UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ELEMENTOS PARA EL DIAGNOSTICO DE RIESGOS EN INFORMATICA

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

JOSE ANTONIO JESUS FLORES TORRES

DIRECTORA DE TESIS:

M. en C. MARIA GUADALUPE ELENA BARRIENTOS GONZALEZ

2000

FACULTAD DE CIENCIAS
SECCION ESCOLAR

VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis:

"Elementos para el diagnóstico de riesgos en informática"

realizado por Flores Torres José Antonio Jesús

con número de cuenta 7607709-0 , pasante de la carrera de Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis M. en C. María Guadalupe Elena Ibargüengoitia González
Propietario

Propietario Dra. Hanna Oktaba

Propietario Mat. Salvador López Mendoza

Suplente Dr. Abdón Sánchez Arroyo

Suplente Mat. Victor Hugo Dorantes González

Consejo Departamental de Matemáticas
Dr. Héctor Méndez Lango

DEDICATORIA

Dedico mi trabajo con todo mi amor:

A mis hijos:

JOSÉ ANTONIO
VALERIA ESTEFANÍA

A mi esposa:

YOLANDA

Por su amor, paciencia, comprensión y felicidad que me han brindado.

A mis padres:

GUADALUPE Y GABRIEL

Por el amor, apoyo y consejos me que dieron y por los valores que me inculcaron.

DEDICATORIA

A mis hermanos:

Roberto

Joaquín

Esther

Francisco

Ana María

Felipe

Alejandra

Mauro

Juan de Dios

Y a toda mi familia por convivir juntos los tiempos felices y difíciles.

AGRADECIMIENTOS

Agradezco a la M. en C. Guadalupe Ibargüengoitia González por haber aceptado la dirección de la tesis, por la atención, apoyo, sugerencias y ánimo que me brindó durante el desarrollo del trabajo.

A los profesores:

Dra. Hanna Oktaba
Mat. Salvador López Mendoza
Dr. Abdón Sánchez Arroyo
Mat. Victor Hugo Dorantes González

Por su valioso tiempo que dedicaron a la revisión del trajo y por los importantes comentarios que realizaron para enriquecerlo y complementarlo.

ÍNDICE

1. INTRODUCCIÓN

1.1 OBJETIVOS DEL TRABAJO

El objetivo del trabajo es el de recopilar la información necesaria en seguridad en informática para realizar diagnóstico de riesgos en informática, dar una introducción sobre las políticas, técnicas y modelos de seguridad y sobre las principales áreas, resaltar las operaciones de mayor importancia relacionadas con la seguridad en informática, y los principales requerimientos para desarrollar el diagnóstico de riesgos.

Así también, proponer una metodología que permita conducir la realización de diagnósticos de riesgos sobre los principales recursos informáticos de una organización, que dé como resultado un informe detallado conteniendo los riesgos más relevantes y un plan de recomendaciones efectivas para que disminuir el riesgo sobre los bienes informático, para que la organización tenga un mayor control sobre su entorno de cómputo y contribuyan al logro de los objetivos de la institución.

1.2 ANTECEDENTES

CAUSA DEL PROBLEMA.

Vivimos en la era de la información donde diariamente se colecciona, preserva, ánaliza, publica y protege información relacionada con nosotros mismos, las cosas que hacemos, tenemos, sobre los productos que generamos, adquirimos, etc.

El uso de las computadoras ha crecido a un nivel tan alto que se ha vuelto indispensable para el desarrollo de operaciones de cualquier organización y en la mayoría de los casos los datos y la infraestructura de cómputo se han convertido en los activos más importantes. La supervivencia de la organización frecuentemente depende de la calidad, oportunidad e integridad de la información, por lo que se ha vuelto crítica la protección de los activos informáticos para la continuidad de sus operaciones.

El nivel gerencial debe preocuparse por salvaguardar los recursos que están bajo su jurisdicción, los recursos humanos y los bienes de capital. En un ambiente computarizado, los recursos humanos están representados por la habilidad para operar el hardware y el software; los bienes de capital están representados por la inversión en la infraestructura de cómputo y los programas operativos.

Parte de las funciones del gerente de procesamiento de datos es proteger los recursos informáticos y salvaguardar los recursos humanos y bienes de capital que son esenciales para seguir dando el servicio.

La alta dirección por su parte, debe estar consciente de los riesgos a que están expuestos y las medidas de protección en caso de que los riesgos se materialicen.

Una amenaza puede ser improbable pero no imposible, por lo que es importante diferenciar entre amenazas probables e improbable para orientar los esfuerzos hacia las amenazas que sean más probables de ocurrir. La seguridad completa es un sueño imposible a menos que se tengan recursos infinitos, es sorprendente que con un bajo presupuesto se pueda lograr una seguridad

razonable, algunas salvaguardas pueden ser implantadas con un modesto gasto de tiempo y esfuerzo.

¿QUÉ ESTAMOS PROTEGIENDO?

Para saber si una organización cuenta con un buen sistema de seguridad, debemos conocer las características de la información, el abuso y el mal uso que se le puede dar. Con este conocimiento se podrá seleccionar el control adecuado.

La información es una representación de símbolos, hechos, conceptos ó instrucciones que sirven para la comunicación, interpretación o procesamiento por gente o sistemas automatizados [PARK98]. La información puede cambiar su forma, combinarse o cambiar de sitio, cada una de estas acciones se pueden realizar en diferentes formas originando que las formas de protección se tengan que ajustar, por ejemplo, cuando combinamos elementos de información cada una con sus propias necesidades de seguridad, se creará una entidad de información con diferentes necesidades de información, un número de cuenta bancaria requiere poca seguridad, pero cuando se combina con elementos como el nombre del banco, dueño de la cuenta y monto de la cuenta, se incrementarán sustancialmente las necesidades de seguridad.

Las características básicas de la información son clase, representación, forma y medio, considerando estas características se pueden definir ampliamente los tipos de controles que escogemos para proteger la información [PARK98].

Los conceptos de las cuatro características básicas son:

- Clase.- La información puede pertenecer a una categoría como es la del conocimiento (información obtenida por estudio o experiencia), instrucciones automatizadas (software), negocios (información financiera, secretos comerciales, de clientes y productos, etc.) monetario, literario o artístico.

- Representación.- La representación de la información puede ser gráfica, símbolos codificados o sonidos, y otras formas de representación como la análoga. Cada tipo de representación que es requerida por el propietario o usuario para desarrollar sus funciones debe estar protegido, asimismo, se deberá proteger los programas que se requieren para realizar el cambio de representación. Diferentes representaciones de la misma información, requiere de diferentes medidas de protección.

- Forma.- La información tiene una estructura como es un formato, gramática, código (cifrado con clave secreta), tablas o sintaxis. Cambiar la forma de la información puede alterar el significado de la información, por lo que existen muchas implicaciones de seguridad con la forma de la información, por ejemplo se puede perder información si se realiza un acto de sabotaje sobre información cifrada del personal y la llave de cifrado es destruida.

- Medio.- La información es representada y materializada en alguna forma física que podamos percibir por ejemplo, sobre papel o en un monitor, y se almacena en algún tipo de medio. Las medidas de seguridad se enfocan en controlar su almacenamiento, uso y respaldo de la información sobre otro medio.

Adicionalmente a las características básicas de la información, existen otras características que ayudan a determinar las medidas de protección en los bienes informáticos y escoger los salvaguardas apropiados, las características adicionales son:

- Integridad. La información es completa, veraz y confiable.
- Disponibilidad. La información es accesible y está lista para usarse.
- Utilidad. La información es útil para lograr un propósito.
- Autenticidad. La información es genuina, precisa y tiene validez.
- Confidencialidad. La información es mantenida en secreto, fuera del alcance del dominio publico o existen restricciones para que sea observada.
- Posesión. La información deberá tener un propietario.

VALOR DE LA INFORMACIÓN

El valor de la información está en función del tiempo, solo tiene valor para un cierto periodo de tiempo, por ejemplo, el plan de ventas de una empresa para 1998 con información al 30 de Septiembre de 1997, será diferente si se considera la información al 2 de Enero de 1998 para realizar el mismo plan. Es una tarea muy importante proteger la información de la manera más adecuada y escoger los salvaguardas precisos en función de la cobertura y el costo financiero.

Para determinar el valor y requerimientos de protección de la información, primeramente, se debe formar categorías y clasificar la información conforme a las guías establecidas por el gobierno y por la empresa. Las consecuencias de no clasificar la información en forma adecuada causarán protección en exceso que resultaría muy costosa, y en caso de considerar escasos mecanismos de protección esto daría lugar a una situación de alto riesgo y que se pueda perder la información. Solamente se debe proteger la información valiosa, los mecanismos de protección se deben aplicar durante un periodo de tiempo y exclusivamente en la forma necesaria [KOVA98].

Generalmente la información considerada valiosa para una empresa, es la información financiera, científica, técnica, económica ó de ingeniería, incluyendo los datos, herramientas, mecanismos, fórmulas, diseño, prototipos, procesos, procedimientos, programas, códigos y estrategias comerciales, se debe considerar la información guardada, compilada, registrada en forma electrónica, gráfica, fotográfica o escrita.

Para determinar el valor de la información se debe considerar los siguientes factores:

- El costo para producir la información.
- El costo para reemplazar la información.
- Qué pasaría si ya no se cuenta con la información.
- Que pasaría si la competencia tiene mi información.
- El costo de los daños por la fuga de la información.
- El costo de mantener y proteger la información.

PREVENCIÓN DE RIESGOS EN INFORMÁTICA.

La forma de prevenir los delitos en informática es mediante la identificación de riesgos y la implantación de medidas de seguridad con un costo razonable que puedan proteger los bienes informáticos, el análisis y toma de decisiones pueden ser realizados por un proceso llamado "Análisis de Riesgos" que maneja tres elementos fundamentales: amenaza, vulnerabilidad y contramedida.

- Amenaza es el posible daño a los bienes informáticos ó personas.
- Vulnerabilidad es un punto donde el sistema es susceptible de ser atacado.
- Contramedida es el uso de técnicas para proteger los bienes informáticos.

No hay un perfil único para identificar a las personas que cometen los crímenes por computadora, sin embargo, los ataques más comunes han sido realizados por jóvenes deseosos de mostrar sus habilidades; por empleados rencorosos que piensan que la empresa donde trabajan no ha reconocido sus esfuerzos; por terroristas que buscan una ganancia financiera, asimismo, es importante resaltar que los errores humanos representan un alto porcentaje de siniestros. Para poder realizar el crimen por computadora, es necesario contar con características y situaciones especificas como son habilidades, conocimiento, recursos, autoridad y motivos.

Además de los ataques realizados por personas, debemos considerar los eventos naturales que representan grandes amenazas, dentro de ésta categoría podemos mencionar a los terremotos, inundaciones, ciclones, tornados, etc.

Finalmente, podemos decir que la seguridad en la información tiene una gran importancia dentro de las organizaciones, con un amplio campo de acción, grandes retos y donde se debe tener bien claro los fundamentos de lo que se debe proteger y de qué se debe proteger.

2. AREAS DE PARTICIPACIÓN

2.1 CICLO DE VIDA DEL DESARROLLO DE APLICACIONES

El software cubre un amplio campo de actuación y se agrupa en diferentes áreas, de las cuáles destacan las siguientes:

- Software de sistemas.
- Software de tiempo real.
- Software de gestión.
- Software de ingeniería y científico.
- Software empotrado.
- Software de computadoras personales.
- Software de inteligencia artificial.

Los proyectos de desarrollo de software de cualquiera de las anteriores áreas se pueden enfrentar con retos, límites o circunstancias que afectan directamente en el producto deseado, como pueden ser los siguientes:

- El proyecto puede durar meses o años de trabajo.
- Atender grandes volúmenes de requerimientos de los usuarios.
- Programar miles de líneas de código.
- Obtener tiempos de respuesta de microsegundos.
- Diseñar cientos de ventanas para usuarios y programación de interfaces.
- Las instalaciones están muy distantes del desarrollador o del usuario.
- Grandes equipos de trabajo o cambio frecuente de sus integrantes.

Para construir el software en forma adecuada, racional y oportuna, independientemente de su área de aplicación y magnitud se debe apegar a un proceso.

El proceso permite definir el marco de trabajo para sus áreas clave, las cuales forman las base del control de gestión de proyectos del software y establecen el contexto donde se aplican los métodos técnicos, se producen los resultados del trabajo, se asegura la calidad y los cambios se administren adecuadamente.

Los métodos indican como construir técnicamente el software y se aplican durante el desarrollo del software en las tareas relacionadas con el análisis de requerimientos, diseño, construcción de programas, prueba y mantenimiento.

El desarrollo de software se divide en tres fases genéricas, la fase de diseño, la fase de desarrollo y la fase de mantenimiento[PRES97].

La fase de definición se enfoca en el "qué", intenta identificar qué información debe ser procesada, qué función y rendimiento se desean, qué comportamiento tendrá el sistema, qué interfaces se establecerán, qué restricciones de diseño tendrá y qué criterios de validación necesita para ser un sistema correcto.

La fase de desarrollo se enfoca en el "cómo", se orientan las tareas en cómo se diseñan las estructuras de datos, cómo se implementa una función, cómo se implementan los detalles de los procedimientos, cómo se caracterizan las interfaces o cómo traducir el diseño en un lenguaje de programación.

La fase de mantenimiento se enfoca en el cambio que va asociado a la corrección de errores, a la adaptación requerida conforme evoluciona el entorno del software.

Durante el proceso del software se aplican las siguientes medidas protectoras:

- Seguimiento y control del proyecto.
- Revisiones técnicas formales.
- Garantía de calidad del software.
- Gestión de configuración del software.
- Preparación y producción de documentos.

- Gestión de reutilización.
- Mediciones.
- Gestión de riesgos.

El nivel de madurez del proceso de software se determina comparándolo con un modelo completo propuesto por el Software Engineering Institute(SEI) que toma como base un conjunto de funciones de ingeniería del software que deben de estar presentes conforme las organizaciones alcanzan diferentes niveles de madurez del proceso.

El Software Engineering Institute establece cinco niveles de madurez del proceso conforme a las prácticas efectivas de ingeniería de software:

- Nivel 1:Inicial
- Nivel 2:Repetible
- Nivel 3:Definido
- Nivel 4:Gestionado
- Nivel 5:Optimización.

Existen diversos modelos para el proceso del software y la selección de un modelo dependerá de la naturaleza del proyecto, los métodos y las herramientas a utilizarse, los controles y entregas que se desean.

Los siguientes modelos tienen como objetivo común ayudar en el control y coordinación de proyectos:

- Modelo lineal secuencial
- Modelo de construcción de prototipos
- Modelo desarrollo rápido de aplicaciones
- Modelo de procesos evolutivos de software, que tiene las siguientes variantes:
    a) Modelo incremental
    b) Modelo en espiral

c) Modelo de ensamblaje de componentes
d) Modelo de desarrollo concurrente

El uso de un modelo en el proceso y el nivel de efectividad con que se aplique afectará directamente al producto, de tal forma, que un proceso débil ó su aplicación dará un producto inoportuno o que no cumpla los requerimientos del usuario.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Cada desarrollo de una nueva aplicación es considerado como un proyecto que tendrá objetivos bien definidos, un responsable de su desarrollo y administrado con técnicas adecuadas que permitan conseguir los objetivos marcados. Los elementos generales que se deben considerar en la evaluación son los siguientes:

- Existencia de una metodología o procedimientos para la administración de proyectos, que guíe las actividades de manera ordenada para la obtención de resultados. Los resultados obtenidos durante el ciclo de vida son:

  a) Aprobación de proyecto.
  b) Descripción de los objetivos, restricciones y departamentos involucrados.
  c) Responsable o director del proyecto.
  d) Prioridad asignada al proyecto.
  e) Equipo técnico asignado.
  f) Comité o grupo de trabajo para seguimiento al desarrollo del proyecto y que tenga poder de decisión en caso de reajustar el proyecto.
  g) Documentación de los problemas que surgen durante el ciclo.
  h) Control de cambios.
  i) Metodología para llevar a cabo el ciclo de vida de desarrollo de sistemas.- Descripción de las actividades que se deben realizar y de los resultados que se deben obtener.

2.2 DESARROLLO DE APLICACIONES

La seguridad y calidad son propiedades de los sistemas, el software con un alto nivel de seguridad debe tener un alto nivel de calidad, cuando el software tiene un bajo nivel de calidad la seguridad se ve disminuida, por ejemplo, una aplicación para manejar la nómina de una empresa, los datos personales y los ingresos de sus empleados pueden estar comprometidos y los cálculos realizados pueden ser erróneos, asimismo, la captura de información y ejecución de procesos ocasionarán confusiones a los usuarios.

Las fallas de seguridad en un sistema pueden ocasionar la violación a sus requerimientos de seguridad, estas fallas pueden ser introducidas en cualquier etapa del ciclo de vida del desarrollo del sistema, si las personas que desarrollan las aplicaciones estuvieran preocupados por la seguridad, ellos podrían evitar algunos tipos de fallas.

El siguiente cuadro presenta las fallas más comunes y se agrupan conforme a su categoría, incluye fallas que pueden ser metidas durante el desarrollo, mantenimiento y operación de las aplicaciones, asimismo, donde las fallas pueden estar localizadas (en el hardware, sistema operativo, utilerias o en aplicaciones) [SUMM97].

Intencionales	Maliciosas	Caballo de Troya	No replicable
			Replicable (virus)
		Trampas	
		Bombas de tiempo	
	No maliciosas	Canales secretos	Almacenamiento
			Cronometro
		Otras	
No intencionales	Error de validación (incompleto/inconsistente)		
	Error de dominio		
	Serialización		
	Inadecuada identificación/autentificación		
	Violación de limites		
	Otros errores lógicos		

Las fallas maliciosas son programas desarrollados por los atacantes que buscan dañar a las aplicaciones y la información ocasionando la suspensión del servicio. En el caso del Caballo de Troya, el código malicioso está oculto dentro de un programa útil para el sistema y que puede aprovechar los privilegios que tiene el usuario, por lo que éste tipo de código es más peligroso cuando el usuario es el administrador del sistema o un usuario privilegiado.

El canal secreto (o canal no planeado) es una trayectoria de comunicación no planeada que puede ser usada para violar las políticas de seguridad del sistema y el daño que puede causar depende de su ancho de banda. Los canales secretos de almacenamiento usan cambios en el sistema para almacenar información, por ejemplo, cuando se termina la memoria usada por las tablas del sistema operativo, realiza un proceso para que ya no haya espacio disponible y de esta manera puede almacenar la información liberada. Los canales de coordinación se basan en la ejecución de eventos en el hardware, por ejemplo en un sistema donde el procesador comparte un bus común, un procesador puede saturar el bus y otro procesador puede detectar ésta condición para completar la tarea. El uso de canales secretos puede atacar las operaciones realizadas con recursos compartidos, por ejemplo, la impresión, uso de graficadores o unidades de cintas, bloqueos de memoria o almacenamiento en disco [SUMM97]..

Las fallas de validación ocurren cuando un programa no valida adecuadamente la información que le ha sido suministrada.

PRINCIPIOS DE DISEÑO PARA LA SEGURIDAD

Derivado de la experiencia de construir sistemas seguros, se han integrado principios de diseño que se aplican a la arquitectura de un sistema y a interfaces externas, un sistema que se diseña de acuerdo con estos principios es más probable que satisfaga los objetivos de seguridad. Un buen diseño es esencial, sin embargo puede verse comprometido por una pobre implementación. Los principios se aplican mejor desde el inicio de un proyecto, ya que, agregar esquemas de seguridad a un sistema existente es mucho más difícil, sin embargo, los diseñadores tienen restricciones de tiempo y económicos y frecuentemente los nuevos diseños deben apoyar viejas interfaces externas y deben usar mucho código viejo.

Los principios para el diseño de sistemas de seguridad que integraron Jerome Saltzer y Michael Schroeder como producto de su experiencia en el desarrollo de sistemas seguros y de su experiencia con el sistema operativo Multics son los siguientes:

- Mecanismos de Economía.- Mantener en diseño de seguridad tan simple y pequeño como sea posible.
- Valores de omisión seguros.- Tomar decisiones de acceso basadas en permisos en lugar de exclusiones. Omitir un parámetro en una llamada del sistema operativo o tener fallas en una llamada deberá ocasionar que el sistema tome más de una alternativa segura.
- Mediación completa.- Todos los accesos a cada objeto deben ser validados, no debe haber trayectorias a los objetos que eviten la validación.
- Diseño abierto.- El diseño mismo no debe mantenerse en secreto, un diseño abierto puede ser revisado por expertos y por usuarios potenciales, de esta manera, los errores o deficiencias pueden ser encontrados y corregidos. Es necesario mantener en secreto passwords y las llaves de cifrado pero no necesariamente en diseño.
- Separación de privilegios.- La seguridad es mejorada cuando dos o más claves son requeridas para abrir un mecanismo de protección o si dos mecanismos deben coincidir antes de permitir una acción.
- Privilegios mínimos.- Cada programa o componente del sistema debe operar con el conjunto mínimo de privilegios que necesita para cumplir su tarea.
- Mecanismos comunes mínimos.- Minimizar el número de mecanismos que operan de parte de muchos usuarios y que podrían comprometer la seguridad si operan en forma incorrecta.
- Aceptabilidad.- La seguridad debe ser fácil de entender y usar.
- Otros principios.- Consideración del medio ambiente, separación de políticas y mecanismos, invisibilidad de la base de datos, auditabilidad y anticipar requerimientos futuros de seguridad.

La seguridad debe afectar todo el ciclo de vida del desarrollo, también, debe contemplarse en los sistemas que se están desarrollando, asimismo al proceso del desarrollo, a sus herramientas y productos intermedios.

Los requerimientos de seguridad deben incluir una propuesta de la política de seguridad que será soportada por el sistema y deben describir las funciones y servicios de seguridad que serán proporcionados por el sistema. Incorporar los requerimientos de seguridad afecta al rendimiento del sistema y a los recursos existentes, por lo que es necesario presupuestar más tiempo y dinero para el desarrollo del sistema [SUMM97].

Para expresar los requerimientos de seguridad de manera precisa y sin alguna ambigüedad, los métodos formales pueden ser utilizados. Estos métodos también ayudan durante el desarrollo del sistema a mantener consistencia entre una etapa y su precedente, soportan una verificación formal para demostrar la consistencia en la descripción del sistema en diferentes niveles. Los métodos formales son requeridos para desarrollar sistemas con un alto nivel de seguridad.

Como un ejemplo de aplicación de métodos formales, está el proyecto Secure Release Terminal (SRT), que es un sistema que permite mover documentos clasificados de un sistema de alto nivel a un sistema de bajo nivel, la terminal es usada por un oficial de seguridad quien revisa un documento y lo mueve de lugar. Los pasos que se realizan en una especificación y verificación formal son:

1. Establecer los requerimientos de seguridad en términos matemáticos.
2. Producir una especificación formal de un alto nivel para dar una descripción matemática del comportamiento del sistema. Probar que corresponde a los requerimientos formales.
3. Producir una serie de refinamientos, cada refinamiento implementa las especificaciones del siguiente nivel superior con mayor detalle. Probar que cada nivel de refinamiento es consistente con el anterior.
4. Codificar el sistema. Mostrar que la implementación es consistente con la especificación formal del nivel más bajo.

Las metodologías formales que han sido usadas para seguridad incluyen a Gypsy, el Método de Desarrollo Jerárquico y el Método de Desarrollo Formal, sin embargo, se han utilizado en pocos sistemas. Las metodologías estructuradas se utilizan en forma generalizada para el desarrollo de sistemas, sin embargo, no tienen integrados con métodos para el diseño de seguridad, los diseñadores frecuentemente consideran la seguridad en forma separada y utilizan análisis de riesgos.

El tipo de lenguaje que sea seleccionado puede tener un gran peso para la seguridad del sistema, el uso de lenguajes de alto nivel genera menos código y tendrá menos oportunidad de que existan errores, los programas son más fáciles de revisar y analizar. Tradicionalmente los sistemas operativos fueron escritos en lenguaje ensamblador o en lenguaje de alto nivel como C porque permitían acceder a todos los recursos del sistema, sin embargos, estos lenguajes son considerados "no seguros" porque no fortalecen o promueven el buen diseño de programas; el código en estos lenguajes es tan difícil de leer y comprender que no se puede constatar su seguridad [SUMM97]. La situación esta cambiando con la creación de nuevos lenguajes que promueven la calidad y la seguridad, lenguajes como Ada soportan modularidad, abstracción y ocultamiento de información; lenguajes orientado a objetos como C++ soportan el concepto de herencia que promueve una buena estructura, permitiendo de una manera más fácil el reuso de código.

El uso de metodologías y lenguajes tienen un gran peso en el desarrollo de sistemas pero son solamente una parte del esquema de seguridad.

Para verificar la seguridad de un sistema se deben cubrir tres puntos:

1. Especificaciones (formales de preferencia), verificación del diseño y análisis e inspección.
2. Desarrolladores calificados y un proceso de desarrollo racional.
3. Realización de pruebas.

Realizar pruebas sigue siendo el principal camino para asegurar que un sistema provee sus servicios especificados y fortalece sus políticas de seguridad. Durante las pruebas, se pueden

encontrar fallas de seguridad en el sistema, inclusive en las políticas, hipótesis, interfaces del usuario y en la documentación. También, se pueden descubrir diferencias entre el modelo de seguridad y los requerimientos del mundo real, asimismo, se descubren errores en el código que fue inspeccionado.

