de información dentro de las organizaciones se enfocaba únicamente al resguardo físico de los equipos y de la infraestructura corporativa , los edificios, las oficinas, las bodegas de almacenamiento etc. Tuvieron que suceder hechos lamentables para algunas organizaciones e incluso para algunos gobiernos para que se empezara a tomar con más seriedad y profundidad el tema de la seguridad de la información.

Además de estos hechos sociales, la tecnología incremento la importancia del aseguramiento de la información. Durante los años de 1960 y 1970, la computación y las comunicaciones se transformaron y con ellas la forma en que los usuarios hacían uso de la información. La multiprogramación, el multiproceso y las redes de comunicación cambiaron dramáticamente las reglas del juego. Ahora era posible que los usuarios podían interactuar directamente con los sistema de cómputo a través de una terminal, otorgándoles más poder y flexibilidad dando como consecuencia nuevas posibilidades de alteración a los sistemas.

Las telecomunicaciones cambiaron radicalmente el uso de las computadoras. La facilidad y flexibilidad del acceso a las computadoras tuvieron gran impacto en la educación y las organizaciones fueron generando nuevos y variados usos de la información.

Como es lógico todas estas ventajas que antes no se tenían generaron un precio, el abuso y manejo de la información el ataque a los sistemas de información, las intrusiones a través de líneas telefónicas, el robo de información y la preocupación constante acerca de la vulnerabilidad de todo el entorno informático.

En los años 80's con la introducción al mercado de las computadoras personales crearon usuarios de todas las edades y ocupaciones en lugares como la casa o la oficina lo que dio origen a que muchos negocios pequeños pudieran automatizar sus operaciones diarias, así pues las PC's trajeron consigo nuevas formas de riesgos. En este aspecto el robo de información se incrementó dado que resulta mucho más fácil copiar información confidencial en un disquette sin ser fácilmente detectado.

Con la llegada de las PC se incrementó la comunicación entre usuarios a través del correo electrónico, la Internet, etc. aumentó el riesgo para los sistemas y al mismo tiempo aumentó la necesidad de la seguridad de nuestros sistemas e información.

Todo este desarrollo de nuevas tecnologías fue el resultado de la necesidad de comunicación que fueron generando las organizaciones para sobrevivir a un mundo cada vez más globalizado. La tarea de la seguridad de nuestros sistemas no es fácil puesto que cada día se generan nuevas formas de ataques, intrusiones, y de virus que destruyen nuestra información, es indispensable contar con herramientas que nos permitan reducir el riesgo invariablemente latente en la vida diaria de nuestros sistemas.

Conceptos básicos acerca de la seguridad

En la presente época informática que estamos viviendo es difícil encontrarse con empresas que se sientan cien por ciento seguras de ataques, virus e intrusiones a sus sistemas. La era actual nos demanda día con día estar al tanto de nuevas tecnologías, así como de las nuevas modalidades de ataques que se pueden presentar en nuestra información. Así pues es indispensable conocer los conceptos básicos que nos permitan entender la importancia de la seguridad en nuestros sistemas informáticos e implantar una cultura laborar que nos permita reducir eficazmente este riesgo.

Para entender el papel de la seguridad de los sistemas en su entorno es necesario entender que no se trata de un ente aislado que se crea ajeno a los sistemas o programas, al contrario para que un sistema de información se considere seguro deberá encontrarse la seguridad presente en todos los ámbitos del negocio u organización.

La seguridad es una estructura que se conforma de varias entidades que por lo general siempre están presentes dentro de una organización pero que comúnmente no conocen el papel que juegan dentro de esta. Ahora bien aunque se encuentre establecida toda una estructura de seguridad esta puede resultar totalmente inútil si no existe la cultura para hacer uso y explotación de esta.

Las entidades que conforman una estructura de seguridad en forma general se podría definir de la siguiente manera: (figura 1)

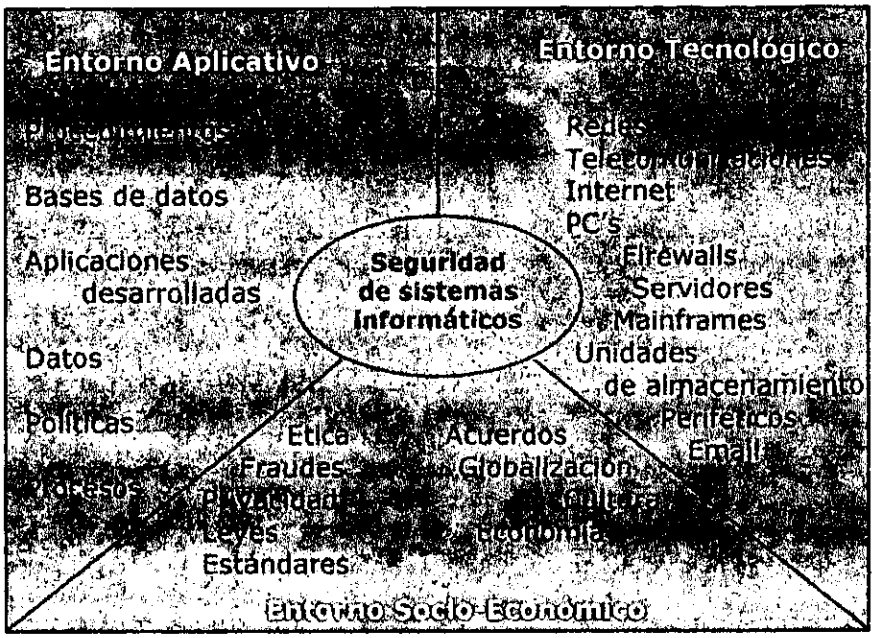


Figura 1. Entorno de la Seguridad de Información

Entorno Socio-Económico.

Organizaciones, empresas, grupo de personas, escuelas, organizaciones gubernamentales, etc. Aunque pudieran resultar distintas entre ellas mismas comparten un objetivo en común: la continuidad de su negocio, es decir ¿quién de estas quisiera ver a su empresa en la quiebra por un ataque de virus o por fuga de información ponga en riesgo a la empresa? .

Los empleados, son ejecutores de nuestros esquemas de seguridad, es decir no pretendamos esperar que una herramienta de seguridad nos diga que hacer y tome decisiones a través de los resultados que nos muestre. Ahora bien es de suma importancia difundir hábitos de seguridad en nuestra empresa, los casos sino más relevantes sí los más comunes ocurren dentro de la organización, es decir por gente que trabaja aparentemente para ayudarnos a cumplir nuestro objetivo en común.

Debido al compromiso social que adquiere una organización al ofrecer cualquier tipo de servicio a sus clientes es necesario que este cuente con un buen control de la información que le proporcionen sus clientes así como el manejo que interno que le de a la misma. Toda esta *información debe ser manejada en forma confidencial de tal manera que no se arriesgue la* veracidad de la misma además de la reputación de la organización poniendo así en riesgo su futuro.

Estos factores y otros más que se presentaran más adelante serán la base de un plan estratégico de seguridad para los sistemas informáticos y por lo tanto será responsabilidad primeramente de *un área específica encargada de vigilar su cumplimiento además de mantenerse a la vanguardia* en cuanto a mejoras de seguridad como a los posibles ataques que pudiera sufrir la organización, sin olvidar obviamente la difusión de una cultura laboral que no ponga en riesgo información relevante.

También es necesario que los gobiernos, sobre todo los latinoamericanos, entiendan esta necesidad acerca de la seguridad de información a través de la implantación de leyes que permitan a las organizaciones y empresas defenderse de ataques a su información y sistemas.

Entorno Tecnológico

El desarrollo tecnológico que actualmente estamos viviendo es sumamente vertiginoso, pudiera decir que para una organización es costoso seguir la carrera que lleva esta, a pesar de esto es necesario tener presente los beneficios que se tienen al estar a la vanguardia en cuanto a tecnología se refiere. Sin embargo esta debe de estar bien respaldada a través de las políticas de uso de las mismas, tampoco es benéfico para una empresa adquirir todo las novedades que se desarrollen sin establecer una serie de pruebas que cumplan con las políticas de seguridad que se encuentren vigentes antes de convertirla en un estándar de trabajo.

El envío, recepción y validación de la información hace uso constante de la tecnología, a través del hardware, redes, satélites, modems, terminales, unidades de control, computadoras, etc.

Aunque la presente tesis no tiene como objetivo explicar la estructura y protocolos de seguridad con los que funcionan estos medios para la transmisión de datos, si es necesario que este punto sea tratado con suma importancia y delicadeza a fin de asegurar "tecnológicamente" el manejo, envío, recepción y validación de nuestra información. Paradójicamente el costo de la tecnología que utilicemos incrementará el esfuerzo, recursos y conocimientos que tendrá que tener una persona o grupo de personas que tengan como objetivo penetrar nuestros sistemas de información.

Entorno Aplicativo

Tal vez este entorno sea el que ponga más a prueba las políticas y tecnología que usemos para el manejo de nuestra información ya que a través de las aplicaciones que se desarrollen o se adquieran es como validaremos el uso adecuado o no de nuestra información.

Una de las medidas posibles que puede tomar una empresa para empezar a reducir los ataques y mal manejo a sus sistemas es implantando medidas de calidad en las cuales se establezcan estándares para el desarrollo y compra de sistemas de información.

Hoy en día es muy costoso darse el lujo de adquirir o desarrollar sistemas sin ningún control de calidad o por simple gusto, en la medida que se eviten la toma de decisiones de este tipo sin un análisis previo tanto del beneficio que nos proporcione, como del riesgo en el que nos incurra la falta de estándares de seguridad para nuestra organización, se estará avanzando en la protección de nuestra información como de la cultura de seguridad que establezcamos en nuestros empleados.

La seguridad en el entorno aplicativo se refiere a el control que debe contener la programación de las aplicaciones o sistemas, lo que implica la estructura de la aplicación para soportar los servicios, segregación de las funciones, ediciones, confirmaciones, así como de los logs o registros que esta genere. Es obvio que se debe tener una restricción a este tipo de información, a fin de que nadie llegara a alterar las funciones de un sistema.

Así pues podemos concluir que estos tres entornos funcionan en conjunto, la falta de alguno de ellos generará en una forma u otra fuertes debilidades en nuestros sistemas de información.

Más adelante se tratará con mayor detalle el tipo de controles que deben de encontrase al menos en el desarrollo o adquisición de un sistema de seguridad y que tan estrictos deben ser estos dependiendo del tipo de información que maneje.

A continuación se explicarán algunos de los estándares y definiciones básicas de seguridad que se conocen para considerar a un sistema de información seguro

¿ Qué es un sistema seguro?

Un sistema de información, redes, comunicación, etc. para ser seguro deberá cumplir con los siguientes tres propiedades básicas de seguridad:

* Confidencialidad
* Disponibilidad
* Integridad

La **Confidencialidad** de un sistema se refiere a que la información contenida en él será mostrada o ejecutada siempre que se cumplan las políticas establecidas, es decir quién o quienes pueden ver o modificar cierta información y quienes no.

Asegura que la información controlada por el sistema no se utilice si se accesa a ella violando las políticas de control de acceso. Los mecanismos de confidencialidad pueden proteger el contenido de comunicaciones, el contenido de archivos y bases de datos, programas, tablas de programas y otros archivos requeridos por el sistema. Se utilizan técnicas de cifrado para proveer confidencialidad.

El proceso de confidencialidad de un sistema de seguridad es responsable de asegurar que los datos y las comunicaciones que han sido obtenidos por programas, o individuos no autorizados, no puedan ser usados; al mismo tiempo que garantiza la no divulgación de la información. El uso de algún mecanismo de confidencialidad refleja el hecho de que los mecanismos de control de acceso pueden no suministrar una completa protección para todos los recursos del sistema. También refleja el hecho de que ciertos recursos (por ejemplo: comunicaciones que pasan a través de medios públicos no seguros) son esencialmente difíciles para proteger usando técnicas de control de acceso.

La **Integridad** se refiere a que nuestra información no sea corrompida o alterada por entidades ajenas a nuestra empresa o negocio, cuidando así el desempeño de nuestros sistemas a fin de que podamos proporcionar un servicio de calidad a nuestros clientes o usuarios.

El componente de integridad de un sistema de seguridad intenta asegurar que la información y las comunicaciones no puedan ser cambiadas. También asegura que los cambios no autorizados a la información y comunicaciones sean detectables aunque no sean reversibles.

Los sistemas deben proveer la integridad a:

- Mensajes y otras información que circulen a través de redes de comunicación.
- Información de negocio en archivos y bases de datos computarizados.
- Programas y otros componentes de sistemas.
- Los componentes del sistema de seguridad propiamente dicho.

Finalmente la **Disponibilidad** en un sistema tendrá como característica un servicio ininterrumpido a fin de contar con él en cualquier horario y circunstancia.

Asegura que todas las facilidades del sistema, incluyendo servicios de seguridad, estén disponibles al ser requeridos para las aplicaciones de negocio y para la infraestructura del sistema. La disponibilidad puede ser mejorada al desarrollar mecanismos que reduzcan el peligro de daños a la integridad del sistema y también al colocar servicios de seguridad redundantes en las diferentes plataformas.

La disponibilidad tiene dos objetivos:

- Asegurar que el sistema de seguridad esté disponible suministrando servicios de seguridad a los cuales se pueda accesar a través de diferentes vías de comunicación.

- Suministrar mecanismos que minimicen el paso por el sistema el cual se volverá no disponible como un resultado de ataques accidentales, o deliberados, a la estructura del sistema (por ejemplo: virus, mensajes adulterados o paquetes denominados cadena de comunicación, daño a: sistemas de operación, programas de comunicación y computadoras físicas y hardware de comunicación).

Ahora bien, aunque estas 3 características son la base de la seguridad existen diferentes entidades que interactuan entre ellas para poder asegurar su buen funcionamiento y así poder hablar de la seguridad de la información tanto generada como trasmitida de nuestros sistemas de información.

Para poder entender mejor el valor de estas características dentro de un sistema de información suponga que, usted es el administrador del sistema de una compañía financiera y en un día cualquiera se interrumpe el proceso. Hoy en día la mayor parte de las organizaciones se encuentran aseguradas y por lo tanto al mismo tiempo tienen evaluado el costo por segundo de la falla de sus sistemas de información; sin embargo esto no elimina el impacto que representa para una organización el no poder brindar sus servicios normalmente. En el caso de una organización financiera es realmente critico la interrupción de sus servicios, suponga que debido a una falla no se ha podido depositar la nómina de una empresa gubernamental y que esta tardará por lo menos medio día.

En este punto nos encontraríamos en la posición de restaurar el ambiente con nuestros procedimientos de recuperación previamente elaborados a través de nuestro plan de contingencia, mismo que se explicará más adelante. Después de recuperado el ambiente se realizaría la investigación de qué , quién, cómo, y con que se efectuó esta falla en el sistema, ahora bien no solo resulta importante contar con dicha información. Finalmente lo que es más importante que otra cosa es el tomar las medidas necesarias para poder evitar, en la medida de lo posible, este tipo de eventos no deseados en nuestros sistemas de información.

Así pues podemos ahora evaluar las tres características principales de la seguridad de la información. La Confidencialidad es una de las más avanzadas áreas de la seguridad de los sistemas informáticos, por lo menos lo es en Estados Unidos, principalmente por el desarrollo que le ha impulsado los Departamentos de Defensa con el fin de mantener esta propiedad en la información clasificada. Esta ardua investigación dio origen al departamento encargado de establecer el criterio de evaluación para sistemas de cómputo confiables, mejor conocido como el DOD (Department of Defense Trusted Computer System Evaluation Criteria) o como el "Orange Book".

Respecto a la Integridad de un sistema de información puede ser evaluada a través de la comparación del estado del mismo en condiciones normales u originales (antes de procesar información) y un estado diferente a este. Un sistema de información que ha sido modificado por un elemento sin la apropiada autorización se dice que este ha sido "corrompido".

Sin embargo no podemos decir que la integridad de un sistema de información es asegurado solo a través del control de acceso a la misma. Esto debido principalmente al desarrollo constante de nuevas tecnologías de acceso a la información y por otro lado a la inminente necesidad de ofrecer servicios de información y transacciones a través del comercio electrónico, entre otras.

Finalmente la disponibilidad de un sistema de información y de sus interfaces accesibles y funcionales asociados a él a fin de que proporcione el o los servicios en el momento y lugar en el que dispongamos del mismo. Cuando ocurre un evento que llegue a alterar esta propiedad se dice que ha ocurrido una negación del servicio. Por ejemplo supongamos que un elemento genera un virus que absorbe demasiado tiempo de procesamiento y esto hace que el sistema se sature.

Esta propiedad es la que se encuentra mejor desarrollada de las tres, esto es por razones técnicas ya que están involucrados verificaciones de estándares para cualquier diseño, obviamente que este requerimiento en especial dependerá de las regulaciones vigentes de cada país. Es aquí en donde se puede entender mejor el valor de contar con estándares, políticas y medidas de calidad que nos permitan, por lo menos disminuir este riesgo en la medida de lo posible. En México este tipo de regulaciones son escasamente practicadas aunque a través de crudas experiencias se ha ido avanzando en este campo, a este tipo de actividades se les conoce como políticas de seguridad.

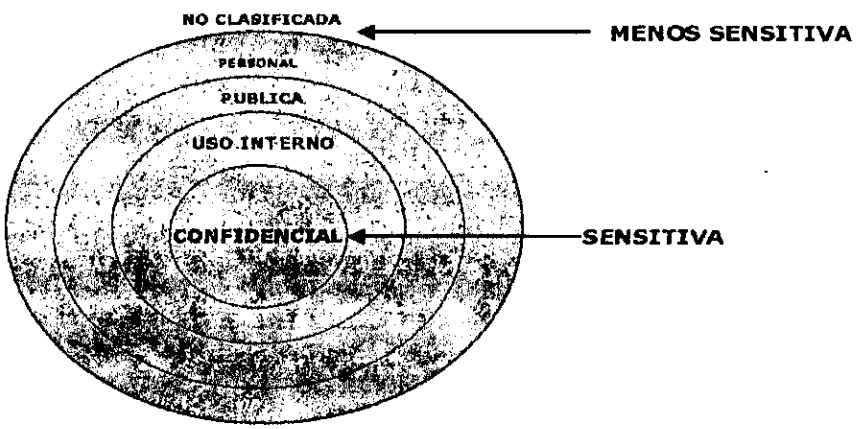
Las políticas de seguridad, básicamente, se definen con el fin de establecer que tipo de elementos pueden comunicarse con que otros objetos. Más adelante en el capitulo IV se explicará ampliamente este tema y su importancia para mantener la seguridad de un sistema de información.

Así pues el paso inicial lógico de la seguridad en computo es el análisis de la información, es decir, que tipo de información manejamos, si ésta es confidencial, privada, pública o personal y si lo es que tan critica es y por supuesto porque razón no lo es. Esto claro dependerá de nuestro negocio, por ejemplo en una institución bancaria se maneja diferente información a la que maneja una empresa de consultoría o una agencia de viajes.

Clasificación de Información

Dentro de cualquier organización podemos encontrar los siguientes tipos de información:

- Confidencial
- Uso Interno
- Pública
- Personal
- No clasificada



La clasificación de la información que manejemos nos ayuda en gran medida a determinar las áreas y puntos focales de nuestra organización más fácilmente que requieren de especial atención y cuidado además nos ayuda a determinar que medidas de seguridad se aplicarán para cada tipo de información

A continuación se presentará una breve explicación de la definición y el manejo del tipo de información más importante:

Información Confidencial

Es aquella, que de ser conocida por terceros, podría dar lugar a ventajas indebidas a los competidores o bien ser perjudicial para la organización o sus empleados, la cual incluye:

- Datos financieros que no se hayan publicado, proyecciones financieras y presupuestos.
- Planes y esfuerzos de desarrollo de nuevos productos y servicios así como ciertas estrategias comerciales
- Prácticas, métodos, sistemas y equipos de proceso y seguridad, cuando no sean de dominio público y representen una ventaja competitiva.
- Identidad de los clientes así como el tipo y magnitud de negocios que con ellos se realiza.
- Errores, deficiencias y problemas específicos que pueden ocurrir en el curso de las operaciones de la organización.
- Cualquier información contenida en documentos explícitamente marcados como confidenciales.

Manejo de Información Confidencial

El acceso a información confidencial debe darse exclusivamente a los empleados que tienen la necesidad de conocerla para el correcto desempeño de su puesto, y no implica autorización alguna para usarla de otra manera ni para divulgarla fuera de la organización o a otros empleados que no la requieran para realizar su trabajo.

Información Interna

Es aquella que se genera dentro del flujo normal de trabajo y se difunde en forma más o menos amplia entre determinadas personas o áreas de la organización. Sin embargo, fuera de su contexto, puede ser mal interpretada y dar pie a rumores infundados o comentarios insidiosos, no solo de personas ajenas sino también entre el propio personal; algunos ejemplos son:

- Políticas y procedimientos de operación, formatos de uso interno, indicadores de productividad y estándares de desempeño.
- Estructuras de organización, funciones y responsabilidades de áreas, perfiles y descripciones de puestos, agendas de labores.
- Estudios y dictámenes de áreas especializadas, información estadística sobre las operaciones y los mercados, memorándums y circulares internas.

Manejo de Información Interna

La información interna puede fluir libremente entre las áreas y personas de la organización para las que sea relevante, sin que esto signifique que se debe promover su difusión a todo el personal, a menos que así lo especifique el área que la origine.

Información Pública

Corresponde a la información que los canales autorizados por la organización han dado a conocer a los medios masivos de comunicación o a entidades externas con el propósito específico de darle la más amplia difusión. Se incluyen:

- Estados financieros periódicos cuya publicación en prensa es una obligación legal.
- Informes periódicos o eventuales que se entreguen a organismos oficiales y/o autoridades.
- Informes de resultados que se entregan a analistas financieros y bursátiles.
- Boletines de prensa que se entreguen a los medios.

Manejo de Información Pública

Es política, para algunas organizaciones, anunciar públicamente datos importantes lo antes posible conforme lo permitan las circunstancias, dada la necesidad de mantener la confidencialidad de la información hasta que se toman las decisiones finales, para no otorgar ventajas innecesarias a la competencia.

Así pues para realizar un esquema para la clasificación de datos se debe incluir:

- Políticas de seguridad que permitan la clasificación de los datos
- Niveles de clasificación de la información
- Procedimientos y reglas para el control de acceso a los datos
- Procedimientos y reglas para el control del almacenamiento, período de retención y disponibilidad de información.
- Control en los logs de información que permitan validar la aplicación y funcionamiento de los procedimientos y reglas.

Existen diferentes tipos de criterios que nos pueden ayudar a realizar la clasificación de la información, una de estos posibles criterios involucra el análisis de la información de las siguientes características:

- Cantidad de información

Es claro saber que la cantidad de información tiene implicación directa con los procesos que maneja dado que implica mayor consumo de recursos informáticos y si en su caso esta información es sensible implicará mayor atención a la misma.

- Edad o tiempo de la información y Vida útil

Toda la información que se genera tiene un tiempo de vida útil, por ejemplo los programas tienen un tiempo de vida de algunos años dependiendo de las nuevas versiones de software que se vayan generando y de la evolución de la tecnología. Los datos de mercadotecnia y planes de trabajo tienen una vida útil más corta debido a sus características.

- Número de dependencias y Alcance

El nivel de clasificación de los datos puede variar de acuerdo a sus dependencias con otros datos o procesos, por ejemplo el CURP (Clave Unica para el Registro de Población) es un dato que se encuentra asociado a la identificación de una persona y que de esta depende que se le otorguen o no ciertos servicios a una persona.

- Criticidad

Aunque la criticidad es comúnmente asociada a los sistemas más que a la propia información sin embargo puede clasificarse de acuerdo a su criticidad. Por ejemplo las estrategias de mercado, lanzamiento de nuevos productos, configuraciones, etc.

Los dueños de la información son los responsables de clasificar los activos de información por los que son responsables. Por lo menos una vez por año, los propietarios de la información deben revisar la clasificación de ésta para asegurarse que siga clasificada correctamente, y que los controles de acceso estén funcionando.

A continuación se presentará un modelo de arquitectura de seguridad aplicable para cualquier organización tomando en cuenta los conceptos anteriormente presentados a fin de comprender los mecanismos básicos de seguridad, entendiendo como mecanismos aquellas herramientas y técnicas usadas para implementar los servicios de seguridad.

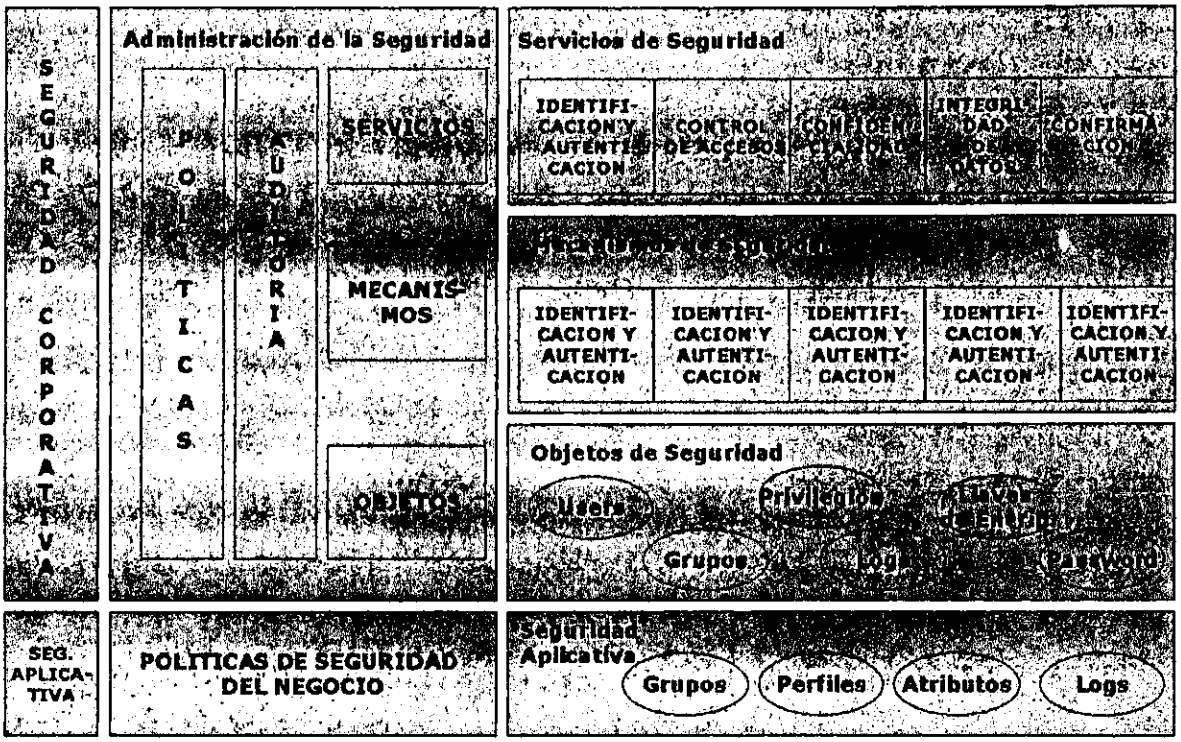


Figura 3. Mecanismos Básicos de Seguridad

Seguridad Corporativa

Esta capa define todos los servicios disponibles para la protección de un sistema o aplicación. El objetivo de esta capa de seguridad es marcar los lineamientos generales que deberán cubrir los sistemas o aplicaciones.

Seguridad Aplicativa

Determina el detalle de seguridad que requiere un sistema o aplicación, tal como qué usuarios deben accesar el sistema y qué perfiles o atributos, la elección de llaves de encripción, etc. es responsabilidad del propietario de dicho sistema, es decir, el usuario en conjunto con el líder de proyecto determinará qué otros rasgos de seguridad que requiera el negocio deberán implantarse.

Objetos de Seguridad

Son aquellos recursos que pueden ser utilizados por cualquier componente del sistema para verificar la autenticación de usuarios, control de acceso a recursos, integridad, confidencialidad de información. Dentro de los diferentes objetos de seguridad podemos encontrar: claves de usuarios, passwords, atributos por usuario, niveles de acceso, llaves de encripción, etc.

Los mecanismos permiten brindar los servicios de seguridad con mayor o menor grado de complejidad. Para fines prácticos es recomendable en una primera etapa utilizar los mecanismos básicos y construir sobre estos los servicios para proveer la seguridad necesaria en forma rentable y eficiente.

Los servicios de seguridad y los mecanismos básicos con los que se pueden proveer estos servicios son mostrados en la siguiente tabla.

	SERVICIOS DE SEGURIDAD				
Mecanismos	Control de Accesos	Confidencialidad	Autenticación	Integridad De Datos	Confirmación
Cifrado		✓		✓	
Firma Digital			✓		✓
Control de Acceso	✓				
Autenticación de la Entidad			✓		
Autenticación de Mensajes			✓		

Figura 4. Servicios de Seguridad y Mecanismos Básicos

Todos los componentes y conceptos de seguridad arriba mencionados servirán como antecedente para comprender los conceptos a aplicar en la metodología para Análisis del Riesgo que se explicará en el capítulo II del presente trabajo.

Capítulo II

Análisis del Riesgo

Definición.

La seguridad en los sistemas de cómputo, como ya hemos visto es extensa por si misma, sin embargo esta es posible llegar a acotarla de tal manera que en la medida de lo posible se llegue a reducir riesgos a nuestros sistemas.

¿Qué es un Riesgo?

Un riesgo se define como cualquier evento no deseado que altere, dañe o destruya nuestros sistemas por ejemplo, los virus informáticos, los ataques de gente ajena o con fines diferentes al de nuestra organización, software mal configurado o desarrollado, falla de hardware, redes, asaltos, fraudes, bombas, etc., durante ciertos períodos de tiempo.

Una amenaza es un evento que puede causar daño a un sistema de información, las amenazas pueden ser causadas por diversos factores como pueden ser: naturales (ejemplo: Terremotos, inundaciones) Intencionales (personas inconformes dentro de la misma empresa, hackers), y el riesgo, es la probabilidad de que una de esas amenazas que pudieran sea una realidad y cause un daño para nuestro entorno informático.

Así pues el Análisis del Riesgo es una serie de pasos a través de los cuales se identifican los riesgos a los que se encuentra expuesto una organización cualquiera, en sus diferentes rubros además de que conocer en cuáles de ellos podemos tomar alguna acción, cuáles se asumirán según su costo y cuáles otros de nuestros activos (edificios, sistemas, aplicaciones, etc,) debemos prestar mayor atención. Además se estiman las pérdidas potenciales resultantes de la(s) vulnerabilidad(es) de los sistemas y cuantificar los daños en caso de ocurrir alguna amenaza.

Por otro lado el análisis del riesgo es una solución que nos permite identificar problemas y su probabilidad de que ocurran estos eventos en un determinado tiempo. Es también un método para estimar las posibles pérdidas en caso de ocurrir algún evento no deseado.

Naturalmente el Análisis del riesgo es uno de los elementos que conforman la seguridad de los sistemas, así misma se compone de otros que permiten identificar a una aplicación crítica de una no critica para finalmente formar parte de un plan de contingencia que nos permita en la medida de lo posible recuperar y dar continuidad a nuestro negocio.

En términos más simples se puede decir que el análisis del riesgo es una metodología que nos permite conocer la importancia de nuestros sistemas de información para nuestra organización y que tan lejos nos encontramos para considerar que estas se encuentran adecuadamente seguras.

El análisis del riesgo no solo involucra a los sistemas, también son considerados como elementos focales los recursos tangibles, el edificio donde se encuentra ubicada nuestra organización, el equipo de cómputo, el cableado, las antenas, etc., de tal manera que podamos evaluar como tratar de protegerlos. Aunque en algunos casos valor de un negocio es determinado a partir de la información que se genera de estos componentes tangibles.

Algunos casos recientes de ataques a sistemas de diferentes organizaciones nos recuerdan la vulnerabilidad que pueden encontrarse las mismas ante este tipo de eventos inesperados; aunque no llegaran a causar graves daños.

Sin embargo el hecho de que nuestra organización no haya sido víctima de este tipo de eventos siempre se encontrará en riesgo de sufrir algún fraude, errores humanos (o de usuario) accidentes y desastres naturales así como de un sabotaje o cualquier otro acto en contra del objetivo de la organización.

La finalidad del presente trabajo no es alarmar a nadie, simplemente es crear una cultura de seguridad que nos permita estar consientes y preparados, en la medida de lo posible, de cualquier tipo de evento que pudiera dañar nuestro entorno de trabajo.

Es necesario entender la importancia de los sistemas de información dentro de nuestra organización desde el punto de vista que estos nos permiten ofrecer calidad a nuestros servicios, proyectando seguridad y seriedad ante la información delicada que nos confíen nuestros clientes basándonos en políticas y reglas de seguridad efectivas que nos permitan cumplir con nuestro trabajo y no entorpecer nuestros servicios.

Objetivo del Análisis del Riesgo

El análisis del riesgo tiene como propósito proporcionar el estado de vulnerabilidad en el que se encuentra nuestra organización en cuanto a la seguridad de nuestros sistemas de información. Esta información resultará de gran importancia para la toma de decisiones tanto de nuestra forma de trabajo, como del futuro a corto y a largo plazo de nuestro negocio.

Es necesario mencionar que el análisis del riesgo no es de ninguna forma una metodología para asegurar al 100 por ciento nuestra organización, sin embargo es uno de los pasos y cultura que debemos de considerar para tratar de prevenir en la medida de lo posible nuestra organización.

Uno de los principales objetivos del análisis del riesgo es el encontrar el balance entre el aspecto económico, el impacto del riesgo y el costo de implantar la prevención y protección de nuestros sistemas.

Beneficios

- Muestra el nivel de seguridad en el que se encuentra actualmente nuestra organización.
- Identifica la(s) área(s) en las que es necesario tomar medidas de seguridad de forma inmediata.
- Justifica las medidas que se tomen para disminuir el riesgo de acuerdo al análisis obtenido.
- Refuerza la necesidad de establecer como política de la organización una cultura de seguridad que nos permita disminuir los riesgos de forma conjunta.
- Proporciona criterios para el diseño y evaluación de un plan de contingencia

Debe comprenderse que el análisis del riesgo de ninguna manera es una actividad estática, ésta debe transformarse y crecer junto con la misión, estrategia y la(s) nueva(s) tecnología(s) que vaya adoptando la organización.

Tipos de Análisis del Riesgo

Existen dos tipos de análisis de riesgos: cuantitativo y cualitativo. Ambos tipos de análisis se inician con la identificación de los riesgos individuales asociados con un medio ambiente, función o característica específica. Los riesgos pueden presentarse en forma de **amenazas** o **disparadores**

Las "Amenazas" son riesgos existentes (conocidos) que amenazan el medio ambiente, la función que esta bajo análisis. Una amenaza pude definirse también con una condición o circunstancia dañina que ha provocado problemas en el pasado. Por ejemplo, la escalera de acceso a un área es muy empinada puede parecer peligrosa, pero si no existen un registro de accidentes en un determinado período de tiempo, en ese caso la escalera deja de ser considerada como una amenaza.

Si han existido accidentes que puedan atribuirse a la escalera, la amenaza aumenta a medida que el número de accidentes aumenta, durante un periodo de tiempo

Los "Disparadores" son condiciones que no existen actualmente pero que pudieran ocurrir y por lo tanto sugerir una situación peligrosa. Un ejemplo de un disparador común es el clima. El clima puede causar desastres de diferentes dimensiones que pudieran llegar a afectar a nuestra organización, de lo cual se hablará más adelante en este capítulo

Disparador es también el término que se utiliza comúnmente para describir una condición que surge solamente cuando otras amenazas o disparadores obligan a alguien a realizar actividades que no son comunes. Un ejemplo podría ser el esfuerzo de recuperación requerido en caso de que se presentaran diversos disparadores:

- La disponibilidad y confiabilidad de los servicios de energía eléctrica y telefónica en un sitio seleccionado para reanudar las actividades de negocios es algo que puede ser más que anticipado.
- Podría asumirse incorrectamente que se dispondrá de medios de transporte para mover al equipo y al personal inmediatamente después de un siniestro.
- Las condiciones climatológicas extremas pueden afectar adversamente los viajes y las comunicaciones de emergencia.
- La seguridad física y lógica así como los procedimientos de acceso en un sitio de recuperación pueden no haber sido suficientemente bien detallados o comunicados a todos los involucrados.

Después de que los riesgos individuales (amenazas y disparadores) han sido identificados las similitudes entre los análisis de riesgos cuantitativo y cualitativo se acaban. Las siguientes definiciones ponen en relieve las diferencias básicas

Análisis del Riesgo Cuantitativo

Es la cuantificación de las probabilidades de ocurrencia de un evento por medio de la asignación de un factor de probabilidad que representa un período de tiempo específico. El análisis del riesgo cuantitativo se utiliza principalmente para el desarrollo de tablas actuariales de seguros.

Análisis del Riesgo Cualitativo

Es la cualificación de las probabilidades de que una situación específica pueda ocurrir o recurrir por medio de la asignación de probabilidad alta, mediana o baja. El análisis del riesgo cualitativo se utiliza principalmente para el análisis del riesgo puramente físicos o lógicos con objeto de establecer las medidas preventivas o correctivas apropiadas así como diseñar, evaluar y adoptar las alternativas necesarias

En la metodología que se presenta en el capítulo VI, se tratará solamente el análisis del riesgo cualitativo que es el que resulta más práctico en términos de lo que puede implantar una organización con su propio personal, dejándole el análisis cuantitativo a las compañías de seguros que son las indicadas de realizar este tipo de estudio de forma más detallada y correcta.

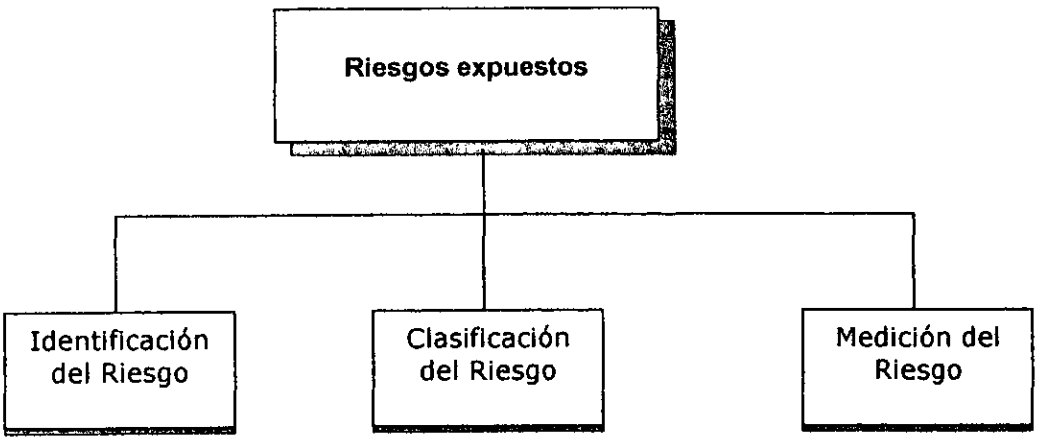
El primer paso que se debe de seguir para iniciar el análisis del riesgo será el identificar los riesgos a los que se encuentra expuesta la organización. Para ello deberán de identificarse los tipos de riesgos a los cuales es posible que se enfrente la organización, por ejemplo: incendio, robo, inundación, plagio, etc. Si alguna de estos eventos ocurriera cuales serían las preguntas lógicas que nos haríamos:

- ¿Qué efecto tendrá en las operaciones de la organización?
- ¿Cuál sería el efecto que causaría la pérdida de documentos vitales en la capacidad de operación de la organización?
- ¿Si fuera secuestrada alguna persona clave en las decisiones de operación del día a día de la compañía quién podría realizar esta función?
- ¿Qué efecto tendría que se dieran a conocer las estrategias del negocio u operación de la organización a personas ajenas a ésta?

Estas son algunas de las preguntas iniciales que debe hacerse el equipo encargado de iniciar un análisis del riesgo.

Para poder lograr esto debemos, como segundo paso, "Estimar la probabilidad de ocurrencia". ¿Cuál es la probabilidad de que ocurran ciertos eventos en el entorno en que se encuentra nuestra organización?. Podría resultar una tarea fácil siempre y cuando se tengan reportes históricos que nos permitan calcularla, obviamente existen algunos eventos que son más difícil de calcular de otros, como la violencia, el espionaje industrial, robos no detectados, desórdenes civiles como las manifestaciones y amotinamientos, etc.

Así pues el tercer paso a considerar es la "Cuantificación de Pérdidas", la cual calcula el impacto o severidad del riesgo si ocurriera alguno de los eventos mencionados anteriormente.



Riesgos Expuestos

Los riesgos o amenazas a los que se encuentra expuesta una organización son variados lo más recomendable es conocerlos y clasificarlos con el fin de ayudarnos a identificar a cuales de ellos nos encontramos expuestos y porqué razón.

Identificación del Riesgo

Con la finalidad de realizar un análisis del riesgo efectivo de nuestros sistemas de información es necesario realizar esta tarea de una manera sencilla y manejable para todos los involucrados, basándose en alguna herramienta de investigación.

Debido a que los sistemas de información generalmente están compuestos por subsistemas es necesario planear cuidadosamente este análisis, esta necesidad de planear resulta de la premisa de que la seguridad de los recursos se encuentra limitada y por lo tanto habrá que realizar un análisis profundo.

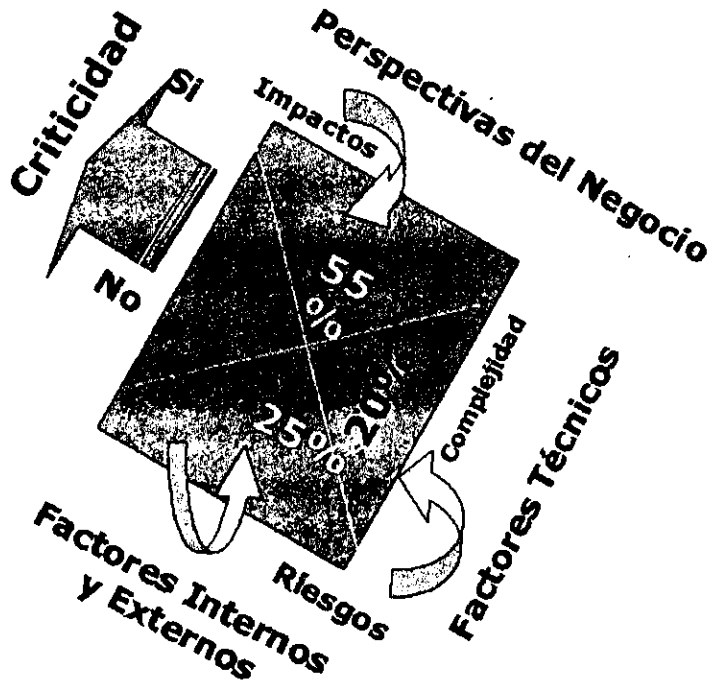
Ahora bien existen dos momentos, si así podemos llamarle, en donde se puede realizar el análisis del riesgo en los sistemas de información, uno es durante la realización del diseño funcional y técnico del sistema; el segundo es ya cuando se encuentra este instalado y operando en producción.