La realización de pruebas puede resultar cara y consumir mucho tiempo, por lo que están limitadas en tiempo y dinero. Las pruebas para la seguridad se agrupan en dos categorías:

1. Pruebas funcionales.- Demuestran que los servicios de seguridad y mecanismos están completos y son consistentes con la documentación.
2. Pruebas de penetración.- Presiona a un sistema a exponer las fallas de seguridad.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

La existencia de elementos de control combinados con los métodos modernos para el desarrollo de aplicaciones y herramientas permitirá proteger a la aplicación que se está desarrollando y asegurar que el sistema producirá resultados de calidad. Los elementos a considerar son:

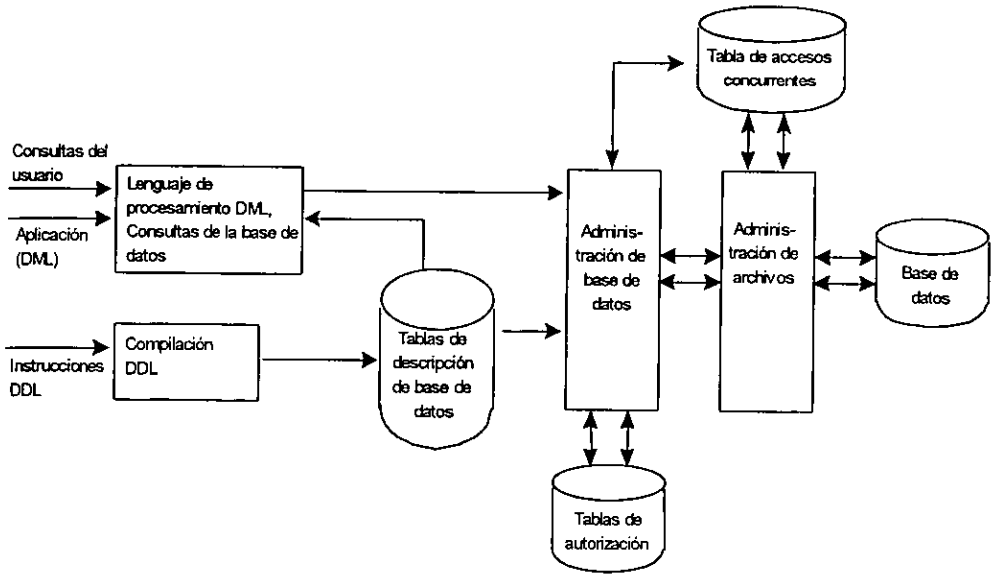
- Uso de metodologías para el desarrollo de sistemas.
- Uso de software homologado.
- Controles para edición, corrección y validación de datos.
- Vista de datos.
- Permisos.
- Password.
- Pistas de auditoria.
- Procedimientos de respaldo y retención de información.
- Controles en línea.
- Criptografía.

2.3 BASES DE DATOS

Cuando se habla de bases de datos, se hace referencia a una colección de datos interrelacionados que pueden ser manejados por el sistema administrador de bases de datos (DBMS).

El sistema administrador de bases de datos es un sistema que provee los elementos necesarios como procedimientos y programas para coleccionar, organizar y mantener archivos de datos o bases de datos, administrar transacciones concurrentes, controlar el acceso a los datos y recuperar la base de datos después de una falla.

La siguiente gráfica muestra la arquitectura típica de un DBMS, incluye módulos funcionales y el conjunto de datos que apoyan a éstos módulos.



Las bases de datos se almacenan en el servidor como archivos, por lo que es importante manipular los datos desde un servidor que tenga incorporados mecanismos de seguridad, para evitar que los usuarios tengan acceso a dichos archivos. El administrador de la base de datos es el responsable de la custodia, acceso y disponibilidad de la información.

La seguridad en base de datos comprende un conjunto de medidas, políticas y mecanismos para proveer confidencialidad, integridad y disponibilidad de los datos y defender al sistema de posibles ataques accidentales o malintencionados realizados por personal interno o externo.

La seguridad de la base de datos abarca los puntos relacionados con la seguridad física, seguridad lógica y la seguridad de su organización. La seguridad física se enfoca en las herramientas, dispositivos y técnicas de hardware y software para prevenir o detectar acceso físico no autorizado a las utilerías para el almacenamiento de datos y para el respaldo o recuperación de la base de datos. La seguridad lógica consiste de controles, modelos y técnicas para prevenir, detectar o disuadir el acceso lógico no autorizado.

La seguridad de la información en una base de datos, incluye tres aspectos principales: La privacidad, la integridad y la disponibilidad de la información.

- Mantener la privacidad de la información significa prevenir, detectar y evitar la difusión de la información en forma inapropiada. Esta característica de la información se refiere a la protección de la información en entornos altamente protegidos, como es el entorno militar y es el concepto más relevante.

- Asegurar la integridad, significa prevenir, detectar y evitar la modificación de la información de manera inapropiada. Esta característica de la información es muy relevante en el medio ambiente comercial, el buen trabajo de la compañía depende de la correcta operación basada en datos correctos y coherentes.

- Asegurar la disponibilidad del sistema significa prevenir, detectar y evitar la negación inapropiada de un servicio provisto por el sistema, por ejemplo en un ambiente militar, el sistema debe estar disponible y se deben disparar los misiles cuando se transmita la orden correspondiente.

Tener seguridad sobre el ambiente de bases de datos significa que se han identificado las amenazas, se han escogido las políticas para identificar qué podrá hacer el sistema de seguridad y

se han diseñado los mecanismos para lograr las metas de seguridad deseadas. También se debe contemplar el grado de cumplimiento a los requerimientos de seguridad y cómo se ejecutan las funciones de seguridad.

Las amenazas para la seguridad en bases de datos son los eventos realizados en forma accidental o que utilizan una técnica especializada para descubrir o modificar la información manejada por un sistema. Las violaciones a la seguridad de la base de datos se refieren a las acciones de lectura, modificación o eliminación de datos realizadas en forma inapropiada.

Las violaciones a la seguridad de la base de datos tiene las siguientes consecuencias:

- Difusión incorrecta de información causada por lectura de datos en forma accidental o intencional por usuarios sin autorización de acceso a ésta información.
- Modificación inapropiada de datos, incluye todas las violaciones a la integridad de datos mediante el manejo o modificación inapropiada de datos.
- Suspención del servicio a los usuarios para acceder los datos o recursos.

Las amenazas se clasifican en fraudulentas (intencionales) o no fraudulentas (accidentales) conforme a la manera en que pueden ocurrir.

Las amenazas no fraudulentas incluyen a los desastres naturales o accidentales como son los terremotos, daños causados por agua o fuego y que pueden dañar al hardware y los datos almacenados. Errores en el hardware o software pueden originar una aplicación incorrecta de políticas de seguridad causando la lectura y modificación de datos no autorizada o la suspención del servicio a usuarios autorizados. Los errores humanos causan violaciones no intencionadas como son la incorrecta entrada de datos y el uso incorrecto de las aplicaciones, estos errores tienen consecuencias similares a las causadas por errores en el hardware o software.

Las amenazas fraudulentas o intencionales son acciones explícitas y determinadas a causar daño. Son llevadas a cabo por usuarios quienes abusan de sus privilegios y autoridad; por personal

interno o externo a la empresa que realiza actos de vandalismo sobre el hardware y software, o que realiza lecturas o modificación de datos sin la autorización correspondiente.

Es necesario conocer los conceptos y acciones que se aplican en una base de datos para saber cómo se va a proteger de las actividades accidentales o intencionales orientados a leer o modificar datos sin la autorización correspondiente, los puntos más importantes a considerar son los siguientes:

- Protección contra acceso no autorizado. Se debe garantizar el acceso a la base de datos solo a usuarios autorizados. El acceso debe ser validado por el DBMS para identificar si tiene la autorización del usuario o de la aplicación.
- Protección contra la inferencia, el acceso a la información confidencial es ganado mediante el uso de información no confidencial. Este problema se presenta en forma particular en base de datos estadísticas, como ejemplo podemos considerar una consulta para obtener el sueldo de las empleadas, posteriormente el número de empleadas, si éste valor es uno el salario de la empleada puede ser inferido.
- Integridad de la base de datos, éste requerimiento de seguridad debe contemplar los mecanismos para proteger la base de datos de los eventos que podrían modificar sus datos, como pueden ser los errores, virus, sabotaje o fallas del sistema que pueden dañar los datos almacenados. Esta clase de protección es obtenida por el DBMS mediante un apropiado control de accesos, y a través de procedimientos de respaldo y recuperación.

La seguridad en una base de datos es lograda mediante mecanismos integrados en el DBMS y en el sistema operativo. El DBMS juega un papel importante en la seguridad de los datos y los principales requerimientos de seguridad que debe cubrir son:

- Control de acceso en las operaciones (lectura, escritura, actualizaciones), en las relaciones existentes entre columnas, vistas de la base de datos.
- Modificación a las autorizaciones de los usuarios.
- Protección en varios niveles.
- Control del flujo.- Valida que la salida obtenida fue realizada mediante acceso autorizado.

- Cierre de puertas traseras.- El acceso a los datos debe ser realizado exclusivamente por el DBMS.
- Controles de inferencia.- Debe evitar que el usuario conozca información sensitiva ó de alta clasificación mediante el manejo de información elemental. Técnicas de restricción sobre las operaciones realizadas mediante consultas para lograr este objetivo.
- Uso de múltiples instancias para prevenir la inferencia.- Permite a la base de datos contener múltiples instancias del mismo elemento, cada uno conteniendo su propio nivel de clasificación.
- Auditoria.- Los eventos relacionados con la seguridad deben ser mantenidos en pistas de auditoria o bitácoras para su análisis y detectar posibles amenazas a la base de datos.

Algunos DBMS que existen en el mercado son Ingres, Oracle, Sybase, Informix y SQL Base, la siguiente tabla muestra algunas funciones de seguridad que están incorporadas en estos productos:

DBMS	Autenti-ficación	Acciones de Super usuario	Alterar indices de tablas	Refe-rencias	Ejecución de Proce-dimientos	Otorgar Privile-gios	Opción de Adminis-trador	Audi-toria
Ingres	Por sist. op.	SI			SI			SI
Oracle	Por password y Por sist. op.	SI	SI	SI	SI SI	SI	SI	SI
Sybase	Por password		SI	SI	SI	SI		
Informix	Por sist. op.		SI					
SQL Base	Por password		SI					

Una descripción general de las funciones de seguridad incorporadas en los anteriores DBMS es la siguiente:

- La autentificación es realizada por el sistema operativo o mediante password, en el caso de Oracle contiene los dos mecanismos.

- Las operaciones de superusuario se refieren a iniciar y apagar el servidor de bases de datos. Adicionalmente, existe otro tipo de operaciones del sistema que están incluidos en todos los DBMS que se han mencionado y sirven para proveer privilegios para crear, alterar tipo y objetos.
- El privilegio de referencias es soportado solo en los servidores DBMS donde existe una restricción de integridad por referencia. El privilegio de ejecución existe en los sistemas donde es posible ejecutar un procedimiento de la base de datos.
- El otorgamiento de privilegios permite a usuarios privilegiados transferir privilegios a otros usuarios. La opción de administrador solo la tiene Oracle y está definida para tener privilegios sobre el sistema.
- La funcionalidad de auditoria permite a los servidores de base de datos registrar eventos relacionados con la seguridad para realizar un análisis posterior y poder reconstruir los eventos.

La seguridad en base de datos pudiera ser vista como algo secundario, ya que pueden existir paquetes de seguridad que proveen algunos mecanismos básicos de seguridad a nivel del sistema operativo como puede ser la autentificación de usuarios, control de accesos o auditoria.

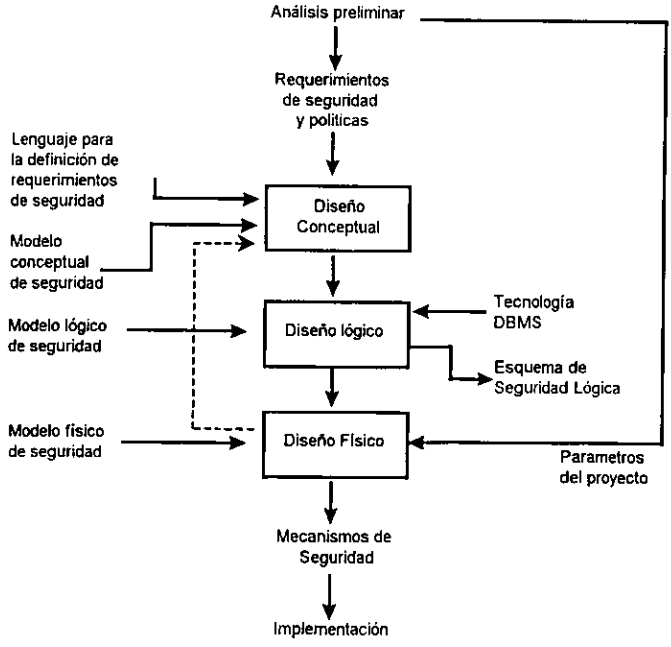
Como ejemplo de los paquetes de seguridad son RACF, Top Secret y CA-ACF2 que se ejecutan en sistemas operativos como MV, VMS y VM. Sin embargo, existen algunos entornos como el militar que requiere contar con un sistema de seguridad diseñado para una situación especifica y los requerimientos de protección verificados de manera formal. En cualquier caso, el diseño de un sistema de seguridad en una base de datos se debe considerar como un problema serio.

El uso de una metodología para incorporar la seguridad en una base de datos ayuda a los diseñadores a establecer claramente los requerimientos de seguridad independientemente del software de seguridad y de los mecanismos que están instalados, asimismo, ayuda en la selección de políticas de seguridad y definición de un modelo de seguridad, y en el diseño de mecanismos de seguridad para implantar el modelo de seguridad [CAST94].

Una metodología propuesta por Silvana Castano para el diseño de base de datos segura, basada en los criterios establecidos por el Departamento de la Defensa de los Estados Unidos [CAST94] contempla las siguientes fases:

1. Análisis preliminar.
2. Requerimientos y políticas de seguridad.
3. Diseño conceptual.
4. Diseño lógico.
5. Diseño físico.

La metodología anterior muestra similitudes con las metodologías usuales para el diseño de bases de datos por lo que el diseño del sistema de seguridad puede ser integrado al diseño de la base de datos. La siguiente gráfica muestra las fases de la metodología propuesta.



La descripción de las fases de la metodología propuesta es la siguiente:

1. Análisis preliminar.- La meta de la fase es realizar un estudio de factibilidad para el sistema de seguridad, que consiste en la evaluación de los riesgos, del diseño y costo del sistema, definiendo que aplicaciones deben ser desarrolladas y asignarles una prioridad.

2. Requerimientos y políticas de seguridad.- El análisis de los requerimientos de seguridad inician con un estudio preciso y seguro de todas las posibles amenazas a que está expuesto el sistema. Esto permitirá a los diseñadores definir los requerimientos de seguridad correctamente y completamente. La política de seguridad ayudará en la definición de accesos autorizados para cada sujeto sobre los diferentes objetos en el sistema. Se deberá seleccionar la política de seguridad que mejor corresponda con los requerimientos de seguridad que fueron definidos. Para escoger la política se pueden aplicar diferentes criterios como privacidad contra integridad, compartir al máximo contra privilegios mínimo o se pueden considerar los atributos usados para el control de acceso.

3. Diseño conceptual.- En esta fase los requerimientos y políticas de seguridad definidos en la fase previa son conceptualmente formalizados, los detalles en esta fase todavía no se consideran. Un modelo conceptual es introducido para la formalización de requerimientos y políticas.

   El modelo conceptual de seguridad es definido mediante la identificación de sujetos y objetos desde el punto de seguridad, identificación de modos de acceso de los sujetos a los objetos reconociendo las posibles restricciones de acceso y un análisis de distribución de autorizaciones mediante privilegios. En ésta fase se introduce un lenguaje para expresar los requerimientos.

4. Diseño lógico. En ésta fase el modelo conceptual de seguridad es traducido en un modelo lógico que está soportado por el DBMS que será usado. Por ejemplo, en una base de datos relacional, las técnicas de seguridad basadas en vistas y consultas son usadas regularmente para control de accesos y las reglas del modelo conceptual tienen que ser ajustadas a dichas técnicas. Las reglas de seguridad se especifican considerando los mecanismos de seguridad de sistema operativo y las funciones de seguridad en los paquetes comerciales de seguridad.

5. Diseño físico. Los detalles de organización del almacenamiento y las formas de integración e instalación de los mecanismos de seguridad son definidos en ésta fase. El diseño detallado de los mecanismos de seguridad considera el diseño de las estructuras físicas de las reglas de acceso, las relaciones con las estructuras físicas de la base de

datos, los diferentes modos para el control de accesos y una arquitectura detallada de los mecanismos que reforzarán a las políticas y requerimientos de seguridad.

6. Instalación de mecanismos de seguridad. Los desarrolladores pueden apoyarse en un conjunto de directrices para seleccionar los mecanismos de seguridad que mejor atiendan sus necesidades. Algunas directrices que se consideran son las siguientes:

   - Economía de los mecanismos. Los mecanismos deben ser tan simples como sean posibles, las ventajas son una inmediata reducción de costos, mayor confiabilidad y mayor facilidad de probar y auditar el sistema.
   - Eficiencia. Los mecanismos deben ser eficientes considerando que son invocados durante la ejecución del programa.
   - Costos. Los costos de operación deben ser proporcionales al uso actual de los mecanismos.
   - Separación de privilegios. Donde sea posible, instalar mecanismos de seguridad para que el acceso sea dependiente de diversas condiciones.
   - Privilegios mínimos. Los programas y usuarios deben tener el nivel mínimo de privilegios, esto es como un principio de una política de seguridad.

7. Verificación y prueba. El propósito de esta fase es verificar que los requerimientos y políticas se hayan aplicado correctamente. El uso de métodos formales e informales pueden ser de gran utilidad para realizar la verificación.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Los riesgos más importantes debidos al uso de la base datos consisten de una mayor dependencia de los servicios informáticos por la concentración de datos, mayor posibilidad de acceso a la información por parte del administrador, incompatibilidad entre sistemas de seguridad de acceso general y del sistema administrador de la base de datos, mayor impacto por los datos erróneos, mayor impacto de accesos no autorizados y mayor dependencia del personal técnico que realiza tareas con el software para la administración de bases de datos.

Los elementos generales que se deben considerar en la evaluación son los siguientes:

- Técnicas de control para establecer tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos.
- Descripción de las responsabilidades de la administración del entorno de la base de datos.
- Descripción de las responsabilidades del administrador de base de datos.
- Separación de funciones entre el administrador de seguridad, el administrador de bases de datos, personal de desarrollo y de explotación de datos, en caso de existir ésta separación de funciones, verificar controles compensatorios.
- Metodologías de diseño de bases de datos, tanto fisico como lógico.
- Modelo de la arquitectura de la información.
- Datos y diccionario de datos corporativo.
- Esquema de clasificación de datos en cuanto a su seguridad y sus niveles de seguridad.
- Procedimientos de carga de datos.
- Procedimientos de explotación de la base de datos.

2.4 REDES DE COMPUTADORAS

El término "redes de computadoras" se refiere a una colección interconectada de computadoras autónomas. Se dice que dos computadoras están interconectadas si son capaces de intercambiar información [TANE97]. El rango de una red puede abarcar desde unas cuantas PC's hasta una interconexión gigantesca que abarca la conexión con otras redes. Conforme al tamaño físico se clasifican de la siguiente forma:

Distancia entre procesadores	Procesadores ubicados en el (la) mismo(a)	Ejemplo
10 metros 100 metros 1 km	Cuarto Edificio Campus	Red de área local (LAN)
10 km	Ciudad	Red de área metropolitana (MAN)
100 km 1,000 km	País Continente	Red de área amplia (WAN)
	Planeta	Internet

La conectividad es una característica que ha facilitado la comunicación y compartir información entre las oficinas distantes de una empresa, sin embargo también expone a la red a un ataque contra su seguridad.

Los mecanismos de seguridad están orientados principalmente a proteger a la red contra el acceso no autorizado, interferencia en las operaciones realizados en forma accidental o intencional y destrucción de las instalaciones.

La organización norteamericana National Computer Security Center (NCSC) ha desarrollado, promovido y publicado diversos estándares y guías sobre seguridad en la información incluyendo The Trusted Computer Security Evaluation Criteria, que fue el resultado del proyecto MAC del Massachusetts Institute of Technology (MIT) y adoptado posteriormente por el Departamento de

Defensa de los Estados Unidos como un estándar (DoD 5200.28-STD) y conocido popularmente como el Libro Naranja (Orange Book) [HUTT95].

Los criterios establecidos en el Libro Naranja han sido los estándares para evaluar productos de hardware y software desde el punto de vista de seguridad en cómputo.

El Libro Trusted Network Interpretation (TNI) también conocido como el Libro Rojo (Red Book), es un complemento del Libro Naranja que da las directrices de cómo se debe interpretar el Libro Naranja en un entorno de redes de computadoras.

Conforme al Libro Naranja existen diferentes niveles de seguridad, cada uno involucra un modelo aplicable a las redes, éstos niveles son incrementales, es decir, todas las características y requerimientos se incluyen en el siguiente nivel. Se clasifican del nivel D como el menos seguro hasta el nivel A1, nivel con mayor seguridad

Nivel **Descripción**

D Sistema sin seguridad.

C Provee controles discrecionales, basado en usuarios individuales y/o grupos que habilitan a los usuarios para compartir acceso. El dueño de los datos determina quien los puede acceder.

- C1 Requiere contraseñas de los usuarios, permite un ID para el grupo. Este medio ambiente es amigable y no requiere fuertes mecanismos de seguridad.
- C2 Requiere contraseña individual para los usuarios con passwords y un mecanismo de auditoria para los eventos más relevantes de seguridad.

B Provee controles obligatorios. El acceso está basado en estándares.

- B1 Protección basada en etiquetas de seguridad.
- B2 Protección estructurada, garantiza trayectorias entre el usuario y la seguridad del sistema. Provee seguridad que el sistema pueda ser probado y que las certificaciones no pueden ser degradadas.

B3 El sistema es muy resistente a la intrusión. Mecanismos de auditoria supervisan eventos relevantes de seguridad y emite mensajes en situaciones sospechosas. El proceso de recuperación para casos de fallas es confiable. La seguridad es caracterizada por un modelo formal viable.

A Provee protección verificada. El acceso esta basado en estándares certificados por él Departamento de la Defensa de Estados Unidos.

A1 Es funcionalmente equivalente al nivel B3 y logra un mayor nivel de seguridad mediante el uso de métodos formales. Está caracterizado por un modelo formal de seguridad y emplea sistemas operativos confiables. Usa especificaciones formales de políticas y sistemas.

La mayoría de las redes instaladas en las organizaciones, están clasificadas en los niveles B1, B2 y C2, el nivel A normalmente se asignan a las redes con uso militar.

La arquitectura de una red debe estar acompañada de una arquitectura de seguridad para la red. Para los sistemas confiables la arquitectura de seguridad describe cómo un sistema está estructurado para satisfacer sus requerimientos de seguridad e identificar los componentes de seguridad más relevantes. La arquitectura de seguridad puede tomar varias formas, para sistemas abiertos se enfoca en qué servicios de seguridad son provistos y en qué capa, en el esquema general se enfoca en servicios específicos.

La arquitectura de seguridad del modelo OSI (Interconexión de sistemas abiertos/Open Systems Interconnection) identifica los siguientes servicios de seguridad: Autentificación, Control de acceso, Confidencialidad de datos, Integridad de datos y No rechazo [OPPL98].

Los servicios de autentificación son para proporcionar autentificación en el proceso de comunicación entre dos entidades o para la autentificación del origen de los datos; los servicios de control de acceso sirven para proteger los recursos del sistema contra la utilización no autorizada; los servicios de confidencialidad protegen los datos de revelaciones no autorizadas; los servicio de integridad de datos protegen a los datos de modificaciones no autorizados; los

servicios de no rechazo proporciona cierta protección contra el remitente de un mensaje o acción que niega serlo, el servicio de rechazo se está haciendo cada vez más importante en el contexto de intercambio electrónico de datos (EDI) y comercio electrónico.

La arquitectura de seguridad OSI también describe mecanismos específicos de seguridad por ejemplo: el cifrado, la firma digital, el control de acceso, la integridad de datos, el intercambio de autentificación y el control de direccionamiento de datos.

Es importante precisar que la arquitectura de seguridad de OSI no se ha desarrollado para resolver una necesidad particular en la seguridad de las redes. Proporciona una terminología común que se puede utilizar para describir y discutir sobre problemas relacionados con la seguridad y sus correspondientes soluciones [OPPL98].

La información en una red está expuesta a amenazas o eventos potenciales que pueden causar daño a los activos informáticos. Estas amenazas tienen el potencial de aprovechar las vulnerabilidades o debilidades de una red. Las amenazas no se presentan siempre de la misma manera y varían de una red a otra, así como la probabilidad de su ocurrencia.

Sí las amenazas se materializan pueden ocurrir pérdidas financieras sustanciales y evitar alcanzar los objetivos de la red. Algunas veces es difícil calcular la frecuencia de la amenaza o estimar la pérdida financiera ya que no son reportados, detectados o tienen un valor difícil de calcular. Algunas organizaciones evitan reportar la información de pérdidas ocasionadas por un siniestro ya que podría causar publicidad negativa, ocasionar pérdidas mayores o inclusive la pérdida del negocio.