Es natural pensar que es más recomendable realizar este análisis el primer momento y así es, sin embargo esta no es una cultura que se lleve a cabo hoy en día en el diseño de los sistemas. Algunas de las ventajas de realizar este análisis en el diseño de los sistemas son:

- Nos ayuda a determinar la criticidad del sistema a desarrollar a fin de planear las consideraciones pertinentes para un buen funcionamiento del sistema.
- Identificamos los niveles de servicio que se deben de cumplir con el negocio.
- Nos ayuda a calcular el costo del desarrollo, operación e impacto del sistema sobre el negocio.
- Determina el grado de seguimiento que se requiere y la forma en que se debe administrar las desviaciones a lo largo del mismo, con el propósito de lograr los compromisos y expectativas en cuanto a Tiempo, Costo Calidad y Alcance originalmente pactadas con el Negocio.
- El grado de seguimiento tiene estrecha relación con la complejidad administrativa y técnica sobre la cual la solución será generada. De tal forma que existen factores internos y externos involucrados como: los compromisos con Institutos regulatorios, requerimientos Institucionales, estrategias corporativas, oportunidad en el mercado, niveles de retorno de la inversión, etc. que influyen sobre la Criticidad del Proyecto.

Además de ser importante el análisis de las distintas fuentes de conflicto, y su rango en cuanto su grado de impacto a los proyectos de manera global, es también importante que se les analice desde la perspectiva de su influencia a lo largo de las fases de los proyectos.

La clasificación de los proyectos en CRITICOS y NO CRITICOS por medio de esta herramienta, está diseñada para realizarse durante la Etapa de Definición del Proyecto (Fases de Análisis Preliminar y Diseño Conceptual), y poder pasar a la Etapa de Ejecución (Fases de Diseño, Desarrollo, Pruebas e Instalación) con el proyecto perfectamente clasificado.



Modelo de Análisis del Riesgo para el Diseño de un Sistema de Información

El segundo "momento" en el que puede realizarse el análisis del Riesgo es cuando este se encuentra operando en producción, es decir ya en su ambiente real, aquí el análisis toma una perspectiva mucho más complicada en el sentido de que ahora el sistema ya esta dando un servicio comprometido a la organización, es decir ya contamos con su operación y por lo tanto ya interactua con el negocio.

Este análisis requiere de un esfuerzo mayor ya que deberemos realizar un análisis de todo su ambiente tanto técnico como organizacional por lo que deberemos localizar todas aquellas áreas que cuentan con su operación y en que grado afecta el que pudiera sufrir algún evento no deseado que nos obligara a no contar con su operación y en cuanto tiempo podremos prescindir de este.

Una de las herramientas a través de la cual podremos iniciar esta identificación del riesgo es la aplicación de un cuestionario ó entrevista con las personas clave dentro de la organización.

Este cuestionario o entrevista deberá cubrir los siguientes aspectos de nuestra organización.:

- Bienes: Aquello que la compañía posee, opera, controla, custodia, compra, vende, diseña, produce, analiza, prueba o mantiene
- Servicios: Aquello que la compañía expone o pone a servicio y que pueda causar o contribuir a sufrir daños, robos, pérdidas ó que causen injurias personales a empleados de la organización.
- Pérdidas: Aquellas evidencias empíricas que puedan establecer la frecuencia, magnitud de las pérdidas basadas en las experiencias propias y las de los competidores.

Una vez obtenida esta información se debe realizar la clasificación de los riesgos encontrados a fin de poder determinar parte de su importancia y por otra parte ayudarnos a determinar el tipo de medidas que se recomendarán para disminuir el riesgo, de lo cual se hablara más adelante.
Durante el desarrollo del presente trabajo se hablará exclusivamente del análisis del riesgo que se realiza a los sistemas de información que ya se encuentran operando en nuestra organización y que pueden llegar a causar que nuestro negocio desaparezca o por el contrario con un buen plan de contingencia se brinde una imagen seria y robusta de nuestra organización.

Clasificación del Riesgo

La clasificación del riesgo se divide en los siguientes 4 rubros que se describen a continuación, obviamente la aplicación de estos dependerán en gran medida del país, situación territorial en el que se encuentre nuestra organización

OPERACIONALES		
Accidentes	Espionaje Industrial	Inundaciones
Actos intencionales	Explosiones	Mala Calidad
Archivos defectuosos	Falta de capacitación	Malas decisiones
Asaltos	Falta de control	Motines
Bombas	Falta de mantenimiento	Negligencia
Calor	Falta de planes de emergencia	Pérdida de mercado
Cambios programados	Falta de reglas de seguridad	Radioactividad
Colapsos en el piso falso	Falta de respaldos	Retrasos de información
Corto circuitos	Falla en la energía eléctrica	Robos
Crímenes computacionales	Fallas en equipos	Sabotaje
Disrupciones	Filtraciones	Sobrecargas
Errores Administrativos	Incendios	Terrorismo
Errores de programas	Instalaciones cerca de un aeropuerto	Tumultos
Errores de Software	Intercepción de microondas	Vandalismo
Errores Humanos	Intrusos	Variaciones en el voltaje
		Virus

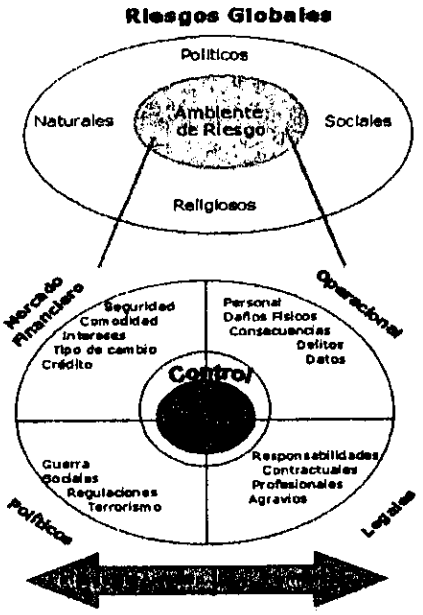
Administración poco efectiva	Falta de seguridad	Información falsa
Ambiente de trabajo	Falta de definición en las responsabilidades	Negligencia
Deficiencias de calidad	Falta de un plan de crisis	Piratería

FINANCIEROS		
Fraudes	Efectos de caídas de otros mercados	Pérdida de Intereses
Devaluación de la moneda	Pérdida de Mercado	

Conflictos Religiosos	Guerra Externa	Terrorismo
Corrupción	Golpe Militar	Tensiones raciales y étnicas
Cambios en políticas tributarias	Huelgas	Rebeliones
Elecciones	Hostilidad hacia inversionistas extranjeros	Sedición
Guerra Civil	Legislación Laboral	

NATURALES		
Contaminación	Huracanes	Sismos
Erosiones	Incendios Forestales	Temperaturas Extremas
Erupciones	Inundaciones	Tormentas
Frío extremo	Nevadas	Tornados
Humedad	Radiaciones	

En la siguiente figura podemos observar como se encuentra representado el riesgo, en forma global, dentro de una organización y en que tipo de rubro se encuentran los diferentes tipos de riesgos o amenazas a los que se encuentra expuesta cualquier organización.



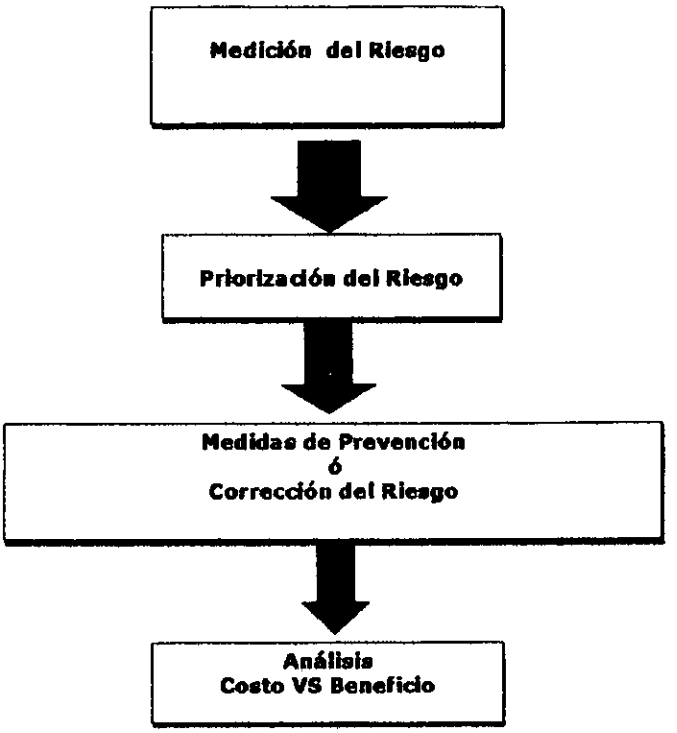
En esta figura se puede observar que existen diferentes tipos de amenazas que pueden llegar a afectar las operaciones de nuestra organización y aunque parezca increíble un conflicto religioso puede causar, a largo plazo, grandes conflictos como pueden ser los: amotinamientos, suicidios masivos (dentro de los cuales pudiera participar personal y/o familiares de nuestra organización). También pueden crear tensión social y por lo tanto desconfianza en inversionistas por lo tanto todos los eventos que ocurran en nuestro entorno nacional como internacional deberán ser considerados de forma alguna tanto para la toma de decisiones, como para la seguridad y continuidad de nuestro negocio.

Mapas de Riesgos

Los mapas de riesgos tienen como objetivo identificar, de acuerdo al tipo de riesgo y su grado, determinadas zonas en un área específica y tomar acciones determinadas a su prevención, control o disminución del riesgo.

En el apéndice A se muestra de forma más detallada los tipos de riesgos naturales a los cuales se encuentra expuesto el territorio Nacional, Estados Unidos y Canadá, mencionando aquellos que resultan más comunes para nuestro entorno y que nos ayudará a tomar decisiones respecto a la ubicación de nuestro negocio, en su caso de un centro alterno o de una sucursal.

La siguiente parte de la presente metodología hace referencia a las siguientes etapas que se deberán seguir a lo largo de esta y que nos ayudarán a completar nuestro análisis del riesgo.



Etapas del Análisis del Riesgo

Ahora bien después de que hayamos identificado y clasificado los riesgos de nuestros sistemas de información, se iniciará la etapa clave de nuestro análisis, la medición del riesgo. Lo que representa en términos cuantitativos para nuestra organización la pérdida, interrupción, ataque, etc. a un sistema de información en una organización.

Medición del Riesgo

Es un elemento esencial para determinar el costo de un evento desfavorable para la organización como puede ser cualquier interrupción en algún servicio o la caída de uno o varios sistemas informáticos, además calcula el período de tiempo en que pudiera ocurrir otro evento no deseado.

Después de haber aplicado el cuestionario sugerido para el análisis de los sistemas de información u aplicaciones críticas de cada área y haber calculado su probabilidad de ocurrencia, obviamente habremos de haber "detectado" que cada una cuenta con sus particularidades así mismo entenderemos de primer instancia que en algunos de estos no se tendrá que establecer ciertos criterios de seguridad que en otros sí, además de identificar aquellas que hayan resultado de más riesgo.

Antes de proceder a realizar cualquier conclusión y antes de proporcionar cualquier recomendación para implantar acciones correctivas, es necesario cuantificar los riesgos potenciales que fueron identificados. Sin embargo esta tarea deberá considerarse como muy delicada e importante ya que marcará el curso tanto de nuestra metodología como de la estrategia de nuestro negocio.

Dado que los resultados del cuestionario que usemos para identificar los riesgos y partes críticas de un sistema de información, se aplica al personal capacitado para dar respuesta al mismo, deberemos estar consientes de que es posible que se llegue a ocultar o minimizar algún componente que fuere crítico.

Así pues se recomienda que en la medida de lo posible este análisis se apoye en un evento de auditoría previo con el fin de comparar y apoyarnos en la identificación de riesgos.

Algunos de los riesgos se pueden clasificar en eventos que pueden llegar a suceder pero que aún no se han llegado a presentar, de estos algunos pueden a aceptarse o incluso a minimizarse, apoyándose siempre con correctas medidas de prevención.

Todo esto nos lleva a la conclusión de que el proceso de identificación y medición del riesgo de un sistema de información es una decisión importante en el aseguramiento de nuestro negocio y por lo tanto de nuestra organización por lo que esta etapa de la metodología debe considerarse como delicada pues esta repercutirá en las siguientes etapas de la misma y podremos estar dedicando dinero y esfuerzo a eventos que realmente no afectan a la operación de la organización.

La medición depende de dos conceptos intuitivos del control de la seguridad como podría ser los físicos (instalación de una alarma) y los lógicos (modificaciones de seguridad a una aplicación). El procedimiento para estas dos formas de conceptualizar el control de la seguridad deben considerar en su totalidad lo siguiente:

- Recursos de información disponibles
- Relación con la probabilidad de ocurrencia
- Tiempo máximo, recursos necesarios y disponibilidad
- Apoyo necesario de los directivos

Una evaluación realista de un plan efectivo de control de seguridad existente o planeado.

ALE (Annual Loss Expectancy)

El ALE es una fórmula que nos permite determinar el costo de la pérdida anual esperada de una aplicación u activo considerando dos factores: el impacto (costo) y la frecuencia[1].

A continuación se presenta una de las formas de obtener este costo.

[1] J.F. Broder, Risk Analysis and the Security Survey

Si la valuación del costo (impacto) del evento es:

$10,	ι=1
$100,	ι=2
$1,000,	ι=3
$10,000,	ι=4
$100,000,	ι=5
$1,000,000,	ι=6
$10,000,000,	ι=7
$100,000,000,	ι=8.

Y la frecuencia estimada es:

Una vez en trescientos años,	f=1
Una vez cada treinta años,	f=2
Una vez cada tres años,	f=3
Una vez cada cien días,	f=4
Una vez cada diez días,	f=5
Una vez por día,	f=6
Diez veces por día,	f=7
Cien veces por día,	f=8.

Formula:

$$ALE = 10^{(f+I-3)} / 3$$

Ejemplo

Un determinado evento ocurre 1 vez cada 100 días su frecuencia estimada es: 4, dado que el impacto valuado es de aproximadamente de $100,000 su impacto I = 5, entonces:

$$F+I-3 = 5 + 4 - 3 = 6$$

Ahora

$$ALE = 10^6 / 3 = \$\ 3,333,333.33$$

Así pues el costo anual de pérdida esperado es de $ 3,333,333.33

Otra forma de calcular el ALE de una forma más práctica es el uso de esta tabla modelo, obviamente esta podrá ajustarse a la frecuencia de los eventos, por ejemplo puede hacerse el calculo de ocurrencia anual en lugar de cada 3 años.

Valores de f

Valores de i							
2				$300	$3K	$30K	$300K
3			$300	3K	30K	300K	3M
4		$300	3K	30K	300K	3M	30M
5	$300	3K	30K	300K	3M	30M	300M
6	3K	30K	300K	3M	30M	300M	
7	30K	300K	3M	30M	300M		

Pérdida Anual Esperada (ALE)

En esta etapa de la metodología es recomendable realizar un análisis de probabilidad más formal que nos permita conocer la frecuencia estimada de los eventos de riesgo que ha sufrido nuestra organización con el fin de contar con datos realistas de las pérdidas anuales esperadas.

Una de las actividades que son rigurosamente necesarias en cualquier organización y que de ella se derivan varias medidas de seguridad y control es contar con una bitácora de estos eventos; la cual nos ayudará, entre otras cosas, a determinar la ocurrencia de eventos reales y cuales fueron las actividades que nos permitieron corregir el riesgo presentado.

Ahora que ya conocemos el costo anual de nuestras pérdidas esperadas es necesario conocer las etapas en las que tendremos que trabajar par completar este análisis del riesgo y así estar consientes de lo que significa la pérdida de un sistema de información para la organización y así tomar las medidas necesarias y pertinentes para evitar el impacto a nuestro negocio.

Priorización del Riesgo

Cuando hablamos de priorizar el riesgo hablamos de todo un análisis previamente realizado, esta priorización es el resultado que nos arroja nuestra matriz de decisión

Matriz de Decisión

Una de las técnicas utilizadas para priorizar el riesgo de pérdidas potenciales es el uso de la matriz de frecuencia versus pérdidas de nuestros sistemas de información con el fin de ayudarnos a clasificar el tipo de efecto que pudiera causar algún riesgo.

Número de Eventos / Tipo de Riesgo	Alto	Medio	Bajo
Alto ***7 a10 eventos***[2]	Invalidación	Baja Prevención e Invalidación	Se transfiere responsabilidad a un Seguro
Medio ***4 a 6 eventos***	Invalidación y Baja Prevención	Baja Prevención y se transfiere responsabilidad a un seguro	Aceptación
Bajo ***1 a 3 eventos***	Baja Prevención	Baja Prevención y Aceptación	Aceptación

Esta matriz tiene como objetivo el presentarnos de una forma accesible los puntos críticos de nuestro negocio de tal manera que nos ayuden a identificar que riesgos podemos tratar de *minimizar o controlar y que otros están fuera de nuestro alcance por sus propia naturaleza.*

Cuando "aceptamos" un riesgo debemos tener en cuenta que éste no es lo suficientemente serio como para justificar el costo de su reducción, o que la interrupción de la operación (si el riesgo se presentara en gran magnitud) resultaría de todas formas un evento aceptable.

Por ejemplo, si el análisis indica que un evento en particular tiene una alta probabilidad de ocurrencia, entonces el evento deberá ser "planeado" como si fuera un evento a llevarse a cabo. La única alternativa aceptable sería tomar las medidas necesarias para disminuir (mitigar) el riesgo

La disminución del riesgo puede lograrse a través de la reducción del grado de impacto que el evento pudiera tener, o por medio de la alteración de los procedimientos o del medio ambiente para evitar totalmente el riesgo. Sin embargo, si el análisis cualitativo indica que un evento tienen baja probabilidad de ocurrencia, generalmente se considera que no es necesario desarrollar procedimientos para hacer frente a ese evento. La decisión de los requerimientos a prescribir, o aún si la decisión es no tomar ninguna acción, se deja al comité de toma de decisiones de la organización el análisis del medio ambiente del evento.

Ahora bien cuando se trata de disminuir o controlar un riesgo debemos de definir que tipo de medidas de prevención o corrección del riesgo se implantarán, cuales aplican y que parte del problema atacarán, lo importancia de estas son obvias, finalmente son las que nos ayudarán a asegurar a nuestro negocio ante cualquier eventualidad.

Medidas de Prevención ó Corrección del Riesgo

Las medidas de prevención o corrección del riesgo son recomendaciones que tienen como finalidad el consolidar, coordinar, mejorar o crear medidas de protección ante los riesgos identificados, las cuales tienen que tener como característica principal la eficiencia para nuestro negocio ya que este es el punto de partida del cual se podrá establecer su costo – beneficio. Estas se pueden dividir en:

[2] Rango de probabilidad de eventos ocurridos en un determinado tiempo (1 año, p.ejemplo)

- Procedimientos (guías de trabajo)
- Físicas (cerraduras, llaves de control, alarmas, destructores de papel, archiveros con cerradura, áreas controladas, etc.)
- Personal de Seguridad

En esta etapa de la metodología debe considerarse que las medidas que se recomienden implantar deberán estar bien fundamentadas ya que esto implica un costo para la organización y es obvio que este gasto debe estar bien justificado tanto técnica como estratégicamente, este trabajo será realizado por el equipo encargado de la administración del riesgo quien estará encargado de presentar ante el comité de toma de decisiones estas medidas. De esto se hablará en el capítulo 3 más a detalle

A continuación se presentan algunas de las áreas en las que es común encontrar la necesidad de reforzar políticas, procedimientos, mantenimiento, organización de nuestra empresa además se hará referencia a los puntos de control que nos determinará o no la necesidad de considerar medidas de prevención o corrección del riesgo. Ante todos estos tipos de medidas en indispensable no olvidar que el objetivo es beneficiar a nuestro negocio bajo un esquema de costo - beneficio, de lo contrario estas medidas solo vendrán a causar estragos en nuestra empresa.

ORGANIZACION

Control

- ¿Existe una adecuada segregación de funciones entre los usuarios y el entro demando donde se contemple la separación de funciones incompatibles, corrección de transacciones.?
- ¿Existe supervisión y control de la alta dirección de la función de sistemas, respecto a nuevos desarrollos, coordinación con usuarios, cambios y mantenimiento de sistemas, prioridades y presupuestos de gastos, etc.?
- ¿Hay una adecuada administración de recursos humanos internamente en el área para lograr una alta calidad del desempeño del personal?

Riesgos

1. Acceso no autorizado a información
2. Error en los datos
3. Cambios no autorizados
4. Bajo nivel de servicio y satisfacción de usuarios
5. Planes de sistemas no acordes con los planes u objetivo global de la empresa
6. Contratación de empleados deshonestos
7. Personal no calificado para el desempeño de sus funciones
8. Personal que labora con funciones incompatibles
9. Manipulación de datos

Contramedidas

Jerarquización externa

a) Revisar y analizar la estructura organizacional y las funciones el área de procesamiento de datos Observar operaciones actuales
b) Observar operaciones actuales
c) Preparara un diagrama de flujo para cada ciclo de procesamiento de las transacciones.

Supervisión de Control

d) Revisar minutas de comités de usuarios, de auditoría interna y de dirección para asegurar que existe control empresarial
e) Revisar la documentación de nuevos sistemas y procedimientos de cambio de los sistemas y revisar que tengan autorizaciones formales.
f) Revisar procedimientos de asignación de prioridades y control presupuestal del área.
g) Revisar los programas de auditoría y verificar que se contemplen auditorías a los sistemas y centros de procesamiento.

Administración de Recursos Humanos

a) Revisar procedimientos de contratación y evaluación de personal, incluyendo pruebas de aptitud, verificación de antecedentes, programas de capacitación y medición de su desempeño.
b) Observar las operaciones del personal de sistemas para asegurar que no cuentan con acceso libre al hardware y archivos, que al personal se le asignan tareas bien definidas.

DESARROLLO DE SISTEMAS

Control

- ¿El área de seguridad junto con el personal de sistemas participan en las fases del análisis, diseño, prueba e implantación de sistemas para asegurar que los nuevos sistemas incluyan adecuados controles y satisfagan las necesidades de los usuarios?

Las convenciones y procedimientos de programación incluyen:

- Estándares de diagramas
- Estándares de codificación
- Estándares en rutinas de programación
- Estándares en la definición de JOB's
- Convenciones de auditoría
- Glosarios
- ¿Existen procedimientos y estándares formales de documentación? ¿Estos incluyen los manuales técnicos de sistemas, programas, manuales de usuarios y de operación?

Riesgos

1. Implantación de sistemas que carecen de adecuados controles de aplicación
2. Desarrollo de sistemas que no satisfacen los objetivos o no operación de acuerdo con las especificaciones originales
3. Implantación de sistemas que no han sido adecuadamente probados.
4. Implantación de sistemas, donde se permiten modificaciones a los datos sin ninguna autorización y control.

Contramedidas

a) Revisar el manual de estándares para el desarrollo de sistemas a fin de comprobar la existencia de políticas, guías, procedimientos de revisión y aprobación.
b) Implantar una metodología para el control y desarrollo de sistemas con el fin de establecer actividades en las que se involucren parámetros de seguridad y estándares de la institución.
c) Difundir y capacitar al personal acerca de los estándares y procedimientos de seguridad para el desarrollo de sistemas en todo su ciclo de vida.
d) Validar la funcionalidad de estándares y parámetros de seguridad de los sistemas de desarrollados en el ambiente de pruebas para poder autorizar la liberación a producción del mismo
e) Entrevistar a usuarios y departamento de seguridad respecto a la integridad de los datos y afectación contable sobre de los sistemas en operación.
f) Validar el seguimiento de la metodología así como la adecuada implementación de los controles y parámetros de seguridad en el sistema.
g) Validar la funcionalidad de la documentación por medio de los operadores y usuarios del sistema pidiéndoles que la revisen y mencionen sus comentarios.
h) Revisar que la documentación contenga la información necesaria tanto para el usuario como para el soporte técnico y que esta sea clara.

MANTENIMIENTO DE SISTEMAS

Control

- ¿Se efectúa monitoreos periódicos a los sistemas que se encuentran en operación?
- ¿Existen procedimientos formales de solicitud de y autorización de cambios a sistemas aprobados por el usuario(s) responsable(s) y el área de seguridad?
- ¿Se efectúan únicamente las solicitudes de cambios a sistemas que fueron aprobados y autorizados?
- ¿Los cambios se efectúan siguiendo los procedimientos, estándares de análisis, programación y documentación?
- ¿El personal de operación puede efectuar cambios a los programas?
- ¿Todos los cambios a programas se aprueban antes de su implantación?
- ¿Si es necesario se capacita a los usuarios y personal operativo respecto a los cambios a programas?
- ¿Se actualiza la documentación que es afectada por los cambios?

Riesgo

1. La integridad de los sistemas puede ser destruida
2. Cambios a sistemas que no tienen adecuados controles de aplicación
3. Cambios a sistemas que no satisfacen los objetivos o no operan de acuerdo a las especificaciones originales, o que no corrigen problemas de operación presentados.
4. Cambios a los sistemas sin ninguna autorización o control

Contramedidas

a) Revisar documentos de trabajo e informes de auditoría respecto al los sistemas de operación.
b) Entrevistar al personal administrador de la operación y de sistemas para determinar que procedimientos y políticas aplican en los cambios a programas
c) Revisar la documentación que soporta los cambios para comprobar que los procedimientos y políticas realmente se llevan a cabo.

OPERACION

Control

- ¿Existen estándares y procedimientos de operación bien definidos respecto a: programación de trabajo y tareas de operación establecido de a cuerdo con prioridades previamente convenidas?
- ¿Operación de equipos y control de su desempeño?
- ¿Procedimientos de ejecución de corridas y registro de la consola de operación?
- ¿Procedimientos de control de almacén y de la biblioteca de cintas, discos y la documentación de sistemas?
- ¿Procedimientos para el control de archivos?
- ¿Supervisión de las actividades de operación?
- ¿Procedimientos de emergencia y de seguridad física?
- ¿En los equipos instalados se cuenta con controles automáticos de hardware para la detección y corrección de errores?
- ¿Los controles de operación aseguran la efectividad de los controles de hardware?
  - Controles sobre los medios de almacenamiento y salida
  - Bitácora de falla de equipos y reportes
  - Controles del ambiente (polvo, temperatura, humedad).
  - Fluctuación e interrupción de energía eléctrica
  - Procesamientos formales de recuperación
  - Mantenimiento preventivo y correctivo.
- ¿El sistema operativo tiene la capacidad para detectar y corregir errores causados por problemas de hardware y software?
  - Rutinas de lectura o escritura
  - Revisión de longitudes de registros
  - Revisión de dispositivos de almacenamiento
- ¿El sistema operativo protégé los datos y programas de uso y/o modificaciones no autorizadas?
  - Protección de almacenamiento
  - Daño a la memoria
  - Uso de passwords

Riesgo

1. Ejecución de tareas de operaciones sin control
2. Pérdida, destrucción y/o manipulación de programas, archivos y documentación de sistemas.
3. Contar con equipos no confiables que ocasionen errores en el procesamiento de datos
4. Fallas del ambiente no detectadas por el hardware y software que impactan en el procesamiento de datos
5. Distorsión en la transmisión de datos que afecten el procesamiento de datos
6. No detección de cambios no autorizados a los datos y programas

Contramedidas

a) Revisar la operación y verificar el uso de estándares y procedimientos
b) Validar procedimientos y estándares en el manejo de la integridad de la información.
c) Contar con un inventario actualizado de equipos, sus características y el software instalado
d) Revisar la bitácora de errores y fallas de los equipos para detectar la frecuencia de errores ocasionados por el hardware y software, determinando la confiabilidad de los equipos

Contramedidas (operación)

e) Revisar los controles existentes para la protección de fluctuación e interrupción de energía, control de temperatura y humedad
f) Revisar y verificar la documentación y procedimientos del operador para el manejo de errores, control de los medios de almacenamiento y procedimientos de recuperación.
g) Revisar el contrato de mantenimiento, reporte de fallas y licencias de equipos para determinar la efectividad del mantenimiento preventivo y correctivo

SEGURIDAD

Control

- ¿Dentro de la organización se efectúan revisiones periódicas respecto a la seguridad?
- ¿Se consideran a las áreas de sistema dentro de estas revisiones?
- ¿Existen controles de seguridad para proteger los edificios y equipos de procesamiento de datos?
- ¿Existen controles de seguridad física y lógica para restringir el acceso a los archivos de datos, programas computacionales y a la documentación?
- ¿Existen controles físico y lógico a las terminales y periféricos locales y/o remotos que estén conectados en línea, con la finalidad de evitar que los equipos, programas y datos sean manipulados por personal y/o visitantes que no estén autorizados?

Uso de llaves de seguridad y ubicación de terminales y periféricos
Control del sistema para reconocer las terminales y periféricos
Asignación y administración de passwords a todos los usuarios definiendo su perfil de acceso a equipos, sistemas, funciones, programas y datos.
Transmisión remota de mensajes y datos utilizando métodos apropiados

- ¿Verificar la existencia de algún plan de contingencia que guíe el personal para respaldo y recuperación de datos, programas y documentación, y establezca procedimiento específicos para lograr continuidad en el procesamiento de datos?
- ¿Se verifica la póliza de seguros con respecto a sumas aseguradas y aspectos que protégé

Riesgo

1. Vulnerabilidad, en caso de desastre, de errores y/o fraudes
2. Diseño y/o pérdida de datos importantes, programas y documentación que son activos esenciales de la empresa
3. Manipulación de programas y datos para beneficio personal y/o visitantes
4. Pérdida de privacía y confidencialidad de la documentación y datos bajo procesamiento

Contramedidas

a) Entrevistas al personal con respecto a la seguridad lógica y física del área
b) Visitar los centros de procesos locales y remotos y asegurarse de los controles de acceso, ubicación y construcción
c) Visitar las áreas sensitivas para verificar la efectividad de los controles de acceso a datos, programas y documentación
d) Validar las terminales y periféricos en líneas locales y remotas para asegurarse de los controles físico y lógico a sistemas, funciones, programas y datos.
e) Revisar los métodos de autenticación de usuarios para evitar que personal no autorizado tenga acceso a funciones, programas y datos.
f) Revisar los métodos de transmisión de mensajes y datos
g) Mantener y actualizar el plan de contingencia y asegurarse de que este resulte efectivo en la práctica para la institución.
h) Solicitar y revisar la póliza de seguros.

CONTROLES DE ENTRADA

Control

- ¿Se calculan totales en lotes (batch) durante el proceso de creación de lotes de transacciones, aparte de mantener un registro de todos los lotes con sus correspondientes totales?
- ¿El tamaño de los lotes, el uso de formas prenumeradas y los campos que se utilizan como control de totales, proporcionan confiabilidad en el procesamiento de lotes?
- ¿Existen evidencias de autorización (firmas y/o iniciales) de todos los documentos bajo procesamiento?
- ¿Existen pistas de auditoría que permitan rastrear las transacciones en su flujo de procesamiento?
- ¿Existen procedimientos adicionales y por separado para identificar, corregir y re introducir transacciones con error?
- ¿Para actualizar los archivos maestros se verifica que todas las transacciones del período estén capturadas sin error?
- ¿Se cuenta con los requerimientos de retención de documentos fuente? ¿Están explícitamente definidos y físicamente se guardan en un lugar seguro?
- ¿Los documentos fuente están adecuadamente diseñados y existen las rutinas de verificación (razonabilidad, dígito verificador, referencia a tablas y archivos, etc.) que aseguren una correcta entrada de datos?
- ¿Sabe el personal como ejecutar sus responsabilidades y funciones asignadas por sistema? ¿Ha recibido el entrenamiento necesario?
- ¿Se efectúan verificaciones previas y posteriores a la captura de datos para asegurar la correcta actualización de archivos maestros?

Riesgos

1. Errores en la codificación y entrada de datos que afectan la obtención de salida
2. Las transacciones pueden ser incorrectamente introducidas por errores en los datos fuente y/o por falta de validación
3. Los datos pueden ser registrados o clasificados inadecuadamente provocando errores en los datos fuente y/o por falta de validación
4. Acceso de datos e información confidencial por falta de controles de entrada
5. Corrección y re introducción de errores sin validación adecuada de los datos
6. Errores de operación durante la entrada de datos.
7. Transacciones válidas o autorizadas que pueden ser omitidas durante la captura de datos (pérdidas de transacciones)
8. Transacciones válidas o autorizadas que pueden ser capturadas más de una vez.

Contramedidas

a) Revisar los procedimientos manuales del departamento usuario para identificar y verificar los controles en la preparación de entradas
b) Revisar el diseño de los documentos fuente para determinar su efecto en la incidencia de errores
c) Revisar la organización de los usuarios y del departamento de seguridad para identificar funciones incompatibles
d) Verificar las validaciones con datos de prueba en la entrada de datos
e) Calcular y balancear el control de totales en procesos de prueba
f) Revisar procedimientos escritos, guías de operación de cada aplicación para verificar la confiabilidad del manejo de las transacciones.
g) Revisar la documentación y archivo de datos para determinar transacciones con error y verificar las pistas de auditoría.

CONTROLES DE PROCESAMIENTO

Control

- Cuando se emplean dispositivos fuera de línea (cintas, diskettes, etc.) ¿Se hacen verificaciones, revisiones externas e internas para asegura el proceso correcto de los mismo?
- ¿Durante el procesamiento de archivos existen bibliotecas y discos separados para los archivos de prueba y los de producción?
- ¿Se proporciona suficiente información (cifras, reportes complementarios), para verificar la ejecución correcta de procesos?
- ¿Existen reportes de excepción que identifican transacciones erróneas previas a la actualización de archivos, y en general en la ejecución de proceso?
- ¿Existen procedimientos de recuperación y restauración para soportar los re procesos en caso de que sea necesario?
- ¿Existen procedimientos de control para proteger la integridad de los archivos en todos los medios de almacenamiento?
- ¿Existen procedimientos de revisión y conciliación de cifras para asegurar que solamente las transacciones correctas y autorizadas sean procesadas?
- ¿Se proporcionan pistas de auditoría con suficiente información para rastrear el flujo de transacciones que están bajo procesamiento?
- ¿Los procedimientos de distribución aseguran que los reportes sean enviados a la(s) persona(s) que lo(s) requiere(n) y que están autorizadas a recibirlos?
- ¿Los requerimientos de retención aseguran que la información permanezca por un período suficiente, aparte de estar físicamente en un lugar seguro?
- ¿Existen instructivos, el personal y/o usuarios están capacitados para asegurar que las salidas se utilicen adecuadamente?

Riesgo

1. Cálculos incorrectos que ocasionan errores en los resultados
2. Procesamiento incorrecto que provoca errores en los resultados
3. Acceso incorrecto y uso de archivos o registros durante el procesamiento
4. El operador puede introducir datos incorrectamente desde la consola de operación
5. Factores o valores de tablas incorrectas que pueden ser utilizadas durante el procesamiento
6. Procesamiento ilógico y/o con una versión errónea de programación
7. Entrada de datos inválida no autorizada o inválida que puede utilizarse durante el procesamiento
8. Transacciones que son automáticamente generadas y que no respetan las políticas internas de la empresa
9. Las transacciones pueden ser leídas y actualizadas más de una sola vez incorrectamente.

Contramedidas

a) Revisar y verificar la documentación de los programas de aplicación para determinar la integridad del procesamiento
b) Revisar los controles de totales y balanceo de cifras para asegurarse de que las diferencias son adecuadamente identificadas y procesadas
c) Revisar las pistas de auditoría de las transacciones sensitivas

CONTROLES DE SALIDA

Control

- ¿Existen procedimientos de revisión y reconciliación de cifras para asegurar que solamente las transacciones correctas y autorizadas sean procesadas?
- ¿Se proporcionan pistas de auditoría con suficiente información para rastrear el flujo de transacciones que están bajo procesamiento?
- ¿Los procesamientos de distribución aseguran que los reportes sean enviados a las personas que los requieren y que están autorizados para recibirlo?
- ¿Los requerimientos de retención aseguran que la información permanezca por un período suficiente, además de estar físicamente en un lugar seguro?
- ¿Existen instructivos, el personal y/o usuario están capacitados para asegurar que las salidas de información se utilicen adecuadamente?
- ¿Existen controles de aplicación en el procesamiento en línea?

Riesgos

1. Las salidas que recibe el usuario pueden ser incorrectas o incompletas
2. Las salidas que recibe el usuario pueden ser incorrectamente clasificadas o evaluadas
3. Las saldas pueden ser distribuidas o desplegadas para el uso de individuos no autorizados
4. Pérdida de eficiencia y efectividad organizacional en la obtención de metas y objetivos
5. Costos excesivos en la obtención de resultados
6. Pérdida de motivación del personal por esfuerzos adicionales y/o por inflexibilidad del sistema en la obtención de resultados
7. Interpretación errónea de los resultados que afecta la operación y toma de decisiones de la empresa
8. Errores de operación durante la obtención de salidas
9. Las salidas que recibe el usuario pueden ser incorrectamente clasificadas o valuadas

Contramedidas

a) Revisar las guías de operación para determinar si el manejo de salidas es suficientemente seguro en el sentido de que el usuario correcto y autorizado sea el que lo recibe y lo use.
b) Revisar las guías de operación para verificar los procedimientos operación detectar errores en la ejecución y distribución de salidas
c) Revisar las guías de usuario para verificar los procedimientos del usuario y detectar errores en las salidas que recibe, la corrección y reentrada de datos.

Análisis Costo - Beneficio

Una vez que se han presentado la propuesta de las contramedidas a los riesgos identificados es necesario realizar un análisis costo - beneficio con el fin de presentarlo al comité encargado de la toma de decisiones. Es obvio suponer que todo aquello que deseemos implementar en nuestra organización para la reducción del riesgo debe de contar con este análisis ya que de esto dependerá que se nos otorguen los recursos necesarios para su implantación.

Este paso de la metodología pudiera resultar fundamental pues el realizar un mal análisis implicará que nuestro trabajo sea tirado a la borda o no, así sepamos que las consecuencias de no tomar acción en un riesgo determinado serán inminentes para la organización.

Así pues el análisis costo – beneficio es todo un arte, que debe ser realizado con sumo cuidado, es recomendable que sea soportado por personal altamente especializado en este tema a fin de no pasar por alto detalles que a mediano o largo plazo nos afecten, de tal manera que podamos presentar un reporte bien fundamentado.

A continuación se presentará una breve reseña, dado que no es objetivo del presente trabajo, del papel que juega en la toma de decisiones este análisis.

Los ejecutivos toman dos tipos de decisiones que son de carácter económico. El primer tipo lo forman las que llamaremos decisiones "globales", "coherentes" o "integradoras", las cuales representarán conjuntos de decisiones y no decisiones aisladas. Las decisiones globales requieren que quien toma la decisión seleccione, entre un número inmenso de posibilidades, combinaciones de actuaciones y que determine hasta donde se avanzará con cada una de ellas. Las decisiones globales más importantes que se toman en las organizaciones son presupuestos y planes.

El segundo tipo amplio de decisiones del nivel ejecutivo lo forman las que llamaremos decisiones "aisladas" o "ad hoc". Estas se originan por la ocurrencia de un problema o por la aparición de una oportunidad. En este caso el ejecutivo trata con una sola decisión en forma aislada.

No es raro que ellas tengan mucho en común; en particular, las dos persiguen la meta económica de "óptima asignación de recursos". Esto significa que ellas tratan de utilizar los recursos de quien toma la decisión donde más convenga. Se puede afirmar que esta meta económica por sí sola domina y abarca a todas las demás.

Se examina tanto la naturaleza de la asignación de recursos como la lógica subyacente en los enfoques de los dos tipos de decisiones: las globales y las aisladas. La lógica subyacente en las decisiones globales se encierra mayormente en el llamado principio de la igualdad en el margen; la lógica subyacente en las decisiones aisladas es la del análisis costo-beneficio.

La utilización más eficiente de los recursos se tiene cuando al excedente de producción (fines, deseos, consecución de metas) sobre insumos (utilización de recursos, costos, sacrificios) esta en un máximo.

La utilización eficiente de los recursos requiere identificar claramente los fines y las metas, conocer qué recursos están disponibles, y saber cómo utilizarlos mejor para producir lo que se desea. Si uno sabe lo que quiere, sabe de qué dispone para trabajar y entiende cómo se podrían usar los recursos disponibles a fin de hacer las cosas que quiere, mediante cálculos muy cuidadosos puede asignar los recursos de tal manera que produzcan un máximo de lo que desea.

Los ejecutivos empleados por las empresas grandes usualmente procuran utilizar los recursos bajo su control en la forma más eficiente. Es decir, casi todas las decisiones de los ejecutivos afectan la asignación de recursos y buscan una máxima producción en relación con los recursos utilizados.

Los ejecutivos, en general, usan medidas concretas de los insumos y de la producción; estas medidas son valores en dinero de los costos y los productos. Es obvio que algunos de los insumos y de los productos son intangibles y, aunque se pueden expresar en cifras monetarias aproximadas, en un comienzo no asumen directamente la forma de dinero. No obstante, a diferencia de los planificadores generales de la economía o de los individuos que asignan tiempo y energía, quienes toman decisiones en los negocios tienen la ventaja de contar con medidas bastante concretas de los insumos y los productos.

Los presupuestos y planes encarnan las decisiones globales más importantes, a cargo de los individuos y las organizaciones. Para prepararlos se requiere una amplia perspectiva que abarque un conocimiento de todas las actuaciones factibles alternas y de todos los recursos disponibles. La meta de quien toma la decisión es lograr el mejor acople posible entre ambos. Estas decisiones implican ponderar las posibilidades alternas, trasladar mentalmente los recursos de un uso potencial a otro y estimar el efecto de esos traslados. No es posible reemplazar este proceso con una serie de decisiones individuales. En consecuencia la base conceptual en las decisiones globales es diferente de la que se emplea al tomar decisiones individuales, aun cuando las dos persiguen el mismo fin: el uso óptimo de los recursos.

Las decisiones globales tales como las de los presupuestos y los planes representan un conjunto muy grande de selecciones separadas pero interrelacionadas; el alto grado de dificultad resulta obvio.

Hay otro factor que las complica aún más: generalmente: en el proceso de elaboración de un presupuesto o de un plan intervienen muchas personas. El responsable de la preparación de un plan o de un presupuesto tiene que depender de otras personas, quienes usualmente tienen un conocimiento muy especializado y solo ellas pueden estimar que se necesita para su actividad y qué beneficio se obtendrá con diferentes inversiones de recursos.

La mayoría de las decisiones de negocios surgen en forma inesperada y deben tomarse en un plazo corto, en contraste con las decisiones que hacen parte de planes y presupuestos, las cuales se preparan de acuerdo con una programación regular. Como es obvio, las decisiones individuales están limitadas por los planes y presupuestos de la empresa, pero en un grado considerable ellas se sostienen por sí solas. Las decisiones individuales también comprenden asuntos importantes: ¿Deberíamos añadir un producto nuevo a nuestra línea? ¿deberíamos introducir ahora un nuevo proceso de producción o esperar otros avances tecnológicos?, etc.

Uno de los pilares de las decisiones individuales es el análisis costo-beneficio. Lo esencial de este análisis es simple y obvio : el "valor" de cualquier actuación, proyecto, inversión o estrategia es igual al excedente de los beneficios que reporta, sobre los costos que ocasiona. En consecuencia, para escoger la mejor de las alternativas disponibles, quien toma decisiones debe estimar los beneficios netos que proporcionaría cada una de ellas y escoger aquella que ofrezca los mayores beneficios netos.

Mas para aplicar el costo - beneficio a decisiones importantes, un ejecutivo de negocios debe resolver varios asuntos complicados, que surgen debido a que el medio ambiente de los negocios es complejo, volátil e impredecible.

Un ejecutivo debe incluir solo los costos y los beneficios que resultan de la actuación ocasionada por la decisión, y no algún promedio o cantidad estándar calculada según una fórmula.