Las principales amenazas de una red se pueden agrupar en las siguientes categorías:

- Errores humanos. La mayor fuente de pérdidas es debido a acciones humanas no intencionales durante sus operaciones. Algunos expertos estiman que más de la mitad de las pérdidas financieras y de productividad son causadas por errores humanos a diferencia de los actos intencionales o maliciosos. Los errores más frecuentes incluyen instalaciones inadecuadas, administración del hardware y software, borrado accidental de archivos,

actualización de archivos equivocados, negligencia para cambiar passwords, captura incorrecta de información, errores durante el respaldo de información y otros actos que ocasionan pérdidas de información, interrupción del servicio y demás.

- Personal interno. Muchas violaciones a la seguridad de la información son realizadas por el personal interno quien compromete actividades no autorizadas o actividades que excedan su autoridad. Este personal puede copiar, robar o sabotear la información sin dejar huella de estas operaciones. Estos individuos pueden retener autorizaciones y pueden ser capaces de deshabilitar operaciones de red, también pueden violar controles de seguridad mediante acciones que no requieren autorización especial.

- Desastres naturales y daño ambiental. Los desastres como inundaciones, terremotos, fuego y fallas de energía pueden destruir la instalación principal y sus respaldos del sistema. Así también existen condiciones ambientales y amenazas que producen daños significantes pero no muy impactantes, como puede ser el rompimiento de las tuberías de agua o suspención del servicio de aire acondicionado.

- Intrusos. Un pequeño pero creciente número de violaciones proviene de intrusos quienes pueden entrar al sistema para obtener ganancia monetaria, secretos industriales o consideran un desafío el forzar la entrada o sabotear el sistema. Este grupo recibe el tratamiento más sensacional en la prensa, incluye a los adolescentes quienes intentan forzar la entrada a sistemas remotos y a los criminales profesionales, espías industriales o inteligencia extranjera

Para proteger a una red y confiar en que las operaciones son seguras, se pueden aplicar las siguientes estrategias [FARL98]:

- Crear un entorno de red seguro, utilizar controles sobre los usuarios y establecer permisos sobre las acciones que se pueden realizar en un sistema, se deben establecer controles de acceso y mecanismos de identificación y autentificación.

- Cifrar datos para evitar que sean leídos o comprendidos por intrusos. La aplicación de esta técnica en las contraseñas, archivos de contraseñas y mensajes son de los puntos más importantes para evitar el robo de información.
- Controles sobre módems. Las conexiones vía módem son particularmente vulnerables para tener acceso ilegal a la red.
- Desarrollar planes de contingencia para conocer las acciones que se deben llevar a cabo cuando se presenta un problema.
- Utilizar barreras de seguridad. Las organizaciones que tienen grandes interconexiones de redes, no deberían permitir alguna brecha en la seguridad en una de las redes y que se extendiera al resto y afectara a la totalidad de la red, por lo que utilizar una barrera de seguridad es el medio efectivo para evitar el acceso a intrusos que dañen o destruyan la red.

Para poder aplicar estrategias de seguridad es necesario estar consciente que la seguridad es necesaria para la protección de los activos informáticos, de esta manera será más fácil aplicar medidas de seguridad. También se debe tomar en cuenta que siempre hay amenazas para destruir o hacer mal uso de la información y de la infraestructura. Cada red debe tener sus propios niveles de seguridad, así como mecanismos y procedimientos propios de acuerdo con el ambiente de cómputo instalado.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Aunque el propósito principal de cualquier red es facilitar la comunicación entre sus miembros, ésta característica facilita los ataques a una red insegura. Un sistema operativo bien diseñado provee el medio para restringir el acceso a los usuarios en forma individual y permitir un cierto grupo de funciones. Para mantener la seguridad de una red, es importante planificar y administrar los sistemas en forma efectiva [FARL98].

Los elementos seguridad más importantes que se deben considerar son los siguientes:

- Control en los servidores y estaciones de trabajo.
- Control en dispositivos de comunicaciones (repetidores, enrutadores, módems, etc.).
- Control sobre las aplicaciones y datos.
- Uso de barreras de seguridad.
- Existencia de un plan de contingencia.
- Control de accesos.
- Software de supervisión para los procesos de la red.
- Medidas de seguridad del sistema operativo:
    - Selección de password, asignación de password, vigencia del password, control en el reciclaje del password y cifrado del password.
    - Control en la asignación recursos en forma individual o por grupo de usuarios.
    - Manejo de claves de acceso únicas.
    - Terminación automática de sesión.
    - Manejo cifrado de paquetes de datos.

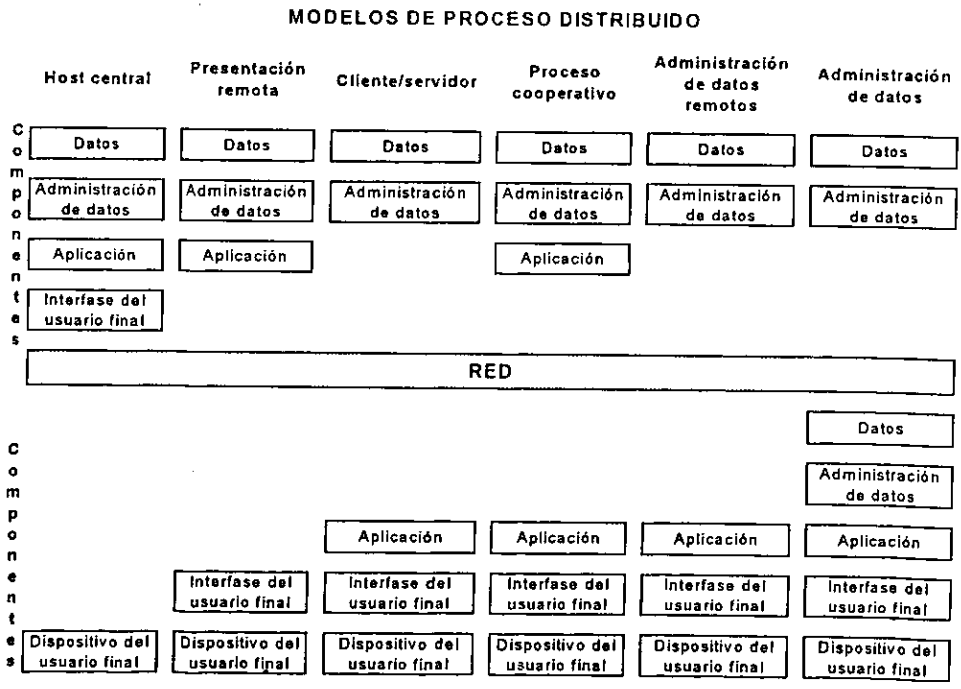
2.5 PROCESO DISTRIBUIDO

El concepto de proceso distribuido tiene diferente interpretación para diferentes personas. Para algunos significa cliente/servidor; para otros proceso cooperativo o como el uso de base de datos distribuidas. Sin embargo, cada usuario debería tener un entendimiento y punto de vista común de lo que es el proceso distribuido.

Una aplicación típica puede ser separada en diversos componentes donde cada uno realiza un proceso específico [DEMP97], el siguiente cuadro muestra los componentes de un típico proceso de cómputo.

Dispositivos para el usuario final	Interfaz para el usuario final	Aplicación	Administración de datos	Datos

Un componente puede ser una unidad separada que realiza una función especifica o varios componentes se pueden agrupar para formar una unidad de procesamiento que puede comunicarse con otros componentes a través de una red. La separación y agrupación de estos elementos en diversas formas pueden ser descritas utilizando modelos de proceso distribuido [DEMP97]. Los grupos de componentes más comunes se ilustran a continuación:



Cuando los componentes de la aplicación incluyen la interfaz con el usuario final, el proceso de la aplicación, la administración de datos y los datos de la aplicación están en un equipo de un procesador, este concepto es conocido como el modelo de procesamiento centralizado en un host.

Cuando el modelo se altera con la incorporación del uso de inteligencia local de una PC para proveer la interfaz para el usuario final mientras los componentes restantes permanecen en el host central, el nuevo modelo es llamado presentación remota.

Si la aplicación se traslada a la PC y los datos se mantienen en el host se tiene un modelo conocido como cliente-servidor. Si la aplicación es dividida en componentes que son ejecutados en el host y en la PC, se tiene un proceso cooperativo. Ahora si todos los componentes están separados en varios procesadores, se tiene un sistema distribuido completo en donde es muy probable que haya desorden a menos que se implante un eficiente sistema de administración [DEMP97].

Un sistema se considera como un conjunto de elementos diferentes que están conectados o relacionados con el propósito de realizar una función única y que no puede ser realizado por un solo elemento. Un sistema distribuido está compuesto por elementos que están distribuidos en diferentes plataformas conectadas mediante una red y que son transparentes para el usuario.

La migración al proceso distribuido y la expansión de la tecnología cliente/servidor y la facilidad que tienen las computadoras para comunicarse, han cambiado dramáticamente el entorno de cómputo de muchas organizaciones. Los grandes sistemas que operaban en entornos de mainframes, de alguna manera ya habían ganado la experiencia de contar con un entorno seguro de operación. En el entorno del proceso distribuido y cliente servidor, los controles de seguridad están distribuidos en las diferentes plataformas y normalmente están fuera del control de un procesador específico. El reto es asegurar que los controles distribuidos trabajen juntos para proteger los activos informáticos.

Los problemas relativos con el proceso distribuido siguen aumentando debido a los requerimientos de interconexión dentro de la empresa y con otras compañías.

Los siguientes problemas son los más comunes que enfrenta el proceso distribuido:

- Débil autentificación. Este procedimiento es la base de la mayoría de los mecanismos de seguridad. Es necesario verificar que las personas o sistemas sean quienes ellos dicen ser. Los actuales métodos de autentificación confían en los passwords o en las direcciones de la red, sin embargo los passwords pueden ser interceptados por alguna persona con acceso a la red, asimismo, las direcciones de la red pueden ser simuladas. Por lo que en estos casos, el mecanismo de autentificación debe ser fortalecido.

- Uso de diversas tecnologías. Debido a la existencia de mucha tecnología, hay muchos estándares o están repetidos, lo que dificulta la instrumentación de soluciones. Existen diversas herramientas de seguridad que son eficientes para resolver problemas, sin embargo, hay dificultades para interactuar entre ellas mismas y para administrarlas en forma adecuada.

- Acceso físico. El acceso físico a los activos informáticos de la red permite a una persona no autorizada tener acceso ilícito a los recursos del sistema.

- Internet. La conexión de una red empresarial a Internet deberá implantarse con muchas consideraciones para no comprometer la seguridad.

- Políticas y procedimientos inapropiados. Las organizaciones frecuentemente no tienen políticas y procedimientos de seguridad adecuados en el entorno de proceso distribuido, se puede incluir las responsabilidades de los empleados en las nuevas políticas y procedimientos.

- Puntos débiles de la red. El punto más débil será el primer punto en experimentar un ataque. Cuando un punto sistema se ha vencido, será usado como una base para comprometer los sistemas más críticos. Se debe lograr una certificación que asegure que todos los sistemas satisfacen estándares; realizar auditorias de todos los sistemas para incrementar el nivel general de seguridad en la institución. Una solución alternativa es

aislar el sistema considerado débil de la red institucional. La seguridad es tan fuerte como el punto más débil de la red.

- Falta de actualización tecnológica. Es difícil para el administrador del sistema mantenerse al tanto de los cambios tecnológicos y amenazas. Muchas brechas de seguridad son desconocidas por la organización y aprovechados por los atacantes. Atacantes expertos en muchos casos conocen más sobre el hardware y software que cualquier otra persona de la organización.

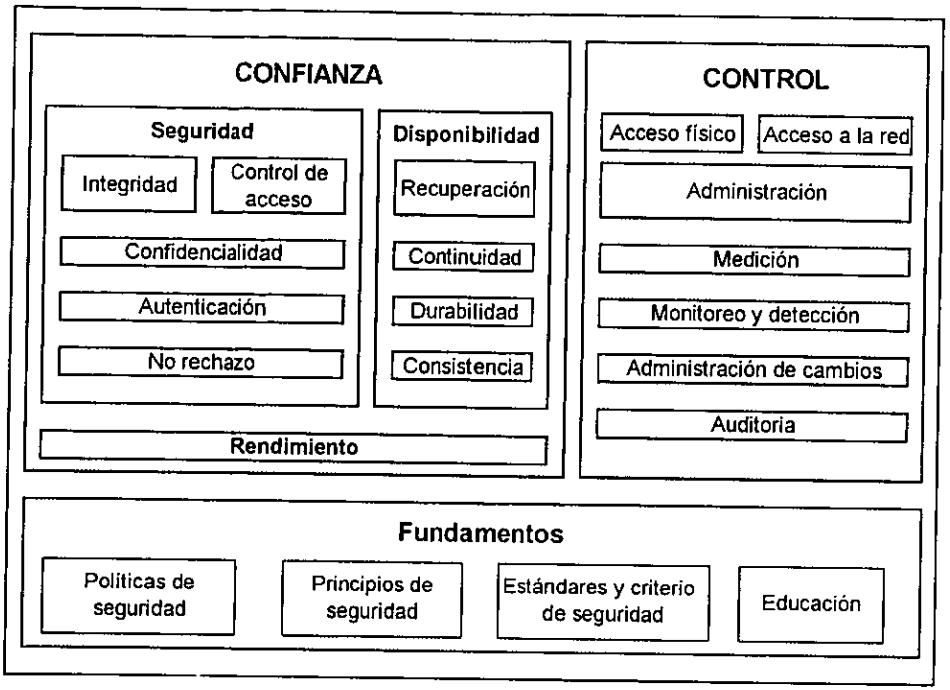
- Planeación inadecuada. Moverse hacia un entorno de procesamiento distribuido causará cambios en el actual modelo de seguridad, los cambios y ajustes en la seguridad no son considerados en la planeación, estos errores causaran conflicto en los controles y generaran situaciones que serán difíciles de manejar y se quedaran sin cerrar muchas puertas de seguridad.

Para contar con los mecanismos de seguridad en el entorno de proceso distribuido es necesario tomar en cuenta todos los componentes de seguridad en las diferentes plataformas distribuidas y considerarlos en una arquitectura de seguridad.

La arquitectura de seguridad puede ser usada para asegurar que el diseño de aplicaciones cumplirá con los objetivos de seguridad requeridos, ayudará a guiar las decisiones entre los sistemas y a través de las plataformas y asegurar que todos los sistemas cumplirán con un nivel mínimo de seguridad estándar.

Una arquitectura de seguridad esta compuesto por diferentes elementos que de forma integral definen un entorno de trabajo para conseguir una solución. Glen Bruce describe una arquitectura de seguridad compuesta por tres grandes componentes (Fundamentos, Confianza y Control) [DEMP97], cada uno integrado con sus propios elementos.

La siguiente gráfica muestra los elementos de la arquitectura de seguridad:



El bloque básico de la arquitectura de seguridad es el de fundamentos, que esta apoyado principalmente por la definición de políticas y principios corporativas, criterios de seguridad definidos y por estándares definidos. El establecimiento de un entorno de proceso distribuido seguro debe ser gobernado por claras y concisas directrices. Las políticas de seguridad proveen un marco para asegurar la protección de los activos informáticos. Los principios de seguridad reflejan la filosofía y estilo de la organización. Los estándares y criterios de seguridad son estándares específicos de seguridad que fueron seleccionados o requeridos para conformar la base de la arquitectura. La educación es apoyada por un programa de concientización y educación en seguridad que servirá para apoyar a quienes son responsables de los procesos y mecanismos de seguridad.

El bloque de confianza esta compuesto por los componentes de seguridad, disponibilidad y rendimiento. Es difícil establecer la confianza en un entorno de diversas plataformas y puede ser establecida cuando se han cumplido los requerimientos de los tres bloques que la componen.

Cuando se ha establecida la confianza en un entorno de cómputo los procesos se pueden realizar con integridad, mantener la confidencialidad de la información privada y realizar las operaciones requeridas sobre bases continuas.

El control abarca las funciones para controlar los mecanismos de seguridad, provee las características de administración y medición que son requeridas para supervisar que las operaciones del sistema sean seguras. Los mecanismos de control incluyen el control del acceso a las computadoras y dispositivos de la red, control del acceso a la red, control de los mecanismos de seguridad. Asimismo, incluye las herramientas para analizar y reportar el rendimiento de los componentes de seguridad, revisar y detectar los problemas actuales o potenciales de seguridad.

Los procedimientos y mecanismos para la administración y mantenimiento de cambios en los componentes de seguridad como son las listas de passwords, listas de control o llaves de cifrado son útiles para mantener la integridad de los mecanismos de seguridad. Contar con seguridad en las funciones de administración debe ser tomadas en cuenta porque pueden ser utilizadas para tener acceso no autorizado al sistema.

La seguridad del proceso distribuido incluye los mecanismos de seguridad en las tecnologías que se utilizan en éste entorno, la seguridad en los sistemas operativos, aplicaciones y en las redes deben considerarse en conjunto para contar con un entorno confiable y las deficiencias que pudieran existir en alguna área deberán ser compensadas en otra área, por ejemplo, si el tráfico de una red esta siendo monitoreada en forma no autorizada, se puede usar alguna técnica de cifrado para compensar la deficiencia.

Algunas consideraciones de seguridad en los componentes del proceso distribuido son los siguientes:

- Confiabilidad de la red. Una red es confiable o segura cuando tiene suficientes controles de seguridad que previenen el abuso de su operación, aseguran la integridad de la red y proveen protección contra acceso no autorizado a la red y contra el monitoreo ilícito de su trafico.

- El protocolo de comunicaciones TCP/IP que es utilizado para comunicar diferentes plataformas y el protocolo UDP/IP presentan diversas debilidades en la seguridad, como puede ser el monitoreo de paquetes, fuga de información de la red, simulación de direcciones o ataques a las rutas y direcciones de comunicaciones, por lo que es necesario incrementar la seguridad en ésta área.

- En los sistemas operativos para red como Netware de Novell, LAN Manager de Microsoft, LAN server de IBM y Vines de Banyan, existen diversos mecanismos de seguridad para realizar las funciones de autentificación, autorización y auditoria, sin embargo es conveniente contar con herramientas adicionales para incrementar la seguridad de las funciones mencionadas.

- El sistema operativo UNIX puede proporcionar diferentes servicios a través de la red como telnet, transferencia de archivos, servicio compartido de disco e impresión, comunicación entre programas, por lo que se deben tomar en cuenta los mecanismos de seguridad para proporcionar los servicios de manera confiable y para proteger la red, en particular deberá reforzar las operaciones de autentificación y autorización, por que las que tiene el sistema operativo UNIX presentan debilidades.

- El entorno cliente/servidor las consideraciones más importantes se refieren a la autentificación entre el cliente al servidor y viceversa. El cliente debe proveer la identidad al servidor, asimismo, el servidor debe probar que es el correcto servidor para el cliente. En este entorno es requerido el uso de técnicas de cifrado para la comunicación entre el cliente y el servidor.

- Las bases de datos tienen mecanismos robustos de seguridad para proteger los datos aún cuando intrusos han tenido acceso a la red. El sistema de administración de bases de datos relacionales (RDBMS) debe contener controles de seguridad para la autentificación de usuarios, definir el perfil de los usuarios, control de operaciones sobre la base de datos. Sin embargo, hay algunos problemas dentro y fuera de la base de datos que se deben cuidar

para tener un entorno confiable, por ejemplo, si la seguridad en el sistema operativo del cliente o del servidor está comprometida, la seguridad de la base de datos puede estar comprometida también, si las aplicaciones en lote utilizan passwords escritos en sus instrucciones, puede comprometerse fácilmente la seguridad, la administración de un gran número de RDBMS requiere de herramientas automatizadas para sincronizar claves, passwords y derechos de los usuarios.

- Los servicios que se proporcionan mediante Internet y el uso que le dé una organización a esta tecnología, como proveer información corporativa, servicio a clientes o información entre clientes, comercio electrónico deben contar con suficientes controles de seguridad, uno de los requerimientos de seguridad es proteger la red de la intrusión no autorizada, si se usa Internet para ejecutar programas realizados con el lenguaje Java, trae implicaciones de seguridad porque se pueden descargar y ejecutar programas desconocidos sin el conocimiento del usuario.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Los siguientes mecanismos realizados en forma apropiada, proveen un medio ambiente de cómputo distribuido seguro:

- Políticas y procedimientos de seguridad para las diferentes plataformas.
- Políticas y mecanismos para el control de acceso físico.
- Mecanismos de autentificación.
- Administración de mecanismos de seguridad.
- Sistemas para monitoreo y detección de actividades en red.
- Administración de cambios de los mecanismos de seguridad.
- Pistas de auditoria.
- Uso de barreras de seguridad.
- Técnicas de cifrado.

2.6 CENTRO DE CÓMPUTO

El centro de cómputo es el lugar físico dentro de las instalaciones de una organización donde se localizan las principales computadoras, el software, el personal que realiza el procesamiento electrónico de información mediante el uso de computadoras y el personal responsable de las operaciones diarias, para llevar a las actividades se necesitan funciones específicas y de especialistas en la materia. Las organizaciones han sido cada vez más dependientes de los procesos automatizados para conducir su negocio y para mantenerse competitivo, la disponibilidad de los servicios del centro de cómputo es muy requeridos por la empresa y sin ellos difícilmente podría funcionar, ya que los procedimientos manuales en caso de existir no están actualizados.

A los responsables de los centros de cómputo les falta mayor conciencia de la existencia de hechos imponderables que pueden ocasionar daños irreversibles a la organización, por ejemplo: no cumplen con los requisitos mínimos de seguridad física; además de no contar con las instalaciones adecuadas para el óptimo funcionamiento de los sistemas, las aplicaciones en operación no tienen un adecuado control interno; el desarrollo de nuevas aplicaciones y el mantenimiento de las existentes carecen de una estrategia para llevar un control de las modificaciones efectuadas; no consideran los objetivos del centro de procesamiento como parte de los objetivos de la empresa; el presupuesto asignado se destina a las necesidades básicas de operación y se olvidan los requerimientos de control interno y seguridad mínimos para garantizar la integridad y confiabilidad de la información; se carece de una planeación a corto, mediano y largo plazo.

Cuando se considera exclusivamente la seguridad física del centro de cómputo, las empresas tienen un entorno ficticio de seguridad cuando en realidad tienen un nivel de seguridad que se encuentra por debajo de los estándares internacionales y el nivel de compromiso de la gerencia con la efectividad es baja.

Se empieza a tener conciencia sobre la seguridad cuando surge un desastre o un abuso de los recursos informáticos.

EXIGENCIAS PARA INCREMENTAR LA SEGURIDAD

Los siguientes factores resaltan el nivel que tiene la seguridad en los centros de cómputo:

1. Concentración del procesamiento y de aplicaciones grandes e importantes que son vitales para el negocio.
2. Dependencia de personal clave.
3. Controles débiles.
4. Terrorismo urbano e inestabilidad social.
5. Constante crecimiento en la conectividad de las redes.

Algunas organizaciones para proteger sus centros de cómputo solamente consideran la seguridad física, este entorno da una situación ficticia de seguridad ya que no toman en cuenta otros factores de seguridad. Para proteger los bienes informáticos en forma integral, es necesario considerar los siguientes elementos de seguridad:

- Políticas definidas sobre la seguridad en computación.
- Organización y división de las responsabilidades.
- Seguridad física.
- Políticas hacia el personal.
- Seguros.
- Estándares de programación y operación de los sistemas.
- Plan de contingencia.

Cada una de éstas áreas tienen su importancia, por lo que la ausencia de alguna dejará una brecha que puede ser aprovechada y abusar de los recursos informáticos.

La seguridad depende finalmente de la integridad de los individuos que conforman una institución. No existe una seguridad total y cada institución depende de su personal para lograr los niveles de seguridad requeridos.

RIESGOS PRINCIPALES

No todas las instalaciones de cómputo tienen las mismas exigencias de seguridad, algunas son mayores que otras. Cuando se establece el grado de riesgo, es importante considerar primero los tipos de riesgos a que están expuestas las instalaciones de cómputo, las más relevantes son los siguientes:

- Accidentes causadas por mal manejo o negligencia.
- Ataques deliberados en forma de robo, fraude, sabotaje o huelga.
- Abuso o mal uso de las instalaciones y bienes informáticos.
- Desastres naturales (terremotos, inundaciones, tornados, etc.).
- Interrupciones en el servicio.

La seguridad efectiva debe garantizar la prevención y detección de un accidente o ataque, la existencia de medidas claramente definidas para afrontar el desastre cuando ocurra y si existe una interrupción en el procesamiento restablecerlo con el procedimiento adecuado.

Las actividades que desarrolla el personal del centro de cómputo deben ser independientes de las funciones de empleados de otros departamentos con quien trabaja en conjunto, la división y asignación de responsabilidades es esencial para aplicar controles efectivos y proteger los datos y el software, por lo que es conveniente tener cuidado en los siguientes puntos:

1. División de responsabilidades.- Permite lograr la revisión y los balances sobre la calidad del trabajo, previene el uso ilegal de computadoras, datos y software, evita la manipulación o modificación no autorizada de los datos y software. Algunas recomendaciones para la división de responsabilidades son:
   - El personal que prepara datos no debe tener acceso a las actividades de operación.
   - El personal de desarrollo de aplicaciones no debe tener acceso a las actividades de operación y viceversa.

- Los operadores no deben tener acceso irrestricto a las funciones de protección de la información, se les debe prohibir la corrección de errores y examinar datos de entrada o de salida.
- Las funciones de desarrollo y mantenimiento deben estar separadas.

Para reforzar la división se pueden aplicar restricciones tanto físicas como de procedimiento y deben aplicarse a los usuarios, las funciones deben estar claramente definidas y autónomas, el grado de división entre las diferentes funciones dependerá del nivel que la instalación requiera.