El término "beneficio" y sus sinónimos "ganancia", "satisfacción", "recompensa", se utilizan casi en forma intercambiable para denotar la consecución de objetivos en su totalidad o en parte.

Finalmente podemos resumir que una decisión de negocios implica seleccionar entre varias acciones alternas. Para hacer esta selección, quien toma decisiones debe evaluar cada alternativa y determinar el modo como cada una de ellas contribuiría a la consecución de los objetivos de la empresa. Para hacer esa evaluación es necesario estimar, al menos mentalmente, el flujo de beneficios y de sacrificios que cada actuación traería consigo. La tarea resulta muy complicada por la incertidumbre que rodea a la mayoría de las decisiones mercantiles. Esta incertidumbre se debe en parte a la falta de conocimiento sobre las condiciones externas pertinentes que prevalecerán cuando se actúe, y que influirán en su resultado; y, en una parte mayor, al conocimiento limitado que uno tiene sobre las consecuencias de las actuaciones propias.

Otra dificultad al calcular el flujo de beneficios y sacrificios asociados, se debe al hecho de que estos ocurren en tiempos diferentes. Como el dinero en el presente es más valiosos que el dinero en el futuro cada egreso o ingreso importante se debe convertir a su valor presente.

Quien toma decisiones solo puede aspirar a estimar el costo en que la empresa incurriría si no adopta la mejor alternativa, y quizá disuadir así una oposición injustificada. Por supuesto habrá algunos factores limitantes que no se puedan superar. Lo que en teoría es la mejor decisión, podría ser una selección torpe si la empresa carece de los recursos para llevarla acabo en forma eficiente.

Capítulo III

Administración Del Riesgo

En el capítulo II, de análisis del riesgo, se describió el proceso de evaluar el riesgo de los sistemas de información, tomando acciones que permitan reducir el riesgo a un nivel aceptable (sin causar trastornos graves a la actividad diaria), y mantener el ambiente en condiciones normales de operación.

El equipo de trabajo responsable realiza un análisis del riesgo en muchos aspectos del negocio, consideran alternativas y sugieren planes para optimizar el retorno de los sistemas a una condición normal. Sin embargo este equipo no es el responsable de tomar decisiones y de aprobar estrategias para el negocio, además de darle una adecuada continuidad y mantenimiento a todo este concepto; es aquí donde se presenta la necesidad de administrar o coordinar los resultados obtenidos y las recomendaciones generadas.

El proceso de la administración del riesgo para sistemas de información permite a los administradores y sus organizaciones construir un departamento capaz de conocer y analizar todos los "objetos" ó "aplicaciones" que conviven dentro de un sistema de información, a fin de que éste sea la puerta de entrada a producción de una nueva aplicación con el mínimo riesgo implícito.

Con este concepto podemos decir que se asegura que la administración del riesgo vaya actualizándose al mismo ritmo que la organización va evolucionando.

Ahora bien es necesario que el análisis del riesgo realizado forme parte ahora de un proyecto con alcance más amplio y serio para la organización; es decir el análisis del riesgo, si bien es parte de la etapa de un proyecto de Continuidad y Contingencia del Negocio es la base del mismo.

Principalmente el análisis del riesgo forma parte esencial de los objetivos principales que busca la seguridad de la información y el negocio que son: Disponibilidad, Integridad y Confidencialidad. Estos tres objetivos junto con el análisis del riesgo refuerzan la necesidad de contar con políticas y controles de acceso adecuados a la misión de la organización. Por lo tanto deberá tenerse especial cuidado en los criterios y decisiones a tomar a partir de este análisis.

En el entendido de la importancia de un proyecto de tal magnitud se debe entender que el comité encargado de la administración del riesgo desempeñará el papel de líder de este proyecto y será el responsable de:

- Diseñar el propósito que tendrá realizar el análisis del riesgo.
- Seleccionar a un equipo de trabajo calificado
- Formalizar la delegación de autoridad
- Revisar los resultados del análisis realizado por su equipo
- Decidir cuales recomendaciones serán aplicadas a la organización, según un análisis de costo - beneficio.
- Establecer la prioridad que llevará cada implementación

Además el equipo deberá plasmar sus resultados enfocándose al objetivo del proyecto, que deberá ser claro y común para todos; conjuntamente éste tendrá que presentarse en términos propios del equipo de analistas.

Además las decisiones que se tomen al respecto deberán estar basadas siempre en un análisis de Costo vs Beneficio, lo que ayudará a presentar a los altos directivos la conveniencia de poner en acción o no ciertas medidas de prevención o corrección las cuales deberán estar siempre reportando mayores beneficios de lo que implica su costo.

Resulta de gran ayuda hacer conocer de forma oportuna tanto al equipo de trabajo como a la organización en general que tópicos sí cubre el análisis y que otros no, con el fin de que tanto el equipo de trabajo no se desvíe a situaciones que no corresponden al objetivo del proyecto como también delimitará el alcance del mismo para la organización en general.

Así pues el papel del administrador del riesgo será el de coordinar a todas aquellas entidades que de alguna forma u otra deberán estar preparados y enterados del funcionamiento y evolución del proyecto en todos sus aspectos(ver figura1).

Círculo de manejo de los riesgos

Ejemplos de ambiente arriesgado y recursos de una compañía para la prevención de siniestros

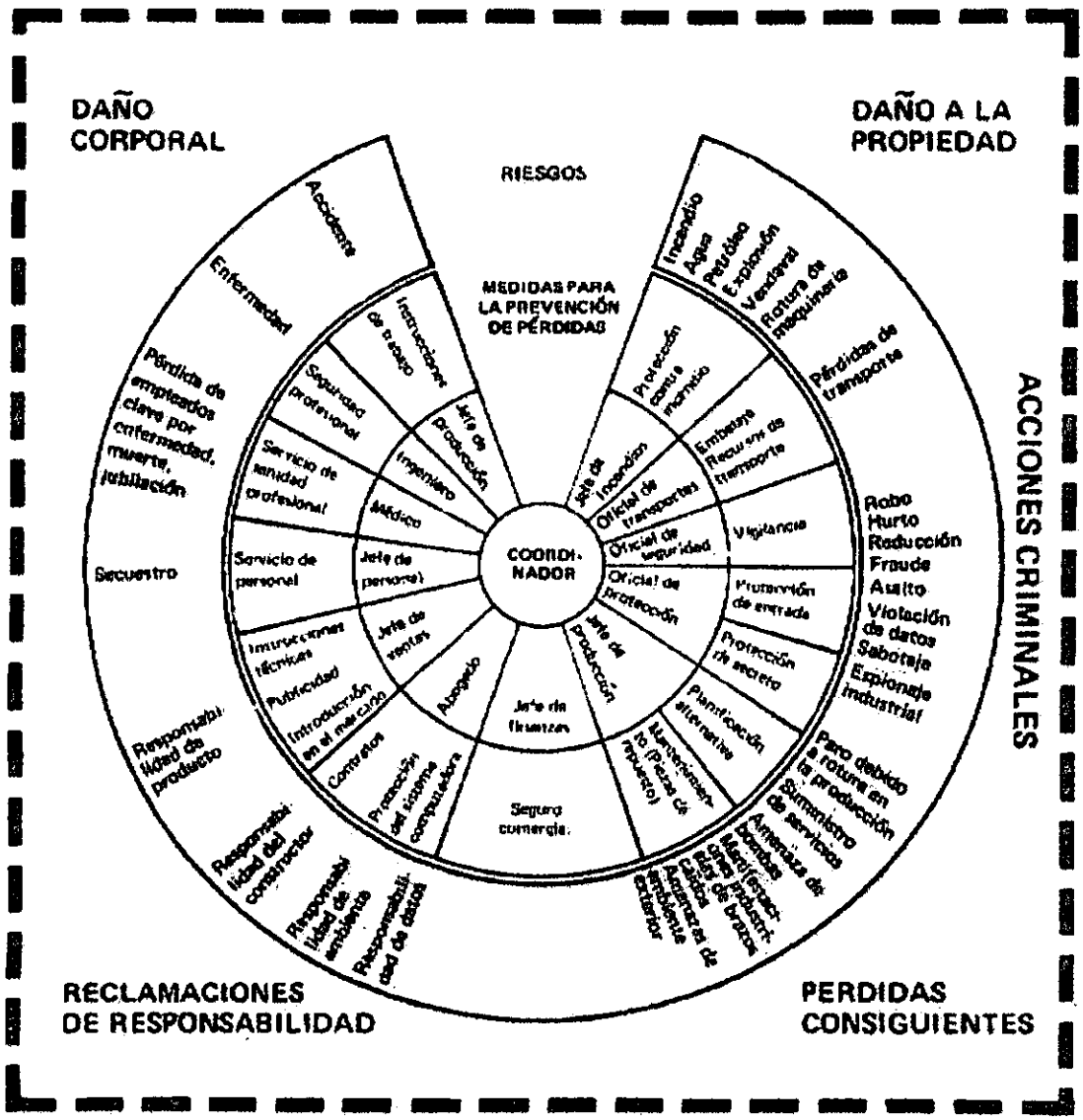


Figura 1. Manejo del Riesgo

Ahora bien debemos entender que este esfuerzo no es solamente de los involucrados en sistemas, considero que es además una nueva cultura de trabajo que nos permitirá encontrarnos *más preparados ante eventos no deseados como se mencionó anteriormente.*

Así pues todo este esfuerzo deberá sustentarse tanto en métodos y procedimientos de trabajo como políticas, controles y difusión de información que considero son las herramientas necesarias e indispensables para que toda la organización pueda salir adelante ante cualquier eventualidad.

A continuación se presentan 5 principios básicos acerca de la Administración del riesgo que finalmente nos llevan a formar toda esta estructura del manejo de riesgos dentro de nuestra organización, los cuales fueron recopilados tanto de experiencias propias de una organización financiera como de personal especializado en esta materia como es la General Accounting Office (GAO), organismo credo por el Gobierno de Estados Unidos de América para tal fin.

El éxito de los programas de seguridad dependerá del reconocimiento y entendimiento de los ejecutivos de que sus sistemas de información son objeto de riesgos y que este riesgo afecta la operación de su negocio.

Además de este esfuerzo por cambiar esta forma de pensar se debe tratar de lograr la mayor seriedad posible por parte de los directivos de la organización a fin de que toda ella participe activamente asegurándonos así de la continuidad de nuestro negocio en un plano laboral.

1. Análisis del Riesgo y sus Necesidades
2. *Enfoque de Administración Central*
3. Implementación de Políticas y Controles Relacionados.
4. Promover el Conocimiento
5. *Monitoreo y Evaluación de Políticas y Control Efectivo*

A continuación se describirán las prácticas generales asociadas a los 5 principios de la administración del riesgo.

1. Análisis del Riesgo e Identificación de Necesidades de la Organización

- Identificación de los recursos de información como una parte esencial de la organización que debe ser protegida.
- Cambiar la cultura de seguridad en toda la organización de tal manera que desde los directivos hasta los ejecutivos crean que la administración del riesgo es de gran ayuda para asegurar su negocio.
- Los programas de seguridad deberán adecuarse a todos los recursos con los que cuenta el negocio.
- Comunicación abierta hacia los directivos de los eventos de seguridad críticos proporcionada por los especialistas en seguridad, así mismo mantiene la importancia de este esfuerzo al corregir las vulnerabilidades detectadas dentro de nuestros sistemas de información.

- Una forma de trabajo que tome en cuenta más seriamente las consideraciones de seguridad que deben de cumplir las nuevas aplicaciones, tecnologías, servicios y eficiencias operacionales que nos permitan continuar con al aseguramiento de nuestro negocio y no ponerlo en riesgo.

- Desarrollo de un análisis del riesgo que vincule la seguridad con las necesidades del negocio

- Establecer estándares y procedimientos para los proyectos, desarrollos, tecnologías, etcétera a fin de que todo esto gire en torno a la protección de los sistemas de información y así minimizar el riesgo desde la concepción de los mismos.

- Algunas organizaciones inician este proceso con el uso de los "checklist", que son documentos con todos los pasos que efectúan para poner en funcionamiento algún servicio.

2. Enfoque de Administración Central

- Designar a un grupo central el manejo de actividades clave. Este grupo de personas estará encargada de desarrollar políticas de seguridad, comunicar a los usuarios una cultura de seguridad, realizar investigaciones acerca de amenazas potenciales, vulnerabilidades y nuevas técnicas de control, evaluarlas, analizar el riesgo y establecer nuevas políticas de seguridad dentro de la organización.

- Difundir la cultura de seguridad entre los ejecutivos encargados de la creación de nuevos proyectos con el fin de tomar las medidas pertinentes acerca de la seguridad de los sistemas a desarrollar en un futuro. Esta asesoría deberá de plantearse de la manera más práctica posible con el fin de no tomar esta como un simple requerimiento que cumplir y así poder obtener los mayores beneficios posibles.

- Es necesario proveer de los mejores equipos de hardware y software, además de capacitación adecuada a este equipo de trabajo con el fin de cumplir adecuadamente con la responsabilidad que el cuidado de la seguridad requiere.

- Dentro del campo de la seguridad de los sistemas informáticos es necesario contar con una capacitación constante y adecuada al perfil de los integrantes de un equipo de seguridad, obviamente esta dependerá de las funciones que desarrolle cada uno de estos. Los que sí es necesario tomar en cuenta de primera instancia es que los administradores de los sistemas informáticos de nuestra organización deberán estar lo más actualizados posibles debido a que son considerados como el primer frente para la detección de amenazas y de actividades anormales además de que son el punto focal de los ataques debido a su condición de administrador.

3. Implementación de Políticas y Controles Relacionados

- Es necesario que las políticas que se vayan a adoptar dentro de nuestra organización se liguen con los riesgos del negocio. Las políticas que se establezcan deberán de ser acordes con el objetivo del negocio puesto que estas son el elemento clave de los programas y estrategias de seguridad que se implementen.

- Se debe hacer una distinción entre lo que es una política y lo que es una guía de trabajo, ya que las políticas hacen referencia a formas de trabajo que se deben de seguir obligatoriamente con el fin preciso de cuidar el negocio, en cambio las guías pueden considerarse solo recomendaciones que pueden o no seguirse.

- Es necesario que se asigne a un equipo de trabajo calificado que sea el responsable de redactar las políticas de tal manera que también cuente con personal de la organización que valide la creación de éstas. Con el fin de que se lleguen a implantar políticas y procedimientos que no concuerden con el cumplimiento de los objetivos del negocio y en lugar de apoyarnos nos impidan realizar nuestro trabajo diario.

4. Promover el Conocimiento

- Es muy importante que cada uno de los esfuerzos que se realicen con el fin de disminuir el riesgo de nuestro negocio se le dé una difusión y seguimiento de acuerdo a lo que la organización espera de estos, de lo contrario invariablemente volverán a aparecer nuevos riesgos ó simplemente se reforzarán los que ya se habían identificado generando así más vulnerabilidad en nuestra organización.

- Aunque estos temas suelen ser de poco interés para los empleados es necesario buscar la forma en que estos resulten más amigables de difundir a través de presentaciones interactivas, páginas web, videos que refuercen los conceptos, trípticos de información, "slogans", etc.

5. Monitoreo y Evaluación de Políticas y Control Efectivo

- Aun en el caso de que ya se hayan implantado todos estos métodos de control es necesario monitorear que estos se cumplan además de que ahora estos fungirán como indicadores de la seguridad de nuestros sistemas de información. Estos indicadores podrán mostrarnos si alguno de los controles implantados son incongruentes con la funcionalidad de nuestro negocio, además podremos conocer si debemos en algún caso ser más estrictos y reforzar el control ó si es necesario adaptar nuevos controles para funcionalidades nuevas o que no se consideraban necesarias.

Estos principios anteriormente presentados forman parte de una cultura de seguridad que hoy en día debe ser considerada como parte estratégica del futuro de cualquier organización y que son basadas principalmente en las Amenazas y Vulnerabilidades a las que se encuentra expuesta nuestra organización y que son la base de la metodología que se presenta en el presente trabajo.

Basados en estos principios podemos definir un perfil adecuado para aquella(s) persona(s) a las que se les encargará esta función dentro de la organización:

Perfil del Administrador del Riesgo

De forma prioritaria:

- ✓ Técnicas de evaluación, diagnóstico y cuantificación de los riesgos
- ✓ Sistemas de prevención y seguridad de las personas y bienes
- ✓ Legislación y jurisprudencia concerniente al riesgo y sus consecuencias
- ✓ Principios y prácticas acerca de los seguros

Otros conocimientos necesarios:

- ✓ Conocimientos acerca de derecho mercantil y responsabilidad civil
- ✓ Económicos, contables y financieros de su empresa
- ✓ Lenguaje técnico utilizado en la empresa para poder comunicarse con Directivo y Técnicos de la misma

Cualidades personales:

- ✓ Facilidad de juicios objetivos pero con capacidad de llegar al detalle.
- ✓ Facilidad de comunicación: tendrá que mentalizar, asesorar y obtener colaboración de todos los niveles de la empresa.
- ✓ Facilidad de planeación y control de resultados
- ✓ Serenidad de actuación ante los siniestros

Proyección Futura

En nuestro país la función del administrador del riesgo todavía no es muy conocida sin embargo por experiencia de otros países se puede asegurar que esta función crecerá y se desarrollará, tanto en importancia como en complejidad.

En importancia pues existe la tendencia en incrementar sus servicios en todas las empresas en situar su función en las decisiones estratégicas de los Comités de Dirección.

En cuanto a complejidad ya que van surgiendo cada día más, lo que llamaremos "nuevos riesgos" fruto directo del desarrollo tecnológico y de los sistemas político sociales que nos obligan constantemente a evolucionar.

Además de estos nuevos riesgos, aparecerán nuevas tecnologías mucho más sofisticadas, frente a las cuales también será necesario su identificación y control ante las amenazas de riesgo.

Todo esto lo podemos sintetizar en dos funciones de la Administración del Riesgo que las organizaciones tendrán que tener en cuenta para valuar su papel dentro de la misma:

- ✓ Necesidad de un justo y adecuado enfoque para lograr una reducción de los costes de la administración de los riesgos y sus consecuencias.

- ✓ Necesidad de tener la completa seguridad que la empresa, ante la aparición de un siniestro importante, podrá continuar su propia existencia y normal desarrollo. Lo que indudablemente hará crecer a la empresa económicamente en el mercado y en la credibilidad y confianza en la misma.

- ✓ Disminución de amenazas de intrusos (hackers) internos y externos

En el capítulo IV se presentarán algunas de las prácticas mínimas indispensables, en cuestión de seguridad (políticas, procedimientos y controles, etc.), que considero deberá conocer y vigilar *la administración del riesgo para después retomarlas como base y complemento para poder* implementar un plan de recuperación del Negocio, en el capítulo V.

Capítulo IV

Servicios de Seguridad

El presente capítulo tiene como objetivo presentar los estándares y guías para soportar las Políticas de Seguridad de la Información dentro de una organización. Estos estándares y guías aplican a los propietarios de datos y aplicaciones que residen en los sistemas de una organización, usuarios de los sistemas de información y empleados que custodian y administran los Sistemas.

Como hemos visto en los capítulos anteriores algunos de los principales riesgos que padecen las organizaciones que cuentan con sistemas es principalmente sobre el uso de la misma información, ya sea por algún error en la operación de la misma, por alteraciones no documentadas y también en mayor grado por permitir el acceso y manipulación de la misma a personal no autorizado.

Así pues a continuación se presentarán los principales conceptos de seguridad que deberá considerar cualquier organización a fin de disminuir el riesgo de perder sus sistemas por falta de una adecuada estandarización y control en sus sistemas de información.

PROCESOS DEL MANEJO DE LA SEGURIDAD

- **Disponibilidad**

Asegura que todas las facilidades del sistema, incluyendo servicios de seguridad, estén disponibles al ser requeridos para las aplicaciones de negocio y para la infraestructura del sistema. La disponibilidad puede ser mejorada al desarrollar mecanismos que reduzcan el peligro de daños a la integridad del sistema y también al colocar servicios de seguridad redundantes en las diferentes plataformas.

- **Evaluación del Riesgo**

Identifica, analiza y documenta las amenazas a la seguridad del negocio, evalúa el nivel de exposición en el que queda la organización por cada riesgo asumido y determina el grado de importancia para la eliminación de cada uno de ellos. También ayuda a identificar a los propietarios de la información de negocio (entendemos por propietario a los ejecutivos responsables por el origen de la información). La evaluación del riesgo provee la base para desarrollar políticas de seguridad.

- **Manejo de Políticas**

Define las políticas de seguridad que serán administradas, publicadas como parte del proceso de toma de concientización de la seguridad y ejecutadas con procedimientos manuales y automatizados.

- **Estructura y Organización**

Consiste en la organización y el personal que es responsable de identificar y analizar las amenazas a la seguridad, desarrollar políticas de seguridad, auditar la práctica de seguridad, y responder a las violaciones de seguridad.

- **Concienciación de la Seguridad**

Involucra un programa continuo diseñado para capacitar y crear consciencia en el personal sobre la importancia de la seguridad y acerca de las herramientas y técnicas para reforzar las políticas de seguridad. Los programas de toma de conciencia están dirigidos a, políticas y procedimientos efectivos orientados hacia el sistema, hacia el ambiente de trabajo, estilo de trabajo y procedimientos de seguridad.

- **Seguridad Física**

Involucra la protección física de los recursos como son las áreas de trabajo en las oficinas, escritorios, computadoras, y líneas de comunicación. Los recursos físicos se encuentran expuestos a riesgos creados por amenazas accidentales y deliberadas.

- **Recuperación**

Involucra los pasos o procedimientos que la organización debe seguir cuando es confrontada por una violación de seguridad o pérdida de sistema a causa de un desastre. Los procedimientos de recuperación frente a una situación de desastre y de violación de seguridad deben ser identificados y documentados cuando se desarrolla el sistema de seguridad.

- **Administración de la Seguridad**

Involucra a las actividades continuas de los administradores de seguridad quienes implantan las políticas y procedimientos de seguridad utilizando una variedad de técnicas manuales y automatizadas.

- **Administración de la Auditoría**

Revisa las prácticas y actividades relacionadas con la seguridad. Evalúa y valida los privilegios de seguridad otorgados a usuarios del sistema, los archivos de información relacionados con los registros de seguridad que se graban a medida que se usa el sistema y los procedimientos manuales y automáticos relacionados con la seguridad de la información.

- **Administración de Alertas**

Notifica a los administradores de la seguridad y a los propietarios de recursos cuando ocurren violaciones a la misma. Los procesos más eficaces de alerta de seguridad notifican automáticamente a la parte correspondiente tan pronto como ocurre una violación. Una alerta debe dar lugar a la iniciación de un análisis, revisión, y de ser necesario, a un proceso disciplinario.

- **Confidencialidad**

Asegura que la información controlada por el sistema no se utilice, si se accesa a esta, violando las políticas de control de acceso. Los mecanismos de confidencialidad pueden proteger el contenido de comunicaciones, el contenido de archivos y bases de datos, programas, tablas de programas y otros archivos requeridos por el sistema. Se utilizan técnicas de cifrado para proveer confidencialidad.

Integridad de la Información

Asegura que las comunicaciones, los archivos o bases de datos, y los programas no hayan sido modificados ya sea inadvertida o deliberadamente. Los mecanismos de integridad también permiten reconocer cuando la integridad de un recurso ha sido violado.

- **Identificación y Autenticación de Usuarios**

Identifica y verifica la identidad de los usuarios y programas que acceden a los sistemas.

- **Control de Acceso**

Protege los recursos del sistema asegurando que estos sólo puedan ser utilizados por individuos o programas autorizados. Las técnicas de control de acceso pueden utilizarse para proteger a una variedad de recursos incluyendo hardware, sistemas operativos, centros de comunicaciones, redes, programas y archivos o bases de datos.

- **Certificación de la Información**

Demuestra que la comunicación de la información señalada como de haber sido enviada a un receptor fue, de hecho, enviada y recibida, y que la comunicación de la información señalada como recibida de un emisor fue, de hecho, emitida por el mismo.

Un programa de seguridad bien definido debe estar dirigido a todos estos procesos. El resto de este capítulo detalla los estándares para los procesos de seguridad los cuales deben ser implantados para complementar las necesidades de seguridad de cualquier organización.

Disponibilidad

El componente de disponibilidad de los sistemas, asegura que el sistema de seguridad esté disponible tanto como sea necesario para soportar el uso de las aplicaciones.

La disponibilidad tiene dos objetivos:

1. Asegurar que el sistema de seguridad esté disponible suministrando servicios de seguridad a los cuales se pueda accesar a través de diferentes vías de comunicación.

2. Suministrar mecanismos que minimicen el paso por el sistema el cual se volverá no disponible como un resultado de ataques accidentales, o deliberados, a la estructura del sistema (por ejemplo: virus, mensajes adulterados o paquetes denominados cadena de comunicación, pudiendo causar daño a: sistemas de operación, programas de comunicación y computadoras físicas y hardware de comunicación).

Estándares:

- ✓ **Contar con un inventario de recursos, tanto de hardware como de software**

Cada recurso proporciona determinados servicios los cuales deben estar clasificados conjuntamente con las áreas que los utilizan. El área de Seguridad, o su equivalente, debe analizar las políticas y estándares a las que se deberán apegar todos los usuarios de estos recursos.

✓ **Identificar la disponibilidad requerida por las funciones críticas del negocio**

Un análisis de impacto al negocio debe ser realizado sobre los sistemas aplicativos, con el objeto de determinar el tiempo requerido en servicio de las funciones críticas. Las funciones de negocio tienen una dependencia muy alta de los sistemas de información, por lo que la interrupción prolongada de alguno de ellos, genera fuertes impactos en la operación. Es importante entonces, identificar los periodos en los que la función crítica deberá estar disponible para todos sus usuarios y las acciones para lograrlo.

✓ ***Contar con controles para la protección de los recursos del sistema***

Establecer e implantar controles para proteger las facilidades de proceso y de redes en contra de riesgos, caídas e interrupción de servicios. La disponibilidad del sistema se verá incrementada si se realiza una adecuada planeación respecto al que hacer en caso de falla y se implantarán una serie de procedimientos tanto preventivos como correctivos cuyo objetivo es el de incrementar la disponibilidad del servicio y eliminar los puntos únicos de falla.

✓ **Análisis de medidas de seguridad para compras de nuevos equipos**

Todas las instalaciones y compras de equipos y servicios deben ser autorizadas y aprobadas para asegurar que no afecten las medidas de seguridad existentes además de contener los niveles de seguridad con los que opera la organización.

✓ **Debe existir protección contra virus en todos los equipos de cómputo**

Las computadoras personales deben estar protegidas en contra de ataques de virus y en una base periódica debe ser realizada la evaluación de la efectividad de la protección en contra de nuevos tipos de virus. Ningún software debe ser cargado en ninguna estación de trabajo sin previamente haber sido autorizado y haber pasado por el proceso de detección de virus.

La proliferación de virus en las computadoras personales ha alcanzado grandes niveles debido al alto número generado de los mismos diariamente, y a la poca cultura informática que tienen los distintos usuarios de las computadoras personales. Esta situación afecta enormemente las funciones de negocio debido a la gran interacción que las computadoras personales tienen con los sistemas mayores. Con el objeto de reducir el impacto de ésta situación, las computadoras personales deben contar con las versiones más actualizadas de software de antivirus y mantenerlo permanentemente de manera activa en la PC. La verificación antivirus deberá ser realizado automáticamente en la estación de trabajo en el momento de inicio. Todos los diskettes que el usuario reciba para leer en su PC, deben pasar primeramente por una prueba de verificación previa. El proceso documentado de limpieza de virus, incluyendo el aislamiento del área infectada, se iniciará cuando éstos sean detectados. La educación a este respecto estará incluida dentro del programa de toma de conciencia de seguridad. Se debe alertar al administrador de seguridad siempre que sea detectado un virus.

Los ataques programados de virus, son otro tipo de amenaza al cual hay que estar alerta, por lo que se debe contar con medidas y/o procedimientos una vez que se haya generado una alerta sobre éste tipo de ataque.

Implicaciones asociadas: Se requiere de un mecanismo adecuado que garantice o permita distribuir e instalar el software de protección en todas las estaciones de trabajo

- ✓ **Los servicios de seguridad deben estar activos aun y cuando los sistemas no estén disponibles**

Los servicios de seguridad deben estar activos aun y cuando los sistemas no estén disponibles. Si se necesita operar en modalidad fuera de línea, un modo alterno de servicios de seguridad debe estar disponible para identificar y autenticar a los usuarios (por ejemplo: servidores locales).

La disponibilidad de las herramientas y servicios de seguridad es un aspecto extremadamente crítico en la operación de la organización. La falta de ésta, expondrá a los sistemas a accesos no autorizados, violaciones a confidencialidad, y otros aspectos de seguridad.

- ✓ **Los servicios de seguridad deben estar en operación previa a la activación en producción de los sistemas aplicativos**

Los sistemas aplicativos no deben ser puestos en funcionamiento si no se cuenta con la protección requerida. Con el fin de asegurar que los activos críticos se encuentran protegidos contra accesos no autorizados, no se deben activar los sistemas aplicativos en caso de no poder contar con los servicios de seguridad.

- ✓ **La operación de la red de comunicaciones deberá contar con funciones activas de monitoreo y alertamiento de su capacidad**

El programa administrador de la red hará un monitoreo de las comunicaciones con el objeto de identificar situaciones en las cuales la capacidad de la red este llegando a su punto de saturación. Aún cuando la red utilizada sea de terceros éste deberá ser un requerimiento que se establezca en el contrato. Cuando esto ocurra, una alerta será enviada a los gerentes y administradores de la red. Se identificarán los recursos no disponibles dentro de la red, y se alertará al administrador para realizar las acciones correctivas que correspondan.

La red de comunicaciones constituye un factor muy importante en la disponibilidad del servicio a los usuarios remotos. Una planeación no adecuada de su capacidad, resultará en un impacto directo en la disponibilidad del servicio. Se requiere que por parte de la red, se tenga de manera constante un proceso que esté monitoreando su comportamiento y retroalimentando con los resultados de éste monitoreo, a los grupos encargados de desarrollar la planeación de ella.

Evaluación del Riesgo

Es necesario realizar un análisis formal para identificar los riesgos específicos asociados con los activos críticos de información.

El resultado más importante del proceso de evaluación de riesgo, es la información que se utiliza para desarrollar e implantar las políticas de seguridad.

Cada Unidad de Negocio debe identificar a un ejecutivo responsable para cada aplicación crítica o conjunto de información. Ese mismo ejecutivo debe conducir un ejercicio de análisis de riesgo cada año como mínimo para asegurar tanto la integridad como la disponibilidad y confidencialidad de la información. Los siguientes riesgos y áreas expuestas deben ser considerados al conducir el análisis de riesgo.

• Impacto sobre el banco si nuestros clientes son atendidos inapropiadamente, o si la información acerca de ellos es inadecuadamente vista, accesada, exhibida, o modificada.

• Impacto sobre la empresa si los empleados violan las licencias, privacidad, o requerimientos legales.

• Impacto sobre la empresa si la gente no autorizada obtiene acceso a información acerca de empleados, estrategias comerciales, información de clientes, políticas y otra información confidencial.

• Impacto sobre el banco si los procedimientos de seguridad reducen la productividad, tiempo de respuesta del sistema o disponibilidad del mismo

• Impacto sobre el banco si las unidades de negocio y/o sucursales consideran que no tienen el control adecuado sobre la protección de información de los clientes a quienes brindan el servicio.

Estándares:

✓ **Debe realizarse al menos un análisis anual de riesgos que permita identificar impactos en el negocio**

Se debe instrumentar un proceso periódico que permita determinar el nivel de exposición a que están sujetos los activos críticos de información que utiliza. Un proceso que permita identificar las amenazas a que están expuestos los activos críticos de información, y el nivel de vulnerabilidad de los mismos, permitirá a la organización reforzar los niveles de protección.

El análisis del valor de la Información de los recursos vulnerables del sistema, que pudieran ser comprometidos por violaciones de seguridad, es otro punto que requiere ser identificado periódicamente. Finalmente, la identificación del impacto que pudiera originar en el negocio la posible violación de seguridad, será una indicador definitivo respecto a los esfuerzos que se deben poner en proporcionar mayor protección a estos.

✓ **La normatividad sobre la utilización de los activos críticos de información debe ser definida por sus propietarios**

Los dueños de los activos críticos de información tienen la responsabilidad de que la misma sea utilizada correctamente y que este perfectamente definido el entorno sobre el cual debe *protegerse la información incluyendo condiciones de desastre.*

Los propietarios de los recursos son responsables por definir las políticas de los recursos y por otorgar los privilegios para usar sus recursos a otros individuos y programas. Los propietarios deberán especificar las reglas discrecionales para el acceso a recursos específicos. Los *propietarios de los recursos son responsables de desarrollar procedimientos y procesos* administrativos para administrar sus recursos. En la práctica, pueden delegar responsabilidades cotidianas para mantener e implantar estos procedimientos a administradores de seguridad.

✓ **El Acceso a la Información debe ser otorgado por su dueño**

Los usuarios y programas deben tener ***explícitamente*** otorgados los privilegios genéricos de utilizar cada tipo de recurso requerido (por ejemplo: un usuario no puede ver ninguna información sobre clientes, a menos que tenga el privilegio genérico de ver la información de clientes).

El dueño de la información debe considerar los requerimientos de acceso a la misma para los distintos grupos de usuarios que la utilizan en el desarrollo regular de su trabajo y con base en ello conceder privilegios de acceso por tipo (o perfil) de usuario, a fin de accesarla hasta el nivel que sea requerido.
A los usuarios no les serán otorgados los privilegios de usar más recursos que los necesarios para que ellos realicen su trabajo. Los privilegios otorgados deben ser consistentes con la función asignada y responsabilidad del trabajo del individuo. Los privilegios deben ser cambiados cuando un individuo es transferido a otra asignación teniendo diferentes responsabilidades.

- ✓ **El dueño de la información debe verificar periódicamente la validez del acceso de usuarios a la información**

El acceso de los usuarios a recursos protegidos, debe ser revisado semestralmente, por lo menos, con el objeto de asegurar que su acceso sigue siendo permitido y que los privilegios asociados con su acceso siguen siendo validos, y están de acuerdo con sus responsabilidades actuales de trabajo.

Para un perfil de usuarios, los requerimientos de acceso a la información cambian con el tiempo. Esto es debido a muchas razones, dentro de las cuales se cuentan por ejemplo: cambios en los procedimientos operativos del negocio, cambio o actualización en las aplicaciones, modificación de políticas y estándares operativos entre otros. Debido a esto, es necesario que el dueño de la información realice de manera periódica una revisión respecto a los privilegios de acceso a la información con que debe contar un perfil particular de usuarios.

- ✓ **Debe realizarse regularmente una comparación entre los requerimientos de acceso de los usuarios y el nivel de acceso con que realmente cuentan**

La falta de control en el acceso de los usuarios a los activos críticos genera desviaciones entre la información que realmente accesan contra lo que debieran accesar. La identificación de éstas desviaciones, es el primer paso tendiente a su corrección.

Un análisis de las desviaciones en el control de acceso de los usuarios permitirá definir que usuarios se encuentran fuera de estándares e instrumentar un proceso tendiente a eliminar las desviaciones en el control de acceso. Es necesario que éste tipo de proceso se realice de una manera periódica con el fin de garantizar que cada usuario tenga el acceso adecuado a los activos de información.

Manejo de Políticas

Define las políticas de seguridad que regularán todas las actividades desarrolladas por los empleados y los proveedores que utilicen los sistemas e instalaciones de la organización. Estas Políticas, serán publicadas de manera que se encuentren al alcance de todos los involucrados, incluyendo tanto al personal interno como externo que labore para la organización.

Estándares:

- ✓ **Todo el personal debe seguir las políticas y estándares de seguridad para controlar y proteger la información**

Este estándar es aplicable al personal de la organización, a sus empleados regulares y empleados no regulares tales como temporales, contratistas, vendedores y consultores. Este Estándar se refiere a toda la información sin tomar en cuenta la forma ni formato.

Todo el personal que labora en la organización ya sea como empleado regular ó temporal debe conocer las políticas y los estándares de seguridad que regulan y controlan uno de los activos más valiosos de la Institución que es la información.

Por este motivo es muy importante planear e impartir programas de concienciación a todos los empleados, consultores y vendedores de tal manera que todo el personal se encuentre comprometido y consciente del cumplimiento de estas políticas.

Implicaciones. Un programa de concienciación que involucra a toda la Institución puede llevar demasiado tiempo ya que depende de áreas que no se encuentran bajo el control del área de sistemas.

- ✓ **Los sistemas, la red de comunicaciones y la Información solamente serán utilizados para fines de negocio aprobados por la dirección responsable**

Tanto la información (especificaciones de producto, bases de datos, listas de correo, software interno, documentación, etc.), como la red de comunicaciones y el acceso a los sistemas debe ser utilizada exclusivamente para propósitos aprobados del negocio y diseñados específicamente por la dirección. Por lo tanto, su uso esta sujeto en cualquier momento a revisión.

La información no debe ser utilizada para beneficio propio y ni ser entregada a terceros que pudieran dar un uso diferente para la cual fue creada inicialmente, afectando los intereses de la organización. Por ejemplo, si información confidencial es entregada a la competencia, la participación de la organización en el mercado pudiera verse impactada. La información y los sistemas son un activo muy valioso, por lo tanto, no debe ser utilizada con fines distintos a los objetivos de la Institución. Es imperativo que se realice un programa de concienciación hacia todos los empleados reforzando este aspecto.

- ✓ **El uso de equipos propiedad de empleados en localidades de la organización debe ser autorizado por la gerencia**

Los empleados pueden utilizar sus propios equipos, dispositivos periféricos, o software en las localidades de la organización siempre y cuando cuenten con la autorización de la gerencia a la cual corresponden. El personal de Seguridad Institucional debe estar enterado y tendrá que llevar un control de los recursos propiedad de los empleados.

- ✓ **Todo software utilizado debe contar con licencia de uso**

Todo el software cargado en las computadoras de la organización, o en las computadoras utilizadas para el negocio debe estar de acuerdo a los compromisos de licencias, las leyes de protección de reproducción y los acuerdos de compra.

Las implicaciones legales originadas por tener instalado software sin licencia de uso en los equipos de la organización son enormes. Las multas en las que se incurre por violar las leyes de propiedad intelectual de autor o derechos de uso son regularmente cuantiosas y serán responsabilidad del empleado que infrinja este estándar. Por lo que todo software utilizado en las computadoras debe contar con la respectiva licencia de uso y en caso contrario debe ser removido inmediatamente.

Los empleados o personal externo no deben restaurar o instalar software no aprobado desde sistemas externos (por ejemplo: de boletín electrónico, de correo electrónico externo, de redes externas de comunicaciones, o de otros sistemas fuera de la organización).

✓ **No esta permitido el uso de software de seguridad por los usuarios del sistema**

A menos que esté específicamente autorizado por el área de Seguridad, los empleados no deben tener en su poder o utilizar software o herramientas de hardware que puedan romper mecanismos de seguridad.

Regularmente, el software de seguridad y el software de monitoreo del sistema exponen la confidencialidad de la información que fluye en la infraestructura de tecnología de información; por esta razón, la utilización de este software será restringida para los usuarios generales del sistema. Solamente personal técnico con la autorización del área de seguridad podrá tener acceso al mismo. Como ejemplos de la funcionalidad que proporcionan esas herramientas se tienen: ayudas para la copia ilegal de software protegido contra copia, ayudas para el descubrimiento de contraseñas secretas de acceso (Passwords), ayudas para el descifrado de información encriptada, o para el monitoreo de tráfico en red.

✓ **Todo usuario de los sistemas debe contar con autorización explícita de uso**

Los individuos y programas deben estar explícitamente autorizados para usar los sistemas y espacios físicos de la organización. Este es un privilegio que sólo será otorgado cuando sea necesario que un individuo realice una función específica de trabajo y se hayan documentado sus responsabilidades y su perfil de acceso.

El desarrollo de las funciones de un puesto en particular, requiere que se habilite el acceso a los sistemas. Este deberá ser otorgado en respuesta a la solicitud de ellas por su gerente; de no existir un requerimiento gerencial, no se concederá el acceso a los sistemas. El acceso a las facilidades de cómputo y de comunicaciones debe ser realizado mediante la identificación individual del usuario (user-ID). El acceso a los archivos, bases de datos, computadoras y otros sistemas mediante identificaciones de usuario compartidas esta estricta y totalmente prohibido.

✓ ***Los terceros podrán hacer uso de los sistemas e instalaciones de la* organización solamente si cuentan con autorización específica**

Personas que no sean empleados no tendrán acceso a los espacios físicos, excepto bajo circunstancias particulares, y estrictamente a la mínima información que requieran conocer y controlados durante un periodo predeterminado. Los externos que necesiten accesar a las instalaciones ya sea para desarrollar algún proyecto o para proporcionar soporte, deben contar con la autorización específica de acceso la cual debe ser generada por la dirección a cargo del proyecto que el tercero esté desarrollando.

✓ **La administración de la seguridad de los sistemas de información debe ser proporcionada por el área de Administración de Seguridad y en forma distribuida por el usuario asignado**

La administración de seguridad para las aplicaciones y/o información que sea propiedad de una sucursal, o unidad de negocio, será responsabilidad del administrador de seguridad designado por el área de negocio o sucursal respectivamente. Esta área de negocio o sucursal puede elegir delegar algunas de sus funciones al área de seguridad centralizada. (por ejemplo: el manejo y administración de las claves de identificación de usuario o restauración de la misma.)

Solamente el área de Seguridad asignada es responsable de controlar la seguridad en las instalaciones de forma local, existirán administradores de seguridad en las diferentes redes

locales los cuales tendrán las mismas funciones y responsabilidades, pero deberá existir una área normativa para regular la seguridad de información.

- ✓ **Cada puesto que se desempeñe dentro de la institución debe estar completamente descrito y el empleado que los desarrolla debe conocer las responsabilidades propias de su puesto**

Los gerentes deben conocer las responsabilidades de los empleados que les reportan, así como cada empleado que desarrolla una función específica dentro de la organización, debe contar con una descripción formal del puesto y las responsabilidades asociadas.

El departamento de Recursos Humanos debe desarrollar, aprobar y difundir a las áreas interesadas las descripciones de puestos de las distintas funciones del negocio. Estas descripciones deben ser utilizadas para identificar los requerimientos de acceso a la información con que deben contar los distintos usuarios.

Implicaciones: La función de Recursos Humanos debe proporcionar las descripciones de puestos

Estructura y Organización

La estructura de la organización de seguridad está compuesta de unidades organizacionales con la responsabilidad de proveer servicios de seguridad para los sistemas.

- ✓ **Debe existir una descripción de puestos para cada posición que se desempeñe dentro de la Función de Seguridad y ésta debe ser comunicada al empleado que la desarrolla**

Cada persona dentro de la función de seguridad debe contar con una descripción formal del puesto y las responsabilidades asociadas del puesto que desarrolla deben ser avaladas por el área de Seguridad.

Los puestos de "administrador de seguridad", "analista de seguridad" y "director de seguridad" se desarrollarán de una mejor manera si se cuenta con una definición exacta de los roles y responsabilidades de cada uno de ellos.

- ✓ **El personal que ingrese a la organización debe certificarse**

El personal que ingrese a la Institución debe certificarse en los conocimientos y prácticas requeridas de Seguridad. Con el fin de asegurar que todos los empleados conocen las políticas de Seguridad que deben ser observadas por el personal, se recomienda que después de haber asistido a los programas de concienciación todos los empleados certifiquen estos conocimientos.