2. Existencia de un sistema de control interno.- Los elementos que constituyen este sistema permiten la verificación de que se está trabajando de acuerdo con las directrices establecidas.

3. Asignación de responsabilidades de seguridad.- En la descripción de labores se deben especificar las responsabilidades correspondientes, la seguridad es un área clave de resultados o de acción. Las responsabilidades se determinan conforme a la política establecida por la empresa. A medida que desciende la jerarquía, las responsabilidades son progresivamente más operativas y detalladas.

4. Sustitución del personal clave.- La existencia de individuos que poseen un nivel alto de conocimientos técnicos origina una situación de alto riesgo para la institución, por lo que un elemento de seguridad consiste en garantizar que para una persona clave existe una sustitución adecuada. Como en la práctica es difícil asegurar la sustitución de todo el personal, es importante definir quien puede ser una persona clave.

SEGURIDAD FÍSICA

La seguridad física ha sido atendida tradicionalmente, sin embargo, aunque hay un nivel aparente de seguridad la protección real por lo general es inadecuada. El objetivo de la seguridad física es proteger los recursos informáticos contra la destrucción accidental o intencional, corrupción, interrupción, robo fraudulento de datos o de divulgación. Los principales elementos que se deben proteger son los siguientes:

- Personal.
- Inmueble.
- Computadoras y dispositivos periféricos.
- Equipo de telecomunicaciones, eléctrico y de aclimatación.
- Medios de almacenamiento (discos, cartuchos, CD-ROM, etc.)
- Documentación.
- Suministros.

Las medidas generales de protección orientadas a la seguridad física del centro de computo son:

1. Ubicación y construcción del centro de cómputo.- La sala de cómputo se debe instalar lejos de las áreas donde pudiera ocurrir un incendio o explosión, debe estar lejos de las instalaciones de calefacción, de electricidad o de los lugares donde se almacenan materiales inflamables. Debe estar lejos de las áreas de mucho tránsito, tanto terrestre como aéreo. La construcción del interior también tiene gran importancia, las divisiones deben ser adecuadas para la seguridad, paredes y techos resistentes al fuego y evitar los vidrios perimetrales que permiten observar las actividades que se están realizando.

2. Aire acondicionado.- El uso de éste equipo es indispensable en el lugar donde se ubique la computadora, sin embargo, un desperfecto puede ocasionar que la computadora se tenga que apagar. Las instalaciones del aire acondicionado son una fuente de incendios y el ataque físico puede realizarse a través de los conductos de aire acondicionado.

   Para afrontar los anteriores riesgos es conveniente instalar aire acondicionado de respaldo, redes de protección en los conductos externos e internos, instalar detectores de incendio en los conductos e instalar monitores y alarmas de sonido. Las entradas de aire fresco no deben estar al nivel del suelo y deben estar lejos de las áreas donde haya polvo.

3. Suministro de energía.- La energía no debe presentar variaciones para no dañar los equipos de cómputo, por lo que se puede instalar un regulador para eliminar este problema. En instalaciones de alto riesgo, se debe contar con un sistema de respaldo donde se conectan los equipos más importantes.

4. Riesgo de inundación.- La ubicación de las computadoras debe estar en las partes altas de una estructura de varios pisos, lejos de las áreas donde se utilice agua como puede ser el comedor de la empresa y lejos de las cañerías ya que una ruptura o bloqueo puede ocasionar una inundación.

5. Protección contra incendios.- El fuego y sus consecuencias (humo, calor, vapores, etc.) son elementos que ocasionan daños a las instalaciones y ponen en peligro la integridad de los datos, por lo que es conveniente contar con un programa de prevención de incendios las principales medidas que se deben considerar son:

    - Detección de incendios.- La instalación estratégica de los detectores de humo con las siguientes características específicas ayudarán a disminuir en forma efectiva el riesgo de incendio:

        1. Los detectores se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado. Deben estar en la sala de cómputo y en el perímetro físico de las instalaciones.
        2. Los detectores deben ser capaces de detectar los distinto gases que desprenden los cuerpos en combustión.
        3. Las alarmas contra incendio deben estar conectadas con la alarma central del lugar o directamente al departamento de bomberos.

    - Extinción contra incendios.- La instalación debe contar con un efectivo sistema de extinción contra incendios, se deben revisar con regularidad sus componentes, así mismo, es necesario definir y documentar los procedimientos que se deben aplicar en caso de incendio y entrenar al personal que los utilizará.

6. Mantenimiento.- Un buen programa de mantenimiento a las instalaciones, llevado a la práctica en forma controlada simboliza una buena administración y aumenta la seguridad en computación.

7. Acceso físico.- Para diseñar los procedimientos de acceso es necesario considerar los siguientes elementos:

    - Aplicación de controles durante el día y la noche.
    - Acceso de terceras personas.
    - Área de recepción.
    - Tarjetas de acceso.
    - Sistema de intrusión física y mecanismos de vigilancia.

POLÍTICAS HACIA EL PERSONAL

El personal del centro de cómputo constituye una brecha de seguridad, muchas fallas ocurridas en el centro de cómputo son ocasionadas por errores humanos en forma accidental o intencionada, para reducir los riesgos generados por el personal es importante que existan políticas y procedimientos para la administración del personal del centro de cómputo y un código de ética. Las políticas y procedimientos aplicables son:

- Contratación de personal.- Aunque la mayoría de las empresas tienen procedimientos bien definidos, se debe verificar las referencias y antecedentes de seguridad, realizar pruebas psicológicas y exámenes médicos.
- Evaluar el desempeño.- Además de evaluar la efectividad del desempeño del empleado, puede servir para evaluar su actitud hacia el trabajo, posición y sentimientos generales hacia la institución.
- Políticas sobre vacaciones.- La reglamentación de vacaciones es importante para asegurar que el personal expuesto al estrés descanse periódicamente de manera apropiada. Esta puede ser una manera de detectar robos, fraudes y planes de

sabotaje. La dependencia de las operaciones en personal clave no debe obstruir la reglamentación de ésta política.

- Actitudes hacia el personal.- Mantener motivado al personal puede reducir las brechas la seguridad, las fallas ocasionadas por la deslealtad y los ataques deliberados pueden ser menos probables.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Para realizar la evaluación y escoger medidas de seguridad, debemos tomar cuenta las posibles amenazas, las más importantes son las siguientes: inadecuada integridad de datos; acceso no autorizado a la información por parte de empleados y personal externo; espionaje industrial; sabotaje a los programas, equipo e instalación; pérdida o daño de datos causados por desastres; deficiente distribución de los recursos en el centro de cómputo; violación a los derechos de autor; infección y contaminación del software y hardware; inadecuada cobertura de los seguros contratados; obsolescencia del equipo, programas y datos; falta de planes de contingencia, respaldo de instalaciones y equipo; y controles inadecuados en el proceso de comunicaciones.
Los principales elementos de evaluación son:

- Separación de actividades.
- Desarrollo de sistemas.
- Control de cambios en los programas.
- Operación del equipo de cómputo.
- Control de calidad en las aplicaciones
- Comunicaciones
- Biblioteca de datos
- Planes de contingencia
- Políticas de acceso
- Políticas para el personal

2.7 COMUNICACIONES

Durante el uso de red de comunicaciones para la transmisión de datos de una empresa se deben considerar mecanismos para la protección de los activos, mantener la integridad de los datos y permitir a las aplicaciones lograr los objetivos en forma eficiente y efectiva. Estos mecanismos deben de ser considerados cuidadosamente durante el diseño y la planeación de las redes para la posterior implantación de medidas de seguridad [WEBE85].

Las principales fallas que pueden ocurrir en la red de comunicaciones son:

1. Errores en la línea causada por ruido.- El ruido es una señal eléctrica aleatoria que ocurre en las líneas de comunicación ocasionando degradación del rendimiento. Las causas de la existencia de ruido son debidas a condiciones atmosféricas, contactos en mal estado, también el ruido se incrementa cuando el usuario transmite una cantidad mayor de datos sobre las líneas de comunicación, el uso de líneas publicas agrega ruido, lo que podría incrementar las fallas.
2. Fallas de hardware.- Fallas intermitentes en los dispositivos pueden corromper la información transmitida a través de la línea de comunicaciones.
3. Fallas de software.- El software del sistema puede ocasionar que todos los usuarios conectados sean afectados con los consecuente errores de transmisión.

Los efectos de los errores durante la transmisión de datos puede ser catastróficos, por ejemplo, un pequeño porcentaje de errores durante la recepción transacciones en línea puede corromper rápidamente la base de datos; la corrupción de un campo en una aplicación de inventarios puede ocasionar errores en el embarque o borrado inapropiado de información en la base de datos.

Los errores pueden ser detectados mediante verificación por repetición (echo check) o la construcción de redundancia en el mensaje transmitido. Las medidas para mejorar la calidad de la transmisión de datos afectan el rendimiento de la línea de comunicaciones, por lo que uno de los retos del diseño es balancear el costo del rendimiento con el costo de detección de errores [WEBE85].

La verificación por repetición implica que el receptor de un mensaje, regrese el mensaje recibido al sujeto que lo envió para compararlo con una copia del mensaje enviado, si hay alguna diferencia, el mensaje se vuelve a transmitir con un protocolo de datos para indicar que el mensaje previo contenía errores. Este tipo de verificación normalmente usa una línea de tipo full-duplex o se aplica donde las líneas de comunicación son cortas.

El uso de redundancia toma la forma de códigos para detectar errores. Los tres principales tipos de códigos son:

a) Códigos de verificación de paridad.

b) Códigos M-de-N.

c) Códigos cíclicos.

En las verificaciones de paridad pueden ser realizados en forma vertical para verificar un carácter o en forma horizontal para verificar una cadena de caracteres, una combinación de verificación vertical y horizontal proveerá mayor protección contra los errores.

En la codificación M-de-N los caracteres deben ser representados como un numero fijo de bits con valores de 0 y 1 para un carácter. Por ejemplo, cuando se usa una codificación 4-de-8, la cadena de bits para un carácter debe consistir de cuatro bits con valor de cero y cuatro bits con valor de uno, si la cadena de bits recibida no se ajusta a éste requerimiento, un error en la línea ha ocurrido. Esta alternativa ofrece una leve ganancia comparada con el uso de verificación de paridad simple.

El código cíclico o codificación polinomial ofrece un mayor grado de protección contra errores en la línea. La forma en que los códigos cíclicos son generados puede ser escogida para minimizar el número de errores no detectados, dando las características de la línea de comunicaciones que se desea usar. La codificación cíclica es más compleja que las dos previas codificaciones, sin embargo, los circuitos para codificar y decodificar son simples.

Cuando los errores se han detectado, el siguiente paso es corregirlos mediante la corrección de códigos o por la retransmisión de datos.

La corrección de códigos permite que los errores puedan ser detectados y corregidos en la estación receptora, sin embargo para que se realice la corrección se necesita un gran monto de redundancia en el mensaje transmitido, también existe un riesgo al intentar realizar la corrección, por este motivo, la detección de errores y la retransmisión usualmente es escogida como una estrategia de corrección de errores en lugar de la corrección de códigos.

Sí la retransmisión es usada para corregir errores, se debe decidir cuantos datos serán transmitidos, pueden ser desde un carácter hasta un lote de varios registros. Retransmitir pequeñas cantidades de datos tiene la ventaja de ser más rápida que retransmitir una gran cantidad de datos, sin embargo, retransmitir pequeñas cantidades de datos tiene como desventaja una detección de códigos de error menos eficiente que la retransmisión de grandes cantidades de datos, ya que ésta última contiene una mayor de redundancia.

Una red de comunicaciones puede ser diseñada para reducir la posibilidad de errores en la línea y la ocurrencia de fallas del sistema, y para minimizar los efectos de los errores y las fallas. La selección de módems, líneas de comunicación y la topología de una red afectan la confiabilidad de la red.

Existen alternativas que permiten incrementar la velocidad y la confiabilidad como es la transmisión por satélite o fibra óptica.

Cuando existe una gran distancia para la transmisión de información, las señales serán distorsionadas y tendrán problemas en la decodificación. El uso de módems permitirá una mayor confiabilidad en la transmisión de datos en grandes distancias y tendrá dos propósitos adicionales: Reducir los errores causados por el ruido en las líneas de comunicación e incrementar la velocidad de transmisión de datos.

Un punto importante que afecta la confiabilidad de la transmisión de datos es la línea de comunicaciones, puede ser una línea pública o una línea privada. En las líneas públicas, el usuario no tiene el control para la transmisión de datos. Las líneas privadas son líneas dedicadas para dar servicio a un usuario en particular. Para pequeños montos de información es más barato el costo de líneas públicas, pero cuando se incrementa el uso, las líneas privadas serán más baratas que las líneas públicas. El uso de las líneas privadas tendrá la ventaja de permitir un mayor nivel de transmisión de datos y que la línea tendrá mayor atributos de calidad.

La topología de una red especifica la ubicación de los nodos en la red, la forma en que están ligados y las capacidades de transmisión de datos entre nodos. El diseño de una topología óptima es un problema complejo que afecta el rendimiento del servicio.

Algunas restricciones sobre la topología de una red son:

1. Limitaciones financiero para la transmisión.
2. Rendimiento y tiempo de respuesta.
3. Disponibilidad y confiabilidad del servicio.

El uso de técnicas de cifrado protegerá la privacidad de los datos, aún en el caso de fallas del software del sistema, del hardware, transmisión de datos o en el caso de acceso no autorizado a los datos.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Existen diferentes modos de proteger las comunicaciones, por lo que se debe considerar el entorno de trabajo para tomar en cuenta las técnicas y procedimientos de protección que se pueden aplicar. Los elementos que se deben tomar en cuenta para la evaluación son:

- Métodos de cifrado.- Administración de llaves, uso de llaves pública o privada, aplicación de paquetes para el cifrado (Pretty Good Privacy, etc.)
- Barreras de seguridad.- La configuración de la barrera de seguridad, determina si está bloqueado el acceso a Internet o si alguna maquina o usuario puede conectarse a otro maquina que está fuera de la red interna.
- Métodos de recuperación en caso del hardware y software.
- Prácticas adecuadas para el respaldo de información.
- Mantenimiento preventivo y correctivo en los equipos de comunicaciones.
- Sistemas para supervisar la actividad de las comunicaciones.
- Técnicas de control de acceso:
  - Uso de passwords generados por el sistema.
  - Longitud y caducidad del password.
  - Número de intentos permitidos.
  - Mensajes de la última vez que se entró al sistema.
  - Uso de archivos cifrados para almacenar los passwords.
  - Restricción al password para usar aplicaciones especificas o bloquear passwords que no han sido usados por mucho tiempo.
  - Uso de tarjetas inteligentes (smart cards).
  - Manejo de password de única vez o no reusables.
- Protección del cableado de la red.
- Identificar las redes conectadas.

2.8 INTERNET

Internet es una federación de redes de computadoras que emplean los protocolos TCP/IP (Transport control protocol/Internet Protocol) para comunicarse y que enlaza computadoras distribuidas en todo el mundo, su uso es generalizado y en la actualidad está creciendo de manera exponencial, une a más de 25,000 redes en el mundo y el número de usuarios se estima en más de 40 millones [HANC96].

La infraestructura instalada para el uso de Internet comprende diferentes medios de comunicación, desde el cable telefónico instalado en casa o en la oficina hasta los sistemas modernos de comunicación vía satélite.

Internet está abierta al público en general las 24 horas del día y utiliza protocolos de telecomunicaciones no protegidos para algunas aplicaciones, las transacciones comerciales o el suministro de información privada se enfrentan a problemas de confidencialidad en el intercambio de información y al monitoreo del acceso.

Ofrece miles de servidores con datos relacionados con temas políticos, sociales, culturales, científicos, etc., foros de debate con expertos en temas específicos, así también, provee un medio para divulgar el trabajo de organizaciones internacionales con el fin de promover y desarrollar a las industrias.

Internet facilita el uso de herramientas y servicios para mejorar la comunicación entre sus usuarios, y son utilizados para consulta o transferencia de información. Mediante FTP, Gopher, Web, WAIS, etc., provee el medio para mantener interactividad entre usuarios a través de correo electrónico, grupos de discusión, videoconferencia, etc. y también existen sistemas telemáticos privados como son los boletines electrónicos [LIUC97].

En Internet el sistema operativo UNIX es de gran uso para la administración de servicios de información o hace algunas tareas más sencillas, a través de este sistema, se configura y se le da mantenimiento a servidores de información, por ejemplo: Web, Ftpmail, etc.

De los servicios de información en Internet, el Word Wide Web (mejor conocido como Web), es el más gráfico y posee las capacidades de enlazamiento más poderosas, sin embargo, hay que tener cuidado ya que a través de los navegadores Web se puede tener acceso a diversas fuentes de información, por lo que es conveniente el uso de barreras de seguridad bien elaboradas para proteger las fuentes de información.

El servidor Web deberá contar con controles de seguridad para el acceso y autentificación de usuarios y restringir el acceso a la información que almacena, aún cuando esté protegido por una barrera de seguridad.

Ftpmail es un servidor de archivos de correo electrónico que obtiene los archivos de Internet por FTP (File transfer protocol). Lee los mensajes de correo que contienen comandos FTP, se conecta a un centro FTP, ejecuta los comandos y envía por correo los resultados de la persona que hizo la solicitud: FTP es la única forma de obtener los beneficios de los programas y datos que se almacenan en los acervos FTP, para la gente que sólo tienen acceso a Internet a través del correo electrónico, para ejecutar un servidor Ftpmail, la computadora debe estar conectada a Internet, el acceso por correo electrónico.

Cualquier servicio que se preste utilizando la telemática se puede proporcionare por un servidor en Internet, por lo que el campo de los servicios que se pueden proporcionar es muy amplio, algunos servicios que comprende pueden ser financieros, viajes, pornografía y juego. Para proporcionar un servicio, el proveedor debe consultar la autoridad pública del país por ejemplo, a través de un abogado local para validar que el servicio está permitido [HANC96].

En Internet se puede manejar el concepto de derechos de propiedad intelectual sobre trabajos que pueden tener la presentación escrita, musical, imagen, software o de bases de datos.

Para no obstaculizar la comunicación y la cultura, se pueden realizar actos de reproducción, transformación, distribución o comunicación sobre trabajos que no requieren la autorización del autor.

Como Internet es de uso mundial, el concepto de derecho de autor puede variar para cada país, es conveniente conocer las disposiciones para publicar o utilizar información, de esta manera, se podrá contar con los derechos de autor y es recomendable contar con una autorización clara y explícita del autor para evitar cualquier problema legal referente a la violación de derechos de autor [HANC96].

Los servicios de información en Internet son considerados como una actividad editorial, por lo que hay tomar en cuenta la legislación que rige en los países donde se instalarán o se utilizarán las publicaciones.

La facilidad que existe para comunicar los servidores por Internet ofrece una gran atracción para los diferentes tipos de intrusos que realizan mas de 70 mil intentos diarios de acceso ilegal en Internet y los enfocan a las compañías de gran escala, universidades e instituciones de gran prestigio.

Existen prácticas comunes para tener acceso ilegal a una red por ejemplo: robo de contraseñas del sistema, escucha furtiva de conexiones, búsqueda de conexiones TCP para descubrir identificación y contraseña de usuarios.

El uso de sistemas de autentificación para proteger el acceso y construcción de barreras de seguridad permitirán bloquear los ataques contra la red de una organización que realizan los hackers que abundan en Internet.

El uso de enrutadores puede controlar los servicios existentes en un segmento de red, para seleccionar los paquetes que pueden ser utilizados, se aplican criterios como el tipo de protocolo, campos de dirección de origen y dirección de destino para un tipo particular de protocolos, con el fin de proteger las redes y los hosts que soportan el protocolo TCP/IP, y también para extender la protección para los hosts que no soportan este protocolo TCP/IP y que estén conectados en la red de la empresa.

Otra alternativa para proteger a la red de una empresa de Internet es con el uso de barrera de seguridad, esta herramienta funciona examinando los paquetes IP que viajan entre el servidor y el cliente, permite el control del flujo de información para cada servicio por su domicilio IP, por puerto y por ambos sentidos.

El uso de barreras de seguridad debe ser usado en conjunto con políticas de seguridad que indiquen claramente lo que está permitido o prohibido. De esta manera la barrera de seguridad deberá asegurar que las acciones que no están permitidas por la política de seguridad fallen, registrar los eventos sospechosos y alertar a la administración interna de los intentos en que van en contra de la política de seguridad.

Existen diversos tipos de barreras de seguridad, de los cuales los más populares son los de compuerta de doble domicilio y las compuertas de anfitrión oculto. La selección del tipo de barreras de seguridad que se instale dependerá de la definición de las políticas de seguridad y la ubicación de los servicios de información que se utilizarán en Internet y del tipo de comunicaciones con los clientes.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Internet por su propia naturaleza al estar abierta al público en general y al utilizar protocolos de telecomunicaciones no protegidos no es posible protegerlo y plantea problemas referentes a la confidencialidad durante el intercambio de información y monitoreo de acceso en ciertas aplicaciones, como es el caso de transacciones comerciales o en el suministro de servicios de información privada [HANC96].

Por lo anterior, si una empresa requiere utilizar aplicaciones en Internet o le permite a sus empleados utilizar los servicios de Internet a través de la red de la compañía debe considerar los siguientes elementos:

- Barreras de seguridad.
- Políticas de seguridad relativas al uso de servicios en Internet.
- Políticas de acceso de información.
- Programas antivirus.
- Técnicas de cifrado.
- Seguridad en el intercambio transferencia electrónica de datos.
- Seguridad en las aplicaciones comerciales en Internet.

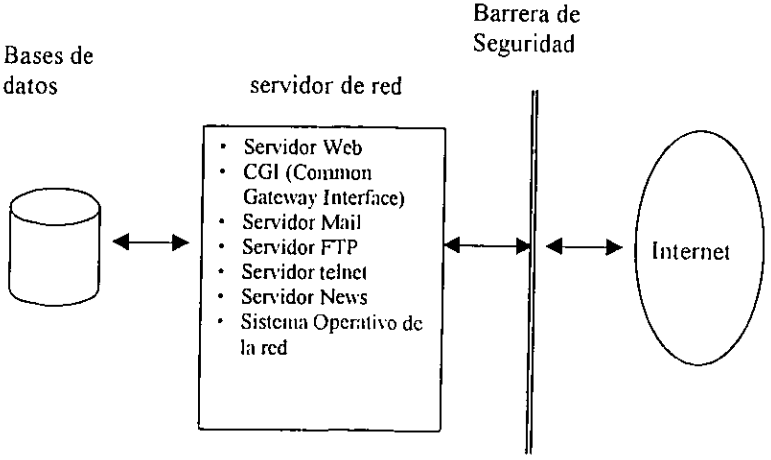
2.9 COMERCIO ELECTRÓNICO

El comercio electrónico (E-commerce) provee a los clientes la opción de comprar, invertir, realizar operaciones bancarias, distribuir e investigar desde cualquier lugar que tenga conexión a Internet como puede ser una oficina, casa, escuela, aeropuertos, hoteles, salas de conferencia, hoteles, etc.

El proveedor de un servicio puede desarrollar su sitio y seleccionar el medio de pago más adecuado para él y para sus clientes. El sistema Web del comerciante consiste de paginas que muestran los productos, las cuales están soportadas por un servidor Web, un servidor de correo electrónico, una base datos que contiene la información de los productos y aplicaciones de apoyo. En este componente se instala un sistema de transacciones que toma las ordenes en linea, trabaja las 24 horas del día durante toda la semana, provee seguridad a las operaciones, permite la integración a los sistemas del negocio y registra los movimientos del consumidor por el sistema.

El sistema existente del comerciante, contiene procesos para la contabilidad, registro y proceso de tarjetas de crédito. La red para el pago permite el procesamiento de transacciones de tarjeta de crédito y otros tipos de pagos como cheques o efectivo.

El consumidor es una persona que tiene una computadora personal, un navegador y acceso a Internet, se debe considerar que puede o no contar con accesorios para soportar sonido, gráficos especiales o formatos especiales para documentos. Los componentes básicos de un sistema para el comercio electrónico se muestran en la siguiente gráfica:



La función general de la bases de datos y de los componentes ubicados en el servidor de red es la siguiente:

Bases de datos.- Usualmente son bases de datos relacionales u orientada a objetos que registran las transacciones, almacenan cuentas válidas y el inventario de los productos comerciales.

Los scripts del CGI son programas que se ejecutan en el servidor Web, son usados frecuentemente para recuperar información de formas almacenadas en sitios y realizar búsquedas en línea en los sitios, también son usados para actualizar las bases de datos y hacen que el Web sea más interactivo. Los scripts son escritos en diferentes lenguajes donde destaca el lenguaje Pearl, debido a que se pueden desarrollar scripts en forma rápida y fácil.

Los servidores mail, FTP, telnet, News permitirán la trasferencia de información adicional de los productos que se comercializan entre el cliente y el proveedor.

Internet al abolir las fronteras que separan a las compañías de los consumidores, a los vendedores de los consumidores y a los proveedores de servicios de los clientes, provee a las empresas comerciales de una nueva arma económica y una herramienta ultramoderna que permite apoyar a sus áreas de publicidad y mercadotecnia. También, Internet puede ser utilizada para ampliar el prestigio de una compañía, aplicar estrategias comerciales, promover sus productos y servicios a bajo costo, así también, puede ser muy útil para analizar mercados y perspectivas de clientes, para concretar transacciones comerciales, para realizar investigación y desarrollo, y para reclutar personal.