Implicaciones. El área de Seguridad deberá implantar los procedimientos que faciliten la certificación de los empleados.

✓ **El personal que ingrese a laborar al área de seguridad debe certificarse**

El Personal que ingrese al área de Seguridad debe certificarse periódicamente en las disciplinas que están involucradas con la Seguridad. Se recomienda que todo el personal que preste sus servicios en la función de Seguridad se certifique, con el fin de asegurar la actualización de conocimientos en las prácticas de Seguridad.

Conciencitización de la Seguridad

Dentro de la arquitectura de la seguridad el componente de toma de conciencia asegura que los empleados comprendan y aprecien la necesidad del negocio con relación a las reglas y procedimientos de seguridad.

Las políticas y estándares de seguridad son de un valor limitado a menos que estén explícitamente documentadas, claramente comunicadas, comprendidas y ejecutadas fielmente por el personal que presta sus servicios tantos internos como externos.

A menudo los usuarios y las personas encargadas de desarrollar los sistemas, ven a las políticas, procedimientos y mecanismos de seguridad, como barreras que reducen sus habilidades para lograr lo que ellos creen como su "verdadero" trabajo.

✓ **Los propietarios de los recursos deben dar guías para definir las políticas y normas de seguridad para sus activos de información**

Los propietarios de recursos de negocio deben comprender la importancia de definir las políticas y normas de seguridad apropiadas.

Uno de los intereses primordiales de los dueños de información de negocio consiste en que existan todos los mecanismos requeridos para que sus activos críticos de información estén plenamente protegidos. Los dueños de la información deben definir la normatividad que regule sus recursos de información, y validar que ésta sea contenida en un programa de conciencia y cultura de seguridad, y que se difunda dentro de la institución a todos los niveles. La participación activa por parte de los usuarios en programas de seguridad, proporcionará a la institución una mayor solidez en el área de seguridad, ya que multiplicará los recursos o personal con interés en que se cumplan los lineamientos de seguridad de la organización.

✓ **El programa de cultura y conciencia de seguridad debe someterse a ciclos de reforzamiento**

Un programa continuo y permanente de seguridad de información reforzará la importancia de la seguridad dentro de la organización. Este será diseñado para cambiar la cultura de la organización y servir de apoyo a las políticas, normas, metas y prácticas de seguridad.

Un programa permanente de reforzamiento de cultura de seguridad tendrá como objetivos principales: el reforzamiento respecto a la importancia que tiene la seguridad de la información dentro de la institución, la difusión de las políticas y lineamientos de seguridad que han sido actualizadas o que han aparecido. Dependiendo de que tan crítico sea para los empleados contar con el conocimiento de estos lineamientos de seguridad, se debe implantar un programa de actualización, que permita a los empleados identificar los cambios que reforzarán e incrementarán la utilización de las políticas y procedimientos de seguridad así como los mecanismos de ejecución.

✓ **Los programas de cultura y conciencia deben puntualizar en la importancia de la seguridad respecto a su contribución al logro de los objetivos de negocio**

Los programas de concienciación de seguridad deben ser desarrollados e implantados para educar a los empleados, con respecto a la importancia de los procesos de seguridad de información, en función del logro de los objetivos de negocio de la organización. Las políticas y los procedimientos explícitos de seguridad deben ser documentados y dados a conocer.

Los usuarios del sistema deben apreciar la importancia para el negocio en relación al seguimiento y apoyo de los procedimientos, reglas y normas de seguridad.
El programa de cultura y concienciación efectivo puede ayudar al usuario de sistemas a considerar los procedimientos, políticas, estándares, lineamientos y normas de seguridad como elementos criticos para el éxito de sus funciones, en lugar de una barrera o problema que reduce su efectividad. Una concienciación integral de seguridad en los usuarios de los sistemas de información redundará en una contribución directa a los objetivos del negocio. Los incidentes de seguridad en que tradicionalmente se incurre por falta de conocimiento y que originan quebrantos se verán reducidos (y en algunos casos, eliminados).

✓ **Los usuarios deben comprometerse por escrito con la seguridad**

El seguimiento de las políticas y lineamientos de seguridad debe estar formalmente establecido entre la institución y los usuarios de los sistemas.

Todos los usuarios deben conocer y comprender la importancia de las normas y procedimientos de seguridad de la información, y deben estar de acuerdo con incorporarlos en el desarrollo de su trabajo diario. Todos los empleados deben firmar (validar) un acuerdo por la seguridad informática y en intervalos regulares de tiempo refrendar su compromiso por cumplirla. El acuerdo requiere que el empleado reconozca que la violación de las políticas, reglas o procedimientos del acuerdo serán causa para tomar acciones disciplinarias que pueden llevar a la rescisión de contrato, esto incluye los intentos de prueba a posibles debilidades de la seguridad de los sistemas.

✓ **Todos los empleados incluyendo nuevos o temporales deben completar un programa de conciencia de seguridad**

Los empleados ya sean nuevos o temporales deben completar un programa de cultura y conciencia de seguridad que les permita conocer las políticas y lineamientos a los que su actividad informática debe apegarse.

✓ **Cada usuario de los sistemas es responsable de reportar en forma inmediata cualquier condición anormal que detecte**

Todo el personal que labore en la organización tiene la responsabilidad de reportar al área de Administración de Seguridad cualquier desviación ó debilidad en la operación de los sistemas que puedan encontrar.

Implicaciones asociadas: Cada analista de seguridad debe implantar y publicar los mecanismos formales de reporte y respuesta a eventos o incidentes de seguridad basados en el procedimiento definido por el área de Seguridad.

- ✓ **Los empleados deben estar conscientes del proceso disciplinario en caso de violación a la seguridad**

Los empleados deberán estar conscientes del proceso disciplinario que se llevará a cabo en caso de una violación a las políticas, estándares y lineamientos de la organización.

En caso de realizarse una violación a las políticas y lineamientos de Seguridad, se realizará un seguimiento a la violación y estarán involucradas las áreas de Seguridad Institucional, auditoría y legal hasta la completa aclaración y en su caso, se llevarán a cabo acciones disciplinarias para el empleado que haya realizado la violación en caso de que así lo determine la investigación.

Seguridad Física

La seguridad física incluye las normas y procedimientos utilizados para asegurar edificios, computadoras y medios de comunicación. La adecuada seguridad física está entre los *mecanismos más efectivos para asegurar los sistemas de información. Puede proteger el* sistema tanto de una violación deliberada (por ejemplo: intentos de individuos no autorizados para obtener el acceso a los recursos del sistema), como de interrupciones accidentales que llevan a reducir la disponibilidad del sistema (por ejemplo: daño accidental a hardware como resultado imprevisto de otras actividades).

La seguridad física es típicamente suministrada por una combinación de reglas administrativas (por ejemplo: reglas respecto a quién le es permitido entrar en áreas sensibles de una oficina) y procedimientos y mecanismos físicos (por ejemplo: cerraduras, tarjetas magnéticas de identificación, aislamiento físico de hardware sensible o funciones de trabajo, etc.).

- ✓ **Los accesos a los centros de cómputo, a las áreas en las que se procesa o maneje información confidencial, conmutador y de control de comunicaciones deben estar estrictamente controlados y restringidos**

Los centros de cómputo y de Telecomunicaciones así como áreas de acceso restringido deben contar con estrictos controles de acceso que permitan únicamente el acceso al personal autorizado que tenga un legítimo interés de negocio por entrar.

Deben existir controles que registren al personal que accesa al Centro de Cómputo y a todas las áreas que soportan una actividad de negocio crítica ó sensitiva debido a la cantidad de *información confidencial que manejan, así como de los objetos que son introducidos.* Es recomendable contar con personal de seguridad que registre los accesos así como los objetos, además se deben establecer revisiones periódicas de los registros de entrada y salida y de ser posible establecer reportes gerenciales que ayuden a la toma de decisiones.

Los controles de acceso a las áreas críticas deben considerar:

a) Supervisión de visitantes
b) Registro y revisión de entradas y salidas de visitantes
c) Revisión de logs de acceso en forma periódica
d) Acceso a visitantes para propósitos autorizados
e) Identificación del visitante en lugar visible
f) Los accesos serán revocados inmediatamente al personal que deja de pertenecer a la organización.

Para implantar éste estándar se debe contar con los siguientes elementos: Bitácora, Gafetes, Cámaras de acceso, Puertas de hierro de doble fondo, etc.

- ✓ **Los respaldos de la información en medios magnéticos (cinta, diskette, cartuchos) deben protegerse adecuadamente**

Los medios magnéticos que contienen respaldos de información crítica de cualquier plataforma deben ser protegidos contra robo y deben estar guardadas en una bóveda externa al centro de datos. El acceso a estas bóvedas debe estar debidamente controlado por medio de registros, y debe existir un control estricto de entrada y salida de objetos. Las bóvedas deben cubrir con el estándar de protección de áreas críticas o sensitivas.

- ✓ **Las áreas críticas o sensitivas contarán con equipo de seguridad física**

Las áreas críticas deben contar con el apropiado equipo de Seguridad Física para evitar daños tanto a la información como a los equipos de hardware y se debe instruir al personal sobre el uso y funcionamiento de los equipos.

Es recomendable la instalación de equipo contra incendio, detectores de humo, alarmas, extintores de fuego y salidas de emergencia. Con el objeto de evitar daños físicos al personal, a la información y a los equipos de hardware. El personal que labora en estas áreas debe estar capacitado para manejar adecuadamente cada una de estas facilidades.

- ✓ **Las áreas críticas o sensitivas que procesan información deben contar con equipo de respaldo para suministros de energía**

Las *operaciones críticas de negocio deben contar con equipo UPS para suministros de energía* en caso de problemas. Por razones de la continuidad en la operación normal del negocio se recomienda disponer de equipos que suministren energía en caso de una falla, es necesario contar con mantenimientos periódicos a estos equipos y realizar pruebas programadas a los mismos para estar siempre en posibilidad de prestar los servicios a los clientes sin interrupciones y evitar *pérdidas financieras.*

- ✓ **Mantenimiento periódico a equipos de cómputo y comunicaciones**

Los equipos de cómputo y comunicaciones deben contar con mantenimientos programados para evitar interrupciones en el servicio. Los equipos de hardware son susceptibles de tener problemas físicos, por lo que es recomendable programar mantenimientos preventivos por componentes y por tipo de equipo. Es necesario desarrollar un plan de mantenimiento conjuntamente con los proveedores de manera que éstos se hagan en tiempos que no afecten la operación del negocio.

En caso de ocurrir un problema de hardware se hará necesario contar con una bitácora que registre el tipo de problema presentado, la hora, fecha así como la fecha y hora en que el problema quedó resuelto. Los cables conductores de energía eléctrica que soportan servicios de tecnología de información deben estar protegidos contra intercepción o daños físicos.

- ✓ **Contar con control de acceso a los componentes críticos de red**

Los componentes de la estructura del sistema de comunicación (por ejemplo: hardware de comunicación, cableado, modems, etc.) deben estar ubicados en armarios bajo llave, solamente los administradores autorizados de seguridad y la gerencia tendrán acceso a esos armarios.

Es recomendable que todos los equipos de comunicaciones sean guardados en muebles con el fin de evitar la substracción de los mismos o la mala utilización de los recursos. Es importante identificar las áreas en las que se pudiera encontrar equipo de comunicaciones y verificar si existen las facilidades para el resguardo del equipo.

- ✓ **Los equipos servidores de aplicaciones deben estar confinados en áreas seguras**

Los servidores centrales y remotos deben estar ubicados en un medio ambiente seguro. Se deben tomar medidas para limitar el acceso físico al servidor que podría llevar a extravío parcial o total del servidor, siempre que sea posible el servidor estará ubicado en un armario o sitio cerrado, sólo el personal autorizado tendrá acceso físico al servidor.

- ✓ **Los equipos servidores de aplicaciones, las estaciones de trabajo y las computadoras personales deben contar con protección de acceso físico**

Los equipos servidores de aplicaciones y las estaciones de trabajo estarán cerradas con llave, de tal manera que no puedan ser físicamente abiertas. Las llaves para las estaciones de trabajo deben ser controladas y administradas por el área de seguridad Institucional.

Las estaciones de trabajo así como las computadoras personales son susceptibles de sufrir robos o extravíos parciales de partes, por esta razón deben protegerse con cerraduras especiales instaladas físicamente en éstas. Las estaciones de trabajo móviles (portátiles) serán guardadas en ambientes bajo llave, o armarios bajo llave, cuando no sean utilizadas por el empleado y durante la operación deben contar con cables de protección contra robo total.

- ✓ **Los números telefónicos para acceso remoto deben manejarse de manera confidencial**

Los números telefónicos de modems sólo serán suministrados a usuarios autorizados. Es importante concienciar a todos los empleados acerca de no proporcionar los números telefónicos de modems a usuarios no autorizados, ya que no son de uso público y ésta situación provocaría accesos a recursos o activos críticos de la Institución.

- ✓ **Los modems deben estar programados para responder a la llamada después del sexto anuncio**

Los modems deben estar programados, para no contestar las llamadas telefónicas entrantes a la primer corriente de llamada. Los modems requerirán al que solicita conexión (originador) la generación de siete ciclos de corriente de llamada, los primeros seis como medida de protección y esperar el séptimo para contestar.

Con el fin de evitar los accesos de usuarios no autorizados por medio de modems, se deben programar para que contesten después de seis llamados y así disminuir la posibilidad de ser accesados. Se recomiendan seis llamadas debido a que existe la posibilidad de que algún usuario no autorizado intente accesar la red marcando en forma automática los números telefónicos, y si un módem contesta inmediatamente el intruso identificará rápidamente los números telefónicos que puede utilizar para accesar la red con equipo rastreador de módem.

✓ **Se debe desarrollar un plan de seguridad física por cada plataforma de sistemas**

Cada área responsable de una plataforma de sistemas (AS/400, RISC, Mainframe, LANs, PCs) desarrollará y documentará un plan de seguridad física. Para evitar daños físicos tanto al personal como a los recursos de cómputo es recomendable desarrollar un plan que identifique las faltas de seguridad y que instrumente medidas tendientes a corregir las deficiencias. El área de Seguridad revisará y aprobará todos los planes de seguridad física.

Administración de la Seguridad

La administración de seguridad consiste en las prácticas de manejo y procedimientos operacionales usados para suministrar un nivel aceptable de protección al medio ambiente.

En suma, los controles administrativos incluyen procedimientos establecidos para asegurar que todo el personal que tiene acceso a los recursos del sistema, tenga las autorizaciones requeridas y privilegios apropiados para realizar sus tareas.

La responsabilidad de la administración de seguridad de los sistemas operacionales, es de los administradores de seguridad del Departamento de Seguridad de la Información, o su equivalente. La administración de seguridad de las aplicaciones y control de acceso para los archivos de datos es responsabilidad de cada departamento. En algunos departamentos, la administración es manejada centralmente, en otros departamentos la administración es delegada a los administradores locales y en otras, la responsabilidad es distribuida.

✓ **La función de administración de seguridad define accesos a información crítica con base en perfiles de usuario**

Se deben definir accesos a los activos críticos de información a partir de los perfiles de usuario especificados conjuntamente con el propietario. El área de administración de Seguridad debe definir perfiles de usuario a los cuales se les concederá el acceso a la información dependiendo del trabajo que desempeñan. Estos accesos deben ser autorizados por los dueños de la información. Se debe tener cuidado de conceder acceso únicamente a la información que necesitan, y verificar que solamente se realizan las operaciones requeridas (lectura, escritura, modificación, control etc.).

✓ **Las políticas de seguridad deben ser consideradas en los procedimientos que se desarrollen para la función de administración de seguridad**

Se deben ejecutar las políticas de seguridad en los recursos del sistema. El personal de seguridad debe conocer perfectamente las políticas y aplicar éstas en cada actividad que desempeñen. Posiblemente durante el desarrollo de sus funciones, tendrá que generar otras políticas, solicitar su autorización y darlas a conocer al personal involucrado.

✓ **Deben crearse perfiles especiales de usuario para la función de auditoria**

Se debe contar con perfiles especiales para ser usados por la función de auditoría. Debido a las funciones que desempeña el personal de auditoría, requiere tener funciones especiales para accesar información del sistema de seguridad. Posiblemente sea necesario planear una capacitación para el personal de auditoría de manera que puedan desempeñar sus funciones sin solicitar la ayuda del personal de seguridad.

✓ **Se debe incluir en el esquema de protección la administración de software de seguridad de terceros**

Se debe contar con la definición del como se hará la administración de los productos de seguridad de proveedores (por ejemplo: licencias de programas, hardware para seguridad). El área de Seguridad debe diseñar procedimientos para vigilar el comportamiento del software de terceros, y de la persona que los ejecuta cuidando que no se viole la seguridad de la información. Puede suceder que el o los proveedores no sean éticos y traten de realizar accesos no autorizados sobre los activos críticos, estos procedimientos deben ser vigilados desde el inicio (instalación de los productos) hasta que se decida si se adquiere el producto.

✓ **Deben desarrollarse procedimientos para la creación de nuevas claves de usuario (user-IDs)**

Se debe contar con un procedimiento para crear nuevas identificaciones de usuario. Con el objeto de facilitar las tareas del área de Seguridad se recomienda realizar procedimientos para la creación de nuevos user-IDs, debido a que son tareas repetitivas.

Los user-Ids deben ser creados por medio de un estándar que se defina previamente de manera que éstos deben indicar el área a la que pertenece el usuario. Se debe contar con un procedimiento para detectar las identificaciones de usuario (user-ID) que no cumplan con los estándares establecidos e iniciar el proceso que los incluya bajo estándar.

✓ **Autorización de nuevas claves de usuario (User-IDs) y accesos para terceros**

El acceso a proveedores y personal que no labora en forma normal en la organización debe ser cuidadosamente analizado, y proporcionar solamente el acceso a recursos requeridos para desarrollar sus labores.

Con el objeto de restringir los accesos a usuarios no autorizados es necesario analizar los requerimientos de terceros para acceso de información y de recursos tecnológicos y solamente proporcionar los recursos estrictamente necesarios. Se requiere que los contratos realizados con proveedores, que utilicen servicios de IT, incluyan los requerimientos y responsabilidades de seguridad.

✓ **Deben existir procedimientos para realizar las tareas del área de Administración de la Seguridad**

Se deben definir procedimientos para las tareas repetitivas del área de seguridad considerando las siguientes:

- Borrar identificaciones de usuarios existentes que ya no pertenezcan a la Institución.
- Restauración de las identificaciones de usuarios vencidas.
- Asignación de perfiles para nuevos usuarios y mantenimiento del perfil para los usuarios existentes.
- Definición de Grupos de Recursos y Grupos de Usuarios.

Para facilitar las tareas y disminuir el tiempo de las actividades repetitivas del área de seguridad deben crearse procedimientos técnicos. Estos procedimientos deben estar formalmente documentados para efectos de poder capacitar de una manera más fácil, al nuevo personal del área de seguridad de la información.

- ✓ **Se debe contar con una definición que agrupe usuarios en función de sus privilegios de acceso a la información**

Los usuarios deben estar asignados a grupos basados en peticiones del administrador local de seguridad. Con el fin de organizar las actividades de seguridad y facilitar su control, se deben definir grupos de usuarios de acuerdo a la estructura organizacional de la Institución.

- ✓ **Los dueños de la información deben verificar los privilegios concedidos a los activos críticos**

Los dueños de la información verificarán cada seis meses, al menos, las definiciones de seguridad sobre los activos de información critica de su propiedad, a fin de garantizar la correcta asignación de privilegios. Con el objeto de asegurar que los activos críticos no sean accesados por personal no autorizado se deben establecer revisiones periódicas de los privilegios concedidos a los usuarios de la información.

- ✓ **El proceso de seguridad debe ser continuamente monitoreado**

Es necesario establecer un sistema de monitoreo con el objeto de conocer como trabaja el proceso de seguridad. El área de Seguridad debe definir puntos críticos con el propósito de monitorear el funcionamiento del proceso de Seguridad.

Si se tiene definido un buen proceso de Alerta y Auditoría, serán de gran ayuda para la toma de decisiones que ayudará a mejorar y retroalimentar el proceso de Seguridad.

- ✓ ***Las claves de acceso a los sistemas deben ser deshabilitadas una vez que* dejen de ser requeridas**

Cuando un empleado deja la organización, el departamento de Recursos Humanos debe estar involucrado en el proceso de eliminar los privilegios a su clave de usuario correspondiente, para el acceso a los sistemas. Con el fin de evitar posibles violaciones a la seguridad, el área de Recursos Humanos reportará al área de Seguridad una vez que un empleado ha dejado de pertenecer a la organización. Por otro lado, no hay que olvidar a los proveedores que frecuentemente obtienen autorización para accesar los activos de información. Las áreas que contratan a terceros, deben informar al área de Seguridad una vez que éstos terminen sus proyectos.

- ✓ **El mantenimiento de claves de usuarios será centralizada y su actualización podrá ser local en caso requerido**

La identificación y el directorio de usuarios serán controlados y mantenidos centralmente; pero administrados localmente, si fuera necesario por razones de productividad, por el área de Seguridad.

Comúnmente existen diferentes plataformas en las organizaciones y algunas están funcionando en sitios remotos; en cada plataforma donde exista un sistema de seguridad, debe existir un administrador de seguridad actuando en forma remota. Las normas para esta administración remota las debe dictar el área de Seguridad.

✓ **La función de Administración de seguridad debe ser capaz de mantener la identificación de usuarios**

El administrador de seguridad debe ser capaz de definir usuarios, borrar usuarios, restaurar contraseñas, restaurar permisos expirados de usuarios (previa autorización), de acuerdo con las autorizaciones delegadas para ellos por los propietarios de la información y aplicaciones.

El personal del área de Seguridad debe estar debidamente capacitado para realizar sus funciones. Es necesario analizar los conocimientos actuales del personal, y preparar un programa de capacitación para el personal a manera de asegurar que todas las tareas asignadas serán realizadas de manera exitosa.

✓ **Se debe contar con herramientas para la administración de seguridad**

Las herramientas de administración de seguridad son utilizadas para mantener la estructura de seguridad del perfil del usuario, privilegios, grupos de usuarios y recursos, y recursos de grupos. Con el fin de facilitar la realización del trabajo del área de administración de seguridad, es conveniente que se tenga disponible un conjunto de herramientas que les facilite la administración de la seguridad y les permita ejercer un control más estricto. (User Manager Domain, Key Security, RACF, Vanguard etc.).

Administración de Auditoría

La administración de auditoría es el componente de la seguridad, que consiste en aquellas actividades que habitualmente capturan y acumulan información relativa a seguridad, sobre la actividad de los sistemas.

La información auditada puede ser usada para generar informes de auditoría de rutina describiendo las actividades del sistema, generar alertas sobre violaciones a la seguridad o intentos de violación que son enviados a los administradores de seguridad, provee pistas de auditoría que pueden ser usadas para trazar actividades del sistema, siguiendo una violación al mismo y suministra información a auditores externos quienes demostrarán el nivel del sistema de acatamiento con las políticas de seguridad y prácticas de seguridad generalmente aceptadas.

✓ **Se debe desarrollar un proceso para la conducción de la auditoria de incidentes de seguridad**

Un proceso documentado asegurará que las violaciones a las políticas de seguridad y procedimientos, llevarán a tomar acciones contra el individuo o programa que haya violado los controles de seguridad. La auditoría será un "círculo cerrado", en el cual las violaciones son identificadas, los propietarios de los recursos y los administradores de seguridad son notificados, y un proceso perfectamente definido es seguido, el cual deberá proporcionar retroalimentación a todo el proceso de seguridad de información con el objeto de mejorarlo y prevenir futuras violaciones.

✓ **Los propietarios de la información deben participar en el proceso de auditoría**

Un proceso de revisión de la auditoría debe asegurar que: existan los informes de la misma, las alertas sean revisadas, se haya completado el análisis de auditoría, se obtenga la conclusión y sean tomadas las acciones establecidas durante el proceso. El comité de auditoria debe ser formalmente estructurado y a él deben pertenecer recursos clave de las distintas áreas de negocio de la Institución.

La dirección del área de negocio involucrada en la violación de seguridad debe encabezarlo e incluir a las áreas de Auditoría, Legal, Recursos Humanos, Sistemas (desarrollo y operación), Seguridad Física y Seguridad.

✓ **La información de auditoria debe estar disponible para su uso**

Una variedad de informes de auditoría estarán disponibles para el comité de auditoría, incluyendo reportes que describan:

a) Como están siendo utilizados los recursos del sistema.
b) Los privilegios asociados con los usuarios, programas y recursos de grupo.
c) Los usuarios y programas a los que se les permite el acceso a recursos específicos

✓ **Se deben crear mecanismos para registrar los accesos a sistemas**

Todos los intentos de conexión (logon), desconexión (logoff), cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, adición de usuarios, reinstalación de usuarios, y supresión de usuarios, serán registrados.

La identificación de los distintos incidentes de seguridad que deben ser rastreados, así como la definición de los elementos de información que deben ser registrados para efectos de auditoría son una de los elementos clave sobre los que estará soportado el proceso de auditoría. Dentro de la información que debe considerarse está la siguiente:

a) Todos los intentos inválidos para accesar a recursos de los usuarios
b) Privilegios para usuarios o programas
c) Acciones de usuarios que tienen privilegios o poderes especiales (por ejemplo: administradores del sistema)
d) Cambios en la información de seguridad
e) Cambios de parámetros de seguridad de los sistemas serán registrados.

✓ **Se debe llevar un control individual de la actividad de cada usuario del sistema**

El registro de la actividad que a nivel individual realiza un usuario, debe ser llevado a cabo para cada una de las transacciones que hayan sido definidas para ser incorporadas en el log de auditoría. Cada transacción definida, debe estar registrada en un log ya sea de tipo aplicativo o de sistema. La información registrada debe incluir información del tipo: que, quien, cuando, donde fue hecha la transacción etc.

✓ **Las aplicaciones deben operar con base en la identificación del usuario que accesa el sistema**

Las transacciones de las aplicaciones deben manejar identificación de usuarios (user-ID), en lugar del de las terminales. La función de auditoria para ser más efectiva, requiere de determinar quien fue la persona que realizó la transacción que modificó la información sujeta a auditoría. Es necesario realizar una adecuación de las aplicaciones heredadas de épocas pasadas que aún están en operación y que no tienen implantada la identificación del usuario que las accesa así como información accesada, ubicación de la terminal, identificación de la terminal, fecha y hora de acceso, aplicación o transacción utilizada.

✓ **Se deben crear mecanismos para consolidar la información de auditoria**

Todos los registros de auditoría de los sistemas, serán consolidados en una base de datos o archivo que facilite la generación de informes.

El requerimiento de contar de manera oportuna con la información de auditoría para dar seguimiento a un incidente, puede ser acelerado de manera ágil mediante su consolidación en bases de datos. Se debe evaluar el esfuerzo requerido para implantar la programación requerida para su explotación.

Administración de Alertas

Este proceso de seguridad está compuesto por mecanismos que automáticamente detectan violaciones de seguridad, e informan a los administradores de seguridad y otras partes interesadas. Las alertas surgen, por lo general, basadas en información acordada con los propietarios, auditores y administradores de seguridad sobre la auditabilidad de la información.

- ✓ **Debe ser definido un modelo para alertas de seguridad**

El área de Seguridad analizará y definirá un modelo estándar para los mensajes de alertas de seguridad, información como fecha, hora de la violación, nombre del recurso y usuario involucrado, deben ser incluidos.

- ✓ **Una estructura de comunicación formal de los incidentes de seguridad debe ser implantada**

Un mecanismo formal será desarrollado para permitir a los empleados informar acerca de violaciones al sistema de seguridad, así como de actividades inseguras y que permita tomar decisiones correctivas o legales, según corresponda.

- ✓ **Se debe contar con mecanismos que analicen los patrones de conexiones cuando sucede una violación de seguridad**

Cuando se registra una Alerta de Violación de Seguridad se deben analizar los medios o patrones de conexión empleados. Cuando se registra una alerta de violación de seguridad se deben analizar el proceso inverso de conexión al sistema para verificar las posibles debilidades que pudieran existir, e inmediatamente tomar acciones correctivas que las eliminen.

- ✓ **Se debe contar con mecanismos que notifiquen al administrador de seguridad sobre el cambio a operación fuera de línea**

Los administradores de seguridad serán notificados cuando el sistema este activado en la modalidad fuera de línea (offline), ya que no habrá registros de auditoría (debido a que no se encuentra disponible la función de registro de auditoría).

Confidencialidad

El proceso de confidencialidad de un sistema de seguridad es responsable de asegurar que los datos y las comunicaciones que han sido obtenidos por programas, o individuos no autorizados, no puedan ser usados; al mismo tiempo que garantiza la no divulgación de la información. El uso de algún mecanismo de confidencialidad refleja el hecho de que los mecanismos de control de acceso pueden no suministrar una completa protección para todos los recursos del sistema.

También refleja el hecho de que ciertos recursos (por ejemplo: comunicaciones que pasan a través de medios públicos no seguros) son esencialmente difíciles para proteger usando técnicas de control de acceso.

La información de cualquier organización debe ser categorizada dentro de una de las tres clasificaciones las cuales tienen distintos requerimientos de control de acceso, pudiendo ser estas: **Confidencial para el Negocio, Interna, y Pública.** Este sistema estándar de clasificación debe ser utilizado en todas las áreas de la Institución. Los dueños de la información son los responsables de clasificar los activos de información por los que son responsables. Por lo menos una vez por año, los propietarios de la información deben revisar la clasificación de ésta para asegurarse que siga clasificada correctamente, y que los controles de acceso estén funcionando.

- ✓ **Toda la información debe estar clasificada**

La información debe ser clasificada con base en su confidencialidad, sensibilidad, riesgo de pérdida o compromiso, aspectos legales, requerimientos de retención y facilidad de recuperación.

- ✓ **El propietario de los activos de información debe estar claramente identificado**

Es necesario establecer a un propietario de la información y este a su vez definir quienes son los individuos que tienen una necesidad legitima para accesar la información (identificando sus privilegios de acceso) para propósitos de negocio.

Dentro de la institución, para cada tipo de activos de información, existe una función en la que recae la propiedad de ésta. La importancia de definir un único propietario del activo de información, a diferencia de una propiedad compartida entre distintas unidades de negocio, resultará en un control más estricto sobre los activos de información.

La responsabilidad sobre todos los aspectos de la información será única y exclusivamente de su propietario, quien ayudado por las distintas funciones dentro de la institución, buscará que se cumplan con todas las actividades necesarias para proporcionar una adecuada protección a la información .

- ✓ **La información impresa en cualquier medio (papel, microficha, etc.) debe estar claramente clasificada**

La información impresa debe contener una leyenda que muestre su clasificación, la fecha de impresión y el proceso que la genera. La seguridad de la información que ha sido impresa, es responsabilidad del usuario que generó la impresión. Este individuo es responsable por la realización de un adecuado estampado del nivel de confidencialidad en esa impresión, el cual debe ser consistente con los criterios de confidencialidad definidos por el propietario de la misma.

- ✓ **La información confidencial debe estar fisicamente almacenada de manera segura**

Toda información clasificada confidencial, cuando no este en uso, debe estar almacenada en un gabinete con cerradura adecuada y por ningún motivo exponerla a ser accesada por usuarios no autorizados.

✓ **La información debe ser destruida de manera segura**

Cuando la información no es requerida por más tiempo, su destrucción debe ser hecha ya sea mediante una trituradora o incineración. Se debe contar con un presupuesto y realizar una evaluación de equipos a adquirir para la destrucción de la información.

✓ **La información confidencial no debe ser almacenada en estaciones de trabajo o PC's**

Las estaciones de trabajo no cuentan con herramientas que proporcionen la protección requerida para los activos de información en ellas almacenada, por lo que los usuarios de éstas deben evitar tener información confidencial en sus estaciones de trabajo o en las áreas compartidas de los servidores.

✓ **Las estaciones de trabajo no deben dejarse desatendidas con una clave de acceso en sesión**

Los usuarios no deben compartir su identificación de usuario/contraseña con otros usuarios. Un usuario debe desconectarse (logoff) del sistema antes de permitir que otro usuario trabaje en la *misma estación de trabajo.*

La responsabilidad que un usuario adquiere al recibir su clave de acceso se extiende a todo el tipo de interacción que esa clave de usuario tenga con el sistema, ya sea directamente por la persona que la recibió, o por cualquier otra persona que pudo haber tenido acceso a ella. Una *medida complementaria que debe ser implantada por el sistema es la de inhabilitar* automáticamente el acceso a la aplicación desde las estaciones de trabajo, en caso de que la misma no haya sido usada por 15 minutos.

✓ **Los usuarios deben accesar los sistemas utilizando su clave de usuario propia**

Un usuario debe trabajar usando su identificación de usuario y contraseña. Un usuario no debe usar una sesión de trabajo iniciada por otro usuario.

En virtud de que la utilización de las claves de acceso implica responsabilidad por parte del usuario a quien fue asignada, las estaciones de trabajo en las cuales esté activa la clave de *acceso de un usuario, no deben dejarse a la disposición de otras personas.*

✓ **Las claves secretas de acceso y llaves de encripción no deben ser comunicadas ni compartidas**

Las claves secretas de acceso (Passwords), llaves de encripción e información similar son confidenciales y no deben ser comunicadas ni compartidas a individuos no autorizados.

El control de las llaves de encripción de la información debe ser estricto. Las llaves de encripción deben ser consideradas como un activo de información altamente crítico y confidencial, por lo *que se deberá de asignar al o los propietarios de las mismas.*

✓ **La clave de usuario será deshabilitada después de tres intentos fallidos al ingresar la clave secreta de acceso**

Tres fallas sucesivas para ingresar la contraseña correcta para la identificación de un usuario, ocasionará que la clave de usuario sea inhabilitada. Sólo puede ser rehabilitada por el *administrador de seguridad con la autorización del Gerente.*

✓ **La información confidencial a ser transmitida sobre la red debe estar encriptada**

La información sensitiva debe estar rutinariamente encriptada, antes de que viaje a través de la red de comunicaciones. La seguridad de la información que se transmite sobre la red de comunicaciones se vuelve mas vulnerable debido a una diversidad de factores tales como: los medios de transmisión que están fuera del control de la organización, la información que se transmite utilizando enlaces públicos, o bien se transmite conjuntamente con información de otras compañías incluyendo la red telefónica pública y la Internet. Esta situación incrementa notablemente el riesgo de que sea capturada por personas no autorizadas quienes puedan dañar a la Institución.

Integridad

El componente de integridad de un sistema de seguridad intenta asegurar que la información y las comunicaciones no puedan ser cambiadas. También asegura que los cambios no autorizados a la información y comunicaciones sean detectables aunque no sean reversibles.

Los sistemas deben proveer integridad a:

- Mensajes y otra información que circule a través de redes de comunicación.
- Información de negocio en archivos y bases de datos computarizados.
- Programas y otros componentes de sistemas.
- Los componentes del sistema de seguridad propiamente dicho.

✓ **Debe existir protección contra la actualización simultánea de un registro**

Cuando se actualiza un archivo, el registro debe ser protegido para que ningún otro programa lo accese. Dependiendo de los sistemas manejadores de bases de datos y de transacciones, *existen o no, distintos mecanismos de protección a nivel registro, a nivel archivo completo y con* distintas implicaciones cada uno de ellos.

Para poder cumplir con éste estándar, es requerido analizar por plataforma, para cada activo critico de información, las facilidades existentes o la falta de funcionalidad que puede existir para *cumplir con el estándar.*

✓ **El personal de las áreas de sistemas no debe modificar información de los ambientes de producción o de prueba**

El personal de las áreas de Desarrollo de Sistemas no deben modificar, o accesar información de los ambientes de Producción o de Pruebas, los cambios a estos ambientes estarán bajo un estricto control. Las responsabilidades de cambiar los archivos de los ambientes de producción y pruebas deben estar claramente identificadas y definidas. El proceso corporativo de Control de Cambios debe ser utilizado.

- ✓ **Deben existir mecanismos que permitan llevar controles de las modificaciones y accesos a las bibliotecas del sistema operativo y de programas producto y programas Fuente**

La función de control de bibliotecas de sistemas operativos, programas producto y programas fuente, debe ser establecida con el objeto de mantener integridad sobre los ambientes de prueba y producción. El manejo adecuado de bibliotecas de sistemas operativos y programas producto requiere efectuar un estricto control de todos los cambios que se realicen en estas bibliotecas, tanto de ambientes de producción como de pruebas. Debe estar identificado y asignado un dueño para las bibliotecas de software, quien debe definir que procesos o usuarios tendrán acceso a ellas, y quien tiene autoridad para modificarlas. Se debe tener un cuidado especial en el acceso a los programas fuente, los cuales deben ser monitoreados en forma regular.

- ✓ **La red de comunicaciones debe contar con controles que garanticen la integridad de la información al ser transportada con información de clientes**

La integridad de la información que fluye en la red puede ser alterada por terceros en caso de no contar con los mecanismos adecuados de protección. Comentarios: Los distintos ofrecimientos de servicios a clientes tales como el Banco Virtual, involucrarán un manejo integrado de sistemas internos de la organización y de clientes. El protocolo principalmente utilizado por las aplicaciones de cliente es el TCP/IP. Esta situación genera una exposición de seguridad ya que bajo tráfico IP, un usuario que desee hacer mal uso del sistema, puede observar y alterar la información que fluye en la red.

Además, existen mecanismos propios de los protocolos (a bajo nivel) de comunicación que permiten identificar si la trama (frame) no fue recibida tal cual fue enviada. Por lo que no es necesario llevar a cabo ninguna verificación integral de comunicaciones en el ambiente local del sistema o al nivel de la capa física (por ejemplo: líneas locales). Debido a que el problema se estaría ocasionando en la transmisión de información o alteración de la misma sin que se involucren los medios físicos.

Identificación y Autenticación de Usuarios

La autenticación es un mecanismo para verificar la identidad de los usuarios y programas.

- ✓ **Todos los sistemas deben contar con los mecanismos que requieran la identificación al usuario o programas que pretendan accesarlos**

Los sistemas computarizados deben contar con la capacidad de forzar a sus usuarios o programas para que se identifiquen previamente al acceso de la información.

El acceso a los sistemas computarizados requiere imprescindiblemente del uso de una identificación de usuario o programa, de esta manera se tendrá un control acerca de los recursos utilizados por cada usuario programa, y en algún momento se estará en posibilidad de detectar intentos de violaciones a la seguridad. El utilizar un indentificador para accesar los sistemas de cómputo, es el objeto que utilizará el sistema para verificar si ese usuario o programa tiene derecho a los recursos que está solicitando.

✓ **Todas las claves secretas de acceso (passwords) deben estar bajo el mismo formato**

Las contraseñas deben ser alfanuméricas y no empezar ni terminar con número, teniendo un mínimo de seis caracteres y un máximo de ocho. Se debe verificar la repetición de caracteres con respecto a la contraseña anterior en aquellos sistemas que el programa de seguridad lo permita. El implantar un formato con ciertas características para las contraseñas asegurará que éstas no sean descubiertas fácilmente, disminuyendo la posibilidad de acceso a usuarios no autorizados. Las normas seleccionadas para la selección de clave secreta de acceso deben estar controladas por medio de procedimientos que aseguren su cumplimiento.

✓ **Las claves secretas de acceso (passwords) de usuario deben ser actualizadas periódicamente**

La clave secreta de acceso del usuario vencerá automáticamente después de 30 días. Los usuarios en posiciones sensibles o funciones delicadas de trabajo (por ejemplo: administradores del sistema, auditores, etc.) pueden necesitar cambiar su clave secreta de acceso más frecuentemente. En el caso de un usuario con clave secreta de acceso vencida será requerido para proporcionar una nueva clave secreta de acceso. Una identificación de usuario con una clave secreta de acceso que no ha sido cambiada por más de 90 días, el sistema de seguridad debe solicitar al usuario el cambio de clave secreta de acceso.

✓ **Tres intentos fallidos en la autenticación de un usuario resultaran en la deshabilitación de su clave de acceso**

El contar con un límite de accesos fallidos disminuye la posibilidad de accesar al sistema por usuarios no autorizados. Todo acceso al sistema, sea éste fallido o exitoso, debe quedar grabado en algún archivo para análisis posterior de auditoría.

✓ **Debe existir una sola clave de usuario (user-ID) por sistema**

Un usuario no tendrá más de un user-ID para accesar a un sistema.

Comentarios.- Un usuario sólo podrá contar con una única clave de acceso para un sistema, ya que esto contribuirá a ejercer un mejor control de los usuarios y de recursos. En caso de que un usuario requiera de entrar a más sistemas, tendrá tantas identificaciones como sistemas solicite. A

Control de Acceso

El proceso de control de acceso previene que individuos o programas no autorizados usen los recursos del medio ambiente del sistema.

✓ **El acceso a los recursos del sistema debe estar protegido**

Todos los niveles de recursos del sistema estarán protegidos por los principales programas de seguridad. Siendo los sistemas de información uno de los activos más importantes con los que cuenta la institución, el acceso a ellos debe contar con los controles más estrictos que proporcionen los principales programas y sistemas de seguridad existentes en el mercado.

Debido a las distintas plataformas que existen, los ofrecimientos de este tipo de programación de protección son muy variados.

En caso de no ser identificado algún producto efectivo que realice el control de acceso a la información para una plataforma específica, se debe evaluar el desarrollar internamente la *protección requerida, o bien el migrar los sistemas hacia plataformas más seguras.* Dentro de la funcionalidad con que se debe contar para éstas herramientas de protección de acceso, están las de toma de acción correctiva y notificación en caso de ser detectada alguna violación de seguridad.

Los recursos de cómputo que atienden a múltiples usuarios deben, por lo tanto, ser capaces de:

a) Identificar y verificar la identidad y si es necesario conocer hasta la identificación y localización de la terminal o estación de trabajo de cada usuario autorizado
b) Registrar los accesos exitosos y fallidos al sistema
c) Proveer un sistema de administración de claves de acceso que asegure la calidad de las mismas.
d) Restringir en caso de ser necesario, el tiempo de conexión de los usuarios

- ✓ **El acceso a los recursos del sistema a través de los procesos batch y/o en línea debe estar protegido**

Todos los activos críticos deben estar protegidos contra los accesos no autorizados por medio de procesos tipo batch y/o procesos en línea.

- ✓ **El acceso a las computadoras personales debe estar restringido**

Todos los equipos personales deben contar con claves secretas que inhiban el acceso a la información cuando éste es encendido (arranque inicial) o cuando es desatendido por mas de cinco minutos.

- ✓ **La información de control de usuarios a la información debe manejarse centralizadamente**

La copia maestra o primaria de toda la información sobre el control de acceso para todos los usuarios será mantenida en una base de datos simple o centralizada.

- ✓ **El acceso a los servicios de cómputo debe ser controlado en función de los requerimientos de negocio**

Los requerimientos del negocio referentes al control de acceso a la información deben ser definidos y documentados por los propietarios de ésta. Cada propietario de las aplicaciones de negocio debe asegurarse de que se tenga una clara definición de las políticas de acceso establecidas, las cuales regulen los privilegios de acceso de cada usuario o grupos de usuarios.

Estas políticas deben tomar en cuenta tanto los requerimientos de seguridad de la aplicación en lo particular como las políticas para su difusión y el establecimiento de los principios sobre las cuales están basadas (por ejemplo: acceso exclusivo para fines de negocio, difusión de información únicamente a aquellos que tengan necesidad de conocerla, etc...)