En la actualidad el comercio está creciendo a un ritmo acelerado, en las Central Source Yellow Pages aparecen más de 10 millones de referencias comerciales en Estados Unidos para participar en negocios en Internet

Para los proveedores de servicio, deben de tomar en cuenta los sistemas legales nacionales existentes que regulan la publicidad de los algunos servicios y productos (cigarros, financieros, médicos, etc.), ya que éstas pueden ser muy severas o prohibitivas. También, las regulaciones

estipulan que la publicidad no debe ejercer ninguna presión al consumidor, esto es con el fin de proteger a los consumidores más vulnerables.

En las transacciones que se realizan por Internet para la venta de un bien o prestación de servicio, tienen la apariencia de correr alto riesgo por no tener un fuerte respaldo legal y por la ausencia de un papel, sin embargo existen contratos que se rigen por reglas generales y especificas sobre contratos particulares. Así también, los pagos realizados a través de Internet con tarjetas de crédito, intermediarios electrónicos o con dinero electrónico ocasionan problemas legales orientados a la protección al consumidor.

Las transacciones comerciales por Internet pueden ser concretadas mediante un nuevo concepto que es el dinero electrónico y por instituciones que actúan como intermediarios comerciales que tienen la finalidad de garantizar la seguridad de las transacciones realizadas a través de Internet.

Los métodos utilizados para realizar operaciones comerciales presentan algunas ventajas y desventajas relacionadas con la confidencialidad, anonimato de las transacciones, facilidad de uso para la compra y la operación para el vendedor y para el costo y velocidad de la transacción.

El desarrollo de la mercadotecnia y comercio puede crear información de clientes ocasionales y los registros de sus visitas se graban, almacenan y analizan para crear perfiles de los consumidores y transmitir información de datos personales a otros países.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Los elementos de seguridad deberán existir en los componentes del sistema destinado al comercio electrónico y de esta manera evitar que los ataques se presenten donde no existan mecanismos robustos de seguridad. Como cualquier otra aplicación, existen riesgos relacionados con procedimientos de personal, personal y seguridad en los que se deben profundizar de acuerdo con el medio ambiente de la organización.

Los siguientes elementos y el software requerido para realizar el comercio electrónico debe contar con los controles de seguridad adecuados:

- La seguridad en el servidor para el comercio electrónico es de vital importancia para el consumidor y para el proveedor, las debilidades del servidor lo expone a los ataques de cualquier parte de Internet.
- Barrera de seguridad.
- Sistema operativo
- Base de datos

2.10 INFORMACIÓN NO AUTOMATIZADA

Ya que la información es un concepto complejo y vago, que puede ser verbal, escrita, gráfica o codificada, que puede residir en libros, discos de computadora o en la mente de alguna persona, se considerará en este apartado como información no automatizada a la información que haya sido impresa, adicionalmente, se comentará la documentación y otras formas de información que son importantes para la empresa.

La información no automatizada puede ser procedimientos secretos, relativa a los clientes, resultados de investigación y los documentos como los cheques, facturas o acciones de la empresa pueden ser vitales para el funcionamiento de la empresa.

Cuantas historias han circulado sobre gente ajena a la información, que tomó documentos conteniendo estrategias y datos de los planes de venta, listas de clientes, nómina y passwords dejados en los escritorios, en la oficina, lugares de tránsito dentro de la empresa, inclusive de la basura en perjuicio de la organización, por lo que es prudente tomar medidas muy sencillas para prevenir estas ocurrencias.

Las medidas de seguridad que se aplicarán a esta información pueden ser de tipo legales como el derecho de autor, secreto de comercio, también se pueden aplicar medidas adicionales. Los libros, mapas y anuncios son información impresa que está protegida por ley, las fórmulas de algunos productos están protegidos por secretos comerciales. Cartas de negocios, memos, notas son documentos que pueden contener información valiosa para la empresa.

Los criterios para mantener la información están determinados por su importancia para la organización y de la disponibilidad que se requiere para la operación, propósitos legales y de auditoria, de esta manera se podrá tomar la decisión de cómo, donde, cuanto tiempo es mantenido y el momento de su destrucción y desarrollar los procedimientos correspondientes para llevar a cabo estas tareas.

El calendario de retención de información debe estar coordinado con la administración de los sistemas de información, ya que la información en papel y el medio electrónico están muy interrelacionados, los registros de retención deben ser compatibles con el calendario de respaldo de los datos en la computadora.

Es importante obtener la aprobación por la alta gerencia para la implantación de los planes, porque la administración de los registros tiene un relevante costo financiero.

Una empresa bien organizada debe contemplar la información no automatizada en sus prácticas de administración de información y puede incluir las siguientes:

- Planes de retención.- Contar con un formato donde se indique el tiempo de retención de los datos.
- Cumplir con los principios de retención para asuntos legales y operativos, se debe actualizar el programa de retención para reflejar los cambios en la ley y los cambios de las formas y procedimientos de la organización.

Los documentos identificados como vitales para la empresa son necesarios para reestablecer la organización después de un desastre, apoyan aspectos legales, productos, activos, incluye documentos relativos a la estructura de la empresa como son las minutas, registro de accionistas, investigaciones, patentes, contratos, dibujos de ingeniería, políticas de aseguramiento, títulos de propiedad y datos de pagos.

En negocios pequeños, esta información es guardada en una sola área, haciendo vulnerable al negocio en caso de un incendio o de un desastre. En negocios más grandes, los registros vitales se protegen realizando copias que se distribuyen en diferentes lugares, es buena idea realizar copias en microfichas, fotocopias ó en la computadora y mantenerlas en lugares físicos distantes de los originales. Cuando los duplicados no son aceptados legalmente, los documentos originales deben ser guardados con protección máxima y de cualquier forma mantener una copia en un lugar lejano. Los departamentos de finanzas, ingeniería, recursos humanos y jurídico deben participar y revisar regularmente el plan de protección, el cuál debe estar completo y documentado de la forma más clara posible.

Las copias en microfichas son muy útiles porque son aceptadas legalmente y para ganar espacio físico, ya que los originales frecuentemente son destruidos después de haberse microfilmado. Las copias de microfichas son económicas y pueden ser guardadas en diferentes instalaciones, y será una valiosa evidencia cuando el documento o la microficha original no esté disponible.

El lugar para mantener la información es variable, los registros actuales pueden ser mantenidos en las áreas operativas y para los registros viejos o inactivos pueden ser guardados en las áreas de almacenamiento de la organización ó contratar a una empresa que tenga los suficientes controles ambientales y los servicios de recepción y entrega de documentos.

También se puede contratar los servicios de una empresa para guardar durante un período de tiempo los registros comerciales y finalmente esta información puede ser destruida.

La destrucción de la información tiene implicaciones importantes de seguridad, preservar la información requiere medidas de seguridad para protegerla, esto implica cerraduras, copias de seguridad o procedimientos.

Cuando ya no sea práctico, los documentos se deben destruir para desalentar la búsqueda y exposición de información no deseada, por lo que existen diversos métodos de destrucción de documentación, la destrucción de altos volúmenes de documentación puede realizarse en las instalaciones de la empresa mediante el uso de equipo específico, con solventes o por incineración cuando le sea permitido a la empresa.

Cuando una empresa o un grupo de personas de la institución proporciona los servicios de destrucción, también debe proveer las medidas apropiadas de protección, los servicios normalmente incluyen el equipo de transporte y operadores para remover el papel y asegurar su destrucción. También debe prevenir el acceso a la documentación a personas no autorizadas.

Las empresas dedicadas al almacenamiento y destrucción de información deben proporcionar a sus clientes un certificado de destrucción, para cubrir legalmente al cliente cuando le soliciten registros para un asunto legal y para demostrar que la indisponibilidad de la documentación es

auténtica y que forma parte de un plan, asimismo, cuando la documentación es destruida en las instalaciones del propietario, debe existir la documentación necesaria que acredite la destrucción. Los documentos como los cheques, son necesarios para pagar a los clientes y a los empleados deben contar con las medidas de protección necesarias para estar preparado en caso de siniestro. Las acciones de la empresa, al igual que los cheques, también requieren controles de un alto grado de calidad. Otras formas que pueden ser utilizadas para realizar fraudes con las facturas y ordenes de compra, por lo que deben estar bajo control. Los suministros que no son del tipo ordinario, que no son fáciles de obtener y que algunas aplicaciones los requieren, deben estar a la mano en caso de emergencia.

ELEMENTOS CONSIDERADOS EN LA EVALUACIÓN

Las organizaciones son más dependientes de la información y debe considerar las medidas de seguridad para proteger documentos, microfichas, imágenes y otro tipo de formas que son necesarias para realizar sus operaciones. También, se debe considerar un plan que incluya las formas y accesorios requeridos por los sistemas. Los elementos que se deben considerar en la evaluación son los siguientes:

- Programa de retención de registros.
- Copias de registros vitales.
- Bitácoras de traslado
- Distribución de los programas de retención a los departamentos involucrados.
- Políticas de destrucción de información sensitiva.
- Acceso restringido a los contenedores de información que será destruida.
- Control en él envió, recepción y almacenamiento de la provisión de cheques.
- En caso de contratar a una empresa para almacenar la información, considerar la documentación de los controles existentes (registros enviados y regresados, certificados de destrucción, protección contra fuego, ubicación física, etc.).
- Controles en la destrucción de documentos.
- Existencia de cheques, formas y suministros en caso de emergencia.

3. METODOLOGÍA PROPUESTA PARA EL DIAGNÓSTICO DE RIESGOS

INTRODUCCIÓN

Los participantes del diagnóstico de riesgos requieren de una guía que oriente sus esfuerzos y desarrollar su labor en forma eficiente y efectiva para obtener resultados de calidad.

Al efectuar diagnóstico de riesgos en informática se puede aplicar el enfoque cuantitativo, donde todos los riesgos son calculados en términos monetarios o puede aplicarse el enfoque cualitativo que agrupa los riesgos en categorías. Cada uno ofrece ventajas y desventajas, sin embargo, no hay una clara visión de cual puede ser mejor.

El método seleccionado dependerá de factores inherentes a la organización que está en estudio y del grupo que realizará la revisión, algunos factores relevantes son: Naturaleza de la organización, experiencia del personal que realice el análisis, el tiempo para recolectar información y para elaborar el reporte, etc.

Este documento presenta los principios, etapas y acciones que se deben tomar en cuenta para realizar un diagnóstico de riesgos, se deben considerar como un marco de referencia, ya que la problemática en materia de riesgos informáticos varia de una empresa a otra. Adicionalmente, si se desea dar mayor alcance a un diagnóstico, la metodología puede ser complementada en sus etapas.

DESCRIPCIÓN DE LA METODOLOGÍA

Las etapas de la metodología están orientadas para proponer recomendaciones que reduzcan o eliminen las amenazas sobre los activos informáticos, considerando el costo-beneficio de su implantación.

Durante las primeras etapas, la metodología guía el análisis de requerimientos para determinar su importancia y alcance del diagnóstico mediante el acopio de información. Posteriormente se pasa a

la etapa de planeación y posteriormente, se trabaja a fondo en recopilar, analizar y certificar la información, utilizando diferentes técnicas y herramientas.

Durante la recopilación de información, se identifican activos importantes, posibles vulnerabilidades y amenazas, etc. La información requerida debe ser más específica, por lo que el diagnóstico se debe enfocar hacia las áreas donde aparentemente debe haber más problemas. Se determinan hallazgos, en forma iterativa se analizan con mayor detalle para confirmar la existencia de áreas vulnerables, se cuantifica la importancia del impacto, el costo adecuado de la recomendación y que tan urgente es ponerla en práctica.

La metodología resalta la importancia de concientizar a usuarios de las amenazas existentes sobre los activos informáticos y cómo el grupo de diagnóstico de riesgos le puede proporcionar ayuda a través de consultoría, para la implantación de recomendaciones.

Durante el desarrollo del diagnóstico de riesgos, se deben aplicar los siguientes principios para que la metodología funcione adecuadamente:

- **Adaptabilidad.**

  Las etapas de la metodología de diagnóstico de riesgos son siempre las mismas, pero se modifican para adaptarse lo mejor posible al ambiente de la organización que esta siendo revisada. Para realizar los ajustes necesarios es conveniente considerar diversos factores como: Tamaño de la organización, áreas de interés, experiencia del equipo de trabajo o productos por revisar.

- **Enfocar el análisis de lo general a lo particular.**

  Aplicar la siguiente secuencia que permita revisar de forma global y detallada los lineamientos de la organización que afectan a los activos informáticos:

  1. Analizar políticas, estructuras funciones y responsabilidades.
  2. Analizar procedimientos, controles e instrucciones resultantes de las políticas.
  3. Revisar las practicas asociadas con los procedimientos y controles de seguridad.

Las políticas son la base y marco de referencia para la identificación e implantación de medidas de seguridad (procedimientos/controles de seguridad). Proporciona dirección para balancear el exceso de control que impedirá la productividad y la escasez de control que incrementará el riesgo.

- **Integrar equipos de trabajo.**

  Es necesario integrar grupos de trabajo con los principales responsables o propietarios de los activos informáticos, de esta forma se comprende mejor cómo operan las áreas, se reduce el tiempo de la revisión y permite transferir conocimientos y experiencia del equipo de diagnóstico hacia el área funcional bajo la revisión.

  La participación de los grupos de trabajo, permite que las recomendaciones sean prácticas y su implantación sea ágil. La seguridad es un tema multidisciplinario que requiere experiencia y conocimiento especializado en muchas áreas.

- **Emplear gente experimentada.**

  Para realizar el diagnóstico de riesgos, es indispensable contar con personal que tenga experiencia porque la aplicación de la metodología requiere de sentido común, madurez y tacto. Sin este requisito, los resultados finales y recomendaciones serán incompletas, posiblemente inadecuados y carentes de la profundidad que gente experimentada puede proporcionar.

- **Notificar visitas.**

  Para que los participantes apoyen a incrementar el nivel de seguridad sobre los activos informáticos, es importante que se informe al personal responsable del área que se revisará, los programas de actividades y objetivos del diagnóstico. Todos los hallazgos y recomendaciones del equipo de trabajo deben ser revisados con la persona responsable de su implantación, para que la información esté completa y cuidadosamente definida, y también para medir y dimensionar el impacto de la recomendación

- **Actuar con actitud positiva.**

  El equipo de revisión debe promover una actitud positiva y constructiva encaminada hacia aspectos de seguridad y control, el equipo de revisión debe indicar donde faltan controles y quién debe ser el responsable de su implantación. Además debe dar el crédito a quien corresponda cuando los controles y prácticas de seguridad sean adecuadas.

- **Visualizar amenazas.**

  Especialmente durante la recolección de datos y el análisis, los miembros del equipo de revisión deben enfocarse en lo que pudiera ir mal, cómo podría cometerse un error o perpetrarse un ilícito y cómo se podrían violar los sistemas de controles. Esto debe hacerse también al entrevistar a miembros del staff quienes tal vez no han pensado en los esquemas de seguridad ni en lo que podría ir mal. Tomar esta posición ayudará al examinador a identificar las vulnerabilidades y guiar las entrevistas para centrarse en las mismas.

- **Mantener confidencialidad en la información.**

  La información generada durante la revisión es muy sensitiva y debe ser controlada cuidadosamente, notas, papeles de trabajo, documentos y reportes debe ser guardados bajo llave, distribuida solo a personas autorizadas y discutida únicamente en lugares adecuados con la gente que requiera conocerla y en la medida en que sea necesario.

- **Solicitar autorización para realizar pruebas**

  Para probar controles de seguridad, se deben realizar con el conocimiento, consentimiento y asistencia del personal responsable o afectado.

ETAPAS DEL DIAGNÓSTICO DE RIESGOS Y PARTICIPANTES EN EL DESARROLLO

Para poder realizar el diagnóstico de riesgos, se deben integrar diferentes grupos de personas con responsabilidades propias, los siguientes grupos son los participantes que deben cumplir con sus responsabilidades para obtener resultados satisfactorios:

- Líder de proyecto.

  Miembro del área responsable de la función de diagnóstico de riesgos, tiene la responsabilidad de coordinar a los integrantes de su área y los trabajos con los responsables del área que será revisada.

- Alta dirección.

  Son los representantes de las áreas donde se realiza el diagnóstico de riesgos o del área responsable de implantar las recomendaciones.

- Equipo principal.

  Formado por miembros de la función de diagnóstico de riesgos y responsables del área a revisar que participarán en todas las etapas.

- Equipo de apoyo.

  Está integrado con miembros de la función de diagnóstico de riesgos y tienen responsabilidades más limitadas y especificas, por ejemplo, aplicar entrevistas y organizar la información.

- Equipo revisor.

  Se integra con el responsable de las principales áreas involucradas, el líder de proyecto, el propietario del activo y un representante de auditoria y contraloría, debe ser un equipo pequeño. La responsabilidad de este equipo consiste en validar el reporte final del diagnóstico y no desempeña funciones operativas.

- Propietario del activo.

  Personal que tiene bajo su responsabilidad la operación o administración del activo informático.

- Equipo implantador.

  Las áreas en cuestión designarán los responsables para atender las recomendaciones específicas.

El diagnóstico de riesgos se puede considerar como un proceso que está compuesto por las siguientes etapas y donde cada participante juega un papel fundamental:

	PARTICIPANTES / ETAPAS	Líder de proyecto	Alta dirección	Equipo principal	Equipo de apoyo	Equipo revisor	Propietario del activo
1	Análisis preliminar	✓					
2	Elaboración del plan de trabajo	✓		✓			
3	Autorización del diagnóstico de riesgos	✓	✓				
4	Confirmación de objetivos	✓		✓	✓		
5	Recopilación de información	✓		✓	✓		
6	Elaboración del reporte preliminar de hallazgos	✓		✓			
7	Revisión, análisis y certificación de hallazgos			✓	✓	✓	
8	Elaboración de borradores del reporte final			✓	✓	✓	
9	Elaboración del reporte final			✓	✓	✓	
10	Presentación del reporte final a la alta dirección	✓	✓				
11	Elaboración del plan de implantación de las recomendaciones			✓	✓		✓
12	Seguimiento a la implantación de las recomendaciones			✓			

Nota: El equipo implantador participa en el paso elaboración del plan de implantación de las recomendaciones.

Cada una de las anteriores etapas se describen en las siguientes secciones.

3.1 ANÁLISIS PRELIMINAR

Participantes: Alta dirección, equipo responsable del diagnóstico de riesgos.

Esta etapa se enfoca en conocer a profundidad el requerimiento y en la construcción de un marco de referencia que permita contar con una visión global de las áreas de oportunidad para realizar el diagnóstico y en determinar la posible existencia de alguna problemática o de riesgos materializados e identificar fuentes de información.

PRODUCTO ESPERADO:	Reporte de análisis preliminar

ACCIONES:

1. - Identificar responsables de las áreas involucradas.
   - Identificar y entrevistar al propietario del activo o al personal directamente involucrado con él.

2. - Obtener y analizar información documental preliminar.
   - Revisar organigramas, diagramas de procesos, reportes significativos, etc. que contribuyan a identificar la magnitud del requerimiento.

3. - Identificar áreas funcionales y aspectos específicos a revisar.
   - Identificar personas internas y externas a la institución y áreas funcionales involucradas con el diagnóstico.

4. - Elaborar el reporte de análisis preliminar, conteniendo los siguientes puntos:
   - Descripción detallada del diagnóstico que se desea realizar.
   - Relación de áreas funcionales y aspectos específicos a revisar.
   - Estimación de recursos a emplear.

3.2 ELABORACIÓN DEL PLAN DE TRABAJO

Participantes : Alta dirección y equipo principal.

La participación de la alta dirección, usuarios clave y responsable del área de informática es indispensable para elaborar el programa de actividades para realizar el diagnóstico de riesgos, se deben considerar los recursos disponibles del área responsable del diagnóstico para fijar metas alcanzables.

PRODUCTO ESPERADO:	Plan de trabajo

ACCIONES:

1. - Documentar el plan de trabajo, considerando los siguientes puntos:

   - Objetivo y alcance de la revisión.
     El alcance de la revisión representa el compromiso que adquiere el área responsable de la función de diagnóstico de riesgos, el cumplimiento de este compromiso se reflejará en el informe del diagnóstico.
   - Actividades que se llevaran a cabo.
     Elaborar una lista de actividades necesarias para realizar el diagnóstico de riesgos.
   - Recursos requeridos.
     Se deben considerar los recursos materiales, humanos, tecnológicos, de tiempo, etc.

2. - Formación del equipo de trabajo.
   Durante esta etapa se definen e integran los siguientes equipos de trabajo y se les asignan responsabilidades:

- Líder de proyecto.
- Alta dirección.
- Equipo principal
- Equipo revisor.
- Equipo responsable de implantar las recomendaciones.

3. – Calendarizar actividades.

- El líder de proyectos debe definir el orden y las fechas de inicio y fin de cada actividad, también debe determinar un responsable y los involucrados en las actividades.

4. –Elaborar una lista de la información relevante.

- Una vez identificada las áreas funcionales y los eventos específicos que serán analizados, se deberá elaborar una relación de toda la información que pueda ser de gran utilidad (manuales, normatividad, reglamentación, etc.)

3.3 AUTORIZACIÓN DEL DIAGNÓSTICO DE RIESGOS

Participantes : Alta dirección del área a revisar y líder de proyecto.

El líder de proyecto debe considerar los elementos necesarios para desarrollar la carta de aprobación del diagnóstico, debe presentar el plan de trabajo a la alta dirección para su autorización para que el equipo de trabajo tenga el apoyo formal y pueda realizar el diagnóstico de riesgos.

PRODUCTO ESPERADO:	Carta de aprobación del diagnóstico

ACCIONES:

1. - La alta dirección del área a revisar debe analizar el plan de trabajo, los recursos involucrados y emitir una carta de autorización con el siguiente formato:

    - Dirigida a los directores, gerentes y a los miembros de sus grupos de trabajo que serán afectados por el diagnóstico.
    - Indicar la alta prioridad del proyecto.
    - Definir brevemente el alcance, objetivos y periodo que cubrirá el diagnóstico.
    - Solicitar explícitamente la cooperación y asistencia para el equipo responsable del diagnóstico de riesgos.
    - Identificar al líder del equipo de trabajo y señalar claramente los resultados esperados del proyecto.

3.4 CONFIRMACIÓN DE OBJETIVOS

Participantes : Líder de proyecto, equipo principal y equipo de apoyo.

Se deben revisar los objetivos y responsabilidades planteados en el plan de trabajo con los miembros del equipo principal y de apoyo.

PRODUCTO ESPERADO:	Minuta de la reunión

ACCIONES: 1. - Reunión de trabajo

- El líder de proyecto, el equipo principal y de apoyo deben estar presentes en una reunión, donde el líder de proyecto exponga en forma clara los objetivos y asigne las responsabilidades que le corresponden a cada uno en el diagnóstico de riesgos para que los participantes tengan una visión clara de lo que se espera de cada uno de ellos y realicen su trabajo con calidad

3.5 RECOPILACIÓN DE INFORMACIÓN

Participantes : Líder de proyecto, equipo principal y equipo de apoyo.

En esta etapa se recolecta y se organiza la información relacionada con el área que se está revisando para analizarla a detalle y conocer la estructura organizacional y funcional del área, identificar los activos informáticos, los controles instrumentados en sus procesos y determinar la existencia de hallazgos en el área diagnosticada.

PRODUCTOS ESPERADOS:	1. - Resumen de entrevistas 2. - Banco de Información

ACCIONES:

1. – El equipo principal y de apoyo deben solicitar la siguiente documentación para su revisión y análisis:
   - Reglamentación interna de la institución.
   - Normatividad del área y departamento.
   - Manual de flujos operativos del área en cuestión.
   - Manual de operación y del usuario.
   - Organigramas.
   - Políticas sobre seguridad organizacional, seguridad física, privacidad y controles.
   - Procedimientos o guías en uso que detallan como ejecutar controles de acceso, datos, servicios, facilidades e información de activos.
   - Reportes presentados en los últimos años por auditores, sobre revisiones de seguridad y de problemas ocurridos.
   - Leyes y regulaciones externas oficiales, nacionales e internacionales.
   - Especificaciones de los activos a evaluar.

   Esta información se debe organizar para que esté disponible a los miembros del equipo. Asimismo, se deben establecer los controles

necesarios para proteger el acceso a esta información de personal que no esté relacionado con el proyecto.

2. - Análisis de la información.

El equipo principal y el de apoyo deben analizar la información recopilada para entender claramente los siguientes conceptos:

- Estructuras organizacionales y funcionales del área revisada.
- Identificar responsables de las funciones de seguridad física y lógica.
- Antecedentes de riesgos y debilidades de control interno que han ocurrido en el pasado.

Sí la información recopilada es muy grande, es conveniente que se distribuyan los documentos entre cada uno de los integrantes de los equipos para que realicen el análisis correspondiente y lo expliquen al resto de los integrantes.

3. - Entrevistas con gerentes de las áreas involucradas.

Durante el desarrollo de las entrevistas, se genera y se recolecta información de los procesos automatizados y de los participantes en los mismos, por lo que es muy importante conducir las entrevistas con gran habilidad y poder contar con información de calidad.

A. Diseño.

- La entrevista se debe realizar por dos integrantes del grupo de diagnóstico de riesgos a sola una persona del área revisada, en caso de presentarse más de una persona se debe orientar la entrevista en el área principal.
- El uso de guías es útil para realizar las entrevistas, sin embargo se deben adaptar conforme la naturaleza de la entrevista.