✓ **Se debe contar con los procedimientos formales de registro de alta y baja de usuarios que accesan los sistemas**

Estos procedimientos deben cubrir todas las etapas en el "ciclo de vida" del acceso del usuario, los cuales comprenden desde el registro inicial del nuevo usuario hasta su baja final, una vez que deje de existir el requerimiento de acceso a la información

Comentarios: Con el fin de evitar el acceso no autorizado a los sistemas que controlan el otorgamiento de privilegios para el acceso a los sistemas de información, se deben mantener un estricto control en el uso y los usuarios de éstos sistemas.

El acceso a éstos deben estar altamente restringido con el fin de evitar que un usuario regular modifique sus propios privilegios de acceso.

✓ **El uso de privilegios especiales debe ser restringido y controlado**

La asignación de privilegios de acceso a la información, debe ser controlada mediante un proceso formal de autorización.

Este proceso debe:

a) Identificar los privilegios asociados con cada programa producto del sistema y la categoría de personal al cuál se deben asignar.
b) Asignar Privilegios únicamente a quien requiera conocerlos y en la base de evento por evento.
c) Basarse en un proceso de autorización y en el registro de todos los privilegios asignados.
d) Promover el desarrollo y uso de las rutinas del sistema para evitar la necesidad de asignarlos a usuarios específicos.
e) Identificar a los usuarios en forma diferente que a los usuarios regulares de las aplicaciones del negocio.

✓ **La asignación de claves de acceso debe ser controlada en forma segura**

Las claves de acceso son el principal medio de validación de la autoridad de los usuarios que accesan los servicios de cómputo.

La asignación de claves de acceso debe ser controlada por un proceso de administración formal que:

a) Obtenga el compromiso de los usuarios por mantener en forma confidencial las claves personales de acceso a los sistemas.
b) Asegure que los usuarios mantengan en forma segura las claves de acceso, obligando a los usuarios a cambiar de manera inmediata aquellas claves temporales de acceso.
c) Notifique de manera segura las claves temporales de acceso a los usuarios. Se debe evitar la notificación de claves de acceso a terceras partes mediante el uso de correo electrónico. Los usuarios deben confirmar la recepción de claves de acceso.

✓ **Los derechos de acceso de usuarios deben ser revisados en intervalos regulares de tiempo**

Para mantener un control efectivo en el acceso a la información y a los servicios, el administrador de seguridad debe realizar en forma periódica, cada seis meses, un proceso formal de revisión de los derechos de acceso de los usuarios.

Este proceso de re - certificación debe asegurar que:

a) Las capacidades de usuarios normales se revisen periódicamente (por lo menos cada seis meses).
b) Los derechos de acceso por parte de usuarios especiales o privilegiados, deben ser revisados con una periodicidad de por lo menos cada tres meses.
c) El proceso de asignación de privilegios sea revisado también de manera periódica de tal manera que asegure que los usuarios cuenten exclusivamente con los niveles de acceso que requieren para desarrollar su trabajo.

✓ **Las restricciones de acceso a la información están basadas en los requerimientos individuales de cada aplicación**

El acceso a los servicios de tecnología de información y de datos debe ser otorgado de acuerdo a las políticas del negocio para acceso a la información y estar basado en los requerimientos individuales de cada aplicación.

La aplicación de los siguientes controles deben ser considerada para soportar los requerimientos de acceso.

a) Proveer menús para controlar el acceso a las funciones del sistema aplicativo.
b) Restringir a los usuarios del conocimiento de datos o funciones del sistema aplicativo que no estén autorizadas a accesar.
c) Controlar las capacidades de acceso de los usuarios.
d) Asegurar que las salidas del sistema aplicativo que manejan datos sensitivos contengan únicamente los datos que son relevantes para el uso de la salida y se envíen exclusivamente a las localidades y/o terminales autorizadas.
e) Incluir revisiones periódicas de las salidas asegurando que se eliminen los datos redundantes.

Certificación de la Información

El proceso de Certificación de un sistema de seguridad, asegura que ninguna de las partes en una conversación entre un programa cliente y un programa servidor podrán ignorar la existencia de una comunicación. La certificación es importante cuando es necesario para cualquiera de las partes demostrar el haber utilizado un mecanismo de comunicación.

Este mecanismo maneja dos situaciones:

a) Permite al emisor de una comunicación demostrar que él, de hecho, emitió un mensaje, que fue recibido por un receptor designado y específico, y por lo tanto, previene que el receptor niegue haber recibido el mismo.

b) Permite al receptor de una comunicación demostrar que él, de hecho, recibió un mensaje que le fue enviado por un emisor designado y específico, y por lo tanto, previene que el emisor niegue haber enviado el mismo.

Las aplicaciones que requieran servicios de Certificación (como lo es el intercambio de información electrónica) serán responsables del rastreo y manejo de los mensajes de actualización de toda la información de negocio. Las aplicaciones individuales pueden ser mejoradas de acuerdo con la necesidad para proveer un mecanismo seguro que prevenga certificación de mensajes ya sea por parte del emisor como del receptor.

La facilidad de certificación está basada en los mecanismos que aseguren la autenticidad de una transacción desde que es generada, enviada, transportada y entregada por una empresa o usuario autorizado.

Los servicios de certificación son diferentes de los servicios de integridad, los Servicios de certificación son críticos para el intercambio de datos en forma electrónica (EDI). La firma digital es el mecanismo principal para implantar los servicios de certificación.

- ✓ **Deben existir servicios de certificación en todo el ciclo de la transacción**

Los puntos en los que se debe contar con servicios de certificación son los siguientes: Requerimiento del servicio, evidencia de la generación, evidencia de la transferencia y almacenamiento de información, evidencia de la verificación, y solución de la disputa.

El mecanismo utilizado para la certificación en las diferentes fases de una transacción comercial, es la firma digital. La firma digital se utiliza como confirmación de recibo de la transacción para las últimas cinco etapas de certificación (Requerimiento del servicio, evidencia de la generación, evidencia de la transferencia y almacenamiento de información, evidencia de la verificación y solución de la disputa). Ésta técnica está basada en la utilización de métodos criptográficos.

Con el objeto de llevar un mejor control en el número de transacciones comerciales que se operen, una buena práctica es la de manejar numeración secuencial de las transacciones por compañía (en caso de trabajar con varias empresas generadoras de transacciones).

Implicaciones: Se deben evaluar los impactos al rendimiento de los equipos (hardware) en la utilización de la firma electrónica.

- ✓ **Las transacciones comerciales que se certifiquen deben contener información de control para la autenticación de la misma**

Información que permita identificar el tipo de transacción comercial que se realizó debe ser contenida en el mensaje que se transmita.

Información de la empresa origen, nombre del usuario origen, número secuencial, fecha en que se originó, hora de proceso que se operó, etc., debe formar parte del contenido regular del mensaje de la transacción comercial que se esté certificando.

- ✓ **Almacenamiento de información de control de certificación**

Durante la fase de origen y entrega de la información, las transacciones deben ser almacenadas en una Base de Datos que conserve tanto la información de control, como los datos de la transacción e información de certificación.

Con el fin de contar con información para dar seguimiento a los problemas que pudieran generarse desde el inicio hasta la entrega de la transacción, se recomienda contar con bases de datos tanto en donde se origina la transacción como en su destino.

Esta información debe estar almacenada y respaldada por un período de tiempo, el cual debe ser acordado con las áreas contables y de auditoría.

- ✓ **Responsabilidad del emisor de la transacción**

El emisor de la transacción debe conocer y asumir la responsabilidad que implica el emitir una transacción y debe almacenar los antecedentes que permitan certificar la información.

Debido a que la persona que genera una transacción tiene una responsabilidad inherente al puesto que está desempeñando, es necesario que esté consciente de la responsabilidad que adquiere en el desempeño de sus funciones.

- ✓ **Responsabilidad del receptor de la transacción**

El receptor de la Transacción debe verificar que el emisor es una compañía y/o usuario autorizado para generar transacciones y validar todos los datos de control de la transacción, en caso de encontrar alguna anomalía debe reportar el incidente al comité de Seguridad, al dueño de la aplicación y al usuario origen de la transacción.

- ✓ **Los servicios de certificación serán manejados por medio de la aplicación**

Las transacciones de aplicaciones que actualicen Bases de Datos externas a la organización, o bien transacciones externas que afecten bases de datos deben incluir interfaces hacia los servicios de Certificación.

Las aplicaciones que realicen transacciones con Bases de Datos externas o internas a la organización tendrán que incluir los servicios de Certificación dentro de su proceso considerando los servicios de certificación en el origen de la transacción, certificación de firmas electrónicas, certificación en la entrega de la información y el grabar la información de control, toda esta información será almacenada en bases de datos tanto en el origen como en el destino de la transacción.

- ✓ **Las normas de operación de transacciones comerciales certificadas deben ser aprobadas y documentadas**

Es requerido un contrato que establezca los compromisos entre las partes involucradas en la transacción comercial operada de manera electrónica.

La sustitución de la firma electrónica por la firma manuscrita como una certificación de que la información es real, es un aspecto que debe ser verificado ante las autoridades legales en nuestro país.

Resumen

Como hemos observado los servicios de seguridad tiene como único objetivo resguardar de la mejor manera nuestra información, uno de los más importantes activos de una organización, de cualquier alteración o mal manejo. Es responsabilidad de cada organización evaluar su entorno y adaptar este tipo de políticas o en su caso generar algunas nuevas a fin de que pueda proteger su información de la mejor manera posible.

Aunado a esto se debe dar seguimiento a las políticas que se establezcan a fin de no entorpecer el funcionamiento y operación del personal, es decir no deben ser un cuello de botella que impida realizar nuestro trabajo diario. También es muy importante que dicha políticas evolucionen a fin de que se adapten a las estrategias del negocio como a las nuevas y poderosas formas de ataque que puede sufrir la información.

Es necesario tener en cuenta siempre que la implantación de cada uno de estos servicios de seguridad implica un costo para la organización, también este costo deberá ser comparado con el riesgo de pérdida anual esperada sobre el activo de información. Esto con el fin de ayudarnos a decidir que servicios de seguridad debemos implantar y cuales otros no tendrán relevancia alguna con nuestra forma de trabajo además de reportarnos más costo que beneficio.

Capítulo V

Plan de Recuperación

Definición

El Plan de Continuidad del Negocio es un proceso que nos permite identificar las funciones críticas de una organización, los cuales fueron identificados previamente a través de la metodología expuesta.

La finalidad de este plan es la de minimizar los efectos que pudieran causar la falla de alguno o de todos los sistemas informáticos con los cuales se proveen los servicios más críticos de nuestra organización a través de la identificación de todos los componentes y recursos humanos que intervienen para darle continuidad a un negocio.

Es necesario enfatizar que la metodología para el análisis del riesgo presentada en este trabajo es parte básica para el desarrollo y aplicación de este tipo de planes dentro de alguna organización, no debemos considerarla como un ente aislado que nos va asegurar la supervivencia de nuestro negocio. En la siguiente gráfica podemos observar en que parte funcional se encuentra el análisis del riesgo para la operación diaria de nuestro negocio.

Las estrategias más comunes que se utilizan como "planes de recuperación" son los respaldos de información, hardware de emergencia, procedimientos que permitan recuperar el o los servicios a un nivel mínimo aceptable.

El plan de recuperación de desastres (Disaster Recovery Planning) es un sinónimo del plan de continuidad del negocio pero el término es producto del centro de datos, este representa la idea de que el plan de recuperación es solo importante a nivel telecomunicaciones y datos. En cambio el Plan de Continuidad del Negocio implica un plan de recuperación de todas aquellas funciones críticas o unidades de negocio de una organización.

En el caso de una institución bancaria, el cual es ejemplo práctico del presente trabajo; supongamos que se daña la Base de datos de las cuentas de cheques de nuestros clientes, obviamente deberemos contar con más de un respaldo de este tipo de información. Así pues nuestra primera actividad será poner en línea el servicio que ofrecemos a este tipo de cuentas, pero quién, cómo, en que condiciones y en cuanto tiempo se realizará, serán algunas de las actividades que deberemos tener bien definidas; y que el plan de continuidad del negocio nos permitirá responder estás y muchas otras preguntas.

Un plan continuidad del negocio es una serie de procedimientos que nos permiten saber que hacer antes, durante y después de un desastre ó una falla en los sistemas informáticos.

El plan continuidad del negocio es generado a partir de la suposición del peor escenario de desastre, esto no implica que no se consideren las emergencias más comunes como sería la falta de energía eléctrica, la "caída" de un servidor ó incluso un incendio.

El plan no debe considerarse como un dictamen, éste debe ser flexible a cualquier evento de emergencia, ya que como es lógico no es posible ni práctico planear para todos y cada uno de los posibles eventos puesto que cada uno tendrá su particularidad.

Así pues se deberá realizar un plan flexible que permita incorporar diferentes condiciones de emergencia según la experiencia que se vaya obteniendo y así ir incorporándolas al plan para *mantenerlo lo más actualizado y realista posible.*

¿Por qué contar con un plan?

Algunos tipos de instituciones como las financieras, las gubernamentales o industriales son reguladas por leyes que les exigen contar con planes continuidad, esto es debido al tipo de servicio que proporcionan.

En el caso de una institución financiera el Banco de México[3] (la organización reguladora) obliga a que sea respaldada la información más crítica de la institución, como las cuentas de los *clientes, sus movimientos, saldos, etc., en caso de que ocurriera un desastre. Además de que* esta información no solo es almacenada en caso de un desastre, también es generada con fines de auditorías ó intervenciones bancarias.

[3] Banco de México.- De la naturaleza, las finalidades y las funciones

ARTICULO 2o.- El Banco de México tendrá por finalidad proveer a la economía del país de moneda nacional. En la consecución de esta finalidad tendrá como objetivo prioritario procurar la estabilidad del poder adquisitivo de dicha moneda. **Serán también finalidades del Banco promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.**

Así pues estas son algunas de las razones por las que debemos contar con plan de recuperación:

- Requerimiento de auditoría financiera
- Pérdida del mercado
- *Responsabilidad fiscal*
- Regulación
- Pérdida y/o distribución de información confidencial de la organización y clientes
- Pérdidas económicas
- Credibilidad y Confianza

En cualquier caso es necesario tener en cuenta que la falta de un plan de recuperación puede resultar más costoso que el propio esfuerzo de generarlo exista o no alguna entidad encargada de regular nuestra organización.

La falta de un plan de recuperación trae como consecuencia desconfianza de nuestros clientes, mala imagen al reflejar falta de interés en nuestro propio negocio y competitividad. La historia nos muestra que entre el 35 y 50 por ciento de las organizaciones que se enfrentan a un desastre sin un plan de recuperación no se recuperan.

La siguiente tabla nos presenta el costo que representa para una organización recuperar 20 MB de información sin un plan[4]:

Ventas	19	$ 20,000
Contabilidad	21	$ 22,000
Ingeniería	42	$114,000

El análisis del riesgo de los sistemas informáticos que componen nuestra organización es producto de la necesidad de minimizar el riesgo de sufrir un desastre a nuestro negocio, también es el punto focal de nuestro plan de recuperación antes tales riesgos ya que este nos indicará cuales son las áreas más críticas de nuestra organización y a las que por lo tanto debemos dedicar el mayor esfuerzo para su pronta recuperación en caso de ocurrir algún evento no deseado.

La metodología que se desarrolla en el presente trabajo no puede ser aplicada sin contar con todos sus elementos con el fin de resultar práctica para cualquier organización, como tampoco puede ser soportada sin una apropiada cultura de seguridad además de su continuidad y actualización.

Planeación

Debido a que este esfuerzo debe considerarse prioridad de la organización es necesario realizar un plan que nos permita ir visualizando los avances e identificando las actividades a las que debemos dedicarle más tiempo y esfuerzo.

[4] Fuente: **Business Recovery Manager Association** de acuerdo a la inflación de 1995 en Estados Unidos. Costo representado en dólares

Los siguientes pasos que se presentan nos conducirán a un plan efectivo[5]:

1. Identificar al coordinador del plan
2. Obtención de recursos y apoyo administrativo
3. Definir el alcance del plan
4. Conducir la identificación del riesgo
5. Análisis del impacto al negocio
6. Desarrollo de estrategias de recuperación
7. Definir el equipo de recuperación
8. Desarrollo de instrucciones y procedimientos para el equipo de recuperación
9. Recolectar información fuente
10. Capacitación y entrenamiento del equipo de recuperación
11. Ejecutar el plan
12. Mantenimiento del plan

Estos pasos establecen los requerimientos para desarrollar el plan de recuperación en caso de desastre y revisiones para asegurar la recuperación en tiempo de los procesos vitales del negocio en caso de contingencia.

Se aplica a todas las unidades operativas y soporte corporativo. Los requerimientos legales especificados en contratos o con el gobierno se deben respetar y pueden suplir algunos requerimientos estándar.

Este estándar identifica los componentes del plan de recuperación en caso de desastre, las revisiones y pruebas necesarias para asegurar la preparación de la recuperación de los procesos vitales del negocio después de un desastre.

1. **Identificar al coordinador del plan**

Su función es asegurar que los servicios normales sean restaurados dentro de los tiempos previstos

Responsabilidades de planeación previas al desastre:

- Tomar decisiones sobre la estrategia total y sobre la recuperación, después de conciliar el punto de vista del usuario y de la alta gerencia.
- Revisar los reportes de proyectos, propuestas y planes para los otros equipos como se van produciendo
- Asegurar que este plan se mantiene al día

Funciones durante el desastre:

- Declarar que el plan de recuperación del negocio será implantado
- Listar la disponibilidad de todos los empleados de la empresa
- Decidir sobre los líderes de equipo y miembros alternos en caso necesario
- Proporcionar una copia de todo el material en el puesto de mando
- Instruir a los líderes de programas y aplicaciones a:
- Conseguir el sistema crítico corriendo desde la localidad alterna
- Imprimir los documentos vitales restantes necesarios para la restauración si no están disponibles de otra forma.
- Decidir sobre la ubicación del puesto de mando

[5] Datos obtenidos por el Instituto de Recuperación de Desastres (Disaster Recovery Institute DRI) como estándares para la definición de una plan de recuperación del negocio

- Conseguir la decisión de la localidad del centro de cómputo restablecido de la alta gerencia
- Administrar la implantación del plan restauración desde el puesto de mando
- Revisar reportes de la función del equipo de control de proyecto sobre el estado de los planes.
- Dar guía a los líderes de otros equipos
- Mantener a la alta gerencia y a las relaciones externas al tanto

2. Obtención de recursos y apoyo administrativo

Ningún esfuerzo o proyecto serán exitosos si no se cuenta con un apoyo pleno y comprometido de los directivos de las organizaciones, sin él no se contará con el compromiso total del personal involucrado por lo tanto la prioridad que se le tome al proyecto se verá directamente reflejada en el éxito o fracaso del mismo.

Es necesario realizar una presentación del proyecto a los involucrados a fin de que estos conozcan no solo la importancia de este sino también su alcance a fin de que el objetivo sea común a toda la organización. Además deberá presentarse la prioridad que tendrá cada aplicación involucrada lo que entre otras cosas definirá el grado de interés extra al que tendrán que comprometerse los responsables de cada sistema de información (aplicativo).

3. Definir el alcance del proyecto y su planeación

Esta fase de la continuidad del negocio es difícil de iniciar ya que esta será la guía de las actividades que se deberán realizar para preparar un plan de contingencia o recuperación del negocio.

La decisión de cómo iniciar un plan depende de:

- La necesidad
- El grado del riesgo al que nos estemos enfrentado.

Esta decisión deberá estar de acuerdo con un comité que deberá estar conformado por personal con excelente conocimiento acerca del negocio y acerca del área a la cual representa dentro de la organización además de poder tomar decisiones que se respeten. Este comité deberá reunirse periódicamente con el fin de discutir los siguientes temas:

- Impacto al negocio
- Funciones críticas
- Estrategias de recuperación
- Descripción del proyecto
- Como alguna función opera en condiciones normales, cómo es entregado y cuáles son sus productos
- Identificar interdependencias
- Recursos Humanos
- Redes
- Aspectos Legales
- Facilidades
- Finanzas

- Telecomunicaciones
- Seguridad y Riesgos

En estas reuniones se deberá tener presentes los temas a tratar con el fin de no invertir tiempo a temas que se discutirán posteriormente y que harán desviarnos de nuestro objetivo, *adicionalmente todos los involucrados deberán conocer previamente la agenda con el fin de que* asistan preparados para los temas que se van a tratar.

4. Conducir la Identificación del Riesgo

En esta etapa es donde hace su presentación la metodología antes descrita, esto nos da una idea de la importancia de esta dentro del proyecto de un plan de continuidad del negocio en caso de un desastre.

5. Análisis del impacto al negocio

En esta etapa se presentan los resultados del análisis del riesgo enfatizando las áreas críticas del negocio, su importancia y las recomendaciones con un análisis de costo beneficio no tan detallado pero que si muestre una idea general del costo de estas para la organización.

6. Desarrollo de estrategias de recuperación

El punto focal de un plan de continuidad es la selección de las estrategias de recuperación que nos permitan realizar de la mejor manera posible la recuperación de nuestras funciones críticas.

Estas estrategias deben ser analizadas a fin de que reporten a la organización el mayor beneficio a un costo menor para la organización. Debido a la inherente dificultad, en algunos casos es virtualmente imposible, de cuantificar los riesgos financieros a que está expuesto en caso de un desastre el centro de cómputo, un análisis de las siguientes opciones deberá proveer la solución más lógica para el negocio, la cual deberá incluir costos estimados, beneficios cuantificables y estar de acuerdo con las metas estratégicas de la corporación.

En algunos planes estas pueden consistir en:

ACUERDO RECIPROCO

Es un acuerdo entre la organización y otra empresa local, donde cada compañía se compromete a compartir los recursos de su centro de computo en caso de ocurrir un desastre.

Ventajas:

- Bajo costo
- Disponibilidad inmediata de equipo si la otra compañía tiene capacidad excedente.
- Efectivo para requerimientos en un período corto de tiempo
- Localización cercana con un mínimo gasto de transporte, alimentación y hospedaje.

Desventajas:

- Socios dentro del acuerdo pueden sufrir los efectos de un mismo desastre
- Equipo adicional y tiempo de cómputo requeridos para acomodar al socio

- El hardware y software de cada empresa puede no ser compatible o tener problemas de duplicidad
- Dificultad en la obtención de tiempo para pruebas
- No es una solución a largo plazo
- Dificultad para obtener un compromiso contractual del socio

RECONSTRUCCION EN UN LOCAL ALTERNO

Se asume que un desastre ha destruido totalmente alguno de los sitios que contienen equipo de cómputo. El plan de contingencia direcciona a la reconstrucción de un nuevo local.

Ventajas:

- Disponibilidad a largo plazo
- Un solo propietario

Desventajas:

- Gastos en la reconstrucción y configuración
- Tiempo perdido en la reconstrucción
- Instalación de equipo necesitado durante esta fase
- Dificultad para probar esta opción excepto si se simula el desastre

ACUERDO CORPORATIVO

Esta es una extensión de la primera opción de acuerdo recíproco. Es un acuerdo entre varios miembros de la corporación que establecen compartir recursos de proceso de datos disponibles con la compañía que sufra algún tipo de desastre.

Ventajas:

- Costos compartidos
- La unión de los miembros disminuye los costos de contratar con una firma que proporcione servicios de respaldo total
- Puede ser efectivo para problemas resueltos a corto plazo
- Disponibilidad en base al contrato

Desventajas:

- Los miembros pueden sufrir de los efectos del mismo desastre
- Puede ser difícil mantener la compatibilidad de hardware y software para todos los centros de cómputo
- Dificultad en la obtención de recursos y tiempo para pruebas
- Los miembros en acuerdo pueden estar localizados geográficamente en una amplia zona por lo que los costos en transporte pueden incrementarse

CENTRO DE COMPUTO ALTERNO PROPIO

Esta opción es básicamente un centro de cómputo alterno propiedad de la compañía en la que se cuente con una configuración que soporte los procesos vitales para continuar la operación de la empresa.

Ventajas:

- Permanencia por un largo período de tiempo
- Un solo propietario

- Disponibilidad inmediata
- Facilidad para pruebas

Desventajas:

- Más costosa que otras opciones
- *Inversión adicional en equipo de cómputo*
- Retorno de inversión a mediano plazo
- Algunos costos de transportación

CENTRO DE RECUPERACION COMERCIAL (HOT SITE)

Esta opción consiste de una compañía externa con disponibilidad casi inmediata de procesamiento de datos, para que en un período temporal (uno o dos meses) pueda ser ocupado por la compañía para realizar su plan de recuperación mientras se reconstruye su propio local. El centro de cómputo esta disponible en lo que respecta a la configuración de hardware. La compañía en desastre debe proporcionar todos los recursos de software y humanos para poder *procesar sus aplicaciones.*

Ventajas:

- Disponibilidad inmediata
- Permanencia a mediano plazo
- *Costos compartidos*
- Tiempo de prueba disponible como parte del contrato de servicio

Desventajas:

- Disponible al límite de clientes que pueda soportar el centro de recuperación *comercial*
- Costos altos para cargos por tiempo de uso excedente
- Cargos adicionales por respaldo en línea
- La compatibilidad de hardware y software debe ser mantenida por medio de revisiones continuas.
- *Gastos en transporte, alimentos y hospedaje.*

7. Definir el equipo de recuperación

El personal que integre el equipo de recuperación debe:

a) Estar familiarizado con la organización.
b) Contar con experiencia en proceso de recuperar
c) Ser fácil de localizar en caso de emergencia
d) Tener conciencia de la importancia de la recuperación

Cada equipo tiene objetivos específicos junto con un plan a cumplir. La suma de los planes individuales de los equipos constituye el plan de recuperación del negocio total; el equipo administrador especifica las relaciones de trabajo de todos los equipos. Los equipos usualmente no trabajan bajo circunstancias de "desastre". Aunque los equipos de recuperación en caso de desastre deben ser activados inmediatamente cuando un desastre ha sido declarado.

Cada equipo tiene una misión específica tan pronto como un desastre ha sido declarado; esta misión tiene precedencia sobre todo otro trabajo hasta que el desastre ha sido declarado como "finalizado". La estructura de comunicación entre los equipos debe ser establecida anticipadamente. Cada líder de equipo y todo los otros miembros que normalmente trabajan en

proceso de datos o en área de usuarios se convierten en miembros de tiempo completo del equipo.

La responsabilidad de cada líder de equipo deberán ser:

- Leer la documentación del plan de recuperación en caso de desastre con atención especial a las secciones relativas a su área.
- Asegurar que el material para el cual el líder del equipo es responsable, es confiable actual y cumple con los estándares del plan.
- Asegurar que las "áreas grises" de responsabilidad dejen de existir. Por ejemplo, decidir que equipo es responsable de la comunicación del sistema central con los sistemas personales y que equipo es responsable de los modems provistos por el vendedor de hardware.

8. Desarrollo de instrucciones y procedimientos para el equipo de recuperación

Esta debe ser una práctica común para el equipo de recuperación, es decir, se deben contar con procedimientos e instrucciones de trabajo en condiciones normales a fin de que prácticamente cualquier persona pueda desempeñar el trabajo de otra.

Estas instrucciones y procedimientos deberán ser lo suficientemente claras para cualquiera y lo suficientemente específicas para no dejar la puerta abierta a dudas sobre su ejecución. Además de permitirnos recuperar nuestro ambiente operativo estas nos permiten ahorrar tiempo en su ejecución.

9. Recolectar información fuente

Esta recolección dependerá del tipo de información de la que estemos tratando, no debemos gastar tiempo en recuperar información que no le sea vital al negocio, es decir que podamos no contar con ella.

Esta información fuente nos permitirá recuperar el ambiente a condiciones normales de procesamiento a fin de que no afectemos los compromisos y obligaciones que tiene comprometidos la empresa.

10. Capacitación y entrenamiento del equipo de recuperación

El objetivo de la capacitación y el entrenamiento del personal de recuperación es convertir la recuperación del negocio de un concepto planeado a una realidad. En esta etapa se debe buscar:

- Identificar resultados esperados
- Determinar tiempos límite por cada tarea

Básicamente el entrenamiento o pruebas que se realicen deberán seguir la siguiente estructura:

Definir Tareas y Responsables

- Notificación de la prueba
- Restaurar software
- Activar proceso
- Recuperar aplicaciones y datos

- Verificar resultados
- Eliminación de datos al final
- Revisión de resultados

Ejecución de la Prueba

- Verificar que el software es operativo en el equipo y proceso temporal
- Comprobar que los registros vitales están actualizados y accesibles
- Validar que el personal tiene la capacidad requerida
- Determinar si la gerencia asignada es capaz de manejar situaciones imprevistas

Elementos Clave

- La involucración del usuario es indispensable ya que este dará visto bueno de la prueba
- Los usuarios pueden realizar su prueba sin proceso de datos
- El plan de recuperación debe ser un proceso normal
- Es válido realizar pruebas desde su desarrollo
- Es necesario probar la integridad de los registros vitales
- Dar soporte a las modificaciones del plan

Revisión de Resultados

- Reunión de Participantes
- Documentar problemas y sugerencias
- Generar planes de acción
- Dar seguimiento a los planes de acción
- Modificar documentación
- Anexar documentación del resultado al plan

11. Ejecutar el plan

La ejecución de un plan de recuperación tiene como finalidad el:

- Reducir el impacto de una contingencia
- Protección de los activos de la empresa
- Soportar la continuidad del negocio
- Restaurar los servicios

Fases de la emergencia

Respuesta
Restauración

Alta Gerencia

Asegurar la existencia del plan de emergencia
Designar un coordinador de seguridad por localidad
Asegurar que existe forma de continuar el negocio

Coordinador de seguridad

Validar que el plan de emergencia cubra los requerimientos
Asegurar que el plan sea actual

Area de Informática

Verificar que las necesidades de proceso se cubran
Asegurar que los procesos de restauración sean actuales

Administración

Coordinadores nivel división y localidad
Asesores de áreas involucradas
Sucesión gerencial para continuidad del negocio
Personal entrenado en emergencias
Personal para controlar la emergencia
Procedimiento de emergencia para cubrir servicios

Personal

Información del centro de control
Personal en el centro de control
Notificación del estado de emergencia
Procedimiento de evacuación
Designación de áreas para refugio
Reserva para emergencia y gastos de operación
Disponibilidad inmediata de una lista de personal
Responsable para localizar a los empleados

Servicios de emergencia

Servicios vitales
Sistema de alerta en caso de emergencias
Equipos de rescate
Unidades de control de daños
Equipo de emergencias
Transportación de emergencias
Facilidades de comunicación
Personal médico
Números telefónicos de emergencia

Continuidad de operaciones

Documentación actualizada
Restauración de información
Reanudación de operaciones

Restauración de servicios

Personal con responsabilidades asignadas
Restaurar en tiempo mínimo en base a recursos

Notificación

Avisar a accionistas, personal de la empresa, clientes, proveedores
Notificar a otras localidades con las que se tenga relación
Contacto centralizado con otras autoridades

12. Mantenimiento del plan

El mantenimiento del plan se dará de acuerdo a las pruebas realizadas y a las experiencia vividas de la organización, esta etapa es vital para el negocio ya que de este dependerá la capacidad de reacción que se pueda lograr en caso de ocurrir algún evento no deseado.

Este mantenimiento deberá estar a cargo de un comité de contingencia y respaldado con el compromiso de todos los involucrados a fin de mantenerlo lo más actualizado y realista posible.

Capítulo VI

Metodología Para el Análisis del Riesgo en Sistemas de Información

Primer Paso

Realizar un análisis general de los riesgos a los que se encuentra expuesta la organización a fin de identificarlos, haciendo uso de visitas guiadas a todas las áreas de la organización. Otra de las herramientas que ayudan a identificar el riesgo es la aplicación de entrevistas a los ejecutivos más importantes de la organización, a nivel subdirección a fin de obtener resultados más realistas.

Segundo Paso

Identificar los tipos de riesgos que se observaron, es decir, en cuál de los siguientes rubros puede encontrase:

- Operacionales
- Legales
- *Financieros*
- Políticos / Sociales
- Naturales

Tercer Paso

Calcular la probabilidad de ocurrencia de dichos riesgos, a través del uso de bitácoras, documentos históricos o estudios realizados por instituciones especializadas

Cuarto Paso

Realizar la medición de dicho riesgo, es decir determinar el posible costo que implicaría a la organización el que se llegará a enfrentar a dicho riesgo o amenaza de acuerdo a la probabilidad de ocurrencia.

Quinto Paso

Priorizar los riesgos, es decir a que riesgos se le va a dar mayor importancia de acuerdo a la afectación que pudiera ocasionarle a la organización. Una de las herramientas para facilitar esta actividad es el uso de matrices de decisión en las cuales se contrapongan el tipo de riesgo vs las pérdidas o consecuencias.

Sexto Paso

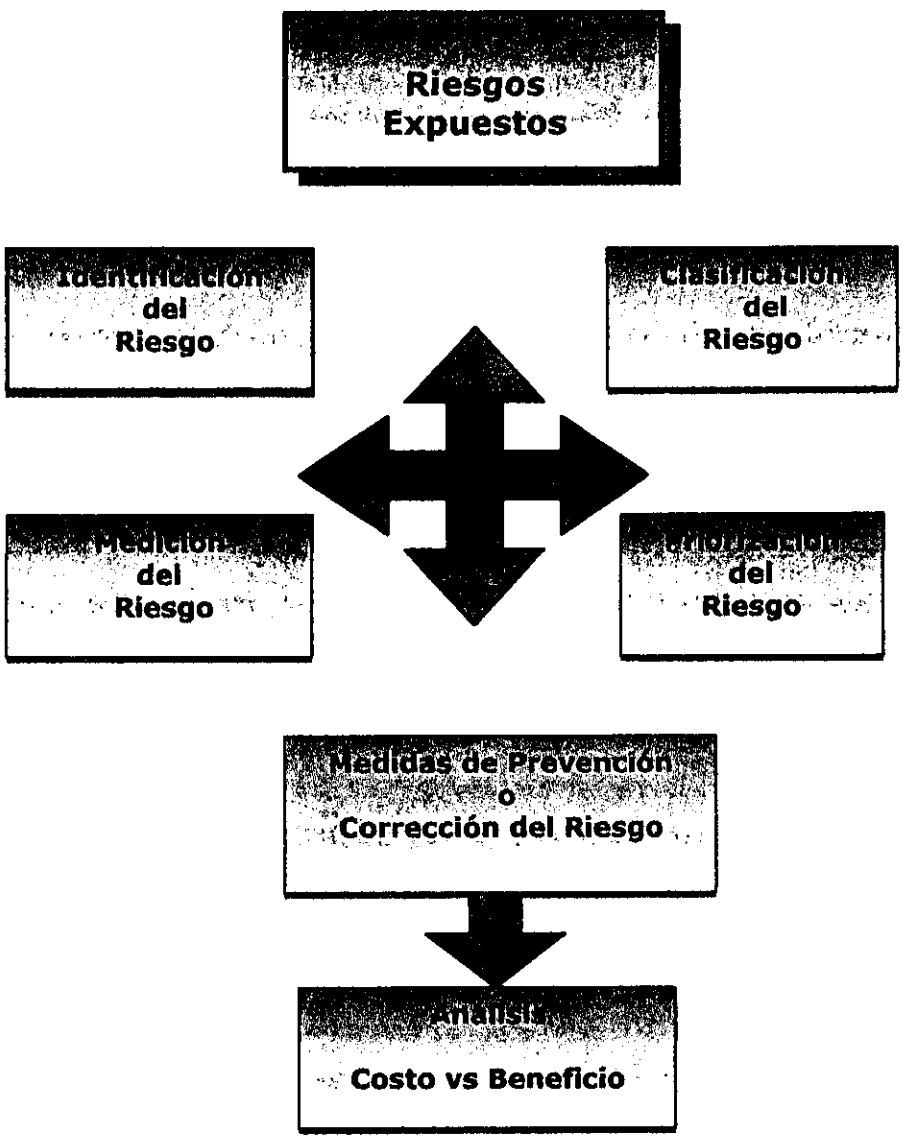
Una vez priorizado los riesgos la siguiente etapa es desarrollar medidas de prevención o corrección de los mismos, estas medidas pueden caer entre los dos siguientes rubros: medidas lógicas o medidas físicas.

Quinto Paso

Una vez definidas las medidas apropiadas de prevención o corrección del riesgo se deberá realizar un análisis de costo - beneficio de cada una de ellas a fin de que ayude a tomar una mejor decisión respecto a cual se implantará y cuales riesgos se asumirán por si mismos debido a su relación costo - beneficio.

Sexto Paso

Finalmente con toda esta información se hará entrega de un reporte lo suficientemente práctico para que las condiciones se generen para tomar las decisiones adecuadas a fin de reducir los riesgos a los que se encuentra expuesta la organización en análisis.



A continuación se presenta un prototipo de la entrevista que deberá hacerse a los especialistas de cada uno de los sistemas de información que deseemos analizar para identificar sus riesgos, esta entrevista/cuestionario es muy flexible con el fin de poderse a adaptar a cualquier tipo de negocio que maneje sistemas de información que desee emprender esta identificación del riesgo.

ENTREVISTA/CUESTIONARIO

ANALISIS DE IMPACTO

SECCION I INFORMACION GENERAL

FECHA	
DIRECCION	
DIRECTOR	
AREA	
RESPONSABLE	
EXTENSION	
NUMERO DE PERSONAL A SU CARGO	

DESCRIPCION DE FUNCIONES

A continuación describa las funciones de los procesos que contribuyen a la operación y actividades del área en términos de los negocios del **Grupo Financiero.**

1. *Liste las funciones de negocio que efectúa su área*
2. Complete la sección II y III para cada función
3. Si esta disponible, anexe una copia del organigrama de su área y un diagrama funcional

1.-
2.-
3.-
4.-
5.-
6.-
7.-
8.-
9.-
10.-

Sección II INFORMACION DE LAS FUNCIONES DEL AREA DE NEGOCIO
(Por favor complete la sección II y III para cada función critica del área)

DESCRIPCION DE FUNCIONES

Nombre de la Función	
Localización de la Función	
Descripción	
Ventana de Servicio	
Frecuencia de la Operación	☐ Anual ☐ semestral ☐ mensual ☐ semanal ☐ diaria ☐ eventual

Picos de Operación	☐ Anual ☐ semestral ☐ mensual ☐ semanal ☐ diaria ☐ eventual
Describe los Picos de la Operación.	
Número de personas que participan	
Quienes son los clientes internos de esta función	
Quienes son los clientes externos de esta función	

DEPENDENCIAS DE NEGOCIO

Considera las entradas y las salidas necesarias para el adecuado funcionamiento del área. Que área o secciones del área o cuales son los recursos de los cuales dependes para completar la función o productos bajo tu responsabilidad.

Entradas

Liste en la siguiente tabla los recursos internos o externos de entrada de los cuales depende para completar la función o productos del área en cuestión

SI ES UNA AREA INTERNA, MARCAR CON UNA "X"	DE QUE AREA O PROVEEDOR RECIBES LA INFORMACION	DESCRIBE LOS DATOS O INFORMACION RECIBIDA	INDICA EN QUE MEDIO (FAX, TELEFONO, MODEM, ELECTRONICO)	FRECUENCIA (DIARIO,SEMA-NAL, MENSUAL, ETC.)

Salidas

Lista en la siguiente tabla los recursos internos o externos de salida de los cuales depende para completar la función o productos del área en cuestión

SI ES UNA AREA INTERNA, MARCAR CON UNA "X"	A QUE AREA O CLIENTE ENVIAS LA INFORMA-CION	DESCRIBE LOS DATOS O INFORMACION ENVIADA	INDICA EN QUE MEDIO (FAX, TELEFONO, MODEM, ELECTRONICO)	FRECUENCIA (DIARIO,SEMA-NAL, MENSUAL, ETC.)

Obligaciones o disposiciones Legales

Identifique y describa las implicaciones legales, contractuales, de normatividad o regulación interna o externa, así como las obligaciones que tiene que cubrir para el cumplimiento de la función o producto en cuestión, como son reportes, políticas, obligaciones, plazos o fechas, etc.)

Legales	
Contractuales	
Normatividad	
Políticas	
Otras	

INFORMACION DE SOFTWARE APLICATIVO

Lista en orden de prioridad el software aplicativo utilizado para llevar a cabo la función en cuestión. Estimando el tiempo de recuperación requerido para cada aplicación descrita en la columna derecha considerando el peor escenario de contingencia

Nombre de la aplicación	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
1.-							
Explique cual es el uso que le da a la aplicación: **En que plataforma de cómputo reside la aplicación (PC,AS/400,Mainframe,NT,UNIX, etc.)?**							
Nombre de la aplicación	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
2.-							
Explique cual es el uso que le da a la aplicación: **En que plataforma de cómputo reside la aplicación (PC,AS/400,Mainframe,NT,UNIX, etc.)?**							
Nombre de la aplicación	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
3.-							
Explique cual es el uso que le da a la aplicación: **En que plataforma de cómputo reside la aplicación (PC,AS/400,Mainframe,NT,UNIX, etc.)?**							
Nombre de la aplicación	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
4*.-							
Explique cual es el uso que le da a la aplicación: **En que plataforma de cómputo reside la aplicación (PC,AS/400,Mainframe,NT,UNIX, etc.)?** * Consecutivamente, por cada una de las aplicaciones involucradas							

FUNCIONES MANUALES

Que procesos manuales podrían funcionar hasta que sean recuperadas y restablecidas las funciones automatizadas en caso de que sea interrumpido el negocio por cualquier causa?

1.- Puede recuperar las transacciones perdidas durante el evento de la contingencia o crisis?
2.- Si la respuesta es si como las recuperaría y en que tiempo?
3.- Si la respuesta fue negativa indique cuáles son los impactos potenciales que se provocarían?
4.- Describa las transacciones perdidas para esta función
5.-Que recursos necesitaría para operar manualmente, si los sistemas no están disponibles (ejemplo: fax, teléfono, manuales, formatos, papelería, etc.)
6.- ¿Cuánto tiempo podría continuar con la operación manual mientras es restaurada la operación automatizada? (Considere el monto y número de transacciones acumuladas)
7.- Explique, ¿Cuál sería la pérdida de datos o de información de mayor impacto en el peor escenario, ubicando el período o frecuencia más desfavorable? (hora, día, mes, semana, etc.)

CAPACIDAD ALTERNA

1.- ¿Puede accesar actualmente a las aplicaciones remotamente desde otra localidad?
2.- ¿Actualmente cuenta con suficiente capacidad de proceso remoto?
3.- Especifique, ¿Qué herramientas requiere o podría requerir para llevar acabo un proceso remoto?

NIVEL DE CRITICIDAD

El Tiempo Objetivo de Recuperación (RTO) es definido como el máximo lapso de tiempo en que la función de negocio, bajo su responsabilidad, se puede sostener como interrumpida por un tiempo definido de crisis en lo que son restauradas las aplicaciones que permiten la automatización con la que es soportada su función.

En su opinión, ¿Cuál es el RTO para su función?, por favor identifique una de las siguientes opciones:

≤ 3 hrs.___ ≤ 12 hrs.___ ≤ 48 hrs.___ ≤ 3 días ___ ≤ 5 días___ ≤ 10 días ___ ≥ 10 días___

Prioritice los siguientes factores críticos que contribuyen al RTO marcado anteriormente donde: 1 es el más importante y 8 el menos importante

PRIORIDAD	FACTOR CRITICO
	Seguridad y salud (de empleados, clientes, terceros, etc.)
	Ventaja Competitiva (pérdida de: clientes, accionistas, proveedores, etc.)
	Servicio al Cliente (servicio no disponible al cliente, etc.)
	Pérdidas Financieras (Por: pago de intereses, cargos, multas, pérdida de ventas, etc.)
	Incumplimiento a disposiciones legales y de Normatividad (impactos significativos por incumplimiento a contratos, leyes, políticas y disposiciones gubernamentales, etc.)
	Interdependencias (Información procesada entre áreas de proceso o de negocio)
	Moral o motivación de los empleados
	Control Administrativo o Decisiones de capacidad de operación o margen de maniobra disponible
	Otro (especifique)

Sección III ANALISIS DE FUNCIONES

IMPACTO OPERACIONAL

A través de los impactos a la operación identificamos los requerimientos de recuperación del negocio, considerando la evaluación de las pérdidas producidas por la falta de disponibilidad de la función.

La siguiente tabla servirá con el fin de identificar sus impactos de operación más severos dentro de las categorías señaladas en el cuadro siguiente con una escala del 0 al 3 por cada periodo de tiempo.

Los valores a utilizar son:
0= ningún Impacto,
1= impacto mínimo,
2= impacto mediano,
3= impacto muy significativo o severo

Considerando la priorización de los factores críticos señalados en la pagina anterior.

FUNCION:

	EFECTO ACUMULADO DESPUES DE CADA PERIODO DE TIEMPO						
Categoría de Impactos	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
1.-Seguridad y salud (Impactos a la salud y seguridad de empleados, clientes y terceros)							
2.-Ventaja Competitiva (pérdida de: clientes, accionistas, proveedores, que puede sufrir sino esta disponible la función)							
3.-Servicio al Cliente (no puede proveer un nivel de servicio aceptable al cliente)							
4.-Pérdidas Financieras (que puede sufrir México con impactos significativos por pago de intereses, cargos, multas, pérdida de ventas, etc.)							

5.-Incumplimiento a disposiciones legales y de Normatividad (impactos significativos por incumplimiento a contratos, leyes, políticas y disposiciones gubernamentales, etc.)							
6.- Interdependencias (Las dependencias operativas entre áreas pueden ser significativas y provocar perdidas por la falta de disponibilidad de esta función)							
7.- Moral o motivación de los empleados (afectación de la moral o motivación de los empleados por la indisponibilidad de la función)							
8.- Control Administrativo o Decisiones de capacidad de operación o margen de maniobra disponible (La falta de esta función podría afectar a la toma de decisiones estratégicas y afectar al control administrativo del negocio)							
9.- Otro (especifique) _____ _____							

IMPACTO FINANCIERO

Estima los impactos financieros de mayor impacto provocados por la falta de disponibilidad de esta función y detállalos en el renglón correspondiente

A.- Administración de Dinero	
Señala el impacto que aplica:	Flujo de Efectivo Movimiento de dinero Demora de Facturación Administración Financiera Otros:
Describe el impacto:	
B.- Ingresos/Utilidades	
Señala el impacto que aplica:	Nuevo Servicio Cobro de Servicios Intereses Devengados Amortizaciones Otros:
Describe el impacto:	
C.- Demoras o Duplicación de Procesos	
Señala el impacto que aplica:	Procesos demorados Procesos Duplicados Retraso en plazos Otros:

Describe el impacto:	
D.- Legales/ Contractuales / Normatividad o Disposiciones Gubernamentales	
Señala el impacto que aplica:	**Sanciones** **Multas** **Reclamaciones** **Juicios** **Incumplimientos Contractuales** **Otros:**
Describe el impacto:	
E.- Gastos Adicionales	
Señala el impacto que aplica:	**Mano de Obra Adicional** **Horas Extras** **Empleos Temporales** **Contrataciones** **Otros:**
Describe el impacto:	

Estima los impactos financieros por la indisponibilidad de la función de acuerdo a los siguientes rangos:

NÚM.	RANGO
0	$ 0
1	<$50,000
2	$50,000 < $250,000
3	$250,000 < $1,000,000
4	$1,000,000 < $5,000,000
5	$5,000,000 < $10,000,000
6	$10,000,000 < $20,000,000
7	$20,000,000 < $50,000,000
8	$50,000,00 < $_____(INDICAR EL MAXIMO ESTIMADO)

Considerando la tabla anterior completa la siguiente matriz para la función en cuestión, insertando el número que refleja el impacto financiero acumulado dentro del período de tiempo en que se presenta el impacto financiero.

FUNCION:

	EFECTO ACUMULADO DESPUES DE CADA PERIODO DE TIEMPO						
Categoría de Impactos	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días
A.- Administración de Dinero							
B.- Ingresos/Utilidades							
C.- Demoras / Procesos Duplicados							
D.- Legales/ Contractuales / Normatividad o Disposiciones Gubernamentales							
E.- Gastos Adicionales							

REQUERIMIENTOS DE RECUPERACION

FUNCION:

Estima el mínimo de recursos requeridos para la función por periodos de tiempo								
Recursos	≤ 12 Hrs.	≤ 24 Hrs.	≤ 48 Hrs.	≤ 3 días	≤ 5 días	≤10 días	≥10 días	actual
Gente								
Escritorios								
Teléfonos								
PC's en Red								
PC's en stand alone								
Impresoras lasser								
Impresoras de Impacto								
Módems								
Fotocopiadoras								
Gabinetes								
Otros: (especifique)								

ARCHIVOS O INFORMACION VITAL

Los archivos o información vital puede estar en papel o medios magnéticos o formatos y es indispensable para el desempeño de la función en cuestión. Por favor identifica y lista toda la información vital en papel para esta función:

FUNCION:

Nombre de o los registros Vitales	Lugar de resguardo o almacenamiento

Recuperación de voz y datos

FUNCION:

¿*Cuantas líneas telefónicas son requeridas para* mantener la función?	
Especifica, ¿Qué dispositivos especiales de telefonía o comunicaciones se requieren para esta función (Correo de Voz, IVR,ACD, etc.)?	
Indique ¿Cuáles números telefónicos de servicio a clientes requiere tener respaldados?	
¿Cuantos entradas o usuarios de e-mail ó requiere?	
¿Cuantas líneas de entrada para fax se requieren?	
¿Cuantos usuarios de Internet requiere?	
¿Cuantas líneas con módem requiere?	

COMENTARIOS U OBSERVACIONES

Comentarios o Consideraciones adicionales de esta función

Nota: Por favor regrese revisar el RTO (Tiempo objetivo de Recuperación) y considerando la información que nos proporciono, reconsidere y efectué los cambios y ajustes necesarios al RTO indicado.

Nombre y Firma

Vo.Bo. Del Director Ext.:

RESULTADOS

A continuación se presentan los resultados obtenidos al aplicar esta entrevista/cuestionario a algunas áreas aplicativas de un Grupo Financiero y que nos ayudarán a resaltar la importancia de su aplicación y los resultados obtenidos para la presente metodología. Adicionalmente se presentará el reporte del análisis realizado sobre todo el entorno en que se encuentran las instalaciones centrales del Grupo Financiero.

NOTA: Debido a la condición de confidencialidad de esta información solo se hará la presentación de los resultados en una forma general y con datos y nombres ficticios.

APLICACIÓN O SERVICIO	OBJETIVO(S)
CHEQUES	▪ Procesar los cheques nacionales e internacionales ▪ Actualizar cuentas de cheques ▪ Manejo de Remesas
SISTEMA INTEGRAL EMPRESARIAL	▪ Promoción del servicio a los clientes (nacional e internacional) ▪ Proporcionar servicios bancarios en forma remota
TRANSFERENCIA DE FONDOS	▪ Transferencia de fondos nacional (SYCOF) ▪ Transferencia de fondos internacional (SWIFT) ▪ Control de talonarios de cheques
OPERACIONES DE MERCADO DE DINERO / CAPITALES	Mercado de dinero: ▪ Manejar las compras y ventas en el mercado de valores ▪ Monitorear las inversiones de los bancos diariamente ▪ Vigilar los vencimientos de los certificados de depósito ▪ Realizar inversiones Mercado de Capitales ▪ Efectuar la planeación del negocio ▪ Actuar como corredores de bolsa
PLAN DE INVERSIONES	▪ Contabilizar las inversiones de 1 día a 2 años ▪ Monitorear el sistema de cheques para asegurar la correcta aplicación de los movimientos ▪ Verificar los productos obtenidos del sistema batch ▪ Conciliar los resultados del sistema con la contabilidad general ▪ Soportar a las sucursales durante emergencias
COBRANZAS DE TERCEROS	▪ Efectuar las cobranzas por medio de terceros
PAGO DE SERVICIOS	▪ Manejar en forma automática los pagos de servicios, pago de impuestos
CARTERA	▪ Monitorear y controlar contablemente el crédito de todos los clientes comerciales del Banco
RIESGOS Y RESPONSABILIDADES	▪ Verificar los estados de cuenta y otra información para toma de decisiones ▪ Enviar información al Banco de México
CARTERA VENCIDA	▪ Manejar las cuentas morosas

CENTRO DE PROCESAMIENTO DE DATOS. SOPORTE TECNICO Y OPERACIONES	▪ Proporcionar servicios de cómputo ▪ Evaluar y efectuar los cambios a los sistemas ▪ Programar la ejecución de los procesos batch ▪ Proporcionar el servicio de User Help Desk ▪ Manejo de Problemas de Producción ▪ Soporte Técnico

APLICACIÓN O SERVICIO	OBJETIVO(S)
PLANEACION DE LA CAPACIDAD	▪ Planeación de la Capacidad para pronosticar recursos de cómputo necesarios para proveer los servicios acordados en los niveles de servicio
INSTALACION Y CONFIGURACION DE HARDWARE	▪ Reconfiguración y mantenimiento de hardware ▪ Planeación física para la instalación de equipo nuevo
PERFORMANCE	▪ Monitoreo del comportamiento del servicio línea y batch

LISTA DE APLICACIONES Y TIEMPOS DE RECUPERACION

APLICACION	TIEMPO RECUPERACION	PRIORIDAD	ENTIDAD NO.	PERIODOS CRITICOS
BCH BCR BCT	24 HRS	1	01	MARZO, JUNIO, NOVIEMBRE Y DICIEMBRE DIAS:15, 29, 30 Y 31 LUNES Y VIERNES
CICSCHQ BCQ BQH	24 HRS	1	02	NOVIEMBRE Y DICIEMBRE. DIAS: 1, DEL 12 AL 16 Y DEL 28 AL 31 LUNES, JUEVES Y VIERNES HORA: 09:00 A 14:00
SWIFT SYCOF	2 HRS (RED)	2	03	MARZO, OCTUBRE, NOVIEMBRE Y DICIEMBRE DIAS: DEL 13 AL 18 Y DEL 28 AL 30 Y 1 LUNES, MARTES, JUEVES Y VIERNES HORA:09:00 A 15:00
BCO CICSBMP	72 HRS	3	04	ENERO, JULIO Y DICIEMBRE DIA: 1, 11 Y 21 LUNES, MARTES Y MIERCOLES
SERVICIO DEL CENTRO DE PROCESAMIENTO DE DATOS	NO APLICA	1	05	NO APLICA

IMPACTOS ECONOMICOS Y COSTOS DE RECUPERACION

APLICACION	PRIORIDAD	COSTO DE RECUPERACION
CENTRO DE DISTRIBUCION	4	$ 5,644.94 US DLLS mensual en contingencia $ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
CORREO ELECTRONICO	4	$ 5,644.94 US DLLS mensual en contingencia $ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
BOVEDA FUERA DE SITIO	4	$ 790.17 US DLLS mensual en contingencia $ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
ADMINISTRACION DE BASES DE DATOS	4	$ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
SYSTEM MANAGEMENT FILE	5	FUNCION SUSPENDIBLE
MEDICION DE CALIDAD SERVICIOS EN LINEA	5	$ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
MEDICION DE SERVICIO BATCH	5	$ 9,534.36 US DLLS anual usando modelo de recuperación tradicional
PROCEDIMIENTOS PARA MANTENIMIENTO DE EQUIPOS	5	FUNCION SUSPENDIBLE

PROCEDIMIENTOS ALTERNOS

APLICACION	¿PROCEDIMIENTOS ALTERNOS?	¿SE HAN USADO?	¿CUANTO TIEMPO SE PUEDE OPERAR CON ELLOS?
CHEQUES	SI	SI	PERIODOS CORTOS

En caso de contar con procedimientos alternos, estos consisten en:

- Procedimientos manuales los cuales son usados por periodos de tiempo cortos, enviando la documentación que no fue transmitida en línea hacia el Centro de Datos para su captura.

PRACTICAS EN OTROS BANCOS

APLICACIÓN	CONSIDERACIONES
CHEQUES	***Esta función se considera prioridad 1, ya que tiene como objetivo:*** ▪ Obtener información acerca del balance de las cuentas, obtener información para ser transmitida en línea y del Centro de procesamiento de Datos, información para el procesamiento de cheques electrónicos. ▪ Procesa cheques nacionales e internacionales actualiza las cuentas apropiadas. ▪ Envía información procesada entre sucursales Esta aplicación tiene relación con otras ya que les proporciona información y servicio. El equipo de desarrollo se encarga de dar soporte y mantenimiento a sus aplicaciones internas involucradas. Este mantenimiento se considera vital para un esfuerzo de recuperación de esta aplicación.
SERVICIO INMEDIATO	***Esta función se considera prioridad 1, ya que tiene como objetivo:*** ▪ Conectar clientes a través de su computadora ▪ Automatizar la atención de operaciones ▪ Administrar archivos de clientes y operaciones de cuentas con problemas Para ser posible la ejecución de este sistema es necesario que las aplicaciones de cheques estén en operación.
MERCADO DE CAPITALES Y DINERO	***Esta función se considera prioridad 1, ya que tiene como objetivo:*** ▪ Se maneja aproximadamente $15,000,000,000 diariamente ▪ Las cuentas del mercado de dinero equivalen a un 80% del procesamiento ▪ Maneja la compra y venta de acciones así como dinero y bonos. ▪ Mantiene un seguimiento sobre fechas compromiso en el mercado
PAGO DE SERVICIOS	***Esta función se considera prioridad 3, ya que tiene como objetivo*** Esta área ejecuta básicamente tres funciones: ▪ Captura de tarjeta de crédito ▪ Pagos ▪ Grabación de tarjeta Una vez que el impacto de la organización es menor, el tiempo máximo que la organización puede estar si esta función es de: 2 días para tarjeta de crédito, 3 para Pagos; 1 semana para Grabación de tarjetas
SOPORTE TECNICO Y OPERACION	***Esta función se considera prioridad 1, ya que tiene como objetivo:*** ▪ Recuperación, Diagnóstico y Resolución de problemas ▪ Administra todos los recursos magnéticos, y actualiza el software del sistema. Las responsabilidades de esta área son vitales para un esfuerzo de recuperación.

DEPARTAMENTOS ENTREVISTADOS

ENTREVISTA NO.	DEPARTAMENTO O AREA	PERSONAL ENTREVISTADO
1	CHEQUES AHORRO REMESAS	Miguel Ubaldo Becerril Noemi Reyes Rueda Alberto Cárdenas García
2	SWIFT SYCOF	Joel Cortina Díaz Edgar Ramírez Fuentes
3	MERCADO DE DINERO	Antonio Guzmán Díaz Georgina Estrada Macias
4	OPERACIÓN Y SOPORTE TECNICO	Israel Mendoza Laura Martínez Cervantes

A través de la entrevista y los resultados obtenidos, resulta más fácil la identificación de las aplicaciones y elementos que necesitan mayor atención y un análisis más detallado ya sea debido a su complejidad o en su caso al servicio que proporciona la organización a través de su buen funcionamiento.

Como se pudo observar los resultados nos servirán de guía para dar prioridad tanto a los siguientes pasos de la metodología como a la importancia y empeño que debamos de poner en las aplicaciones que deseemos analizar.

Además nos ayudará a contactar a los responsables de cada una de las aplicaciones para una futura afinación de este análisis y en su caso de los procedimientos a seguir a fin de tomar medidas de corrección y prevención del riesgo.

Reporte Final

Riesgos

Riesgos y Disparadores Identificados

1.1.1.Terremoto

EL terremoto de 1985 en la ciudad de México causó aproximadamente 10,000 muertes así como pérdidas y daños por billones de dólares americanos. El acceso ciertas partes de la ciudad quedo cortado por más de dos semanas. Pasaron meses antes de que los servicios de energía, agua y comunicaciones y transporte fueran restaurados en algunas áreas. La escasez crítica de vivienda, alimentos, agua potable, abastecimientos médicos, ropa y artículos necesario para la higiene afectaron a aproximadamente 13 millones de residentes.
El temblor ocurrió a las 7:19 a.m. el jueves, 19 de septiembre, cuando la placa tectónica de la corteza terrestre chocó a lo largo de una franja de 125 millas en la costa del pacífico. El temblor, en su epicentro, registró 8.1 grados en la escala de Richter. Sin embargo el daño a las ciudades y villas situadas a lo largo de la costa y las montañas fue mínimo. Los movimientos de la tierra causados por el temblor fueron absorbidos por la tierra o mitigados por las montañas de roca sólida que separan las costas de la ciudad de México.

Pero la ciudad de México está construida sobre el lecho seco de un lago. Cuando las ondas sísmicas resonaron a través de la tierra, penetraron en una capa de lodo suave, de 50 a 100 pies, bajo la ciudad. Esto causó dos efectos desastrosos. Uno; las capas suaves de sedimentos y arena en el subsuelo comenzaron a colapsarse, y dos; el lodo amplificón una banda estrecha de ondas sísmicas que ocasionó una frecuencia de resonancia en muchos edificios de la ciudad. La combinación del acomodo subterráneo de la tierra y la vibración de las estructuras de acero y vidrio provocaron daños masivos en los edificios de mayor altura.

La probabilidad de recurrencia de este tipo de terremoto, y de la estimación del daño que podría causar a las estructuras actuales de la ciudad de México no puede ser determinado utilizando los medios normales. Generalmente se toman lecturas sísmicas en forma periódica en puntos estratégicos a lo largo de la línea de la falla. La actividad sísmica futura puede entonces estimarse en base a la frecuencia e intensidad en la escala de Richter de la actividad registrada. Sin embargo, el terremoto de 1985 ocurrió a aproximadamente 200 millas de la ciudad. La mayoría de los intentos de los sismologos por predecir una recurrencia de una actividad sismológica mayor en la ciudad de México no han sido concluyentes.
El "daño" esperado a ser ocasionado por un temblor hoy día se reflejaría en la pérdida de las comunicaciones por línea terrestre y los servicios comerciales. El Grupo Financiero esta preparado para esa situación por medio de la:

Utilización de comunicaciones vía satélite, microondas y radio.
Activación de los generadores diesel ubicados en sus instalaciones para proveer los requerimientos de energía.
Utilización de facilidades de recuperación de agua en sus instalaciones.
El Grupo Financiero también cuenta con sus propias instalaciones médicas de emergencia, con personal capaz de tratar heridas y enfermedades no graves

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños Lógicos	Estimación de Daños Físicos
ALTA*	ALTO**	BAJO***	ALTO****

*De acuerdo con varios estudios profesionales, la placa tectónica conocida como la Placa de Cocos, se volverá amover antes del año 2037

**El riesgo de pérdida financiera para el Grupo Financiero se presentaría en la forma de una disminución en los depósitos en general, etc. Una tendencia temporal a la baja es común en las instituciones financieras como consecuencia de un desastre a nivel de toda la ciudad. Los dos disparadores que pueden seguir a un desastre de esta naturaleza son:

Accesabilidad

Para los empleados, proveedores y el personal para mantenimiento y reparaciones.
Para los clientes el acceso a las sucursales que estén operando
Para los servicios de mensajería, correos, vehículos blindados, etc., que hacen el servicio entre los clientes, las instalaciones centrales y las sucursales.

Disponibilidad

De los servicios y materiales requeridos para reparaciones
De combustible diesel para los generadores
Gasolina para los vehículos

Abastecimientos desde los requeridos para el apoyo de las funciones del negocio hasta aquellos necesarios para proveer de subsistencia a los empleados.

Nota: Si los empleados no pueden trabajar, o si no pueden concentrarse en su trabajo debido a las necesidades de sus familias, la recuperación será más difícil. La sección de administración de crisis del plan de recuperación del Grupo Financiero debe reconocer este hecho, y adoptar una política y una estrategia conceptual para tratar esta eventualidad

***Daños a la estructura de la instalaciones centrales, reparables, así como a algunas sucursales. Los nuevos reglamentos deben generar nuevas estructuras no sensibles a daños por resonancia de vibraciones sísmicas similares. La falla generalizada de energía eléctrica es muy probable, así también como la falla de servicios comerciales.

****Las líneas de teléfonos, tanto públicas como privadas, se encuentran instaladas de manera subterránea en la mayoría de las áreas de negocios de la ciudad de México. Un terremoto similar en magnitud al de 1985, causará los mismos problemas de comunicaciones ocurridos en ese entonces.

1.1.2 Clima

Generalmente, el clima en el área de la ciudad de México no es considerado un problema. Las temperaturas, aunque altas en ocasiones, generalmente oscilan entre los 10 y los 32 grados celsius y alta humedad son la excepción y no la regla. Sin embargo, actualmente se dice que el clima de la ciudad de México es demasiado suave para el bien de la ciudad.
Dos de los problemas actuales de la ciudad, la contaminación del aire y la escasez de agua, se deben en parte al clima extremadamente suave. Ni las altas corrientes de aire, ni los vientos de superficie, poseen la fuerza necesaria para disipar las impurezas del aire. Y la ligera y moderada lluvia anual es insuficiente para rellenar las reducidas reservas de agua.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
INSIGNIFICANTE	INSIGNIFICANTE	BAJO

Los riesgos técnicos del Grupo Financiero se centran alrededor de las comunicaciones y la preparación y prácticas para restaurar o reemplazar el medio ambiente de las instalaciones centrales.

1.2.1. Comunicaciones

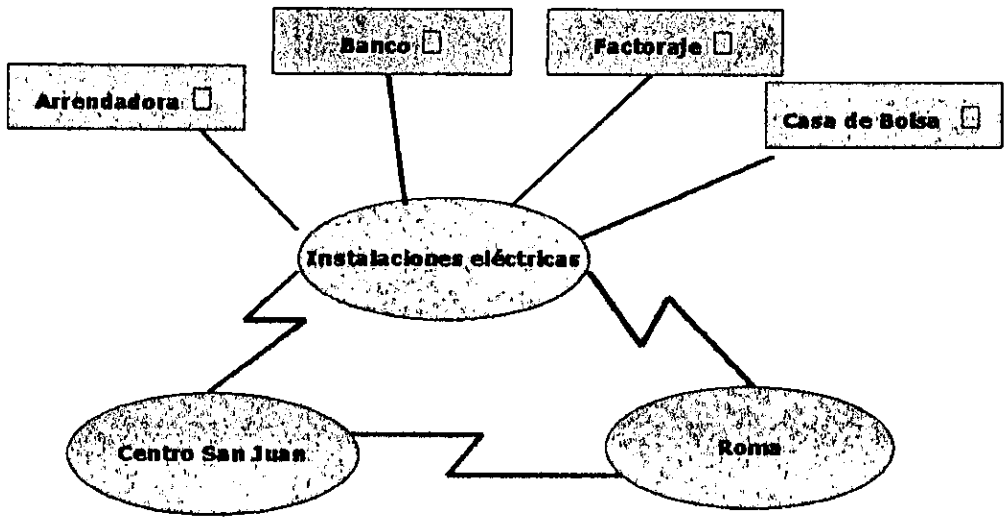
Las comunicaciones son un reto importante debido a la complejidad de tener un número importante de actividades de procesamiento y funciones del negocio dependientes de una fuente centralizada. La economía de escala ha provocado no solamente que las actividades bancarias normales se centralicen, sino también que todos los intereses del Grupo Financiero dependan de diversas funciones de apoyo proporcionadas por el mismo. Las comunicaciones de voz y datos del banco, factoraje, la casa de bolsa y la empresa de arrendamiento pasan a través de la red central.

1.2.2. Transmisión de datos

La red de datos del Grupo Financiero desde tres nodos de control principalmente:

Instalaciones centrales
Centro San Juan
Roma

Cada uno de estos nodos "controla aproximadamente 1/3 por ciento" de la red de sucursales del área metropolitana. Supuestamente, un desastre en cualquiera de estas tres instalaciones traería como consecuencia una pérdida máxima de solamente un tercio de la capacidad de comunicaciones requerida, sin embargo, esto aplica únicamente a las sucursales mencionadas, ya que las instalaciones centrales soporta desde el punto de vista red a las distintas compañías del Grupo Financiero, tales como: Factoraje, Arrendadora y Casa de Bolsa, las cuales en caso de un siniestro en las instalaciones centrales quedarían fuera de servicio.



Probabilidad de Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daño
ALTA*	ALTA**	ALTA***

* Debido a que el riesgo más grande encontrado para el Grupo Financiero es el del terremoto, y aún cuándo la estructura del edificio no sufriera daños considerables, las comunicaciones se verían afectadas dado que se puede perder la acometida RDI, las antenas pueden sufrir daños, el cuarto de comunicaciones puede ser inaccesible, etc.

** Ya que el nodo central, controla aproximadamente el 100% de la red de sucursales metropolitana, es el centro de comunicaciones de las empresas del Grupo Financiero, es el punto de acceso de centro regionales, se considera que el grado de riesgo para el Grupo Financiero es alto.

*** Por lo expuesto en el punto anterior.

Probabilidad De Ocurrencia nodo San Juan	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA*	ALTO**	MODERADO***

* Debido a que el centro San Juan se encuentra ubicado en una zona sísmica de alto riesgo dentro de la ciudad, como se evidenció en el terremoto de 1985, el riesgo de pérdida de este nodo se considera alto.
** Ya que el nodo centro San Juan, controla aproximadamente el 1/3 % de la red sucursales metropolitana, y es el respaldo de los centros regionales para sus transmisiones de datos, se considera que el grado de riesgo para el Grupo Financiero.

***Se considera moderado porque en caso de pérdida de este nodo se interrumpiría un tercio de las sucursales metropolitanas y el respaldo de centros regionales.

Debido a que el nodo Roma se encuentra dentro de la zona sísmica de alto riesgo de la ciudad, el riesgo de pérdida de este nodo se considera alto

1.2.3. Transmisión de Voz

La transmisión de voz puede ser un problema debido al tiempo que tarda TELMEX en dar mantenimiento o proveer de nuevos servicios. Uno de los entrevistados informó que habían sido solicitados y aprobados hacia casi un año. Uno de los entrevistados informó que TELMEX tardó casi cuatro meses para reparar la caída del servicio en una de las instalaciones.
Debido a esta situación hay otros lugares que actualmente están utilizando los sistemas de transmisión de voz proporcionados por las instalaciones centrales. Además de los departamentos ubicados dentro del mismo, el PBX de este centro así como otras instalaciones de voz dan apoyo a:
El grupo de información a clientes
Arrendamiento
Oficinas de Afore

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimacion de Daños
ALTA*	MODERADO**	MODERADO***

* Debido a que el riesgo más grande encontrado en las instalaciones centrales es el de terremoto, y aún cuando la estructura del edificio no sufriera daños considerables, las acometidas de troncales, la acometida de RDI e incluso el cuarto donde se encuentran los conmutadores, se verían afectadas.

** Aún cuando en las instalaciones centrales, se encuentra concentrada la mayoría de los conmutadores del Grupo Financiero y estos dan servicio al banco y a las otras empresas, se considera que le grado de riesgo en caso de pérdida de conmutadores es moderado ya que todas la empresas del grupo cuentan con su propio conmutador y su propia acometida de líneas públicas, el principal riesgo es interrumpir el servicio a clientes que traten de comunicarse a las instalaciones centrales.
*** Por lo expuesto en el punto anterior.

1.2.4. Respaldo de Aplicaciones

Este es el riesgo más grande que fue detectado, una falta de la adecuada información de respaldo que permita reanudar las operaciones de cómputo y la red en una ubicación alterna en forma oportuna. El Grupo Financiero ha implantado procedimientos de respaldo de información y recuperación que han permitido que las aplicaciones más importantes de producción batch hayan pasado exitosamente las pruebas de recuperación en su centro alterno.

Los respaldos de bóveda fuera de sitio para todos los sistemas batch y de línea son viajadas al centro alterno, en donde las cintas son verificadas por el departamento encargado, puesto que son usadas al momento de efectuar las pruebas de funcionamiento de nuevos sistemas, como parte del proceso de control a cambios, los datos utilizados para estas pruebas provienen de las mencionadas cintas, de esta manera se valida la información contenida en ellas.

En general, otros archivos de producción se respaldan a intervalos de tiempo suficiente para restaurar los archivos y reiniciar procesos con problemas o errores. Todos los archivos de sistemas batch, archivos maestros, etc., son respaldados (espejeo) al mismo tiempo que son creados hacia el centro alterno.

Una vez que algunas funciones han quedado detenidas por un periodo largo de tiempo, surgen otros impactos:

Otras funciones que dependen de la información computarizada y manual generada por la función caída, experimentan dificultades pudiéndose presentar hasta la suspensión del proceso.
El tiempo requerido para dejar a los sistemas en "estado actual" puede causar problemas adicionales debido al tiempo que toma el ciclo de proceso.
Si otros sistemas continúan procesando información, la sincronización del sistema y la información (especialmente para la información recreada) se vuelve más complicada a medida que el tiempo transcurre.

Ejemplos sobre impactos en estos puntos quedan respaldados con las respuestas del cuestionario aplicado

Prestamos Hipotecarios:

La recuperación tendría que sincronizarse con el sistema de cheques y con las tasas de interés apropiadas en base a las fechas de cierre, etc. No se podría cumplir con las fechas de cierre si trataran de funcionar manualmente.

Crédito y Cobranzas:

Sin el sistema, no podría iniciarse la cobranza en cuentas nuevas cada semana. Ellos podrían continuar trabajando en actividades iniciadas anteriormente por aproximadamente un mes. Pero después de eso, el banco estaría perdiendo millones de pesos diariamente.

Finanzas del Grupo Financiero:

Es necesario procesar todas las aplicaciones financieras del banco, y operando manualmente tomaría tres días solamente la recepción y el proceso de la información de un día. Con una semana sin sistema los procesos financieros del banco que se apoyan en las aplicaciones del sistema central estarían en serias dificultades.

Negocios para Empresas en las Sucursales:

La captura de las transacciones no esta respaldada. Después de la captura, las transacciones se pierden. Las transacciones con el mercado de valores se llevan a cabo por una sucursal en la casa de bolsa; la misma situación se aplica a las transacciones de entrada. Servicios empresariales también provee la mayoría de los servicios de cajeros automáticos. Todas estas funciones se consideran como "de demanda inmediata".

Cualquier interrupción podría resultar en pérdida o insatisfacción de clientes, multas y penalizaciones en los compromisos contractuales y problemas tanto con las agencias internacionales como nacionales.

Contabilidad General:

Sin los sistemas del equipo central, se requerirían 150 personas y 3 días para procesar la información de un dia. La regulación del gobierno exige que determinada información sea presentada a solicitud. Como resultado de una falta de sistema prolongada, la información que se enviará carecería de total verdad e inexacta.

Probabilidad De Ocurrencia de no tomar respaldos	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
MODERADA A ALTA*	MODERADA A ALTA**	BAJA A ALTA***

* Se consideró así debido a que el estándar de programación se establece que todos los archivos de entrada a un proceso deben de tener su respectivo respaldo en sitio (probabilidad moderada). Para archivos de bóveda fuera de sitio, se tiene al menos respaldo de todos los archivos maestros de la aplicación (probabilidad alta)

** Para recuperación de archivos en sitio, se cuentan con todos los elementos necesarios para recuperación por lo que el riesgo se clasificó como bajo. Sin embargo no todos los archivos tienen su respaldo fuera de sitio por lo cual es riesgo se clasificó como moderado

***Para recuperación en sitio, siempre se tiene manera de utilizar el respaldo. Para bóveda fuera de sitio solo se han probado 24 aplicaciones batch.

1.2.5. Respaldos de Información en LAN o PC

Algunos archivos importantes en LAN o PC se encuentran intercaladas entre los grupos de negocios y los departamentos ubicados en sitios separados.

Algunos de los entrevistados están consientes de que no existen políticas establecidas para el manejo de información; no hay "estándares" recomendados; no existen herramientas específicas; no hay una instalación externa apropiada para el almacenaje (segura y con medio ambiente controlado) que proteja la información crítica de redes LAN/WAN y en PC necesarias para las funciones del negocio.

Nota: Consultar la sección de Mitigación para información específica identificada y su necesidad de respaldo y almacenamiento fuera de las instalaciones

a) Resumen de Respaldos de Información en LAN o PC

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimacion de Daños
BAJO*	ALTO **	ALTO

Por no contar con políticas ni estándares establecidos

** *La probabilidad de pérdida o integridad de información es alta por no contar con políticas ni* estándares.

1.3.1. Contaminación del Aire

La ciudad de México es una de las más grandes del mundo por lo tanto no es difícil figurarse la gran cantidad de vehículos que circulan por ella, también cuenta con muchas empresas manufactureras, muchas de las cuales han contribuido al gran velo de contaminación que cubre la ciudad.

La mayoría de los empleados del Grupo Financiero son nativos de la ciudad de México y están, por lo tanto, condicionados a la calidad del aire.
No se encontraron indicios de que la calidad del aire presente un riesgo específico para las unidades de negocio del Grupo Financiero, aunque esto no es garantía de que en un futuro no pueda ser una causa de ausentismo

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA*	BAJO**	BAJO

Este problema irá volviéndose más crítico sin las medidas necesarias por parte del gobierno.

** Mientras se tomen medidas de mejoramiento en la calidad del aire.

1.3.2. Escasez de Agua

La población de la ciudad de México ha crecido rápidamente a través de los años, por lo que la ciudad ha sobrepasado la disponibilidad de muchos de sus recursos vitales. Entre ellos, el agua es probablemente el recursos más crítico del cual hay escasez, la causa de la escasez tiene, en realidad, muchas raíces. Una buena parte del agua potable de la ciudad viene de plantas de tratamiento distribuidas alrededor de lagos y reservas. Algunos de estos lagos han sido contaminados más allá de los esfuerzos de restauración.

Por ejemplo el lago de Chápala estuvo muy cerca de ser declarado área de desastre ambiental, el flujo del agua que alimentaba al lago era un décimo del flujo normal, y se descubrió que el agua del lago tenía un alto contenido de mercurio, plomo y materia fecal. El turismo a los diversos lagos de México desapareció como consecuencia el valor de las propiedades alrededor de los lagos se desplomó.

Sin embargo a través de la Comisión Nacional del Agua fueron implantados controles para reducir la contaminación de las áreas industriales y las ciudades localizadas a lo largo de las corrientes de río y lagos. Todos estos esfuerzos han ayudado enormemente, el agua que fluye desde las corrientes y los ríos hacia los lagos ya es más limpia.

La tendencia correctiva de rellenar los abastecimientos de agua puede verse coartada por el crecimiento de la población, ya que esta continua creciendo dramáticamente lo que significará que la demanda de agua podría sobrepasar los nuevos abastecimientos.

A no ser que las condiciones de escasez de agua puedan ser aliviadas, los intereses del Grupo Financiero en la ciudad de México pueden verse adversamente afectados en los próximos 5 a 10 años. Como muchas otras de las grandes ciudades la ciudad de México podría padecer lo siguiente:

La combinación de sobrepoblación y la escasez de agua provocará disturbios civiles.

Algunos negocios cerrarán

La tasa de crecimiento de la población se reducirá, pues puede sobrevenir algun grado de éxodo.

Nota: Otras tres grandes ciudades que se han enfrentado a períodos de "crecimiento negativo" durante periodos de paz, incluyen las ciudades de Nueva York, Berlín y Hong Kong. Estas tres ciudades alcanzaron el punto de saturación en su población a principios de los 80. La saturación llegó cuando el número de pobladores excedió la capacidad de los servicios de la ciudad, los colectores de basura ya no pudieron mantener limpia las calles, los productores de energía no pudieron proporcionar energía eléctrica en forma consistente y confiable.

La prestación de otros servicios se convirtió en menos confiable y más costosa a medida que la demanda aumentaba. En el tiempo en que tomó el corregir el problema en cada una de estas ciudades, la población había disminuido, muchos negocios pequeños habían cerrado sus puertas, y algunas de las grandes corporaciones habían cambiado sus oficinas a lugares con medio ambiente más estable.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
MODERADA*	BAJO (actualmente)**	INFORMACION INSUFICIENTE PARA HACER ESTIMACIONES

El riesgo aumentará a medida que la población y nuevos negocios aumenten.

** El riesgo aumentará a medida que la demanda de agua aumente.

1.3.3 Riesgos Vecinales

Se estudió la zona en la que se encuentra el Grupo Financiero y se dibujó un círculo con un radio de aproximadamente 3 kilómetros, el círculo fue dividido en cuadrantes para poder establecer patrones de investigación sistemáticos.

Los hallazgos generales se presentan a continuación:

a) Positivos

- *Una importante estación de policía se localiza a aproximadamente 1.5 km. al noroeste.*
- El hospital General de Xoco está a medio kilómetro al este
- El hospital 20 de Noviembre esta a aproximadamente 1 km.
- Las zonas residenciales al norte y al noroeste incluyen algunas casas de apariencia muy costosa (las casas costosas generalmente indican un aumento en la presencia policiaca)
- *Un pequeño hospital de emergencia se localiza a no más de medio kilómetro al sur*

b) Negativos

- Las estaciones de bomberos más cercanas son la estación Merced Balbuena, aproximadamente a 20 minutos al noreste del Grupo Financiero, y la estación de Tlalpan, *aproximadamente a 20 minutos al sureste. Además de este tiempo estimado se debe* considerar que el tiempo de desplazamiento en horas de tráfico lo puede incrementar.
- El Grupo Financiero está bordeado al sur por el Centro Comercial Coyoacán y por el de Plaza Universidad que se localiza aproximadamente a dos cuadras al norte.

Nota: *Debe recordarse que en la Plaza Universidad ya se dio un caso de explosión de bomba.* Los centros comerciales son generalmente considerados como blancos fáciles para terroristas, asaltos y disidentes políticos por la gran cantidad de gente que se puede llegara concentrar.Hay un edificio perteneciente al gobierno de la ciudad de México a menos de un kilómetro al norte; instalaciones de este tipo pueden fácilmente convertirse en sitios de disturbios civiles.

La industria ligera que se localiza son empresas farmacéuticas, fabricas de perfumes y pequeños fabricantes de muebles y no representan un riesgo para el Grupo Financiero y sus clientes.

El área de Coyoacán que rodea las instalaciones centrales parecer ser muy estable con excepción al tránsito alrededor de los centros comerciales, es tranquila.

Los riesgos principales que se identificaron de las condiciones vecinales son:
Respuesta lenta debido a la distancia y el tiempo de desplazamiento desde la estación de bomberos más cercana. En Estados Unidos, los tiempos de desplazamiento son medidos por el análisis de riesgo. Los tiempos de respuesta para los bomberos son:

10 minutos o menos = OPTIMO
De 10 a 20 minutos = MODERADO
Más de 20 minutos = MALO

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA*	MODERADO	BAJO A ALTO

* En base a los problemas de tránsito potenciales atestiguados.

1.3.4. Tránsito y Acceso

El acceso de los vehículos a las instalaciones centrales está limitado a una calle que corre de norte- sur bajo el Grupo Financiero y hay un espacio de estacionamiento en la esquina sur- este para los empleados. La calle norte- sur está dedicada principalmente a vehículos especiales.
Hay varias áreas de estacionamientos localizadas en el vecindario las cuales no tienen vigilancia visible. Es posible que autos bomba estratégicamente colocados pudieran cortar el acceso al área inmediata.

Las instalaciones cuentan con diferentes entradas, una para empleados, otra para clientes y una más para los proveedores.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJO*	BAJO	BAJO

* Debido a que cuenta con un buen sistema de seguridad proporcionada por la Institución.

1.3.5 Negocios en los Alrededores

Con la excepción de los grandes centros comerciales y las oficinas de gobierno, no se encontró evidencia de amenazas o disparadores relacionados con negocios situados dentro de un radio de 2 kilómetros de las instalaciones centrales. No se detectaron peligros por fuego presentados por estos negocios, tampoco se encontró evidencia de problemas por manejo de traslado y distribución de substancias químicas peligrosas.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJO	BAJO	BAJO

1.3.6. Autoridades Civiles

Como "Autoridades civiles" se describen a aquellas agencias que podrían brindar ayuda al Grupo Financiero en caso de algún desastre. Existe preocupación ya que la estación de bomberos más cercana se localiza lejos de las instalaciones, ya que ha habido dos conatos de incendio, los cuales fueron extinguidos rápidamente por el personal de seguridad de la institución. Recientemente se ha iniciado un entrenamiento especial tanto al personal de seguridad como a parte del personal de la institución contra este tipo de eventos con lo cual se busca que por lo menos dos personas por módulo conozcan los procedimientos a seguir en caso de ocurrir un evento como este.

La explosión de una bomba en el World Trade Center de la ciudad de Nueva York provocó varios incendios a lo largo de los niveles bajos de la estructura; en las áreas donde trabajaron los rociadores de agua, los incendios fueron controlados. Sin embargo, la explosión de la bomba había dañado varias fuentes importantes de suministro de agua así como algunos de los sistemas en sectores de los pisos superiores. EL personal de seguridad trató de aislar y combatir el fuego y, al mismo tiempo evacuar al personal herido. Solamente después de que muchos bomberos profesionales y dos bombas de la localidad llegaron, el personal de seguridad se pudo dedicar a evacuar el edificio. Un artículo del periódico Newsweek reportó que, de acuerdo a las autoridades civiles que habían estado presentes, la primera bomba de agua llegó dentro de los cinco minutos siguientes de la explosión, lo cual muestra que de haber sido más tiempo mucha más gente hubiera resultado muerta o herida.

Lo mencionado anteriormente no tiene la intención de reducir la importancia de contar con personal de seguridad y/u otro tipo de personal "entrenado" para manejar incendios. La intención es la de enfatizar que tan rápido puede expandirse el fuego a niveles que aún los profesionales no podrían controlar.

Debido a que el diseño del edificio Grupo Financiero, a base de espacios abiertos, con respiraderos abiertos y verticales, y la ausencia de rociadores u otros sistemas automatizados, es posible que:

- El fuego pueda arder por varios minutos antes de que lo detecte la alarma detectora de incendios.
- La alarma detectora de incendios podría estar a gran distancia aún a un piso de distancia de donde se genere el fuego.
- Un incendio instantáneo, tal provocado por una explosión o combustión, podrá extenderse rápidamente.
- Un incendio no controlado dentro de los primeros minutos podría extenderse vertical y horizontalmente a través de la estructura.

Nota: Las observaciones aquí presentadas son el resultado de un análisis, en este caso, de sentido común pues no se pretende ser experto en el manejo de incendios, por lo que resulta recomendable si así lo consideraran realizar un análisis detallado al respecto.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA	MODERADO A ALTO	MODERADO A ALTO

1.3.7. Medios de Subsistencia

El Grupo Financiero no cuenta con un plan para proporcionar medios de subsistencia a los miembros de los equipos de recuperación en localidades remotas, sin embargo debido a la naturaleza del negocio, medidas para proveer de medios de subsistencia de emergencia, en forma de créditos aprobados, debería ser una cosa simple.

A continuación se presenta una posible política de subsistencia:

- Un determinado número de cuentas de crédito puede ser establecido.
- Una o más tarjetas de crédito para cada cuenta pueden ser depositadas en uno o más sitios seguros fuera de las instalaciones.