B. Calendarización.

- Para evitar sorpresas, los gerentes de las áreas bajo revisión deben ser informados de los objetivos y del calendario de actividades establecidos en el plan de trabajo, de tal forma que ellos puedan recomendar en su caso, al personal apropiado a entrevistar de cada área y asegurar que estén disponibles para las entrevistas.

- Mantener la continuidad del programa de entrevistas, es decir, los encuentros deben ser conducidos tan pronto como sea posible. Si un gerente no está disponible la primera semana, un asistente debe ser entrevistado y posteriormente el gerente, a la brevedad posible.

C. Desarrollo

- Durante el desarrollo de la entrevista, se confirma la responsabilidad funcional del área, y se le brinda la oportunidad al entrevistador para que exprese sus opiniones sobre el esquema de seguridad implantado y proponga sugerencias sobre el desarrollo del diagnóstico, con el objetivo de fomentar la participación del personal involucrado y contribuir a incrementar el nivel de seguridad.

- Después de cada entrevista, el entrevistador debe llenar el formato "Resumen de entrevista", para concentrar los principales aspectos de la entrevista.

El equipo principal y de apoyo debe analizar la información para identificar las funciones más importantes y al personal que domine la aplicación, la operación ó que tome decisiones.

4. - Entrevistas con personal clave.

La información generada por estas entrevistas también debe ser de calidad, por lo que el grupo de trabajo debe tener cuidado para organizar cada una de las etapas de la entrevista.

A. Diseño

- En este caso, los dos entrevistadores pertenecen al grupo de apoyo y mantienen la posición de entrevistar a una sola persona a la vez.

B. Calendarización.

- Después de haber terminado la primera serie de entrevistas, los integrantes del grupo de apoyo deben elaborar el calendario para la siguiente serie entrevista, este mismo equipo será el responsable de llevarlas a cabo.

C. Desarrollo

- De igual forma que en la primera serie de entrevistas, los entrevistadores se deben preparar para aplicar la entrevista, es recomendable utilizar la guía para entrevistas como un complemento para generar información de calidad.

Después de cada entrevista, el entrevistador deberá elaborar un "Resumen de la entrevista", el cual permite concentrar los principales aspectos de la entrevista realizada.

3.6 ELABORACIÓN DEL REPORTE PRELIMINAR DE HALLAZGOS

Participantes . Líder de proyecto y equipo principal

Durante esta etapa se deberá analizar la documentación recopilada, elaborar y analizar el resumen de las entrevistas efectuadas, para identificar posibles hallazgos, clasificarlos, elaborar y actualizar un reporte preliminar, que sirva de base para la validación de los hallazgos durante las juntas de revisión.

PRODUCTO ESPERADO:	Reporte preliminar de hallazgos

ACCIONES:

1. - El grupo principal y de apoyo se deben reunir para analizar la documentación recopilada y la información generada durante las entrevistas para identificar posibles hallazgos.

2. - Revisar los aspectos generales del nivel de seguridad y los controles presentes de las áreas funcionales. Los miembros del equipo deben comentar la relevancia y exactitud de los hallazgos.

3. - En cada sesión es recomendable contemplar los siguientes pasos:

   - Identificar los activos más importantes.
   - Revisar los controles que están protegiendo a los activos y compararlos contra los normados y con las prácticas empleadas en otras organizaciones.
   - Contemplar las políticas de seguridad, estándares y controles existentes en la organización. Los hallazgos deben ser usados para clasificar las amenazas y debilidades en controles de seguridad y sus procedimientos.
   - Enunciar brevemente todos los hallazgos.

- Clasificar los hallazgos tomando en cuenta el área de interés.
- Desarrollar escenarios de amenazas potenciales y nuevamente detectar los puntos débiles en seguridad.
- Hacer análisis de amenazas para identificar la principal amenaza de los activos y para asignarles una prioridad relativa.
- Incluir los hallazgos en las siguientes categorías de acuerdo con su prioridad, presencia e impacto dentro de la organización:
  - ✓ Alto
  - ✓ Medio
  - ✓ Bajo

- El equipo principal elabora un reporte preliminar, donde se describen los hallazgos y lo presenta al equipo revisor en una junta de revisión. Durante las juntas de revisión, el equipo revisor analiza los hallazgos y determina si la importancia es correcta y si hay algún hallazgo que deba eliminarse de la lista por carecer de suficiente importancia o si es necesario certificarlo.
- Este proceso se repite hasta que finaliza la etapa de recopilación de información.
- Se sugiere la siguiente estructura para la elaboración del reporte:
  - ✓ Area de interés.
  - ✓ Numero de hallazgo.
  - ✓ Descripción de hallazgo.
  - ✓ Referencia del reporte de donde proviene el hallazgo.
  - ✓ Prioridad.
  - ✓ Situación de la certificación.
  - ✓ Referencia del reporte donde fue certificado el hallazgo.
  - ✓ Número de acción a tomar.
  - ✓ Descripción de la acción a tomar.

3.7 REVISIÓN, ANÁLISIS Y CERTIFICACIÓN DE HALLAZGOS

Participantes: Equipo principal, equipo de apoyo y equipo revisor.

El equipo revisor se reúne para analizar y certificar los hallazgos presentados, por el líder de proyecto, en la versión más reciente del reporte preliminar de hallazgos, así como para orientar las acciones futuras del diagnóstico que deberá realizar el equipo principal

PRODUCTO ESPERADO:	Reporte de hallazgos certificados.

ACCIONES: 1. - Juntas de revisión

- El objetivo principal de estas sesiones es la certificación de hallazgos. El equipo revisor se reúne con el fin de discutir cada uno de los hallazgos, dando su punto de vista y cuestionando todos aquellos hallazgos que no se consideren válidos. También se discute la clasificación de los hallazgos de acuerdo a las áreas de interés.
- Estas sesiones permiten orientar la investigación, es decir, son la guía para determinar en que hallazgos hace falta mas o menos investigación. La información concerniente a los hallazgos clave debe ser obtenida de dos fuentes o verificada través de una segunda fuente.
- Este proceso se repite hasta que el líder juzga que la lista de hallazgos constituye una base suficientemente sólida que justifique comenzar a desarrollar recomendaciones, impacto, etc. en virtud de que no se esperan cambios sustanciales a la lista de hallazgos.
- Dependiendo de la magnitud y alcance del diagnóstico, generalmente el número juntas de revisión puede ir de uno a cinco. La duración de cada junta puede ir de una a dos horas; máximo.

- Los métodos de certificación se utilizan cuando no son suficientes las evidencias presentadas y es necesario certificar la veracidad de las mismas. El esfuerzo de la certificación debe ser proporcional al impacto del hallazgo.

  Entre los principales métodos de certificación utilizados en el diagnóstico se encuentran la documentación, la observación directa, las entrevistas adicionales y las pruebas; en cada uno de ellos se obtiene un reporte de resultados. Para llevar un mejor control de estos reportes se sugiere enumerarlos utilizando una letra que identifique el método de certificación empleado y un número consecutivo. Por ejemplo si consideramos los siguientes métodos:

  D – Documentación

  V – Visita

  É – Entrevista

El identificador "D-02", se refiere al reporte 02 de su documentación.

3.8 ELABORACIÓN DE BORRADORES DEL REPORTE FINAL

Participantes : Equipo revisor, equipo principal y equipo de apoyo.

La elaboración de borradores para el reporte final, se realiza en forma iterativa conforme a la determinación de los hallazgos y con su prioridad.

PRODUCTO ESPERADO:	Borradores del reporte final.

ACCIONES: 1. - Clasificación de hallazgos.

El equipo revisor debe clasificar todos los hallazgos de acuerdo con el impacto que representa para la institución. Se determina el impacto de los hallazgos en la organización. La medición del impacto está basada en un método que considera principalmente el análisis de riesgos, y que dentro del cálculo contempla tres parámetros: Costo, Probabilidad y Alcance

Para el determinar el impacto, se debe considerar los siguientes pasos:

A Determinar categorías de importancia y asignar un valor o rango de valores a cada una de ellas, estos valores se utilizarán en cálculos posteriores.

B. La persona o personas con mayor experiencia deben calificar el hallazgo dentro de una categoría por cada uno de los parámetros.

C. Identificar el valor asociado conforme a la categoría donde se calificó el hallazgo.

D. Multiplicar los tres valores asociados con los parámetros, para obtener un valor que servirá para determinar el impacto del hallazgo y asignar la prioridad correspondiente.

E. Ubicar el valor resultante dentro del rango de la escala de impacto para determinar la prioridad con que debe ser atendido el hallazgo.

Descripción de los parámetros.

Parámetro Costo.

Se refiere al monto en dinero que la organización podría perder en un año si el riesgo detectado se materializa; este monto incluye las pérdidas directas e indirectas. Debido a que las organizaciones tienen diferentes infraestructuras y para facilitar el cálculo, se consideran valores proporcionales a los activos.

Este parámetro considera las siguientes categorías:

Categoría	Valor
Crítico	10,000
Muy alto	1,000
Alto	100
Medio	10
Bajo	1

Descripción de las categorías del Costo:

- Crítico.- Puede implicar la quiebra de la organización (Posible pérdida del centro de cómputo).
- Muy alto.- Pérdidas muy cuantiosas, con esfuerzos la organización puede sobrevivir. Son pérdidas que no pueden recuperarse a través de seguros u otros medios (Daño mayor en una supercomputadora).
- Alto.- Pérdidas cuantiosas que no amenazan la supervivencia de la organización, los seguros cubren un porcentaje limitado de estas pérdidas (Daño en un mainframe).
- Medio.- Pérdidas importantes que podrían ser cubiertas por los seguros o absorbidas por la empresa (Daño en un servidor).
- Suficiente.- La pérdida es pequeña pero lo suficientemente importante para tomarse en cuenta (Daño en una computadora personal).

Parámetro Probabilidad

Se refiere a la posibilidad de que se materialice el riesgo asociado con el hallazgo. Como las categorías se han determinado de manera subjetiva, debe aplicarse el sentido común para determinar que umbral queda más cerca. La probabilidad de cada evento debe calificarse en forma independiente

Categoría	Valor
Alta	1
Media	0.6
Baja	0.1

Descripción de las categorías de la probabilidad

- Alta.- El evento se presenta en promedio 10 veces o más al año
- Media.- El evento se presenta en promedio de 1 a 9 veces al año.
- Baja.- El evento se presenta 1 vez cada 10 o más años.

Parámetro Alcance

Se refiere a la cantidad de áreas funcionales afectadas dentro de la institución si el riesgo se materializa.

Categoría	Valor
Alto	100
Medio	10
Bajo	1

Descripción de las categorías del parámetro Alcance.

- Alto.- Toda la institución se ve afectada por la pérdida.
- Medio.- Se afectan las operaciones de un área o grupo de áreas funcionales.
- Bajo.- Afecta a un solo departamento o a un grupo pequeño de ellos.

Determinación del impacto y prioridad.

Con la multiplicación del valor de los parámetros anteriores se obtienen las unidades de impacto. De acuerdo al rango en el que se encuentre el impacto resultante se determina la prioridad con la que debe implementarse la recomendación:

Impacto	Prioridad
100,000 a 1'000,000	Crítica
10,000 a 100,000	Muy Alta
1,000 a 10,000	Alta
100 a 1,000	Media
0 a 100	Suficiente

Descripción del impacto

- Crítica. – Iniciar la implantación inmediatamente (1 a 3 meses).
- Muy alta. – Iniciar la implantación a corto plazo (3 a 6 meses).
- Alta . – Iniciar la implantación en el mediano plazo (6 a 12 meses).
- Media. – Iniciar la implantación a largo plazo.

2. – Elaboración y validación de recomendaciones.

Por cada uno de los hallazgos certificados, el equipo principal debe trabajar en proponer recomendaciones.

Cada recomendación debe ser validada por el equipo revisor. Puede presentarse diferentes puntos de vista y controversia durante el análisis de las recomendaciones lo que llevará a realizar nuevas pruebas y modificar las recomendaciones.

Es importante que las recomendaciones que ya han sido validadas, se presenten en el reporte final con una estructura uniforme.

El equipo principal debe cuidar que el formato de las recomendaciones tenga los siguientes aspectos:

- Describir las recomendaciones con suficiente detalle, para que la gente responsable de canalizarlas conozca exactamente lo que se espera.
- Es esencial que las recomendaciones sean factibles, esto ayudará a que sean aceptadas por la alta gerencia.

Los eventos sensitivos deben ser tratados separada y confidencialmente con los gerentes apropiados.

A partir de la elaboración del segundo borrador del reporte final, es necesario determinar de manera muy general, los recursos financieros necesarios para la implantación de cada recomendación, ubicándolos dentro de las siguientes categorías: Alto, Medio, Bajo.

También a partir del segundo borrador, debe establecerse una calendarización probable para la implantación de cada recomendación y determinar el área responsable de esta tarea.

3. – Obtención del borrador.

Los miembros del equipo de trabajo deben desarrollar el hábito de escribir borradores de hallazgos y recomendaciones cuando sean identificados y discutidos; solamente deben actualizarlos cuando se realicen cambios o se obtengan nueva información. El tiempo requerido para escribir un reporte puede ser crítico si todos los trabajos se dejan para el final.

El borrador del reporte debe ser distribuido para revisarse y comentarse con los miembros del equipo principal y de apoyo con la finalidad de que los puntos que se toquen sean los suficientemente claros; deben tener cuidado en mantener la integridad en el reporte.

3.9 ELABORACIÓN DEL REPORTE FINAL

Participantes : equipo revisor, equipo principal y equipo de apoyo.

Durante esta etapa se debe preparar un reporte que concentre el resultado obtenido de las principales tareas del diagnóstico de riesgos.

PRODUCTO ESPERADO:	Reporte final.

ACCIONES: El líder del equipo de diagnóstico de riesgos debe consolidar los reportes de las tareas realizados previamente y complementarla para obtener un reporte final completo. Las secciones que debe contener el reporte son las siguientes:

I.- Resumen ejecutivo.

1. Requerimientos iniciales.
2. Tabla de hallazgos de alta prioridad y recomendaciones.

   Se toma como base el ultimo borrador del reporte final y se obtienen diferentes matrices, cuya estructura debe reflejar claramente los resultados obtenidos en el diagnóstico. A continuación se muestra la estructura para la presentación de resultados:

   A. Área de interés en la que se presenta el hallazgo.

   B. Descripción de la recomendación sugerida.

   C. Número de referencia donde se detalla el hallazgo y la recomendación.

   D. Prioridad de atención.

   E. Área responsable de implementar el hallazgo y la recomendación.

F. Recursos financieros para realizar la implantación.

G. Calendarización de cuando debe iniciarse la implantación de la recomendación.

II - Introducción.

1. Requerimientos iniciales del diagnostico.
2. Objetivos y alcance del diagnóstico.
3. Descripción de la metodología utilizada

III.- Implantación estratégica propuesta

IV.- Hallazgos y recomendaciones.

IV.- Anexos

Anexo 1. Personas entrevistadas.
Anexo 2. Visitas efectuadas.
Anexo 3. Documentación revisada.
Anexo 4. Pruebas efectuadas.

El reporte debe ser clasificado como confidencial y controlado apropiadamente; las secciones sensitivas deben ser distribuidas solamente con una petición de conocimiento.

El líder de proyecto debe coordinarse con algún integrante del equipo para preparar la presentación a la alta dirección solicitante del diagnóstico. La presentación debe ser concreta y debe contener los aspectos más relevantes.

3.10 PRESENTACIÓN DEL REPORTE FINAL A LA ALTA DIRECCIÓN

Participantes : Líder de proyecto y alta dirección.

La presentación del reporte a la alta dirección está orientada a obtener su apoyo para la implantación de las recomendaciones.

PRODUCTO ESPERADO:	Carta de respaldo de la alta dirección para implantar las recomendaciones.

ACCIONES:

1. El líder del equipo de diagnóstico de riesgos debe hacer una presentación oral para la alta dirección, con el objetivo de obtener el respaldo para la implantación de las recomendaciones, mediante una carta elaborada por el líder de proyecto y que deba contemplar los siguientes aspectos:

   - Enfatizar que el propietario del activo es el responsable de la implantación de las recomendaciones; es él quien debe solicitar a las áreas ejecutoras y de soporte su participación activa para llevar a cabo las medidas propuestas.
   - Señalar que a partir de ese momento, la misión del área encargada de la función de diagnóstico de riesgos es la de promover y asesorar en la implantación de la recomendaciones, dejando a un lado su papel de responsable directo y líder.

   La presentación permitirá a la alta dirección clarificar algún evento y revisar los puntos elaborados en el reporte; el líder de proyecto debe revisar los hallazgos y las recomendaciones con ella.

   La propuesta final debe ser consistente con los objetivos y alcance definidos al inicio del proyecto.

3.11 ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS RECOMENDACIONES

Participantes : Equipo implantador.

En esta etapa se establecen los objetivos, funciones, responsables y plazos para la implantación de las recomendaciones.

PRODUCTO ESPERADO:	Plan de implantación de recomendaciones

ACCIONES:

1. El área responsable de la función de diagnóstico de riesgos tendrá como misión promover la implantación de las recomendaciones, cambia el papel que desempeña y pasa a ser un participante más del equipo que pondrá en práctica las recomendaciones. El nuevo equipo (equipo implantador), es guiado por el propietario del activo o por él área responsable de implantar las recomendaciones, según el caso.

   Es importante que el propietario del activo solicite la asesoría del área responsable de la función de diagnóstico de riesgos, considerándola en cada una de las etapas de la implantación y seguimiento de las recomendaciones.

   El área responsable de la función de diagnóstico de riesgos debe verificar que a lo largo del proyecto y durante la vida productiva del activo tomen en cuenta aspectos de seguridad. Su participación abarca:

   - Colaborar con el equipo implantador (asistencia a juntas, retro-alimentación de reportes del equipo, certificación de productos, etc.).

- Apoyar o eventualmente realizar la investigación de soluciones o inclusive evaluaciones técnicas y de costo/beneficio (de manera limitada).

2. El equipo implantador debe identificar los objetivos, funciones, responsables, involucrados, recursos y actividades que serán realizadas para implantar las recomendaciones. La elaboración del plan debe incluir también la definición del esquema de seguimiento para fines de seguridad informática; esto es, como el área responsable de la función de diagnóstico de riesgos va a enterarse o revisar periódicamente el avance en el desarrollo del proyecto.

3. Es necesario que el equipo implantador identifique (en caso de que exista) o diseñe e implante (en caso de que no existan) indicadores que permitan "medir" o estimar la eficacia de las recomendaciones, una vez que estén en funcionamiento.

3.12 SEGUIMIENTO A LA IMPLANTACIÓN DE LAS RECOMENDACIONES

Participantes: Área responsable del diagnóstico de riesgos.

Se debe realizar una evaluación del funcionamiento de las recomendaciones implantadas y detección de nuevos requerimientos. Una vez concluida la implantación de las recomendaciones, el área responsable de la función de diagnóstico de riesgos debe monitorear el funcionamiento de las recomendaciones para saber si son efectivas y en su caso hacer correcciones y/o generar nuevos requerimientos.

PRODUCTO ESPERADO:	Reporte de evaluación de la eficacia de las recomendaciones.

ACCIONES: 1. - Evaluación de la eficacia de las recomendaciones.

- Tomando como base los indicadores identificados o implementados para la medición de la eficiencia de las recomendaciones, un representante del área responsable de la función de diagnóstico de riesgos debe establecer revisiones con la finalidad de verificar si las medidas han sido implementadas en forma adecuada, si los riesgos han disminuido como se esperaba, si no se tienen medidas contraproducentes, etc.
- Las revisiones se deben realizar periódicamente, para actuar en el momento requerido en caso de que los riesgos no hayan disminuido como se esperaba. En algunas ocasiones será recomendable volver a realizar otro diagnóstico, por ejemplo en el caso de que no existan indicadores que nos permitan saber con certeza el acierto o fracaso de la implantación de las mismas.

2. - Monitoreo y detección de nuevos requerimientos.

   Las recomendaciones deben ser monitoreada a través de sus indicadores en un mediano plazo (6 a 12 meses).

Puede suceder que los indicadores identificados o los implementados no muestren cambios favorables con respecto al riesgo identificado, esta situación puede deberse a varias razones:

1. Falta de apego a los controles
2. Implantación realizada en forma inadecuada
3. Surgimiento de nuevos problemas o cambio de circunstancias
4. Error en la definición de las recomendaciones
5. Error en la identificación o ponderación de las vulnerabilidades

Para los casos 3,4 y 5 es recomendable realizar un nuevo diagnóstico, en donde ya existe el antecedente y alguna información puede ser útil.

4. REQUERIMIENTOS TÉCNICOS PARA REALIZAR LA EVALUACIÓN

4. 1 ANTECEDENTES

El campo de la seguridad en los sistemas de información continuará creciendo, conforme siga evolucionando y creciendo la tecnología de información, la conexión y la expansión de redes. Los cambios en la tecnología además de tener un gran impacto en los negocios, empresas o en la competencia económica, afectará en las actividades de la seguridad de los sistemas de información. La función de evaluación de la seguridad para poder satisfacer las necesidades de las empresas, deberá mirar hacia el futuro en los campos de la sociedad, tecnología, negocios, competencia y en la impartición de justicia en el crimen por computadora.

En la actualidad la gente encargada de la seguridad está teniendo más educación e información del mundo y de la tecnología, y demandan cada vez más participación a los gobiernos y a la sociedad para llevar a cabo su función, y por su parte, los responsables de la seguridad de los sistemas de información demandan a su personal mas profesionalismo, lo que tendrá un alto impacto en los programas de capacitación en seguridad.

Durante los últimos años se han escrito varios libros sobre la seguridad en sistemas de información los cuales se enfocan en los aspectos técnicos de la seguridad en sistemas de información y cómo se debe proteger la información, sin embargo, existen pocos recursos al alcance para prepararse para establecer y desempeñar la función de seguridad en sistemas de información.

4.2 IDENTIFICACIÓN DE REQUERIMIENTOS

Para identificar los requerimientos para el personal que se encargará de evaluar la seguridad en los sistemas de información, es importante conocer el entorno donde trabajará y los retos que ofrece.

Es necesario conocer la preparación que deberá recibir, los requerimientos de educación y experiencia que deberá contar. También, debemos saber por dónde empezar, cómo organizarse y cómo administrar la función.

La gente que desea incursionar en el área de seguridad en los sistemas de información, deberá conocer como trabaja el hardware, firmware y el software, para que pueda proteger los sistemas y la información que ellos procesan, guardan y transmiten.

El propósito de la función de seguridad en los sistemas de información es proveer servicio y soporte a los negocios a través de un programa efectivo de seguridad en informática que realmente satisfaga las necesidades de la empresa, de lo contrario se puede caer en el caso de contar con un programa de trabajo caro y que no está actualizado, ocasionando que se ignoren los resultados del trabajo, lo que afectaría negativamente la imagen de la función, que se pierda credibilidad y oportunidades de participar en nuevos proyectos, inclusive pudiera llegar a la pérdida del empleo.

4.3 CAPACITACIÓN

Para las personas que están interesadas en la seguridad en los sistemas de información, deseosas de desempeñarse en este campo y que tengan poca experiencia, se pueden preparar en diferentes formas para realizar con éxito la función deseada.

Existen cuatro de formas de prepararse y hacer una carrera en seguridad de sistemas de información:

1. Tomar estudios o una carrera para tener una formación profesional.
2. Tomar cursos orientados a la educación y entrenamiento para un puesto específico.
3. Obtener experiencia para algunos puestos.
4. Certificación.

Por lo que respecta a la educación profesional para desempeñar la función, es conveniente escoger al personal que proviene de una educación profesional técnica como pueden ser la carrera de ciencias de la computación, ingeniería en sistemas, matemáticas, comunicaciones, etc.

Como en los últimos años se ha incrementado la competencia para desempeñar estas funciones, es necesario contar con experiencia, educación avanzada o certificaciones para lograr una oportunidad de trabajo.

Para complementar la educación, se debe entrenar tanto como sea posible mediante cursos, conferencias, talleres para obtener información sobre diferentes tópicos de seguridad.

La siguiente lista muestra los temas más comunes para el entrenamiento en seguridad:

- Infraestructura de llave pública.
- Fraude mediante teléfono celular.
- Seguridad en Comercio Electrónico
- Desarrollo e instalación de políticas de seguridad en Internet
- Sign-On Simple.

- Prácticas de seguridad en informática
- Seguridad en Sybase y SQL server
- Seguridad en UNIX, TCP/IP y barreras de seguridad.
- Seguridad en JAVA y ActiveX
- Kerberos SESAME
- Seguridad en Sistemas Abiertos
- Técnicas y herramientas de Hackers
- Protección en base de datos Oracle
- Software de Criptografía.
- Seguridad en Windows NT y en servidores WEB.
- Seguridad en HP/UX.
- Aspectos legales de conexión en Internet.
- Seguridad en redes empresariales.

Es importante considerar las conferencias que se desarrollan periódicamente, de las que destacan nueve conferencias anuales consideradas como las más importantes y donde se puede recabar información especializada en seguridad. La mayoría de las siguientes conferencias se desarrollan en ciudades de los Estados Unidos:

- National Information Systems Security Conference.- Se han realizado los últimos 20 años en las áreas de Baltimore o Washington DC durante el mes de Octubre.
- Computer Security Institute Conferences.- Estas conferencias se iniciaron desde 1974 y se han llevado a cabo en las grandes ciudades de Estados Unidos.
- MIS Training Institute Conferences. Estas conferencias han existido por mas de 20 años.
- Information Systems Security Association Conferences.
- Computers, Freedom and Privacy Conferences. Patrocinada por IEEE Computer Society, Association for Computer Machinery (ACM) y organizaciones locales de Estados Unidos.
- IEEE Computer Security Conferences. Conferencias con asistencia limitada, patrocinadas por el Institute of Electrical and Electronic Engineers Computer Society y que siempre se

llevan a cabo en Oakland, California, donde la élite de investigadores en seguridad y académicos presentan documentos altamente técnicos.