- A raíz de un desastre, un número apropiado de tarjetas se distribuiría al personal del equipo de recuperación para ser utilizado para el pago de hospedaje, alimentos y otros artículos de uso personal requeridos en una emergencia.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA*	BAJO	BAJO**

* En base a otros riesgos potenciales
**Siempre y cuando se inicien las políticas y procedimientos para prepararse para esta eventualidad, el no hacerlo podría causar problemas para obtener el alto grado de responsabilidad que se requiere de los equipos para un periodo de tiempo logrado.

1.3.8. Tránsito Aéreo

Las instalaciones centrales del Grupo Financiero se encuentra situado a aproximadamente a 20 kilómetros sur – suroeste del aeropuerto de la ciudad de México. Esta distancia se considera, generalmente como "moderada segura" o "segura" en la mayoría de los aeropuertos. Sin embargo en varias ocasiones se ha presenciado sobrevuelo de aviones comerciales a altitudes de aproximadamente 2000 pies de altitud.

Los funcionarios del aeropuerto de la ciudad de México aseguraron que las instalaciones centrales del Grupo Financiero no se encuentra incluido en las rutas aéreas del aeropuerto. Sin embargo, mencionaron que cuando hay tráfico aéreo en el área y debido a los vientos prevalecientes o a las condiciones del tiempo, a menudo se le indica al tráfico local que "acelere" o "retrase" el acercamiento, en ambas situaciones los pilotos:

- Vuelan directamente a una marca externa del aeropuerto desde cualquier posición que tenga en ese momento (atravesando las rutas de tráfico normales).
- Vuelan haciendo "vueltas en S" a ambos lados del corredor de vuelo normal, para retrasar el momento del acercamiento final a la pista.

Cualquiera de estas prácticas como es de suponerse pueden provocar que ocasionalmente un avión comercial pase sobre o cerca de las instalaciones centrales del Grupo Financiero.
Aparte de una colisión aérea, un avión en vuelo bajo ocasiona problemas o suspensión en las comunicaciones. Los sistemas de radio a bordo pueden interferir con las ondas de radio VHF y UHF que transportan la información, y el radar a bordo puede interferir las transmisiones de microondas.

Se verificó con la gente encargada (operación red) para determinar si los aviones en vuelo bajo podrían causar problemas de comunicación y solamente se ha presentado algunos problemas ocasionales (uno en un período de tres meses) que pudieran ser achacados a los aviones.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJO*	BAJO	BAJO**

* Tanto para colisiones como para interrupciones de las comunicaciones
** Dependiendo del tamaño del avión, la carga de combustible y el punto de impacto.

1.4.1. Físicos

a) Historia de la Estructura

Las entrevistas con el personal de seguridad clave no revelaron grandes eventos o siniestros que hayan ocurrido en las instalaciones centrales desde que fue ocupado en 1979. Ni aún cuando sobrevino el temblor de 1985 se registraron daños que pusieran en peligro a los ocupantes del edificio, tampoco se restringió el acceso.
EL efecto más desastroso originado por el terremoto fue la ruptura de las líneas telefónicas de tierra, lo cual cortó las comunicaciones al exterior.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJO	BAJO	BAJO

1.4.2. Seguridad Física.

Solo se encontraron cinco puntos de preocupación en relación a la seguridad física en general tanto del campus como del edificio:

1. Durante una caminata alrededor del perímetro del campus, se descubrió que algunos árboles plantados pueden brindar un acceso potencial a intrusos.
2. Las antenas de satélite están situados en un área pequeña y enrejada en el lado oeste del edificio. Parece que estos platos podrían ser blancos fáciles en un intento de sabotear la comunicaciones del Grupo Financiero.
3. Aún cuando siempre hay un considerable número de guardias de seguridad cerca de la entrada para empleados, es presumible que intrusos, ataviados con ropas de negocios pudieran ingresar a las oficinas.
4. Con excepción del centro de datos, la cintoteca y otras áreas vitales, las oficinas de negocios no cuentan con sistemas automatizados para controlar incendios. La mayoría de estas oficinas tienen cubículos y muebles de madera y otros materiales inflamables. También se encontró que muchas estaciones de trabajo tienen pilas de papeles en muchos de los escritorios y gabinetes así como cajas de cartón. El riesgo asociado es que está permitido fumar prácticamente en todas estas áreas de negocios.
5. El funcionamiento de varios dispositivos para seguridad no es el adecuado. Detectores de metal, cámaras de monitoreo, sistemas de detección de fuego, y aún los sistemas de acceso con tarjeta pueden funcionar bien en un momento y en otro no. El sistema de detección / combate de incendios se considera obsoleto en las áreas de CPU, discos y cintas.

1.4.4. Seguridad del Personal.

a) Evacuación.

El diseño de las instalaciones centrales está hecho de tal forma que permite a los empleados contar con espacios abiertos para escapar o evadir algún peligro; campos de visión claros a

través de largos pasillos del edificio para detectar un peligro que se acerque, y suficientes escaleras para evacuación en caso de así requerirse.

Existen letreros indicando los procedimientos de evacuación, así como los procedimientos a seguir para incendios o temblores, que están pegados en lugares visibles a través de todo el complejo.

La decisión sobre la necesidad de evacuar la toma el personal de seguridad y es transmitida a través del servicio de altavoces que abarca a todo el complejo.

1.5.1. Atención Médica al Personal

El personal de seguridad de la institución está entrenado para proporcionar primeros auxilios, además cuenta con un servicio médico de emergencia dentro de sus instalaciones. Este personal está equipado para atender heridas menores para transportar a los empleados más graves a uno de los centros médicos más cercanos en ambulancia, ya que cuentan con un servicio de ambulancia en sitio.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJO	BAJO	BAJO

1.6. Riesgos de Ubicación (lógicos)

1.6.1. Accesibilidad del Sistema

El primer paso para determinar un riesgo potencial relativo al sistema de acceso, es la evaluación de un posible acceso no autorizado. Se dio especial interés a aquellos casos donde una PC o terminal del sistema central (mainframe) pudieran ser conectadas a una aplicación de producción y esta quedara sin atender, prácticamente en ningún momento se detectó un evento así. El acceso a las aplicaciones del sistema central se controla vía RACF.

Las aplicaciones se ven seguras y estables para una rutina normal de producción. El acceso a las aplicaciones será una de las primeros temas a tratar al momento de desarrollar los procedimientos de recuperación para el centro de datos.

En base a lo anterior, durante esta etapa del análisis de riesgos se entrevistó a los administradores de seguridad de la información, donde se trataron los siguientes puntos.

- Administración de seguridad
- Control de Acceso a la Información
- Control de Acceso a los servicios en línea
- Control de Acceso a las aplicaciones
- Control de Acceso a la red de telecomunicaciones
- Auditorías
- Riesgos

A continuación se describe con detalle los puntos tratados.

- Administración de seguridad

La administración de seguridad es atendida por tres operadores de la gerencia de Seguridad de la Información, cuya función principal es:

a) Mantener controlados los niveles de seguridad de las aplicaciones tanto en línea como en batch
b) Controlar los accesos a las aplicaciones a través de claves de usuario con diferentes niveles de seguridad dependiendo las funciones y puesto específico del personal, debiendo ser de 8 caracteres alfanúmericos, restringiendo o no el uso exclusivo de una terminal específica.

La asignación de claves de acceso se da a través de los manuales de nomenclaturas lo cual facilita
su creación y administración.

El control de las claves secretas (passwords) lo proporciona el RACF, el cual solicita de manera automática el cambio de password después de un intervalo de tiempo definido por las políticas de la institución, cuenta también con la capacidad de guardar generación de claves secretas con el fin de no permitir que este sea repetido al momento de solicitar el cambio.

El procedimiento para asignar una clave de usuario se encuentra definida a través de políticas especificas siguiendo la siguiente secuencia:

Requisitar un formato previamente definido de manera completa, de tal manera que ninguno de los datos se omita, los datos que se solicitan son: Nombre completo; registro de empleado (en caso de ser empleado), área a la que pertenece, justificación de la solicitud, firma del jefe y subdirector inmediato, en caso de ser proveedor la empresa a la que pertenece. Además deberá leer y firmar las políticas de uso de claves vigentes por el Grupo Financiero al momento de llevar su solicitud. Es responsabilidad del jefe inmediato del solicitante notificar al área de Seguridad de la Información cuando la clave deba ser cancelada.

El área de Seguridad de la Información cuanta con un procedimiento automático para dar de baja las claves de usuario cuando no hayan sido utilizadas durante cierto periodo de tiempo, lo cual elimina además las claves de empleados que ya no laboran en la institución y cuya baja no hubiese sido reportada.
Todas las funciones administrativas se llevan a cabo únicamente con las utilerías propias del producto; por el momento solo se cuenta con una herramienta semi - automática que ayuda al administrador a tener el registro de todos los requerimientos que éste recibe.

Los procedimientos de administración de seguridad son creados por el área de Ingeniería de seguridad encargada de proveer las herramientas necesarias para la administración de la seguridad, la administración de dichos procedimientos es llevada a cabo por el supervisor de los administradores del sistema. Toda la información que se maneja en esta área esta protegida, pudiéndose accesar únicamente por personal de Seguridad de la Información.

Un aspecto importante de mencionar es que existen usuarios de emergencia en caso de ocurrir algún problema durante la noche a fin de que ayuden a resolver problemas presentados, estos usuarios solo pueden ser utilizados bajo estas condiciones y bajo responsabilidad del supervisor del centro de mando del turno en que se requiera este. Además estos usuarios son monitoreados y auditados constantemente.

El respaldo de la información de seguridad esta se encuentra contenida en 2 bases de datos espejeadas, cuando falla una prácticamente de inmediato la otra entra en funcionamiento, además por ser datos confidenciales estas se encuentran en volúmenes de discos muy especiales.

Respecto a la protección del sistema operativo y de algunas utilerías y comandos poderosos estos se encuentran estrictamente protegidos y controlados y el acceso es permitido solo a personal altamente calificado.

- Control de Acceso a la Información

Unicamente ciertas áreas que brindan soporte técnico a la producción tienen acceso a archivos críticos con el fin de poder solucionar cualquier problema presentado; sin embargo es necesario mencionar que a pesar de esta "libertad" todos estos componentes del sistema son auditados diariamente; por lo que cualquier alteración a la información por parte de personal permitido o no debe ser documentada y en su caso justificada al área de Seguridad de Información.

El nombre de los archivos y bibliotecas se encuentran estandarizados de tal manera que facilite el control de acceso a los mismos y aunque la instrucción o comando se envíe de un sistema a otro se validan las autoridades necesarias para permitir su ejecución, tal como el usuario, la clave secreta y el acceso específico a cada componente del sistema.

- Control de Acceso a los servicios en línea

Los servicios en línea también son controlados por el área de Seguridad de Información, el cual restringe el acceso relacionando las claves con sus permisos.

- Control de Acceso a las aplicaciones

Las aplicaciones se encuentran protegidas de acuerdo al tipo de usuario que sea asignado, las cuales permiten el acceso y los atributos que usarán para el desarrollo de sus funciones.

- Control de Acceso a la red de telecomunicaciones

El acceso a la red de comunicaciones al sistema central se encuentra restringido para las áreas de desarrollo de sistemas y no se encuentra disponible para usuarios finales de aplicaciones. Este permite su acceso a través de las claves de usuario y su perfil de acceso.

- Auditorías

Existen dos personas encargadas de auditar a todas las áreas usuarias de sistemas, así como el uso de usuarios de emergencia y soporte técnico; además audita también al administrador de seguridad de tal manera que este no sea juez y parte.

También son auditados todos aquellos componentes (archivos, bibliotecas, programas, utilerías, etc.) que son considerados críticos para la institución.

Por último los logs del sistema son auditados diariamente y son utilizados como pruebas técnicas en caso de algún evento desfavorable para la institución.

- Riesgos

  a) Cuando una persona deja de laborar en la institución no existe un método eficaz e inmediato que notifique al administrador para dar de baja las claves de usuario

b) El sistema que ayuda a mantener el registro de solicitudes todavía se encuentra en una etapa de adecuación y pruebas.
c) Nos e notifican cambios de áreas y puestos, con el fin de actualizar el perfil de la clave del usuario.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
BAJA A MODERADA	BAJA A MODERADA	BAJA A MODERADA

1.6.5. Transmisión de Datos

El Grupo Financiero utiliza transmisiones vía satélite, microondas, y UHF, además de líneas privadas, líneas telefónicas terrestres, para enviar información de un sitio a otro. El principal medio de comunicación entre las instalaciones centrales y las áreas distantes es vía satélite. Es necesario mencionar que ya se presentó el caso de que el satélite que da servicio a la institución salió por algunos instantes de su órbita lo cual afecto no solo a esta institución, sin embargo el problema fue resuelto en poco tiempo.

El sistema de satélite permite la conectividad de las comunicaciones desde el centro de control de la red en las instalaciones centrales a todos los centros regionales así como a las sucursales principales.

Las microondas se utilizan principalmente para respaldar las comunicaciones vía satélite; además los conos de microondas se utilizan para comunicaciones metropolitanas con las sucursales y edificios corporativos.

1.6.6. Transmisión de Voz

Debido a que muchas organizaciones del Grupo Financiero, mas otras que se localizan en la zona metropolitana, dependen de las instalaciones centrales para sus transmisiones de voz, por lo tanto se visualiza la transmisión de voz como un riesgo primario.

Cuando menos el 25 por ciento de los departamentos entrevistados consideró al servicio de voz como una "necesidad crítica del negocio", por ejemplo, algunos departamentos que tienen contacto con el mercado de valores, inversiones internacionales, intercambio de divisas, aprobaciones de crédito y cobranzas prácticamente no pueden funcionar sin una línea telefónica.

1.6.7 Registros Vitales y Documentos Controlados

Una de las áreas de mayor preocupación para todos los entrevistados se relaciona con el almacenamiento y protección de los documentos importantes. Muchas áreas del Grupo Financiero tiene la necesidad de mantener los documentos en papel prácticamente "para siempre". La "necesidad" parte de los compromisos contractuales con los clientes, los reglamentos gubernamentales, del Banco de México y de la Comisión Bancaria y de Valores, y la misma necesidad de la institución de protegerse y proteger a sus clientes contra pérdidas.

Actualmente, la mayoría de los departamentos que han expresado esta necesidad particular almacenan sus documentos fuera de las instalaciones centrales en una bodega que la institución tiene para tal fin.

Sin embargo otros departamentos que tienen esta necesidad utilizan diferentes métodos como:

- Una bóveda localizada en las mismas instalaciones centrales.
- Gavetas para archivo de material resistente al fuego
- Gavetas localizadas en los mismos departamentos

Aún cuando cada departamento utiliza el recurso de almacenar sus documentos críticos dentro y fuera de la localidad, la decisión para que esto se lleve a cabo se basa en las siguientes dos consideraciones:

- La necesidad de tener acceso a los documentos "con poco o sin previo aviso" y frecuentemente.
- El costo implicado en el empaque, transportación, almacenaje y recuperación de los materiales.

Algunos de los departamentos entrevistados indicaron que la pérdida de ciertos documentos resultaría no solamente "costoso" para la función de los negocios sino que también "bochornoso" y de mala imagen para el Grupo Financiero, por ejemplo:

- Los contratos de los Fondos de Fideicomiso representan el vínculo legal entre las cuentas financieras que contienen los fondos y los beneficiarios de los mismo. El contrato del Fondo del Fideicomiso vincula al benefactor, los fideicomisiarios, administradores y beneficiarios. Si estos documentos se pierden o destruyen se crearían graves problemas para los beneficiarios que trataran de determinar su crédito en base a el saldo en le fideicomiso. El fideicomiso puede valer millones, pero el banco podría negar aún un crédito mínimo.
- El Grupo Financiero debe retener cierta información sobre los préstamos hipotecarios durante toda la vida del préstamo(15 años en la mayoría de los casos). En el caso de que cualquiera de esta información se perdiera o destruyera, la institución se haría acreedora a varias penalizaciones legales y multas gubernamentales.

Probabilidad De Ocurrencia	Grado de Riesgo para el Grupo Financiero	Estimación de Daños
ALTA	MODERADO	BAJO A MODERADO

RECOMENDACIONES

1. Recomendaciones para Mitigación de Riesgos

1.1. Mitigación Física

1.1.2. Recomendaciones sobre Sismos

Dado que la ciudad de México, es la capital de la república y el centro del comercio del país, NO es recomendado que el Grupo Financiero reubique sus oficinas corporativas para evitar el riesgo de un sismo. Un movimiento de este tipo, en caso de darse, deberá realizarse poco a poco, en distintas fases a fin de prevenir pérdidas en el mercado de negocios.

El único riesgo posible que puede y debe ser mitigado lo más rápido posible, es la reubicación del centro alterno hacía otro ambiente más seguro puesto que este tiene más probabilidad de daño en caso de ocurrir un sismo. Este centro alterno deberá ubicarse en un lugar con las siguientes características:

- Menos probabilidad de daño en caso de ocurrir un sismo
- Esté a más de 20 kilómetros de la costa más cercana para reducir la posibilidad de huracanes
- Pueda soportar requerimientos de entrenamiento de personal con escuelas y universidades
- Proporcione soporte de proveedores para operaciones del centro de datos
- Incluya acceso por aire, tren y carretera al área.
- Pueda producir el suministro de servicios tales como comunicaciones, electricidad, agua y gas para soportar un centro de cómputo del tamaño necesario para recuperar el ambiente de producción del Grupo Financiero.

Las ciudades más importantes en México, están localizadas en zonas con riesgos sísmicos que van de moderados a altos, sin embargo, la ciudad de Monterrey, está localizada en el área sísmica de menor riesgo. Por lo tanto es recomendada esta ciudad para cubrir los requerimientos de un centro alterno.

1.1.2. Recomendaciones sobre el Almacenamiento de los Registros Vitales

- Instalar un sistema adecuado para llevar el inventario de documentos archivados en el almacén.
- El diseño del almacén para formatos incluya control de temperatura y sistemas de detección / supresión de fuego y agua.
- Instalar sistemas automatizados de supresión de fuego, detección / expulsión de agua y monitoreo de temperatura en el almacén de registros vitales de papel
- Instalar controles automatizados para supresión de fuego y humedad en las áreas donde se archivan las microfichas y microfilms

1.1.3. Restricción de NO fumar en Ciertas Areas

La principal amenaza de incendio la representa el permiso de fumar en prácticamente todo el complejo. Se recomienda que se restringan las áreas para fumar, que pueden ser oficinas cerradas sin ningún material inflamable, lejos de las áreas de negocio y críticas.

1.1.4. Preparación para Apoyar al Personal de Recuperación de Emergencias

La parte de administración de crisis del Plan de Recuperación de Desastres tendrá que incluir una política y procedimientos para proveer de subsistencia (vivienda, alimentos, ropa, etc.) al personal que viaja para trabajar en localidades remotas.

Se recomienda que esta política sea adoptada de inmediato y que se le informe al personal los procedimientos y restricciones del uso de tarjetas de crédito especiales para estos casos.

2.2. Mitigación Lógica

Temas: *Acceso No Autorizado*
Procesos para Baja del Personal
Seguridad de la Red
Uso de Códigos

2.2.1. Computadoras Personales

Durante el proceso de entrevistas, se encontró que existe una gran cantidad de información importante la cual es procesada en computadoras personales. No existen procedimientos estándar para obtener respaldos de este ambiente así como tampoco donde almacenarlos.

Basado en lo anterior se recomienda que se refuercen las políticas generales acerca de cuando y como realizar respaldos de información de las computadoras personales, así como su correspondiente almacenamiento fuera de las instalaciones centrales.

2.2.2. MAIL e E-MAIL

El Grupo Financiero tiene implantado dos aplicaciones que son utilizadas para los mensajes internos, sin embargo uno de estos que se encuentra instalado en el sistema central no se encuentra relacionado con el sistema de administración de seguridad por lo que su administración no es muy confiable dado que en este se maneja información interna. Se recomienda que este sea ligado con el sistema de seguridad con el fin de manejar la administración desde un solo punto.

Respecto al uso de mail se recomienda que se difundan más ampliamente las políticas de uso de este servicio con el fin de evitar que este sea utilizado con fines diferentes al de la institución como el de las cadenas de mensajes comerciales, de suerte, historias o personales.

Una de las aplicaciones críticas con las que convive cualquier institución hoy en día es el uso del E-MAIL puesto que es el medio por el que comúnmente son infectadas o atacados nuestros sistemas de información de lo cual se habló en el capítulo 4, así pues se recomienda que el uso de este servicio sea restringido y solo sea otorgado a personas cuya función sea muy especial.

2.2.5. Aplicaciones

Cuando un empleado o proveedor deje de prestar sus servicios en la institución, deberá existir un procedimiento de terminación de relación adecuado con el fin de cancelar la clave de acceso y privilegios asignados dentro del sistema central, red y demás servicios proporcionados.

Se recomienda la implantación de un sistema automatizado para el registro y control de todos los requerimientos que el departamento de seguridad de información recibe y atiende.

Se recomienda que se reduzca los intervalos de tiempo establecidos para desactivar o dar de baja las claves de usuario.

CONCLUSIONES

La evolución tecnológica que se ha estado viviendo de forma tan acelerada durante la última década ha obligado a las organizaciones a cambiar o en su caso actualizar su forma de hacer negocios y de sobrevivir en el mercado. Así mismo como hemos visto nacer y crecer al Internet también hemos tenido que enfrentarnos a nuevas y variadas formas de amenazas a nuestro entorno laboral y social, los virus informáticos entre otros es un ejemplo claro de esto.

En el entorno en el que actualmente se desenvuelve cualquier organización ha obligado a que estas tomen una mayor conciencia de la importancia de la seguridad de la misma tanto en su aspecto lógico como físico. Es natural entender que los riesgos siempre van a existir, esto es algo de lo que el ser humano es incapaz de evitar; sin embargo sí es posible llegar a tomar conciencia de estos y llegar a minimizar sus consecuencias.

El análisis del riesgo no es una práctica realizada comúnmente por las organizaciones, a pesar del gran valor agregado que aporta a las mismas; la causa principal de esto es la falta de una cultura de seguridad que nos permita visualizar riesgos potenciales en nuestro entorno laboral y social.

De las diversas formas que existen para analizar el nivel de seguridad con el que cuentan las organizaciones, la que resulta más práctica y útil es el Análisis del Riesgo pues es la única que proporciona información acerca del costo - beneficio de las medidas de prevención y/o corrección del riesgo de tal manera que facilita en gran medida la toma de decisiones.

Quizá esta sea una de las características más importantes del análisis del riesgo, pero también es la más crítica dado que en esta se basará el rumbo y supervivencia de la organización por ser, como ya he comentado, base para la toma de decisiones, sin embargo no debemos olvidar que también estas tienen un riesgo implícito.

Comúnmente cuando una organización desea conocer a que tipo de riesgos esta expuesto hace uso de Auditorías para este fin, aunque ciertamente es una técnica muy válida esta se encuentra enfocada a realizarla sobre situaciones ya creadas, es decir se práctica sobre algo que ya se encuentra en funcionamiento. Por otro lado el análisis del riesgo aunque comparte esquemas con la auditoría esta es menos rígida en el aspecto que este puede realizarse en cualquier etapa en la que se encuentre la organización, es decir se puede realizar un análisis del riesgo desde la concepción misma de un proyecto, en su fase de desarrollo (identificando riesgos que no se habían contemplado), en su etapa de pruebas, en producción y en su etapa de mantenimiento.

Otro de los grandes méritos del Análisis del riesgo es que provee las bases para desarrollar políticas y procedimientos de seguridad además de que nos ayuda a identificar quién(es) es el propietario y responsable de cierta información del negocio.

Este tipo de información nos ayuda en gran medida a sentar las bases para la definición de un plan de recuperación del negocio, ya sea en condiciones críticas como en condiciones de presentarse un problema no tan crítico, esto con la finalidad de definir una matriz de alertamiento de acuerdo al tipo de problema que se presentara, lo que sin duda nos ahorrará tiempo valioso.

Es necesario aclarar que no es posible llegar a tomar acción sobre todos los riesgos que se identifiquen en este análisis, así que habrá que asumir algunos de acuerdo a su relación costo - beneficio. El análisis del riesgo deberá ser capaz también de indicarnos a que grado de vulnerabilidad se encontraría la organización en caso de asumir cualquiera de los riesgos identificados ayudándonos una vez más tomar la decisión más adecuada.

Como se puede observar en este tipo de análisis es necesario contar con un equipo de trabajo especializado a fin de que se pueda detectar todas aquellas vulnerabilidades lógicas y físicas en las que se desenvuelve la organización, por lo tanto el apoyo y compromiso de esta deberá darse hacia todos sus niveles.

La metodología expuesta en el presente trabajo tiene como finalidad el presentar un modelo para realizar este tipo de análisis, sin olvidar que cada una de las organizaciones en las cuales se desee llevar a cabo tendrá sus particularidades muy especificas que no necesariamente compartirán las demás, es decir desde el simple hecho que cada organización maneja diferente tipo de información esto la hace diferente por sí sola.

Finalmente es necesario mencionar que la información que se desprende de este análisis es de uso exclusivo para la organización por lo que deberá tenerse especial cuidado en el manejo que se le dé a la misma. No olvidemos que la seguridad es responsabilidad de todos.

Apéndice A

RESEÑA SOBRE EL ATLAS NACIONAL DE RIESGOS

Objetivo.

Ofrecer una panorámica general de los riesgos de origen geológico, hidrometeorológico, químico, sanitario, y socio-organizativo a los que está expuesto el territorio nacional.

Es importante destacar que la clasificación de calamidades utilizada en este documento es la señalada en las Bases para el Establecimiento del Sistema Nacional de Protección Civil. En el presente apéndice se destacan solo aquellos fenómenos de cada grupo que sobresalieron por su incidencia periódica, extensión territorial y magnitud de daños ocasionados. La información presentada se estructuró en tres apartados fundamentales, considerados como la base mínima para su conocimiento:

Con base en la información estructurada, se han podido determinar aquellas zonas que presentan un mayor riesgo, así como los efectos que se estiman pudieran derivarse, con el propósito de establecer los mecanismos de prevención de desastres en las distintas regiones del país.

SISMOS

Descripción del Fenómeno.

Lo que usualmente experimentamos como un sismo o temblor es la propagación de ondas a través de las rocas que constituyen nuestro planeta. Esta propagación es posible porque la Tierra se comporta como un cuerpo elástico.

Desde el punto de vista de riesgo sísmico, nos interesan los grandes terremotos que ocurren naturalmente en zonas bien definidas de nuestro planeta.

Actualmente sabemos que dichos terremotos ocurren por el rompimiento abrupto de las rocas como consecuencia de las fuerzas de tensión o compresión a las que están sujetas. Estos rompimientos ocurren a lo largo de superficies se conocen como fallas geológicas.

La razón por la que se presentan esas fuerzas de tensión o compresión es debida a que el cascarón más externo de nuestro planeta, la litosfera, formada por la capa rocosa rígida más superficial de la Tierra, esta fragmentada en un mosaico irregular de placas rígidas y móviles llamadas tectónicas, a manera de casquetes, que pueden contener tanto porciones continentales como porciones de corteza del fondo oceánico. Estas placas se mueven, una con respecto a la otra a lo largo de grandes zonas de fractura, y es ahí donde se generan los más grandes terremotos.

La sismisidad en el territorio nacional se debe principalmente a la actividad de las placas tectónicas y fallas geológicas que lo cruzan y circundan. La República Mexicana se encuentra ubicada en una de las zonas de más alta sismisidad en el mundo; esto se debe a que su territorio está localizado en una región donde interactúan cinco importantes placas tectónicas: Cocos, Pacífico, Norteamérica, Caribe y Rivera.

El territorio Nacional se ve afectado por fallas continentales, regionales y locales. Dentro de las fallas continentales se consideran la de San Andrés, que marca la frontera entre las placas de Norteamérica y del Pacífico , desde Nayarit hasta Chiapas, y la de Motagua Polochic, que marca el desplazamiento entre las placas del Caribe y de Norteamérica.

Existe también un gran número de fallas regionales y locales de diversas longitudes, distribuidas en todo el territorio nacional, con distintos grados de actividad sismica . Entre estas pueden mencionarse, el sistema de fallas en el área de Acambay, en el centro del país, y en el sur de la República, el sistema de fallas de Ocosingo en Chiapas.

Parámetros sísmicos

Los sismos se manifiestan como movimientos ondulatorios violentos del suelo, que se propagan en sentido horizontal y vertical. Se originan en un foco o hipocentro, en el interior de la corteza terrestre o en puntos aún más profundos, cuya proyección sobre la superficie terrestre se denomina epicentro o epifoco.

El Foco marca el punto en el que se inicia el proceso de ruptura. Conforme se desarrolla la ruptura de la falla, la región focal puede extenderse sobre un área considerable.

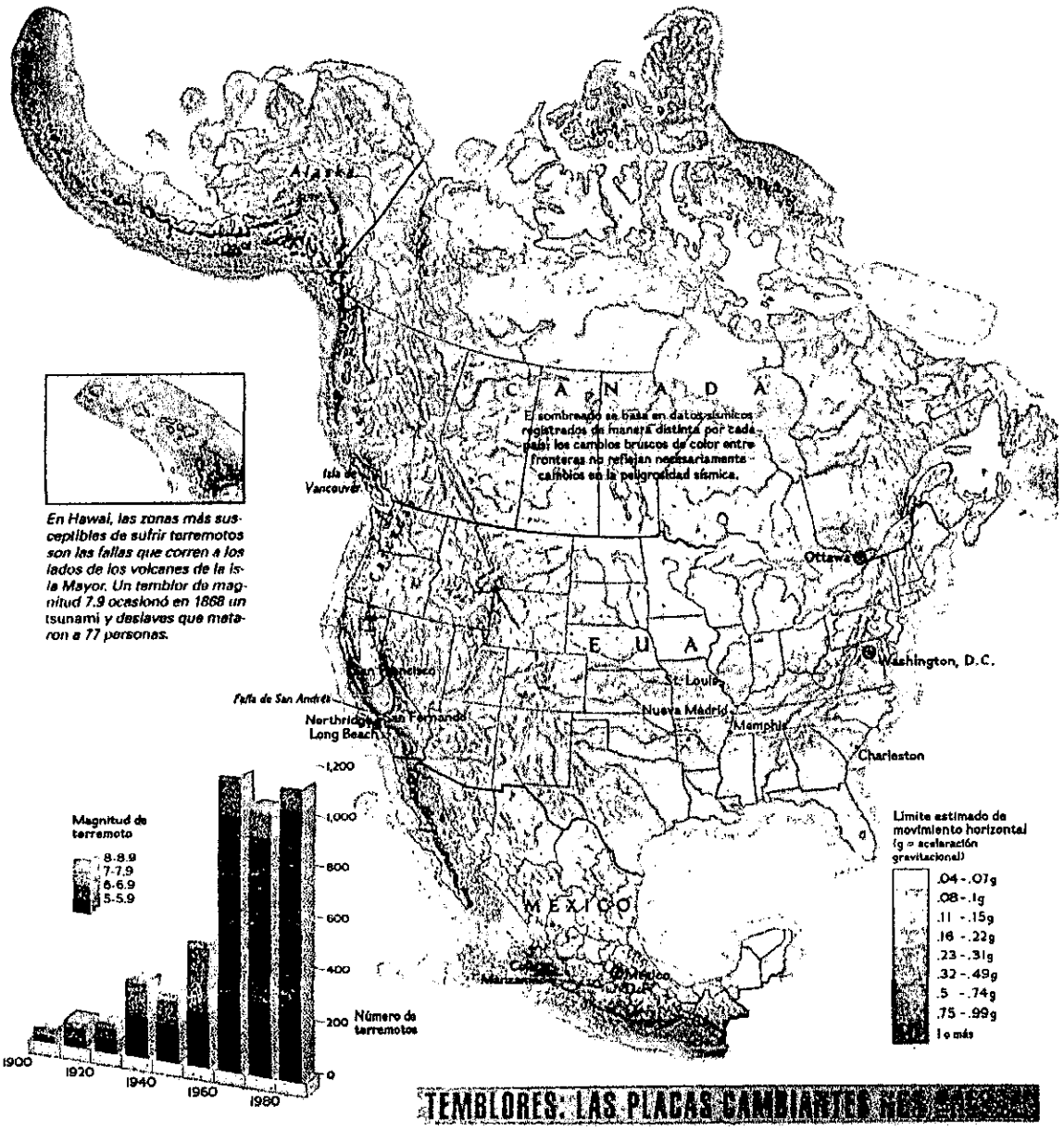
Destructividad

La destructividad de un sismo se determina fundamentalmente por la magnitud y naturaleza del proceso de ruptura, la distancia del epicentro a las áreas urbanas, la profundidad del foco, la respuesta local del suelo, la densidad de población y el tipo de destrucción.

Efecto de los sismos

La vulnerabilidad ante un sismo se ve reflejada en los principales componentes del sistema afectable, tales como:

- Vidas humanas: cuyas pérdidas son ocasionadas por derrumbes de construcciones, incendios y explosiones entre otros.
- Viviendas y edificios: la cimentación se desestabiliza y los elementos estructurales sufren fuerzas de corte y de tensión que causan agrietamientos e inclusive el derrumbe total de la estructura.
- Presas Hidráulicas: se afectan el piso, la cimentación, la estructura, ocasionando filtraciones en el vaso y la cortina, que reducen, en mayor o menor medida, su eficiencia de almacenamiento; las filtraciones también pueden provocar el derrumbe de la presa.
- Servicios Públicos: se afectan las redes o líneas vitales de agua potable, energía eléctrica, transporte y comunicaciones, trayendo como consecuencia la interrupción de los servicios y produciendo efectos secundarios, tales como incendios y paro de las actividades económicas e industriales



En Hawai, las zonas más susceptibles de sufrir terremotos son las fallas que corren a los lados de los volcanes de la isla Mayor. Un temblor de magnitud 7.9 ocasionó en 1868 un tsunami y deslaves que mataron a 77 personas.

Desde 1900 se han registrado 4,643 temblores mensurables en América del Norte; de ellos, la magnitud de 17 ha sido de ocho o más: uno en la costa occidental de Canadá, ocho en México y ocho en Alaska. El aparente aumento en el número de temblores se debe a los adelantos en los métodos de detección.

TEMBLORES: LAS PLACAS CAMBIANTES

El peligro de sufrir terremotos es mayor donde una placa tectónica choca contra otra, fricciona o pasa por debajo de ella. La subducción de placas bajo Alaska y el suroeste de México convierte estos puntos en los más propensos a ello del continente. Cada uno de estos lugares es azotado por más temblores intensos que el estado de California, cuya falla de San Andrés es también una zona sísmica activa. La ciudades del Pacífico noroeste, por otro lado, están amenazadas por la zona de subducción de Las Cascadas, que también hace de la población de la costa oeste de Canadá el grupo de mayor riesgo en todo ese país. Pese a ser menos activo sísmicamente, el este también ha sufrido temblores intensos; además, debido a que la roca subterránea de esa parte del territorio es más rígida que en el oeste, las ondas sísmicas llegan más lejos. Si los temblores que sacudieron Misuri en 1811 y 1812, (cuyas magnitudes fueron de 7.8 a 8.1) se repitieran, los daños alcanzarían desde Saint Louis hasta Memphis.

Figura 1. Sismos

➢ Vulcanismo

Descripción del Fenómeno

El transporte de los materiales terrestres desde el interior del planeta hasta la superficie, da origen al fenómeno conocido como vulcanismo. Aunque el vulcanismo comprende una serie de eventos diversos, las erupciones volcánicas constituyen el eje de interés de este tipo de manifestaciones y son, desde un punto de vista social, las que representan el mayor peligro para la población. Las erupciones volcánicas consisten esencialmente en la salida de materiales terrestres (magma) a través de un conducto o fisura en la corteza del planeta.

Riesgo Volcánico

El grupo de trabajo sobre Estudios Estadísticos de Peligros Naturales de la UNESCO, define el riesgo como la posibilidad de pérdida, tanto en vidas como en bienes o en capacidad de producción. Esta definición involucra tres aspectos relacionados por la siguiente fórmula:

Riesgo = vulnerabilidad x valor x peligro

En esta relación, el valor se refiere el número de vidas humanas amenazadas o, en general, a cualesquiera de los elementos económicos (capital, inversión, capacidad productiva, etc.), expuestos a un evento destructivo. La vulnerabilidad es una medida del porcentaje del valor que puede ser perdido en le caso de que ocurra un evento destructivo determinado. Por ejemplo la vulnerabilidad de las construcciones a la acción de flujos piroclastos es prácticamente del 100%, puesto que éstos causan la destrucción total a su paso; por el contrario, la vulnerabilidad a los materiales de caída (cenizas) depende del tipo de construcción y puede reducirse en aquellas diseñadas para disminuir su impacto y acumulación en los techos. En el caso de las vidas humanas, su vulnerabilidad se reduce si la población es evacuada oportunamente de las áreas de peligro. El último aspecto: peligro o peligrosidad, es la probabilidad de que un área en particular sea afectada por algunas de las manifestaciones destructivas del vulcanismo. Esta variable depende en general, de la actividad del volcán que causa el riesgo, ya sea por la probabilidad de que sufra un paroxismo destructivo por la proximidad y situación topográfica del sistema afectable considerado con respecto al volcán.

Clasificación de los volcanes

Los volcanes pueden ser clasificados de diversas maneras; así se habla de volcanes extintos y activos.

Zonas de Riesgo Volcánico

Volcanes monogenéticos y poligenéticos. Estos términos se aplican a los volcanes que muestran una o varias etapas de actividad respectivamente. Volcanes tales como el Jorullo o el Paricutín en el estado de Michoacán, fueron formados en un solo período eruptivo y es muy improbable que vuelvan a hacer erupción. Por el contrario, volcanes como el de Fuego o Colima en el estado de Colima, muestran una vida muy activa y sus edificios se han construido a través de una serie de erupciones.

En México se presentan ambos tipos de vulcanismo, ejemplo de ellos son los grandes volcanes del Cinturón Volcánico central. Asimismo, existen grandes campos monogenéticos en los estados de Colima, Jalisco, Guanajuato, Michoacán, Puebla y el Distrito Federal.

Erupciones Volcánicas

Se han clasificado los tipos o estilos de erupción utilizando para la nomenclatura, erupciones hawaianas, estrombolianas, vulcanianas, peleanas, merapianas, etc. Estos estilos se definen a continuación:

- Hawaiana: cuando el volcán arroja lentamente lava líquida poco espesa, sin escape explosivo de gases ni efusión de material sólido, la lava de esta actividad es muy fluida y caliente y la salida de los gases tiene lugar sin violencia catastrófica y raras veces con explosiones leves.
- Estromboliana: efusión de lava fluida o viscosa y explosiones no muy intensas con emisión de gases y material sólido; las nubes que produce la erupción son incandescentes
- Vulcaniana: efusión de lava viscosa que se solidifica rápidamente. Tiene explosiones fuertes con emisión de gases y fragmentos de roca. La roca es lanzada en dirección angular mientras que los gases se elevan en forma vertical desde el cráter, formando una nube densa y obscura en forma de coliflor
- Peleana: efusiones sin lava pero con gases y materiales sólidos. La mezcla de gases y partículas a altas temperaturas son arrojadas lateralmente en forma de nubes ardientes de alta peligrosidad para la zona cercana.
- Merapiana: erupciones que consisten en salida de lava muy viscosa que se derrama en forma de bloques por las laderas de un volcán. El nombre viene del volcán Merapi, en Indonesia, que presenta erupciones de este tipo; en nuestro país tenemos un ejemplo con el volcán de Colima.

De una manera general los estilos de erupción pueden clasificarse en tres grupos:

1. *Erupciones efusivas, si consisten esencialmente en la emisión sin violencia de lavas y gases*

2. Erupciones explosivas, cuando los materiales son arrojados violentamente; en este tipo de erupciones una gran proporción de materiales se encuentran en estado sólido.

3. *Erupciones mixtas, son aquellas que presentan características de las dos anteriores*

Un mismo volcán puede presentar durante su vida y aun durante una etapa activa varios estilos de erupción, aunque desde luego las erupciones de tipo hawaiano, por ejemplo, son características sólo de Hawai.

Entre los riesgos secundarios asociados a una erupción volcánica se encuentran los sismos y la deformación del terreno, las ondas de choque y la ocurrencia de rayos. Como se verá más adelante la amenaza que presentan es limitada pero no inexistente y puede causar ciertos daños.

Afectabilidad

De acuerdo a su actividad, los volcanes presentan tres niveles de riesgo:

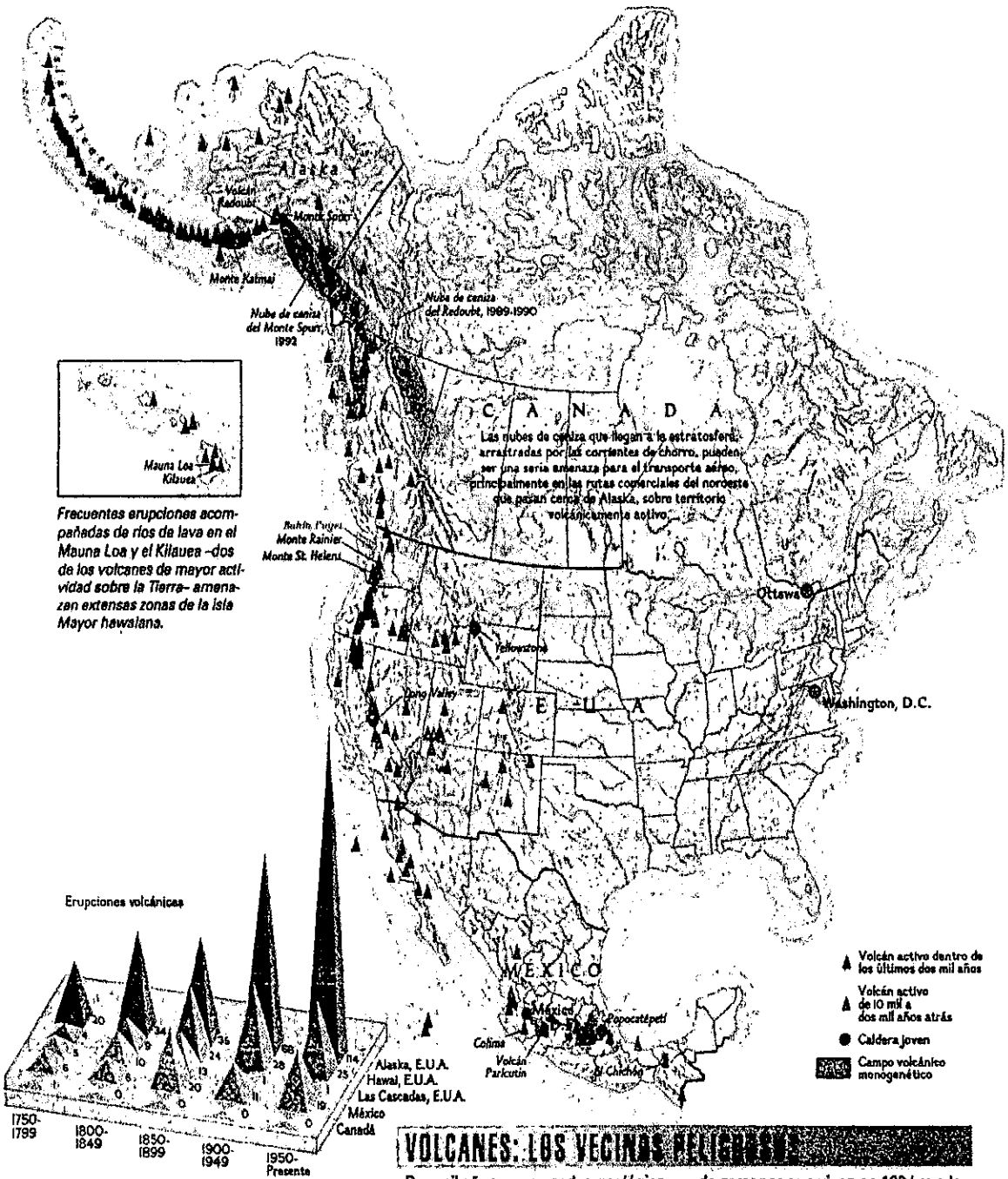
Alto Riesgo: Los volcanes de Colima
Popocatépetl
Pico de Orizaba
San Martín Tuxtla
Chichón
Tacaná y
La Primavera.

Riesgo Intermedio: El Ceboruco
El Sanganguey
El Paricutín
Jorullo
Xitle

Estos últimos como representantes de regiones monogéneticas; aunque el peligro asociado al vulcanismo monogénetico es difícil evaluar por la aparente ubicuidad de su ocurrencia dentro de campos de gran extensión como los señalados anteriormente, solo puede decirse a este respectoque existe una probabilidad significativa de nacimiento de un nuevo volcán. Sin embargo, dada la extensión del campo, para un lugar dado, dicha probabilidad es baja.

Riesgo Moderado: Tres Vírgenes
Barcena
Everman
Humeros

La Cordillera Neovolcánica o Faja Volcánica Mexicana, abarca completamente el territorio de dos entidades federativas y parte de otras 12, cuya población asentada en la zona de influencia se estima aproximadamente en 36 millones de habitantes, esta zona barca 610 municipios.



Según los registros de 250 años, América del Norte ha sufrido 454 erupciones volcánicas, 391 de ellas en lo que actualmente es Estados Unidos. El incremento aparente de los casos en Alaska se debe a que los métodos de detección han mejorado. Aunque a lo largo del siglo xx han estado tranquilos, los volcanes de Las Cascadas podrían volver a la vida.

VOLCANES: LOS VECINOS PELIGROSOS

Dos mil años: un parpadeo geológico rara vez tomado en cuenta al planear una construcción o un plantío. En Canadá, México y Estados Unidos ha habido 91 volcanes han entrado en actividad en los últimos dos mil años (74 de ellos en Estados Unidos, que lo convierten en el tercer punto candente del mundo); la mayoría se encuentra en zonas de subducción. Resulta particularmente *preocupante* el caso del volcán Popocatépetl, de México, que comenzó su actividad en 1994 y amenaza a 22 millones de personas que viven en 100 km a la redonda. En Las Cascadas, por otro lado, surge imponente el Rainier, capaz de producir detritos que llegarían hasta la bahía Puget. Los geólogos vigilan las calderas jóvenes que, como la de Yellowstone, en Wyoming, y la de Long Valley, en California, han mostrado actividad sísmica últimamente. Existen áreas llamadas campos monogenéticos, cuya actividad es *más difícil de* registrar pero que no dejan de ser peligrosas, como el Paricutín en México.

Figura 2. Volcanes

AGENTES PERTURBADORES DE ORIGEN HIDROMETEOROLOGICO

Dentro de la diversidad de calamidades, las de origen hidrometeorológico son las que más daños han acumulado a través del tiempo por su incidencia periódica en áreas determinadas del territorio nacional. Este tipo de fenómenos destructivos comprende: ciclones tropicales, inundaciones, nevadas, granizadas, sequías, lluvias torrenciales, temperaturas extremas, tormentas eléctricas, mareas de tempestad e inversiones térmicas.

A continuación se tratan por su importancia los primeros cinco fenómenos anunciados.

CICLON TROPICAL

Descripción del fenómeno

Ciclón tropical es el nombre genérico que se le da a cualquier perturbación atmosférica, desde que tiene características de una depresión hasta que evoluciona a huracán. Los ciclones tropicales son fenómenos naturales que se originan y desarrollan en mares de aguas cálidas y templadas, con nubes en espiral. Generalmente su diámetro es de unos cientos de kilómetros, con presiones mínimas en la superficie, vientos violentos y lluvias torrenciales, algunas veces acompañadas por tormentas eléctricas; tienen una región central conocida como ojo de huracán o vórtice, con diámetro de algunas decenas de kilómetros, vientos débiles y cielos ligeramente nublados.

Desde siempre los ciclones tropicales han tenido fama de ser devastadores y el esfuerzo del hombre por mitigar sus efectos ha sido contante. Cuando un ciclón tropical se desplaza muy próximo a las zonas costeras, o penetra en tierra firme, es capaz a de originar daños a la población y a sus bienes, debido ala generación de cualquiera de las siguientes situaciones: marea de tempestad, de hasta 6 m de altura, vientos fuertes con ráfagas hasta de 360 km./ h, e inundaciones. Los costos directos causados por los daños en la producción agrícola, en la infraestructura y en otros renglones de la economía nacional, ante la presencia de estos meteoros, anualmente pueden sumar miles de millones de pesos. Por fortuna, el costo invaluable por los daños causados a las vidas humanas se ha visto reducido, gracias al mejoramiento de los sistemas de detección y aviso que han desarrollado organizaciones locales e internacionales responsables en la materia, así como de las acciones de prevención civil.

A continuación se describe la evolución de un ciclón tropical.

Depresión tropical

Se considera tal cuando la velocidad promedio, durante un minuto, de los vientos máximos de superficie en la perturbación, es menos o igual a 62 km/h.

Tormenta tropical

Se determina cuando la velocidad promedio, durante un minuto, de los vientos máximos de superficie es de 63 a 118 km/h. En esta fase evolutiva se le asigna un nombre por orden de aparición anual y en términos del alfabeto, de acuerdo a la relación determinada para todo el año, por el Comité de Huracanes de la Asociación Regional IV Región (asociación mundial en la que en la República Mexicana se ubica en la IV Región.

Huracán

Es un ciclón tropical en el que la velocidad promedio, durante un minuto, de los vientos máximos de superficie, es igual o mayor a 119 km/h.

Ubicación Geográfica

Los huracanes que afectan a nuestro país directa o indirectamente, se originan en cuatro zonas principales:

- Golfo de Tehuantepec
- Sonda de Campeche
- El Caribe
- La Región Atlántica

En función de las condiciones climatológicas, siguen trayectorias más o menos definidas, y en ocasiones erráticas, pudiendo penetrar o no a tierra firme. Las áreas de la República Mexicana regularmente afectadas por las perturbaciones ciclónicas abarcan más del 60% del territorio nacional.

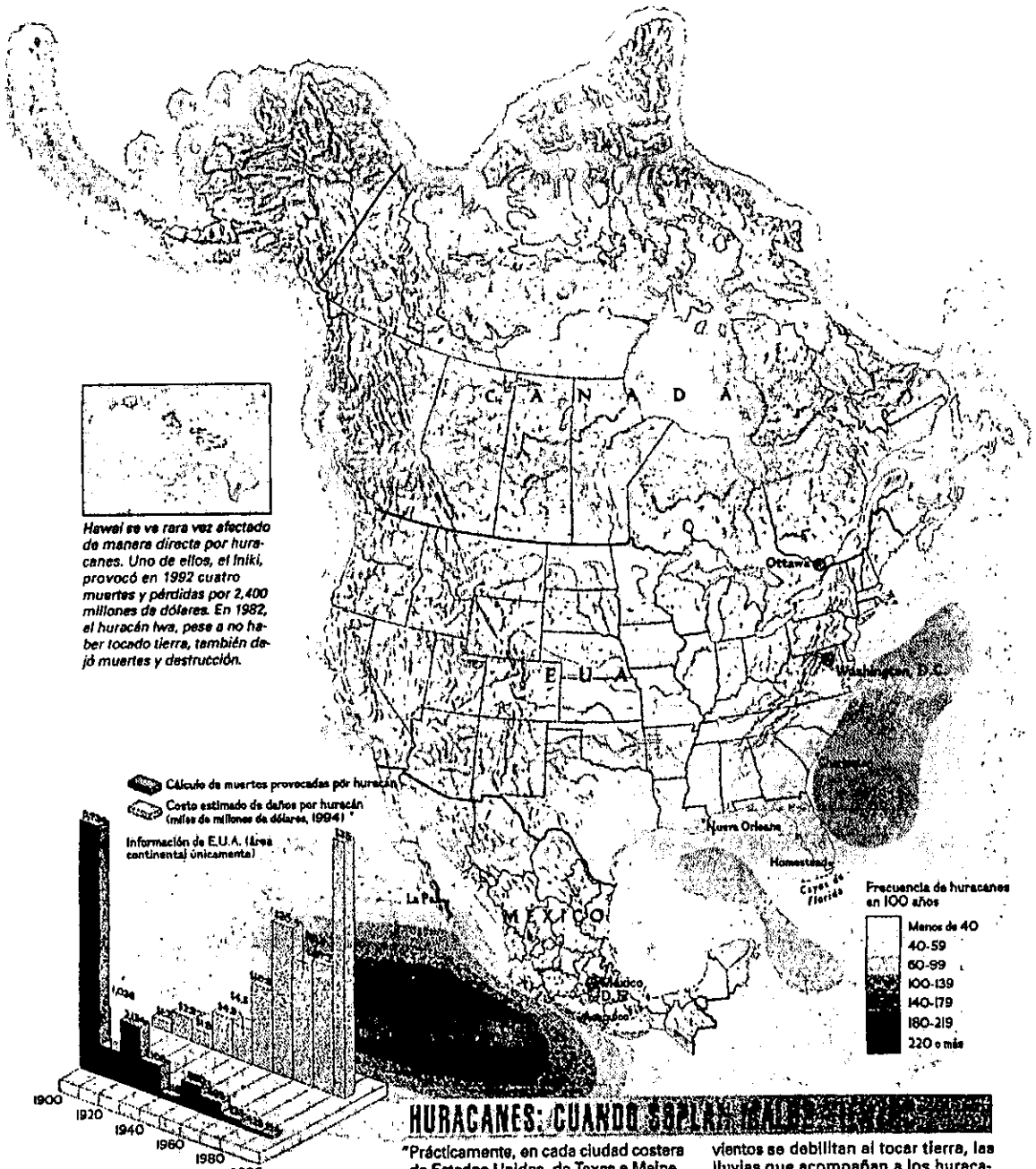
Afectabilidad

En las últimas décadas, con un proceso de urbanización acelerado, se han vuelto más evidentes los daños potenciales que pudieran provocar los ciclones tropicales en áreas de grandes concentraciones humanas.

Asimismo, pueden verse afectados los medios de comunicación y los transportes aéreo, terrestre, fluvial y marítimo.

Con base a las zonas de ingreso, se infiere que los estados de Baja California sur, Michoacán, Sinaloa, Sonora y Tamaulipas, presentan una mayor recurrencia de dichas penetraciones (2 a 4 años). En otras entidades, la recurrencia de penetración ciclónica oscila entre los 5 y 7 años; en ellas se estima que aproximadamente 2 millones de personas están expuestas a sufrir sus efectos. Este grupo lo integran los estados de Baja California, Campeche, Colima, Quintana Roo y Jalisco, en cuyos 19 municipios costeros se asienta el 26.3% de su población total.

Por último, el grupo conformado por las entidades de Nayarit, Guerrero, Tabasco, Oaxaca, Veracruz, Chiapas y Yucatán, tienen un período de recurrencia o penetración de ciclones de 8 a 26 años.



Hawai se ve rara vez afectado de manera directa por huracanes. Uno de ellos, el Iniki, provocó en 1992 cuatro muertes y pérdidas por 2,400 millones de dólares. En 1982, el huracán Iwa, pese a no haber tocado tierra, también dejó muertes y destrucción.

Aunque la tecnología aplicada a la detección de huracanes ha permitido disminuir el número de muertes, el desarrollo de las regiones costeras ha permitido que más gente esté expuesta a los huracanes y los daños sean mucho mayores. Las pérdidas sufridas durante los noventa rebasan la suma de las dos décadas anteriores.

HURACANES: CUANDO SOPLAN [illegible]

"Prácticamente, en cada ciudad costera de Estados Unidos, de Texas a Maine, se está en camino a un desastre por huracán." Con esta frase termina un reporte de la Administración Nacional Oceánica y Atmosférica (NOAA). Las poblaciones costeras son vulnerables a las inundaciones ocasionadas por tormentas, que provocan 90 por ciento de las muertes por huracán.

Florida, Texas, Luisiana y las Carolinas se llevan la peor parte, sobre todo entre agosto y septiembre. Si bien los vientos se debilitan al tocar tierra, las lluvias que acompañan a los huracanes pueden causar severas inundaciones hasta el interior de Canadá. De los que se forman en el Pacífico y el Atlántico –en el primero el número casi dobla al del segundo– la mayoría se interna en el mar sin representar ya peligro alguno. En promedio, 1.6 huracanes tocan tierra estadounidense cada año. Aun así, los vientos, la lluvia y los tornados ocasionan graves daños a cientos de kilómetros del ojo del huracán.

Figura 3. Huracanes

➢ Inundaciones

Se considera inundación al flujo o la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta o insuficiencia de drenaje tanto *natural como artificial.*

Las inundaciones generalmente son consecuencia directa de otros fenómenos hidrometeorológicos y, en ocasiones, son inducidas con fines técnicos y de beneficio económico social. En general la magnitud de una inundación provocada por calamidades depende de la *intensidad de las lluvias, de su distribución en el espacio y tiempo, del tamaño de las cuencas* hidrológicas afectadas, así como las características del suelo y del drenaje natural o artificial de las cuencas.

Las inundaciones pueden clasificarse por su origen como pluviales, fluviales y lacustres.

- *Pluviales: se deben a la acumulación de la precipitación (lluvia, granizo y nieve,* principalmente), que se encuentra en terrenos de topografía plana o en zonas urbanas con insuficiencia o carencia de drenaje.

- Fluviales: son aquellas que se originan cuando los escurrimientos superficiales son mayores a la capacidad de conducción de los cauces.

- Lacustres: se originan en los lagos o lagunas por el incremento de sus niveles y son peligrosas por el riesgo que representan para los asentamientos humanos cercanos a las áreas de embalse.

Las causas generadoras de inundaciones son:

- Lluvias Intensas
- Ciclones Tropicales
- Tormentas Puntuales
- Granizo
- Nieve
- Presas

Daños causados por inundaciones

Directos: Consisten principalmente en el menoscabo físico de las propiedades y de la producción. Las actividades y bienes que en mayor medida pueden ser afectados por ese tipo de daño son: la agricultura, la ganadería, la silvicultura, la industria, el comercio, las obras públicas y las edificaciones.

Indirectos: Son las pérdidas económicas de los productos y servicios de una región derivadas de la interrupción temporal de las actividades agropecuarias, forestales, industriales y de comercio. También se incluye dentro de este concepto, el gasto que se destina para la ayuda a los damnificados.

Intangibles: Dentro de este concepto se engloban los damnificados, los heridos y las pérdidas de vidas humanas.

Ubicación Geográfica

En las regiones del país donde el período de lluvias es más prolongado y abundante, como sucede en la llanura de Tabasco, los ríos son permanentemente caudalosos. En el territorio nacional existen 47 ríos importantes, mismo que fluyen en tres diferentes vertientes: del Golfo, del Pacífico y del Interior.

- **Sequías**

La sequía es el agente destructivo que se caracteriza por la falta de agua en el suelo, afectando la vegetación, ya que ésta pierde el agua por la evaporación o debido a que la precipitación en una etapa es menor que su promedio característico. Cuando esta deficiencia es prolongada, daña las actividades humanas y económicas, así como el equilibrio de los ecosistemas.

La clasificación de las sequías se realiza en función del clima prevaleciente o por su magnitud.

Por clima

- Permanentes: se producen en zonas de climas áridos
- Estacionales: se observan en sitios con temporadas lluviosas y secas bien definidas
- *Contingentes: se presenta en cualquier época del año debido a períodos prolongados de* calor, a falta de lluvias o a la coincidencia de ambos
- Invisibles: ocurren cuando las lluvias del verano no cubren las pérdidas de humedad por evaporación.

Por magnitud

- Leves: son aquellas que tienen como causa la escasez parcial de lluvias y no repercuten de manera importante en la producción ni en la economía.
- Moderadas: son las originadas por una disminución significativa en la precipitación pluvial que afecta a la producción agrícola.
- Severas: son las que se producen por la disminución general o total de lluvias, con daños cuantiosos a la producción.
- Extremadamente severas: son producto del proceso permanente de escasez de agua que provoca crisis en la agricultura y en la ganadería, con los consiguientes efectos al conjunto de la economía y la sociedad.

Efectos de los daños

- Desequilibrio ecológico

  Genera deshidratación y muerte de la flora; migración y/o muerte de la fauna; degradación y/o destrucción de los bosques, y debilitamiento, aridez y desertificación de los suelos.

- Deterioro de la producción agrícola

  Genera pérdida de cultivos y el consecuente empobrecimiento de los campesinos; escasez de alimentos que deriva en desabasto y encarecimiento de los productos, provocando acaparamiento y especulación.

- Disminución del hato ganadero

Provoca pérdida de animales, por animales y aparición de epidemias.

- Reducción de la actividad industrial

  Redunda en cortes de producción y descenso en la calidad de los productos, lo cual repercute en la capacidad de expansión de la economía, en los niveles de captación de divisas y en la generación de empleos, principalmente.

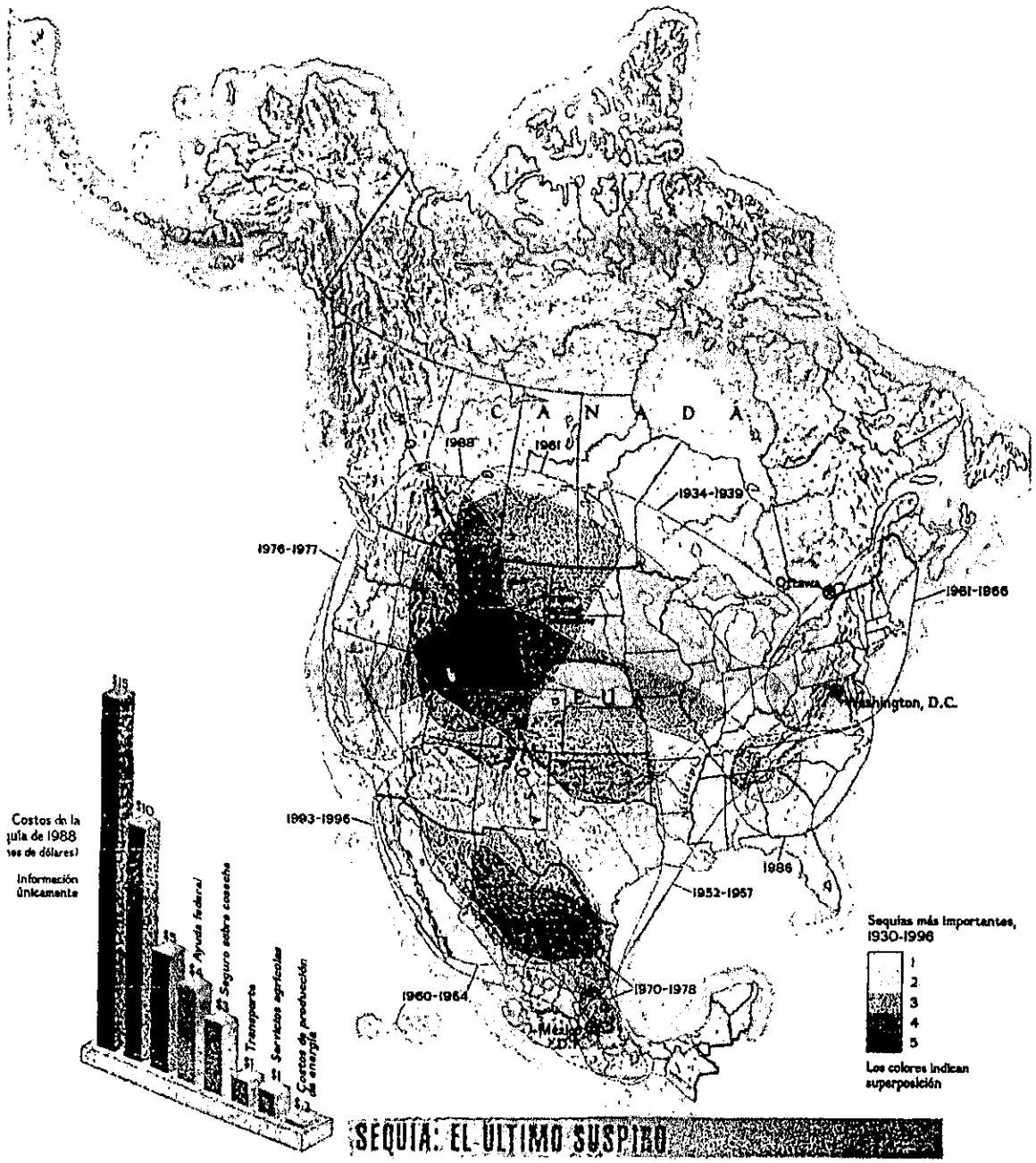
- Deterioro de los rangos de salud pública

  Provoca falta de higiene y sus consecuencias en la generación de epidemias, hambrunas y mortandad.

- Migración campesina

  Genera migraciones masivas del área rural ante las condiciones negativas de subsistencia

Las entidades en las que se presenta el mayor número de sequías anuales son: Coahuila, Guanajuato, Durango, Zacatecas, Guerrero, Jalisco, Tamaulipas, Nuevo León, San Luis Potosí y Querétaro.



SEQUÍA: EL ÚLTIMO SUSPIRO

La sequía de 1988 ha sido el desastre natural más costoso para Estados Unidos. La pérdida de las cosechas equivalió a poco menos de la mitad de pérdidas de 39,200 millones de dólares, los incendios consumieron 5 millones de hectáreas, la energía hidroeléctrica cayó y el tránsito del Misisipi disminuyó en unos 220 millones de dólares.

Las sequías se forman con más lentitud, se expanden con mayor alcance, duran más tiempo y afectan más vidas que ningún otro desastre natural. Las regiones más afectadas por sequías son las praderas canadienses, el oeste y el centro de Estados Unidos y el centro-norte de México. Las cosechas se pierden, los precios de los alimentos se disparan, el ganado muere de hambre, los mantos freáticos desaparecen, los incendios estallan y el calor cobra vidas humanas. La sequía más tristemente célebre, conocida como Dust Bowl ("El tazón de polvo"), que ocurrió en los años treinta, consumió las cosechas desde las praderas canadienses hasta las grandes planicies. En México, la sequía vivida entre 1960 y 1964 devastó la ganadería. Una atroz sequía dejó a Yellowstone en brasas en 1988 y entre 5 mil y 10 mil muertes provocadas por el calor. Los periodos naturales de poca lluvia y la creciente competencia por los pocos suministros de agua reflejan que la vulnerabilidad ante las sequías crece.

For information about available maps write to National Geographic Society, P.O. Box 11650, Des Moines, IA 50350-1650.
You can reach us on the World Wide Web at www.nationalgeographic.com.

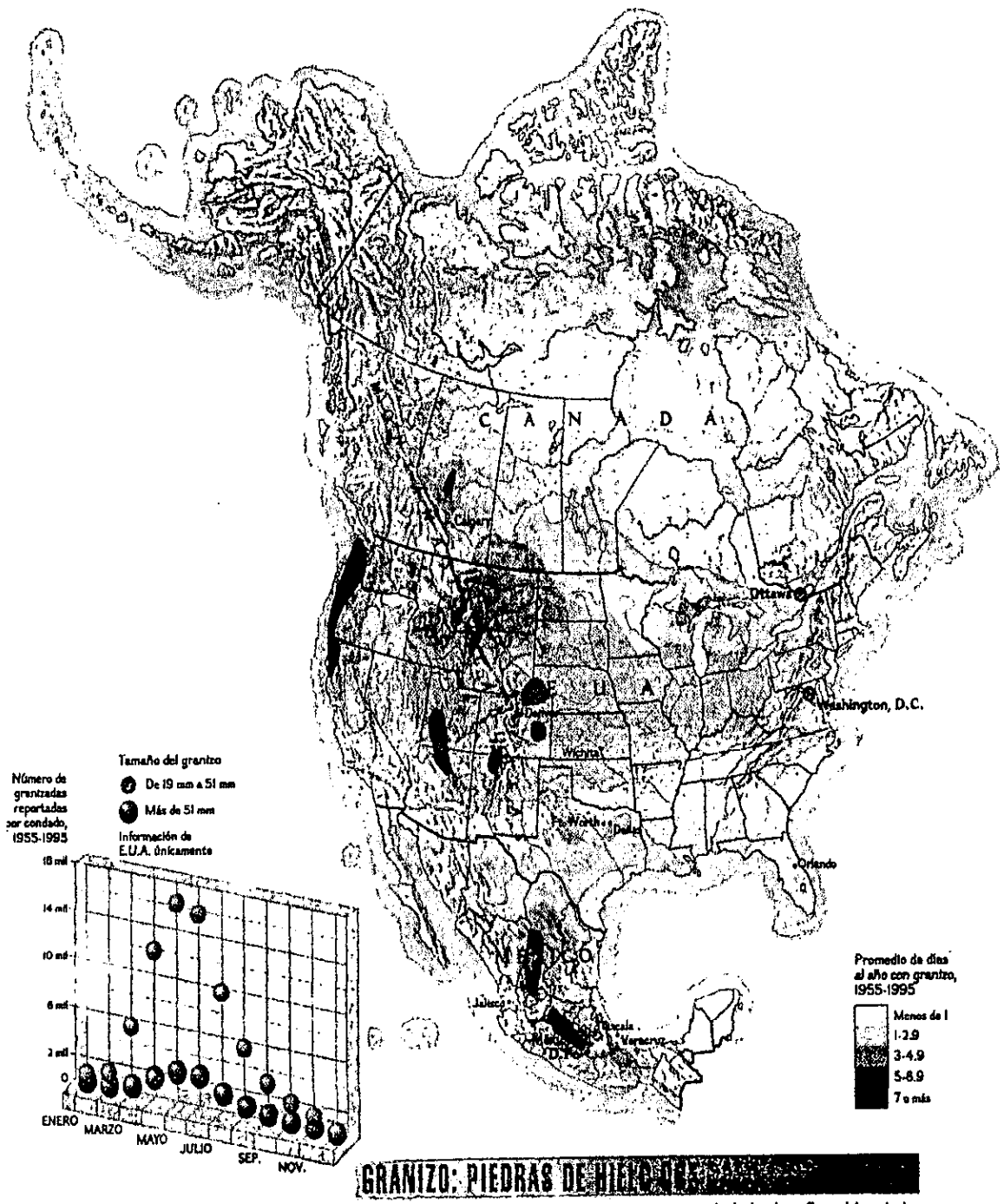
Figura 4. Sequía

➢ **Tormentas de Granizo y Nevadas**

Las tormentas de granizo son precipitaciones sólidas en forma de granos de hielo que están relacionadas con tormentas eléctricas. En función de la cantidad y el tamaño del granizo, será la magnitud del posible daño. En las zonas rurales, destruyen las siembras y plantíos y en ocasiones provocan pérdidas de animales de cría. En las zonas urbanas provoca problemas de tránsito, daños a las viviendas, construcciones y áreas verdes, debido a su acumulación cobre techos y a la obstrucción del sistema de drenaje, lo que provoca inundaciones de duración relativamente larga.

La nevada se define como una precipitación de cristales de hielo. En México tiene su origen en las masas de aire provenientes del Artico, de Alaska y de la región noreste de Canadá. Ocurre cuando las condiciones de temperatura y presión referidas a la altitud de un lugar y al cambio de humedad del ambiente, se conjugan para propiciar la precipitación de la nieve.

Las entidades federativas que sufren comúnmente este tipo de situaciones son: Coahuila, Chihuahua, Durango, Sonora y Guanajuato.



GRANIZO: PIEDRAS DE HIELO

Agradables tardes de mayo y junio han presenciado las casi 91 mil granizadas reportadas desde 1955. Los daños materiales comienzan por lo general cuando el granizo alcanza 2 cm de grosor. El más grande registrado hasta ahora se encontró en Kansas en septiembre de 1970: 19 cm de diámetro y pesaba 766 gramos.

En el noroeste del continente, el granizo es suave y pequeño. Cerca de las Rocallosas –desde Alberta hasta las altas planicies de Texas– el granizo es pesado y cae con una fuerza fatídica que mata al ganado y destruye las cosechas, los autos y los tejados. "Nos hemos expuesto más al granizo al construir blancos más grandes", dice el climatólogo estadounidense Stanley Changnon respecto a la contradicción entre el número estable de granizadas y el enorme aumento en los daños. A medida que las ciudades han florecido a lo largo del cinturón de granizo, los daños materiales han igualado a los que padecen las cosechas, cerca de 2,300 millones de dólares. En Canadá, las pérdidas en las cosechas suman 175 millones de dólares. Sin ser necesariamente un peligro letal, en los noventa el granizo ha causado la muerte de ocho personas en Estados Unidos; en 1976 mató a 12 en México, D.F. Sembrar las nubes ha resultado un buen método de eliminación del granizo.

Figura 5. Granizo

GLOSARIO

Administración de la Seguridad

La *administración de seguridad consiste en las prácticas de manejo y procedimientos* operacionales usados para suministrar un nivel aceptable de protección al medio ambiente. En suma, los controles administrativos incluyen procedimientos establecidos para asegurar que todo el personal que tiene acceso a los recursos del sistema, tenga las autorizaciones requeridas y privilegios apropiados requeridos para realizar sus tareas.

Administración de Alertas

Este proceso de seguridad está compuesto por mecanismos que automáticamente detectan violaciones de seguridad, e informan a los administradores de seguridad y otras partes interesadas. Las alertas surgen, por lo general, basadas en información acordada con los propietarios, auditores y administradores de seguridad sobre la auditabilidad de la información.

Administración de Auditoría

La *administración de auditoría es el componente de la seguridad, que consiste en aquellas* actividades que habitualmente capturan y acumulan información relativa a seguridad, sobre la actividad de los sistemas. La información auditada puede ser usada para generar informes de auditoría de rutina describiendo las actividades del sistema, generar alertas sobre violaciones a la seguridad o intentos de violación que son enviados a los administradores de seguridad, provee *pistas de auditoría que pueden ser usadas para trazar actividades del sistema, siguiendo una* violación al mismo y suministra información a auditores externos quienes demostrarán el nivel del sistema de acatamiento con las políticas de seguridad y prácticas de seguridad generalmente aceptadas.

ALE (Annual Loss Expectancy)

El ALE *es una fórmula que nos permite determinar el costo de la pérdida anual esperada de una* aplicación u activo considerando dos factores: el impacto (costo) y la frecuencia

Amenaza

Una amenaza es un evento que puede causar daño a un sistema de información, las amenazas pueden ser causadas por diversos factores como pueden ser: Naturales (ejemplo: Terremotos, inundaciones) Intencionales (personas inconformes dentro de la misma empresa, hackers), Operacionales, Legales, Sociales, Políticos, etc.

Análisis del riesgo

Identifica, analiza y documenta las amenazas a la seguridad del negocio, evalúa el nivel de exposición en el que queda la organización por cada riesgo asumido y determina el grado de importancia para la eliminación de cada uno de ellos. También ayuda a identificar a los propietarios de la información de negocio (entendemos por propietario a los ejecutivos responsables por el origen de la información). La evaluación del riesgo provee la base para desarrollar políticas de seguridad

Análisis del Riesgo Cuantitativo

Es la cuantificación de las probabilidades de ocurrencia de un evento por medio de la asignación de un factor de probabilidad que representa un período de tiempo específico. El análisis del riesgo cuantitativo se utiliza principalmente para el desarrollo de tablas actuariales de seguros.

Análisis del Riesgo Cualitativo

Es la cualificación de las probabilidades de que una situación específica pueda ocurrir o recurrir por medio de la asignación de probabilidad alta, mediana o baja. El análisis del riesgo cualitativo se utiliza principalmente para el análisis del riesgo puramente físicos o lógicos con objeto de establecer las medidas preventivas o correctivas apropiadas así como diseñar, evaluar y adoptar las alternativas necesarias

Aplicación(es).

Conjunto de programas que definen una función de negocio o de uso común

Auditoria de Seguridad

Establece servicios y mecanismos de revisión que permitan asegurar el total cumplimiento de las políticas, procedimientos y estándares de seguridad vigilando su ejecución tanto por personal interno como externo en la integración de nuevas tecnologías, aplicaciones y servicios.

Autenticación

Asegura que el mensaje es genuino, que sea recibido exactamente como fue enviado y provenga de la fuente declarada. Puede incluir la verificación de la identidad de un individuo o entidad. El servicio de autenticación puede ser de dos tipos: Autenticación de origen de datos y Autenticación de entidades

Autenticación de Origen de Datos

Es la corroboración de que la fuente de los datos es quien presume ser. Los mecanismos para este tipo de autenticación están basados en tres tipos de información:

- Quién eres, basados en información tal como huellas digitales o firmas
- Qué posees, como una tarjeta de identificación o una llave física
- Qué conoces, como un número de identificación personal o las respuestas a otras preguntas.

Autenticación de Entidades

Es la corroboración de que una entidad envuelta en una comunicación o asociación es quién dice ser.

Bienes

Aquello que la compañía posee, opera, controla, custodia, compra, vende, diseña, produce, analiza, prueba o mantiene

Certificación de Seguridad

El proceso de Certificación de un sistema de seguridad, asegura que ninguna de las partes en una conversación entre un programa cliente y un programa servidor podrán ignorar la existencia de una comunicación. La certificación es importante cuando es necesario para cualquiera de las partes demostrar el haber utilizado un mecanismo de comunicación

Ciclo de Vida

Es el período de tiempo que empieza cuando el producto de software es identificado y termina cuando el producto ya no es utilizable. El ciclo de vida del software tipicamente incluye las fases de requerimientos, diseño, desarrollo, pruebas, instalación y puesta en marcha, mantenimiento y baja del producto.

Clasificación de la Información

La clasificación de la información ayuda a identificar como es que ésta debe ser manejada dentro de la organización.

Concientización de la Seguridad

Involucra un programa continuo diseñado para capacitar y crear consciencia en el personal sobre la importancia de la seguridad y acerca de las herramientas y técnicas para reforzar las políticas de seguridad. Los programas de toma de conciencia están dirigidos a, políticas y procedimientos efectivos orientados hacia el sistema, hacia el ambiente de trabajo, estilo de trabajo y procedimientos de seguridad.

Confidencialidad

Propiedad de la información que garantiza que la información no estará disponible o será divulgada a individuos, entidades o procesos no autorizados

Control de Acceso

Protege los recursos del sistema asegurando que estos sólo puedan ser utilizados por individuos o programas autorizados. Las técnicas de control de acceso pueden utilizarse para proteger a una variedad de recursos incluyendo hardware, sistemas operativos, centros de comunicaciones, programas y archivos o bases de datos.

Criptoseguridad

Componente de la seguridad de comunicaciones que resulta de la provisión de sistemas de cifrado y su uso apropiado.

Disponibilidad

Asegura que todas las facilidades del sistema, incluyendo servicios de seguridad, estén disponibles al ser requeridos para las aplicaciones de negocio y para la infraestructura del sistema. La disponibilidad puede ser mejorada al desarrollar mecanismos que reduzcan el peligro de daños a la integridad del sistema y también al colocar servicios de seguridad redundantes en las diferentes plataformas.

Estructura y Organización

Consiste en la organización y el personal que es responsable de identificar y analizar las amenazas a la seguridad, desarrollar políticas de seguridad, auditar la práctica de seguridad, y responder a las violaciones de seguridad.

Información Confidencial

Es aquella que, de ser conocida por terceros, podría dar lugar a ventajas indebidas a los competidores o bien ser perjudicial para alguna organización o sus empleados.

Información Interna

Es aquella que se genera dentro del flujo normal de trabajo y se difunde una forma mas o menos amplia entre determinadas personas o áreas de una organización.

Información Pública

Corresponde a la información que los canales autorizados de la organización han dado a conocer a los medios masivos de comunicación o a entidades externas con el propósito específico de darle amplia difusión.

Ingeniería de Seguridad

Efectuar estudios de investigación continua para supervisar el desarrollo tanto de nuevas tecnologías de seguridad, como de prácticas utilizadas para infringirlas

Integridad

El componente de integridad de un sistema de seguridad intenta asegurar que la información y las comunicaciones no puedan ser cambiadas. También asegura que los cambios no autorizados a la información y comunicaciones sean detectables aunque no sean reversibles.

Listas de Control de Acceso

Son listas que contienen información acerca de cuáles usuarios o programas, tiene acceso a qué recursos de información y los tipos de acceso permitidos (lectura, escritura, borrar, crear, etc.)

Manejo de Políticas

Define las políticas de seguridad que serán administradas, publicadas como parte del proceso de toma de concientización de la seguridad y ejecutadas con procedimientos manuales y automatizados.

Mapas de Riesgos

Los mapas de riesgos tienen como objetivo identificar, de acuerdo al tipo de riesgo y su grado, determinadas zonas en un área específica y tomar acciones determinadas a su prevención, control o disminución del riesgo.

Mecanismos de Seguridad

Son aquellas herramientas y técnicas usadas para implementar los servicios de seguridad. La necesidad de seguridad del negocio son las que determinan cuál de ellas usar.

Medición del Riesgo

Es un elemento esencial para determinar el costo de un evento desfavorable para la organización como puede ser cualquier interrupción en algún servicio o la caída de uno o varios sistemas informáticos, además calcula el período de tiempo en que pudiera ocurrir otro evento no deseado.

Medidas de Prevención

Las medidas de prevención o corrección del riesgo son recomendaciones que tienen como finalidad el consolidar, coordinar, mejorar o crear medidas de protección ante los riesgos identificados, las cuales tienen que tener como característica principal la eficiencia para nuestro negocio ya que este es el punto de partida del cual se podrá establecer su costo – beneficio

Objetos de Seguridad

Son aquellos recursos que pueden ser utilizados por cualquier componente del sistema para verificar la autenticación de usuarios, control de acceso a recursos, integridad, confidencialidad de información. Dentro de los diferentes objetos de seguridad podemos encontrar: claves de usuarios, passwords, atributos por usuario, niveles de acceso, llaves de encripción, etc.

Pérdidas

Aquellas evidencias empíricas que puedan establecer la frecuencia, magnitud de las pérdidas basadas en las experiencias propias y las de los competidores.

Propietario

Poseedor al más alto nivel de responsabilidad respecto a la disponibilidad, confidencialidad e integridad de la información y decidir quién debe tener acceso a ella y cual debe ser la autorización de acceso sobre ella

Pruebas de sistema

Categoría de pruebas donde participa una combinación de pruebas en un ambiente muy similar a producción que incluyen pruebas funcionales y de convivencia con otros sistemas y que al ser realizadas exitosamente, aseguran que el sistema cumple con los requerimientos.

Recuperación en Caso de Desastre

El proceso de recuperación de la seguridad incluye la estructura, procedimientos y actividades necesarias para restaurar el sistema después de que su integridad haya sido comprometida o un desastre mayor haya ocurrido.

Seguridad de Cómputo

Son los dispositivos tecnológicos y procedimientos administrativos que pueden ser aplicados a hardware, programas y datos para asegurar la disponibilidad, integridad y confidencialidad de los recursos de cómputo, asegurando también que las funciones comprometidas sean realizadas como fueron planeadas.

Seguridad de Comunicaciones

Son las medidas de protección tomadas para negar a personas no autorizadas información valiosa que pueda derivarse de la posesión y estudio de las telecomunicaciones. Y son el resultante de aplicar: Criptoseguridad, Seguridad de Transmisión y Seguridad de Emisión a las telecomunicaciones y de la aplicación de medidas de seguridad física a la información de seguridad de comunicaciones.

Seguridad de Información

Son los procedimientos y acciones diseñados para prevenir los intentos no autorizados de divulgación, transferencia, modificación o destrucción de información, ya sea accidental o intencional.

Seguridad de Emisión

Componente de la seguridad de comunicaciones que resulta de todas las medidas tomadas para negar a personas no autorizadas información valiosa que pueda derivarse de la intercepción y análisis de las emisiones efectuadas del equipo de cifrado y de los sistemas de telecomunicaciones.

Seguridad Física

Componente de la seguridad de comunicaciones que resulta de todas las medidas físicas necesarias para salvaguardar equipo, material y documentos clasificados, del acceso u observación de personas no autorizadas

Seguridad de Transmisión

Componente de la seguridad de comunicaciones que resulta de todas las medidas diseñadas para proteger las transmisiones de intercepciones y explotación no autorizadas.

Servicios

Aquello que la compañía expone o pone a servicio y que pueda causar o contribuir a sufrir daños, robos, pérdidas ó que causen injurias personales a empleados de la organización

Validación

La fase de pruebas del ciclo de vida que asegura que el producto final cumple con las especificaciones.

Verificación

Todas las actividades de control de calidad a través del ciclo de vida que aseguran que los productos intermedios cumplan con sus especificaciones.

Vulnerabilidad

Es una debilidad en los procedimientos de seguridad en los sistemas, diseño de hardware, controles internos, etc., los cuales pueden provocar el acceso a recursos no autorizados o información sensitiva.

Bibliografía

- F Broder, James. Risk Analysis and the Security Survey, Butterworth Heinemann, Second Edition, 1999

- Krause, Micki. Tipton, Harold. Handbook of Information Security Management 1999, Auerbach

- Secretaría de Gobernación, Atlas Nacional de Riesgos, Diciembre de 1991

- Rosales Herrera, Humberto David. Determinación de Riesgos en los Centros de Cómputo, Editorial Trillas, Primera edición 1996

- Oxenfeldt, Alfred. Análisis de Costo - Beneficio para la toma de decisiones (El peligro del simple sentido común), Editorial Norma, Edición 1985

- Summers C, Rita. Secure Computing (Threats and Safeguards), MacGraw-Hill, First Edition, 1997

- IBM Learning Services, Plan de Recuperación de Operaciones, 1999

- Purpura P., Philip. Security and Loss Prevention (an introduction), Butterworth-Heinemann, Third Edition

- Fites, Phillip, and P. J. Kratz ,Martin. Information Systems Security (A Practitioner's Reference), Van Nostrand Reinhold (VNR)

Sitios en Internet

- National Institute of Standards and Technology http://csrc.nist.gov/publications/

  Organismo estadounidense que trabaja con el sector industrial y gubermental para establecer sistemas tecnológicos para la seguridad de la información a fin de proteger la integridad, disponibilidad y confidencialidad de la información.

- General Accounting Office (GAO) http://www.gao.gov

  La GAO se encarga de realizar evaluaciones, auditorias, análisis e investigaciones para promover los valores de la disponibilidad, integridad y confiabilidad de la información proporcionando a través de su trabajo políticas y disposiciones legales para el buen manejo de la información.

- Risk World http://www.riskworld.com/books/topics

  Sitio en donde puede encontrarse con reportes de incidentes de seguridad ocurridos en todo el muendo, además es una buena guía para encontrar publicaciones acerca del análisis del riesgo lógico.

- Computer Security Resource Center http://csrc.nist.gov/

  Sitio en donde se localizan referencias sobre los actuales productos de seguridad para los sistemas de cómputo además de las más recientes investigaciones de seguridad.

- Centro Nacional de Prevención de Desastres http://www.cenapred.unam.mx/

  Promueve la aplicación de las tecnologías para la prevención y mitigación de desastres; impartir capacitación profesional y técnica sobre la materia, y difundir medidas de preparación y autoprotección entre la sociedad mexicana expuesta a la contingencia de un desastre

- Banco de México http://www.banxico.org.mx

  Organismo Regulador de las Instituciones Financieras de México.