- Computer Security Applications Conferences. Se han realizado desde 1984 y son patrocinadas por Aerospace Computer Security Association.
- Compsec Conferences. Una de las más importantes conferencias en Europa y se han realizado desde 1984.
- National (actualmente International) Computer Security Association Conferences.

En México, en los últimos años se ha realizado anualmente un evento conocido como El Día Internacional de Seguridad en Cómputo y que ha sido apoyado por la ACM (Association for Computer Machinery).

Adicionalmente a la capacitación, se deberá adquirir o reforzar las siguientes habilidades:

- Administración.- Proyectos, Manejo de personal, Planeación, Control, Finanzas.
- Políticas y procedimientos de seguridad.
- Análisis de riesgos.
- Seguridad en las comunicaciones.
- Seguridad física y del medio ambiente.
- Capacitación en seguridad.
- Planes de contingencia.
- Seguridad en las aplicaciones.

Este grupo de habilidades ayudará a establecer buena comunicación con otros, mantener buenas relaciones de trabajo, aportar cambios que influyan al personal de una manera positiva, apoyar la toma de decisiones, deslindar responsabilidades. Asimismo, le ayudará a organizar su función y la manera de llevarla a cabo. Adicionalmente, se requiere que tengan un alto nivel de integridad y fuertes valores éticos.

4.4 DESARROLLO DE ACTIVIDADES

Para realizar adecuadamente la función, es importante conocer los siguientes puntos de una empresa:

1. Su historia.
2. Los productos que provee.
3. El medio ambiente donde realiza su negocio.
4. La competencia que enfrenta
5. Los planes a largo plazo.
6. Los planes a corto plazo.
7. El costo de hacer negocios.
8. El valor de sus productos o servicios.

Estos puntos son importantes para hacer más efectiva la función de evaluación de seguridad, ya que no es un producto que pueda ser vendido fácilmente en el mercado y se tiene la impresión de que no genera ganancias a la empresa, además, el costo para realizar la función es tomado de las utilidades del negocio, sin embargo, en un mercado donde la competencia se está incrementando, la función de seguridad en los sistemas de información puede ayudar a mejorar los procesos y la imagen del negocio, de esta manera contribuir a incrementar su mercado y sus ganancias.

Las tareas principales que tiene bajo su responsabilidad el personal del diagnóstico de riesgos son las siguientes:

- Evaluación de riesgos sobre la información y los sistemas.
- Definición de alternativas de protección.
- Estimación del costo de las alternativas de protección.
- Beneficios involucrados.
- Elaboración de recomendaciones.

Para desarrollar su trabajo, algunos especialistas en seguridad en sistemas de información son contratados por grandes organizaciones para realizar la evaluación de la seguridad y reportan frecuentemente al departamento de Sistemas de Información, algunas veces a la dirección de la organización. Otros especialistas trabajan como consultores, normalmente para alguna firma de consultoría y en menor frecuencia como consultores independientes.

Para trabajar en forma organizada y para desarrollar la función exitosamente, es importante contar con un plan global que se pueda integrar, o al menos que sea compatible con el plan estratégico de la organización, y que incluya direcciones a tomar, metas y objetivos del plan de actividades. Este plan debe seguir los principios de bajo costo y alto impacto en la organización, también debe buscar minimizar la probabilidad de la vulnerabilidad en la seguridad, minimizar el daño en caso de que la vulnerabilidad sea explotada y proveer métodos eficientes y efectivos en caso de sufrir un daño.

4.5 RETOS EN EL SIGLO XXI

Es importante considerar el futuro para visualizar el campo e identificar los riesgos en la información y en los sistemas de información y de esta manera estar prevenidos para los retos que se deberán afrontar.

Los grandes retos que se visualizan en el siglo XXI son los siguientes:

1. Un incremento constante y globalización de Internet y su conexión a los negocios e intranets de las empresas. El crecimiento de aplicaciones sofisticadas que operan en Internet son objetos de ataque, el uso de técnicas de cifrado puede proteger algunos servicios, sin embargo existen amenazas que deberán ser protegidas con otras técnicas.
2. Incremento de amenazas de espionaje económico.- Existen corporaciones que conducen negocios internacionales, que enfrentan una fuerte competencia y desean protegerse del espionaje económico de sus adversarios. Hay países que realizan actividades para abusar de la información de su adversario con el propósito de causarles pérdida del mercado, ganancias y negocios, de esta forma puede mejorar la competitividad económica de su país.
3. Incremento potencial y amenazas de tecno-terroristas. Los terroristas no solo están usando la tecnología para obtener fondos para sus actividades, están buscando la manera de usar la tecnología de la información para llevar a cabo una guerra contra sus enemigos.
4. Amenazas potenciales por la guerra de la información (acciones para lograr superioridad en la información para apoyar estrategias militares), lograda por la afectación y daño de la información y sistemas de información del adversario, mientras protegen su información y sus sistemas de información.

Para atender los retos anteriores es importante entender el uso potencial de las herramientas y del daño que pueden causar, por lo que será más importante que nunca establecer las medidas de seguridad como son los controles, usar tecnología e implantar programas con el objetivo de disminuir las amenazas derivadas de los nuevos retos [KOVA97].

5. HERRAMIENTAS PARA EFECTUAR EL DIAGNÓSTICO DE RIESGOS

5.1 ANÁLISIS DE RIESGOS

El análisis de riesgo es un proceso sistemático para evaluar las vulnerabilidades de los activos informáticos ante las amenazas de su entorno. El análisis identifica las consecuencias probables o los riesgos asociados con las vulnerabilidades y provee la base para establecer un programa eficaz en función de los costos de seguridad para eliminar o minimizar los efectos de los riesgos.

El proceso de análisis de riesgos provee información que se necesita para hacer juicios en lo que concierne a recuperación en caso de desastre y la seguridad. Identifica los procedimientos y políticas de seguridad que deben establecerse para conservar la capacidad de la compañía para lograr sus objetivos en caso de mal uso, pérdida, o indisponibilidad de sus activos informáticos.

Las metas del análisis de riesgo incluye identificar preparativos, procedimientos y controles que:

- Respondan adecuadamente ante las vulnerabilidades y desastres potenciales
- Elimine o minimice la probabilidad de un acto accidental o deliberado
- Elimine o minimice el efecto de un desastre sobre operaciones de la compañía.

El análisis de riesgos deberá conducirse con la regularidad suficiente para asegurar que el enfoque del estudio realizado es una respuesta realista a los riesgos actuales que están asociados con los activos informáticos.

El éxito de un programa de análisis de riesgo depende de la participación comprometida de la alta dirección. Es importante que dentro de la planeación estratégica de sistemas, se incluyan planes sobre seguridad informática.

El desarrollo del análisis de riesgo debe ser coordinado por la función de seguridad de la compañía y con participación de representantes de las áreas de informática. La información generada durante todo el proceso, se debe mantener en forma confidencial.

El análisis de riesgos se debe desarrollar sobre los activos informáticos que son más críticos para la operación de la compañía.

El análisis de riesgo presume que el costo de controlar cualquier riesgo no deberá exceder la máxima pérdida asociada con el riesgo. Para llegar al costo de las soluciones efectivas de seguridad, el análisis de riesgo requiere identificar la pérdida probable o cuantificar el valor de un activo.

Los elementos claves en el análisis de riesgo para identificar el costo de una pérdida son:

1. Una estimación del impacto o costo de una amenaza específica si sucede, y
2. Una estimación de la probabilidad de que se materialice el evento no deseado en un período de tiempo.

Después de haber estimado el valor de una pérdida, se pueden tomar diferentes posiciones para manejar el riesgo:

- Tolerar el riesgo.
- Contratar seguros contra el riesgo.
- Implantar medidas menos costosas para reducir el impacto monetario o para bajar la probabilidad de ocurrencia de la pérdida.

Después de determinar el monto monetario de una pérdida, el equipo de análisis de riesgo está listo para identificar medidas alternativas de seguridad y proveer recomendaciones para soluciones eficaces en función de los costos de implantación.

El uso de indicadores de costo se debe utilizar para comparar y determinar las medidas protectoras más efectivas desde el punto de vista costo-beneficio. Donde sea posible, se debe

indicar los beneficios tangibles, monetarios y algunos otros como reducción de intentos de mal uso y reducción de tiempos de entrega.

El equipo de trabajo del análisis de riesgos, deberá presentar los hallazgos a los directivos de la compañía para su revisión. Finalmente identifica las medidas protectoras para su implantación.

El informe de análisis de riesgo sirve como el vehículo para presentar a la dirección de una compañía, los hallazgos y recomendaciones para la seguridad de los bienes informáticos, y debe contener la información necesaria para que los directivos puedan tomar acertadas decisiones en materia de seguridad.

5.2 MUESTREO

La aplicación de la teoría estadística a una prueba selectiva del ambiente consiste en estimar las características de un universo por medio de la interpretación matemática de los resultados obtenidos al inspeccionar la muestra.

Las técnicas estadísticas son particularmente apropiadas cuando el universo que se desea examinar es numeroso, también cuando se desea tener un control muy preciso sobre la extensión o alcance de la pruebas dado el alto costo que cada una de las partidas representa, también cuando se trata de cierto tipo de transacciones de las cuales se sospecha que hay un alto riesgo.

El muestreo permitirá conclusiones sobre todos los elementos que se tienen que examinar mediante el examen de solamente una parte de ellos y tiene las siguientes ventajas:

- Economía.- El tiempo para revisar una parte es menor al que se requiere para la totalidad.
- Oportunidad.- La revisión de un número menor de partidas, se refleja también en ahorro de tiempo lo que permite emitir un informe de manera más anticipada.
- Minuciosidad.- El examen de un número grande de elementos puede hacer imposible la minuciosidad del trabajo, al reducir el número de elementos se hace posible que cada elemento sea examinado y procesado en forma más completa y satisfactoria.

El uso del muestreo reduce la probabilidad de ciertos riesgos de error porque permite una mayor concentración en el trabajo. El examen del universo puede incrementar la probabilidad de error debido a la monotonia mental del trabajo.

Aceptar cierto grado de incertidumbre se justifica por la relación entre los factores como son el costo y tiempo requerido. Cuando no es aceptable incertidumbre alguna solo queda la revisión exhaustiva. La medición de la incertidumbre del muestro estadístico se expresa en términos de dos parámetros: la precisión y el nivel de confianza. La precisión expresa el rango de los limites dentro de los cuales se espera el resultado de la muestra, mientras que el nivel de confianza

significa la probabilidad matemática de lograr que ese hecho ocurra dentro de los límites de precisión.

Para usar el método del muestreo, es conveniente conocer de modo genérico los fundamentos del calculo de probabilidades, en la medida que el usuario profundice en los conocimientos matemáticos y estadísticos relativos al muestreo encontrará mejores posibilidades de entender su esencia y dar versatilidad a sus aplicaciones.

Para aplicar el muestreo estadístico es necesario cumplir con los requisitos de que el universo sea masivo y que la muestra sea seleccionada aleatoriamente. Si se va utilizar constantemente el muestreo estadístico, es necesario que se domine el significado de los siguiente conceptos: Nivel de confianza, nivel de precisión y tasa de ocurrencia.

Nivel de confianza o confiabilidad.- Representa el porcentaje de probabilidad que se desea que la muestra sea representativa del universo, si por ejemplo se selecciona un 95%, significa que se acepta un 5% de riesgo de que la muestra no llegue a representar el universo.

Nivel de precisión o error tolerable.- Representa la cantidad o porcentaje que se acepta que se desvíe el valor obtenido en la muestra del verdadero promedio del universo, mientras la precisión es el margen dentro del cual la respuesta puede variar y aún ser aceptable, el nivel de confianza mide la probabilidad de que la respuesta caiga dentro de dicho margen.

Tasa de ocurrencia.- Se le llama también frecuencia de error o porcentaje de desviación, representa el porcentaje de errores que puede existir en el universo.

Existen características que se pueden controlar como son: el tamaño de la muestra, la precisión requerida y el nivel de confiabilidad deseable. Las características que no están bajo el control son: tamaño del universo, variación en el tamaño de los componentes y el número de errores o desviaciones encontradas en la muestra examinada.

Existe una relación entre el tamaño de la muestra, la precisión requerida y el grado de confianza deseable, cuando se establece cualquier combinación de dos de ellos, el tercero será determinado matemáticamente basado en los dos anteriores, en el tamaño de la población o universo y en un estimado de los errores que se van a esperar.

Los principales aspectos que se deben documentar en un muestreo son los siguientes:

1. Objetivo y descripción de la prueba.
2. Definición de lo que se considera como error o desviación.
3. Definición del universo.
4. Definición del nivel de seguridad, error tolerable y el error esperado.
5. La determinación del tamaño de la muestra.
6. Los métodos de selección y estratificación.
7. La evaluación de los resultados de la muestra que comprende la proyección de los errores, causas de los errores, los riesgos del muestreo y finalmente las conclusiones.

El objetivo de una prueba asegura que el universo del cual se va a obtener una muestra es el apropiado para obtener el logro del objetivo. Por ejemplo, si el objetivo de la prueba es determinar si todas las transacciones de cuentas por cobrar representan las cantidades que se le deben a la compañía, la muestra podría ser seleccionada de la lista de las cuentas por cobrar.

La definición de errores debe ser establecida con anticipación, por ejemplo: si la reserva para cuentas malas está basada en todos los saldo que están sobre 90 días de antigüedad, los errores de clasificación de las cuentas que están entre los 30 y 60 días no deberían de afectar a los cálculos de dicha reserva, por consecuencia no se deben considerar como errores para propósito de la evaluación de los resultados del muestreo.

El universo donde se van a tomar las muestras debe ser definido con anticipación ya que los resultados de la muestra son evaluados en los términos de su efecto en el universo.

El error tolerable es el máximo error que se desea aceptar, no es posible establecer una relación precisa entre el error tolerable y el tamaño de la muestra, generalmente cuanto más grande es el error tolerable más pequeña necesita ser el tamaño de la muestra.

La cantidad de error esperado puede estar fundamentada en factores como los resultados de las pruebas de años anteriores, cambios en el personal o en los sistemas de control interno.

El nivel de seguridad que normalmente se requiere, es uno de los factores más importantes en la determinación del tamaño de la muestra, el nivel de seguridad requerido está muy relacionado con la seguridad de otros procedimientos de control, en caso de no apoyarse en estos procedimientos, se deberá establecer un nivel alto de confianza.

El nivel de la seguridad afecta directamente con el tamaño de muestra, si el nivel de seguridad se incrementa entonces el tamaño de muestra se incrementará y viceversa.

Para seleccionar la muestra se pueden emplear dos métodos:

1. Muestreo a criterio.- La persona encargada del muestreo debe decidir de antemano los criterios que utilizará.
2. Muestreo aleatorio.- Cada unidad de la población tiene la oportunidad de ser seleccionada, los métodos del muestreo estadístico se pueden utilizar para hacer inferencias sobre la población por medio de muestras solamente si la muestra fue seleccionada en forma aleatoria.

   El muestreo aleatorio puede ser con o sin reemplazo, el procedimiento más empleado para realizar la revisión es el muestreo sin reemplazo.

   La muestra más eficiente para realizar predicciones acerca del población es la que se conoce como muestra aleatoria pura, en éste caso, para obtener la muestra el encargado de la muestra puede utilizar una computadora o una tabla de números aleatorios.

Una alternativa para el muestreo puramente aleatorio es el muestreo aleatorio sistemático, bajo ciertas circunstancias este método puede tener una ventaja operacional sobre el muestreo puramente aleatorio. Si la muestra no está listada en secuencia numérica es mucho más fácil seleccionar una muestra al azar empleando el muestreo sistemático, el peligro en el muestreo sistemático es que cada unidad puede corresponder a una secuencia ya existente de la población de manera que los elementos de la muestra se estén seleccionando siempre de una misma sección de la población siguiendo un patrón recurrente.

5.3 ENTREVISTAS

Una entrevista tendrá mejores resultados si está bien diseñada y planeada, asimismo, el apoyo que brinde la gerencia es importante durante todo el análisis. Los siguientes puntos conforman una guía que se puede aplicar en una entrevista.

1. DISEÑO.

   La entrevista es más efectiva cuando se aplica solo una persona, sin embargo a veces el entrevistado requiere la presencia de más personas para poder brindar la información necesaria, la línea a seguir es mantener el objetivo de la entrevista en el área principal y no tratar de cubrir múltiples áreas.

   Los entrevistadores pueden utilizan guías para desarrollar preguntas durante la entrevista, sin embargo deben estar bien estructuradas y evitar caer en el uso de conjunto de preguntas rígidas ó listas de verificación que pueden provocar desconfianza y en muchos casos lleva a los entrevistados que no es necesaria la presencia del entrevistador.

   Las listas de verificación son herramientas válidas que deben utilizarse cuando sean apropiadas y requeridas.

2. CALENDARIZACIÓN.

   El equipo debe establecer un calendario de entrevistas donde el entrevistador conozca primero al responsable del área funcional del área bajo estudio y, posteriormente, con la gente con quien trabajará en esas áreas. Por lo general, el equipo entero debe coordinar la primera serie de entrevistas. Dos miembros del equipo deben ser asignados por cada entrevista. Idealmente las entrevistas deben ser calendarizadas cuando se inicia el proyecto, sin embargo, esto no es práctico. Una vez que las entrevistas con los gerentes de las áreas involucradas han terminado, los miembros del equipo deben calendarizar sus entrevistas como sea más apropiado.

La calendarización de las entrevistas debe tener un esfuerzo continúo por parte del equipo. Es importante considerar tiempos disponibles para actividades que no sean del proyecto y para entrevistas con gente recomendada durante las propias entrevistas.

3. APLICACIÓN.

Con base en los objetivos del plan, los entrevistadores deben tener en mente exactamente que esperan determinar en cada entrevista. Deben desarrollar algunas preguntas específicas y un panorama del área entrevistada e incluirlos en un esquema breve; esto ayudará a que la entrevista sea más eficiente y asegurar que se toquen los puntos más importantes. El entrevistador debe preparar a los entrevistados sobre las preguntas que les hará a través de una carta o un memorando que les enviará días antes de la entrevista.

Los entrevistadores deben presentarse y describir brevemente los objetivos, alcances y metodología del proyecto para asegurar que el entrevistado entienda su naturaleza e intenciones antes de proceder. Los entrevistadores deben confirmar también que los entrevistados hayan recibido la carta introductoria del proyecto. Si existen dudas respecto al proyecto o al proceso de la entrevista, es importante aclararlas antes de empezar con las preguntas.

Inicialmente los entrevistadores deben hacer preguntas muy generales e indicar las áreas de interés, posteriormente, preguntar cosas más específicas para satisfacer los requerimientos de información predeterminados.

Los siguientes puntos deben tomar en cuenta durante las entrevistas para crear un entorno amigable y conseguir información relevante que será analizada posteriormente:

- Ser amigable.- Los entrevistadores deben respetar a los entrevistados y reconocer que su experiencia, información, ideas y sugerencias son importantes.

- Anotar conceptos.- Los entrevistadores deben tomar notas de forma que no distraigan a la persona entrevistada, ya que puede olvidar decir algo.

- Ayudar al entrevistado.- Los entrevistadores pueden sugerir vulnerabilidades que se presentan en situaciones reales y dar ideas al entrevistado para que piense en lo impensable es decir, en problemas significativos o en probables pérdidas. Las sugerencias pueden estar o no basadas en eventos históricos.

- Aprender a escuchar.- Si las personas entrevistadas desvían el tema, los entrevistadores no deben hostigarlo a que regrese a él; de cualquier forma, la mayoría de la información es útil. Los entrevistadores deben hablar más que el entrevistado. En general, es importante instruir al entrevistado sobre aspectos de seguridad y control, pero el principal objetivo de la entrevista es obtener información.

- Conocer los conceptos de seguridad.- Los entrevistadores deben conocer las definiciones de activos, controles, vulnerabilidades, amenazas y exposiciones. Deben recordar que las pérdidas pueden incluir la modificación, reemplazo, contaminación, destrucción, negligencia de uso, desastres y toma de información.

  Cuando se analicen los controles el equipo debe recordar que los controles pueden ser diseñados para protegerse en contra de actos intencionales o no intencionales y pueden tener propósitos muy diferentes (prevención, detección, recuperación o corrección). Puede ayudar el realizar un diagrama del modelo de seguridad.

- No estar mucho tiempo.- Las entrevistas que tardan más de una hora normalmente son resultado de un enfoque inadecuado o de intentar cubrir muchos temas. En general, es mejor para los entrevistadores regresar que estar más de una hora.

- Estar juntos como un equipo.- Los miembros deben reunirse antes de una entrevista para confirmar el área de enfoque y los aspectos especiales a tratar. Durante la

entrevista los miembros del equipo deben cooperar siempre, permitiendo que uno y otro realicen preguntas, desarrollen puntos y apoyándose mutuamente. Un miembro puede realizar preguntas y tomar notas resumidas, mientras que otro miembro puede estar tomando notas detalladas y preparándose mentalmente para hacer las siguientes preguntas.

- Estar seguro de entender al entrevistado.- En puntos críticos se recomienda que el entrevistador repita su interpretación de la información presentada. Asumir y comprender sin confirmar puede llevar a errores. Cuando sea relevante y posible, el entrevistador debe recolectar información de ejemplos específicos descritos por el entrevistado.

- Evaluación.- Solo cuando es apropiado, se le pregunta al entrevistado su opinión sobre las recomendaciones que el equipo está considerando.

Para finalizar, el entrevistador debe preguntar sobre algunas recomendaciones: Si hay alguien más que deba ser entrevistado (alguien a quien realmente le concierne o se interesa en seguridad), documentos para leer y procedimientos a observar.

- Terminar la entrevista positivamente.- Los entrevistadores deben hacer saber al entrevistado que es posible que regresen y que están muy agradecidos por su tiempo y asistencia. También debe asegurar que el entrevistado puede contactarlos, en caso de que tenga puntos adicionales o preguntas. Finalmente, los entrevistados deben solicitar copia de los documentos relevantes identificados y ofrecidos durante la entrevista. En caso de que las copias no estén disponibles en el momento, los entrevistadores debe asegurarse de que queda claro el procedimiento para su obtención.

4. ANÁLISIS DE RESULTADOS.

Lo más pronto posible después de cada entrevista, los entrevistadores deben volver a leer y de ser necesario, expandir sus notas. Estas deben ser resumidas en un formato especifico; es esencial contar con notas legibles organizadas para un fácil acceso.

Se recomienda una estructura que proporcione un mecanismo para revisar la información de las áreas funcionales, recopiladas a través de las entrevistas.

- Nombre del entrevistado, área funcional, título, número telefónico, fecha de la entrevista y nombre del o de los entrevistadores.
- Breve descripción de la razón de la entrevista (puede ser expresada como el principal enfoque del área, las preguntas realizadas o los eventos analizados).
- Lista de hallazgos o información obtenida; cada tema discutido debe ser escrito en una o dos oraciones cortas.
- Aspectos que pueden ser vulnerabilidades y que sea importante discutir con el equipo.
- Otros puntos a considerar (gente adicional a contactar, documentos a leer, o procedimientos a observar sugeridos durante la entrevista, junto con el tema a analizar).
- Acciones que el equipo debe hacer antes de completar la revisión.
- Breve descripción de las recomendaciones sugeridas durante la entrevista.

Cada resumen de la entrevista debe ser archivado en la sección funcional a la que mejor se ajuste. Si se requiere, la misma entrevista puede aparecer en más de una sección.

Cada miembro del equipo debe asegurar que se hagan copias de respaldo de las notas y que sean almacenadas apropiadamente. Algunas organizaciones tienen la práctica de fotocopiar las notas de las entrevistas y distribuirlas entre los miembros del equipo principal. En general, la página del resumen es suficiente para el respaldo y distribución a los otros miembros del equipo.

5.4 SOFTWARE PARA EL ANÁLISIS DE RIESGOS

Una alternativa para realizar el proceso de análisis de riesgos es mediante paquetes de software que están disponibles en el mercado. La mayoría de los paquetes corren en computadoras personales y solo unas cuantas corren en mainframes.

Las empresas deben determinar que paquete utilizarán para realizar el análisis de riesgos y durante su uso se debe combinar con alguna metodología cuantitativa o cualitativa.

El software para el análisis de riesgos debe contemplar diferentes áreas como riesgos materiales, sabotajes físicos, comunicaciones, desarrollo y explotación de aplicaciones, fraude, robo de información y de software y problemas de personal.

Actualmente las metodologías que´se desarrollan utilizan software para realizar el análisis de riesgos, algunos paquetes que podemos mencionar son los siguientes: ANALISY, BDSS, BIS RISK, COBRA, CRAMM, DDIS MARION AP+, RISK PAC y RISKWATCH.

Cada software se aplica conforme a procedimientos específicos. Algunas características son:

- Se complementan con cuestionarios y parámetros.
- Utilizan probabilidades o valores numéricos obtenidos de la esperanza matemática.
- Utilizan datos de encuestas anuales de incidentes.
- Pueden exportar resultados a procesadores de texto y hojas electrónicas.
- Para realizar la simulación utilizan un enfoque "Que pasa si".
- Manejan una evaluación subjetiva del riesgo.

La selección del software debe realizarse con cuidado para que pueda cubrir las necesidades del estudio y se tenga la experiencia necesaria en seguridad para poderlo aplicar.

Un grupo de personas con habilidades especiales para participar en proyectos de análisis de riesgos debe tener claro los conceptos y definiciones de los términos más comunes sobre análisis de riesgos

La selección del software más apropiado requiere planeación, los siguiente elementos son esenciales para realizar la selección:

- Colección de datos, análisis y emisión de resultados.
- Debe ser compatible con el hardware y software de la organización.
- La metodología debe reflejar las políticas de la empresa.
- Los resultados del análisis de riesgos deberán ser útiles al nivel gerencial para ponderar las alternativas y seleccionar medidas confiables y de gran costo-beneficio.
- Contar con documentación para instalar y operar en forma efectiva la herramienta automatizada.
- Habilidad para registrar los datos coleccionados.
- Considerar costos derivados por la instalación, capacitación, soporte, mantenimiento y compras por múltiples licencias.

VENTAJAS

El proceso manual de los datos coleccionados puede durar varios meses, en cambio si se utiliza una herramienta automatizada la evaluación de las debilidades es mucho más rápido. El análisis puede desarrollarse rápidamente y asegurar que los resultados obtenidos reflejan la situación actual del sistema.

El software es adaptable a los sistemas de la organización de cualquier tamaño y permiten al usuario explorar rápidamente los resultados de implementar determinadas medidas de seguridad.

DESVENTAJAS.

La mayor desventaja es que no existe un método estándar para realizar el análisis de riesgos y no se puede asegurar que un método en particular sea el correcto.

6. SOLUCIONES A PROBLEMAS DE SEGURIDAD

6.1 ÁREAS INVOLUCRADAS EN EL DIAGNÓSTICO DE RIESGOS

La seguridad de los sistemas no puede estar bajo el cargo de un solo equipo de programadores o de un solo grupo, todo el trabajo que se realice debe considerarse como un trabajo en equipo donde cada uno de los integrantes desarrolla tareas específicas.

Para desarrollar un proyecto es importante considerar la magnitud del proyecto, recursos existentes, la experiencia requerida, tareas y asignar responsabilidades que no se traslapen e impidan el desempeño de funciones.

Durante la realización del proyecto se realizan diversas actividades por distintos grupos funcionales que participan en forma multidisciplinaria. Las principales actividades y tareas asociadas son:

ACTIVIDAD	TAREA
1. Planeación y coordinación	Determinar los objetivo, identificar las necesidades, desarrollar un enfoque principal y estrategias, administrar y resolver problemas.
2. Creación	Elaborar medidas de protección para cada uno de los componentes que integran el programa y medidas para casos de emergencia.
3. Consultoría	Asesoría técnica en los sectores especializados.
4. Reglamentación y documentación.	Creación y documentación de las normas y métodos.

5. Implantación y operación del programa.	Diferentes grupos asignados por la dirección tienen la responsabilidad de estudiar y verificar el reglamento de seguridad.
6. Funciones administrativas generales.	Participación de los sectores administrativos en actividades financieras, jurídicas y otras.
7. Verificación y revisión	Supervisión, evaluación y búsqueda de mejoras acordes al programa.

Durante la planeación del proyecto es importante identificar y definir diversos niveles de responsabilidad de los distintos componentes que forman el proyecto. Buscar y reunir al personal especializado en la materia con una habilidad para el desarrollo y la activación del programa.

De la anterior tabla de actividades se desprenden las siguientes responsabilidades:

- Global.- Los altos ejecutivos tienen la responsabilidad de planear, analizar las necesidades, coordinar e implantar el programa de seguridad, serán el medio de enlace entre grupos de trabajo y la dirección y evaluar los logros obtenidos.
- Por cada grupo involucrado.- Debe tomar las decisiones administrativas que afectan su área, plantear sugerencias, mantener comunicación directa entre los responsables de la tecnología de la información y los altos ejecutivos.
- Asignadas.- Son tareas específicas generadas por los componentes que exigen tener conocimientos especializados.
- Asociadas al funcionamiento. Responsabilidades asociadas con las funciones que tienen asignadas dentro de la organización.
- Asociadas a los procesos de verificación y control.- Análisis de la información recopilada y elaboración de recomendaciones.

Al describir la naturaleza de las responsabilidades, los directivos de la empresa facilitarán los medios financieros para el desempeño de sus funciones.

RESPONSABILIDADES DE LAS ÁREAS PARTICIPANTES.

Para el buen funcionamiento de un proyecto de seguridad se requiere la participación de diversos grupos internos o externos y cada uno de los participantes debe asumir las tareas donde su experiencia le permita tener un buen desempeño.

Aún cuando los altos directivos son los responsables de la seguridad de los recursos informáticos, pueden delegar la responsabilidad a la unidad organizacional adecuada.

Las principales áreas, grupos y puestos funcionales que participan en el diagnóstico de riesgos en informática y sus responsabilidades relacionadas con la seguridad en informática son las siguientes:

- Sistemas de Información.

  Implantar normas y técnicas de protección, la política de seguridad en informática y coordinar acciones entre recursos humanos coordinador de seguridad, supervisor internos y el administrador de datos.

- Coordinador de Seguridad en Informática

  Evaluar los riesgos que amenazan la seguridad de los sistemas y elaborar los informes pertinentes, sugerir medidas de seguridad y para casos de emergencia.

- Auditoria

  Auditor interno.- Examinar las fases de desarrollo de sistemas para asegurar el uso de controles adecuados, examinar controles y lineamientos relacionados con la operación de los sistemas, vigilar la implantación de medidas de verificación, detectar la disparidad entre los sistemas ocasionada por fallas accidentales o intencionales, aconsejar a la dirección la adopción de medidas que reduzcan o neutralicen las consecuencias de las fallas detectadas durante el proceso de verificación.

- Administrador de datos

  Una de las responsabilidades más importantes es determinar los privilegios de acceso a los datos, controlar el acceso a la información y examinar el acceso autorizado a la información.

- Recursos Humanos

  Garantizar que la contratación y despido del personal se apegue a los reglamentos establecidos y apoyar el programa de cultura de seguridad en informática.

- Usuarios de sistemas de información

  Determinar los requerimientos de control de procesamiento, autorizar, preparar y convertir los datos de entrada y examinar la bitácora de operaciones para detectar cualquier error.

Estas son las principales responsabilidades de los participantes en el diagnóstico de riesgos, sin embargo existe la posibilidad de que algunas empresas no cuenten con alguno de los grupos descritos, en este caso las responsabilidades pueden recaer en otros puestos.

6.2 CRIPTOGRAFÍA

La criptografía es la ciencia de transformar información para asegurar su autenticidad y su secreto. El criptoanálisis es la ciencia de romper el cifrado de la información, y la criptología abarca a la criptografía y el criptoanálisis.

La criptografía tiene las siguientes aplicaciones en informática:

- Autentificar transacciones bancarias.
- Autentificar transacciones entre negocios o entre negocios y el gobierno.
- Proteger la integridad de transferencias electrónica de fondos.
- Proteger el secreto de información personal, militar y comunicaciones personales.
- Proveer integridad y confidencialidad en las transacciones por Internet.
- Proteger la integridad de software y base de datos.
- Autentificar la identidad de usuarios y entidades de una red.
- También puede ser utilizada para resolver problemas de confidencialidad en la comunicación de voz para la verificación de tratados internacionales.

La criptografía es una herramienta muy poderosa para proteger la confidencialidad de la información y de otras amenazas, sin embargo, es tan enorme el poder de ésta técnica que propietarios y usuarios de la información pueden causarse daño ellos mismos y a terceros por su mal uso. La información puede ser perdida por una falla de software o hardware, o si la llave es olvidada, perdida o destruida, o si el usuario cifra mal la información importante. La falta de comprensión de la técnica por parte de los usuarios para la administración de llaves y los problemas asociados con la generación, almacenamiento, distribución ha ocasionado que algunas organizaciones prohiban el uso de esta herramienta.

Los sistemas de criptografía están compuestos por mensajes, texto cifrado, transformaciones y llaves. Proveen las propiedades de confidencialidad, autenticidad, integridad en la información y también pueden proveer la propiedad de no rechazo.

Hay dos tipos de sistemas de criptografía: Convencionales y de llave pública.

1. Los sistemas de criptografía convencionales, son también conocidos como clásicos, simétricos, llave sencilla, llave secreta o llave privada.
2. Los sistemas de llave pública son también llamados asimétricos o de dos llaves.

El estándar más común para cifrar con llave privada es el Data Encryption Standard (DES). Este sistema es usado ampliamente en las redes financieras, cajeros automáticos y redes punto de venta. El algoritmo usa una llave privada de 56 bits y opera sobre un bloque de datos de 64 bits. El proceso de cifrar información puede ser ejecutado usando software o hardware. El algoritmo de cifrar todavía es seguro, sin embargo, con el incremento de la capacidad de las computadoras, este algoritmo puede ser vulnerable. El uso de triple DES, usando el algoritmo DES tres veces con dos llaves, se logra fortalecer y alargar la vida del algoritmo.

Se deben tener consideraciones en el uso de este algoritmo, ya que todos los cajeros automáticos usan DES para proteger los datos que son transmitidos, la misma llave es usada para cifrar y descifrar, si una llave es descubierta puede crear una gran exposición en todos los lugares que utilizan la misma clave, por lo que es almacenamiento y uso de la llave deber ser realizado de una manera segura.

El algoritmo de llave pública, también conocido como cifrado asimétrico, usa dos llaves, cada usuario tiene un par de llaves, una de las cuales es mantenida estrictamente confidencial (la llave privada) y la otra es compartida con otros usuarios o computadoras (llave pública). Las dos llaves están relacionadas matemáticamente y son usadas en el proceso de criptografía, un mensaje cifrado con la llave pública puede ser descifrada solo con la llave privada. La ventaja de éste método es que la llave privada nunca es compartida y puede ser utilizada para la creación de firmas digitales. Una firma digital es usada para verificar al usuario que realiza el envío y el contenido de un mensaje electrónico.

El algoritmo RSA (de Ronald Rivest, Adi Shamir y Leonard Adleman) es un algoritmo de llave pública que usa dos llave relacionadas y complementarias, una llave es mantenida en secreto para el proceso de cifrado y la otra es disponible de forma pública, solamente la llave privada es

conocida para el proceso de cifrado y debe ser mantenido secreto. El tamaño de la llave es variable, el tamaño más común es de 512 bits. El uso del algoritmo RSA es usado en el área de mensajes electrónicos, correo electrónico y también puede proveer una firma digital para autentificar mensajes. El algoritmo RSA puede usar una llave más grande que la utilizada por DES, por lo que es más fuerte, sin embargo, en un estudio realizado una llave de 429 bits pudo ser rota después de muchas horas de computadora.

ADMINISTRACIÓN DE LLAVES

La administración de llaves es el proceso completo de manejar llaves, incluye la generación, distribución y protección de llaves y eventualmente la manera de destruirlas. El esquema de la administración de llaves debe estar restringido, las amenazas sobre las llaves son la revelación, modificación, sustitución, inserción y eliminación.

La mayoría de los esquemas de administración de claves distinguen entre llaves maestras y llaves de sesión. Una llave maestra es usada para cifrar otras llaves, las llaves de sesión son usadas exclusivamente para una sesión de comunicación.

Para la generación de llaves en un sistema de llave secreta, un usuario debe seleccionar una llave o una instrucción de hardware o de software para generar una llave secreta.

El proceso de distribución de llaves debe ser eficiente, seguro, proteger la integridad y confidencialidad de la llave. Las llaves cifradas son todavía distribuidas sobre un canal seguro de forma manual o semiautomática. La distribución en forma manual trabaja donde el volumen de llaves es bajo, los mensajeros son confiables y la llave no puede ser espiada, sin embargo, este método es lento y costoso y en muchos ambientes puede ser no seguro. La alternativa es la forma semiautomática llamada módulo para transporte de llave, consiste en un modulo donde se guardan las llaves cifradas y posteriormente se carga a dispositivos como los cajeros automáticos o terminales punto de venta [SUMM97].

Como las llaves se distribuyen por canales inseguros, se cifran con otras llaves para su protección. Algunos esquemas usan dos niveles de llave (una para cifrar datos y otra para cifrar llaves). Otros esquemas pueden tener una llave jerárquica de tres o más niveles.

Por lo anterior, es importante realizar acciones que permitan mejorar el uso de la criptografía y aplicarla de forma eficiente. Antes de aplicar la criptografía los siguientes pasos se pueden realizar para asegurar la protección general de la información:

- Entrenar gente confiable que maneja información sensitiva para que determine la forma de protegerla y para resistir los engaños de personal no confiable que intenta conseguir información importante.
- Aplicar controles para salvaguardar información impresa o que esté desplegada, por ejemplo destruir la información después de haberla usado, evitar desplegar información donde pueda ser vista por otras personas, establecer políticas de escritorio limpio, numerar y controlar las copias de los documentos.
- Controlar medios de almacenamiento intercambiables, como discos, cintas, cartuchos.
- Aplicar controles de intrusión en computadoras y comunicaciones.

Después de haber aplicado las anteriores medidas de seguridad, se puede usar criptografía en la siguiente secuencia:

1. Establecer una administración segura y eficiente de llaves.
2. Aplicar la criptografía a situaciones donde haya peligro.
3. La información vital que se usa en formato de texto plano, se debe cifrar cuando es guardada en computadoras portátiles, enviada por microondas o por tecnología inalámbrica y cuando se envía por Internet.
4. Aplicar la criptografía donde sea práctico y usarla para satisfacer estándares de seguridad.

6.3 IDENTIFICACIÓN Y AUTENTIFICACIÓN

El elemento más básico de un sistema de seguridad es la habilidad para identificar quien es la persona, es necesario conocer si es un usuario válido o un enemigo antes de asignarle acceso a valiosos recursos del sistema.

Probar la identificación es la forma en que el usuario le dice al sistema quien es, la identificación del usuario debe ser única.

Autentificación es el proceso de probar a los usuarios quienes dicen ser: Las formas clásicas para probar son:

- Algo que conoce.- Es información secreta que solo el usuario conoce, puede ser su fecha de nacimiento, nombre de la esposa, número telefónico, etc.
- Algo que posee.- El usuario tiene que presentar fisicamente un objeto, como puede ser una tarjeta y que puede ser reforzada la seguridad con el uso de un número secreto.
- Quién es.- Ese método utiliza dispositivos biométricos para autentificar individualmente a la persona, utiliza por ejemplo la palma de las manos, huellas dactilares, retina o iris de los ojos.

En la actualidad la mayoría de los sistemas usan claves de usuario y passwords para realizar la identificación y autentificación como su primera línea de defensa y forma parte de la rutina de inicio de sesión en su computadora, esto representa un mecanismo ampliamente aceptado y que no es difícil de implementar, sin embargo, conseguir un password válido es la manera más común de ganar acceso no autorizado al sistema. Las principales amenazas sobre los passwords son los siguientes:

- Adivinar el password.
- Ataques basados en engaños.
- Ataques al archivo de passwords.

ATAQUES PARA ADIVINAR EL PASSWORD.

Los atacantes esencialmente siguen dos estrategias para adivinar el password:

- Búsqueda exhaustiva (fuerza bruta). - Utiliza todas las posibles combinaciones de símbolos y hasta cierta longitud.
- Búsqueda inteligente.- Intenta con passwords relacionados con información del usuario como es su nombre, dirección donde vive, número telefónico, etc. ó intentar con passwords populares.

Para proteger los passwords se pueden utilizar las siguientes defensas:

- Poner passwords.- Si el administrador o el usuario olvidan poner el password, el atacante no tendrá problemas para adivinar el password.
- Cambiar passwords por omisión.- Cuando el sistema es entregado, vienen con los passwords por omisión como "system" ó "manager" que son obvios para el atacante, por lo que se deberán cambiar.
- Establecer la longitud del password.- Un password de longitud mínima deberá ser exigido.
- Formato del password.- Incluir letras mayúsculas, minúscula, numéricos y otros caracteres no alfabéticos.
- Evitar passwords obvios.- El atacante puede usar una lista de passwords populares, por lo que se deberá escoger con mucho cuidado el password.

El sistema puede proporcionar ayuda para mejorar la seguridad del password de las siguientes formas:

- Verificadores de password.- El administrador del sistema puede usar una herramienta para verificar passwords "débiles".
- Generación de password.- Algunos sistemas operativos generan passwords aleatorios, los usuarios adoptan estos passwords propuestos.

- Vencimiento de passwords.- Una fecha de vencimiento se deben poner para obligar al usuario a cambiar su password y como medida adicional, se puede establecer el uso de viejos passwords.
- Limitar el número de intentos.- Cuando se han realizado determinado número de intentos, el sistema puede bloquear la cuenta definitivamente o temporalmente para prevenir o desalentar intentos adicionales.
- Informes para el usuario.- Después de la entrada, el sistema puede desplegar un breve informe para el usuario donde indique el número de intentos fallidos en la entrada al sistema con la intención de concientizar al usuario que un posible ataque se realizó.

Los usuarios son un aspecto muy importante a considerar, ya que es probable que tenga dificultades para memorizar su password y lo escriben en un papel muy cerca de su computadora, también lo cambian a su password favorito o lo hacen simple y predecible. Cuando el usuario olvida su password interrumpe su trabajo y el del administrador del sistema ocasionando que se abra una ventana para un nuevo ataque.

ATAQUES BASADOS EN ENGAÑOS.

El ataque se realiza cuando el usuario mete su password la computadora verifica la identidad del usuario, pero no conoce exactamente quien lo recibirá, los ataques basados en engaños toman ventaja de ésta situación y representa un problema real que compromete el password.Un ejemplo de un ataque con engaño es cuando el usuario legítimo mete su clave y password en la pantalla de entrada, estos datos son guardados por el atacante y el programa es abortado. Cuando el usuario intenta nuevamente entrar y tiene éxito, no está consciente que su password ha sido comprometido.

Los siguientes acciones se pueden tomar ante un ataque basado en engaño:

- Desplegar el número de intentos fallidos.- Puede indicar que un ataque se ha realizado.
- Establecer trayectorias confiables.- Garantizan que la comunicación con el usuario es con el sistema operativo y no con programas sospechosos.

- Autentificación mutua.- Si el usuario requiere una estricta garantía para autentificar el sistema que desea utilizar (por ejemplo en sistemas distribuidos), el sistema podría ser requerido para autentificarse el mismo con el usuario.

En el caso de aplicaciones en Internet que utilicen páginas Web y que requieren passwords, es recomendable salirse del navegador y de la aplicación para evitar que el password sea identificado.

ATAQUE AL ARCHIVO DE PASSWORDS.

Para verificar la identidad del usuario, el sistema compara el password que fue metido contra un valor guardado en el archivo de password, por lo que éste archivo representa de gran atracción para el atacante. Descubrir o modificar el contenido del archivo de password representa una gran amenaza.

Para proteger el archivo de passwords se tienen las siguientes opciones:

- Usar criptografía.
- Mejorar el control de accesos mediante el sistema operativo.
- Combinar la criptografía control de accesos para disminuir los ataques.

Si es insuficiente la seguridad provista por el password, se puede usar otras alternativas, como puede ser la restricción de la entrada desde terminales especificas, por ejemplo, los administradores y operadores solo pueden entrar desde la consola de operación y los usuarios solo pueden entrar desde la estación de trabajo de su oficina.

6.4 PLAN DE CONTINGENCIA

La organización que tiene gran dependencia del procesamiento electrónico de datos, debe considerar un plan de contingencias dentro de las estrategias del negocio, para que en caso de sufrir un desastre que interrumpa los servicios del procesamiento de datos, la organización tenga un conjunto de bienes y acciones que permitan reanudar el servicio dentro de un periodo razonable de tiempo y minimicen el impacto negativo del desastre.

Un plan de contingencia es un documento detallado y comprensible de todas las acciones que deben ser tomadas antes, durante y después de que un desastre ocurre. Como el plan contiene políticas estratégicas de la organización e información técnica, la mayoría de las compañías declaran confidencial el plan y mantener todas las copias seguras, solamente los responsables de las áreas participantes del plan de contingencia deben poseer una copia.

Para evitar que problemas rutinarios se vuelvan mayores y lleguen a convertirse en un desastre se deben contemplar medidas preventivas mínimas, por ejemplo: contar con equipo de repuesto, respaldos periódicos, personal de operación preparado, mejorar los mecanismos de protección contra el fuego, riguroso control de acceso físico, procedimientos operativos y existencia de políticas corporativas.

Se debe tener mucho cuidado para planear e implementar un plan de contingencia que satisfaga los requerimientos de la organización. No es una tarea fácil, puede involucrar considerable esfuerzo y gasto.

Las principales actividades de la planeación e implantación de un plan de contingencia son:

1. Determinar los requerimientos del negocio.

   Se debe realizar un análisis de riesgos para conocer el tipo de riesgo a que es vulnerable la organización, lo que permitirá determinar las medidas preventivas para minimizar el impacto del desastre y que riesgos de manera consciente no serán cubiertos.

También, se debe realizar un análisis de impacto sobre el negocio para determinar la cantidad de tiempo que la organización puede soportar sin el servicio. Este estudio permitirá definir que procesos se incluyen en el plan, de la interrupción por cada proceso, el máximo tiempo de interrupción de cada proceso, la prioridad del proceso, la dependencia entre procesos y el nivel aceptable de transacciones no recuperables por unidad de negocio.

Los resultados de estas dos actividades mostrarán los requerimientos del negocio y las estrategias que se incluyen para el desarrollo del plan.

Existen procesos del negocio que se deben evaluar para conocer su impacto en el negocio en caso de ocurrir un desastre, ya que puede ocasionar pérdidas de ingresos o la pérdida del negocio. Es importante clasificar los procesos del negocio por orden de importancia y cuando los recursos estén limitados, se deben atender los procesos críticos y esenciales para la supervivencia de la organización.

2. Determinar los requerimientos de procesamiento de datos.

Una vez establecidos los requerimientos del negocio, deben ser convertidos en términos de procesamiento de dato para determinar los procedimientos y recursos necesarios para restaurar el servicio. El plan de contingencias contempla la restauración de aplicaciones y datos, por lo tanto, para diseñar este plan se deberá identificar los siguientes requerimientos para recuperar aplicaciones y datos críticos:

- Tiempo máximo de caída por cada aplicación.
- El máximo monto de datos perdidos en un desastre.
- Los datos que debiera tener cuando el servicio se reanude.
- Requerimientos de hardware:
  - ✓ Capacidad del procesador.
  - ✓ Capacidad de disco duro.
  - ✓ Número de unidades de cinta por modelo y tipo.
  - ✓ Otros dispositivos como impresoras, scanners, etc.

- Requerimientos de red:
  - ✓ Topología
  - ✓ Tiempo máximo de caída aceptable
  - ✓ Ancho de banda
  - ✓ Departamentos que se conectaran durante la restauración del servicio.

- El nivel de servicio que se proporcionará después del desastre.

Este conjunto de información es llamado inventario de la aplicación. Se debe complementar ésta información con los datos requeridos por la aplicación y con las relaciones que tiene esta aplicación con otras. Las siguientes tablas muestran la organización de la información.

	Nivel critico	Tiempo de interrupción	Máxima pérdida de datos	Datos accesados	Interpelación con otras aplicaciones
Aplicación 1	Medio	18 horas	últimas 3 horas	base de datos pool 1	entrada para la aplicación 1
Aplicación 2	Bajo	36 horas	últimas 500 transacciones	lote pool	lote xyz
Aplicación 3	Alto	10 minutos	ninguna	base de datos pool 2	ninguna
...					
Aplicación n	...	...	...	...	...

	Funcionalidad del procesador	Almacenamiento en disco Gb	Carga en la red (Baudio)	Volumen de impresión (paginas/día)
Aplicación 1	7.0	1.1	2x9600	10,000
Aplicación 2	6.1	12.8	2x64k	40,000
Aplicación 3	1.4	6.2	1x4800	5,000
...				
Aplicación n		...	...	...
Total	32.0	70 GB		160,000

Cuando el inventario de la aplicación está completo, se debe identificar todos los componentes de cómputo necesarios para dar soporte y correr las aplicaciones. Estos requerimientos se deben incorporar en el diseño del plan.

Las necesidades del negocio pueden tener diferentes vistas por las diferentes áreas de la organización y pueden dificultar el consenso en lo primero que se debe recuperar, por lo que es importante identificar e incluir a los siguientes participantes:

- Gerentes de Sistemas de Información, Finanzas, Negocios.
- Dueños del proceso del negocio.
- Dueños de la aplicación.
- Personal de programación/soporte de sistemas.
- Personal operaciones, redes, seguridad de datos.

3. Diseño del plan.

Para el diseño del plan se debe balancear los siguientes criterios para contar con una adecuada solución: Costo del plan, cobertura, rapidez de la recuperación, datos completos.

Una vez de haber determinado los requerimientos para el procesamiento de datos, se encuentra en posición de diseñar el plan de contingencias donde se describe los mayores características y los principales elementos de la solución.

El nivel de detalle del diseño dependerá del requerimiento de la organización, cuando quiera conocer el costo estimado de las alternativas posiblemente no necesite el detalle. En cambio, cuando se ha elegido una solución y se desea implementar, un nivel mayor de detalle será requerido.

Los elementos que se contemplan en el diseño son:

✧ Alcance del plan

Se debe definir claramente lo que se esta recuperando y en que limite de tiempo para evitar alguna confusión. La definición del alcance debe incluir:

- Qué tipos de desastres están incluidos y los que se excluyen.
- La secuencia en que las aplicaciones serán recuperadas.
- El tiempo máximo de recuperación para cada aplicación.
- Los datos que serán recuperados.

✧ Respaldo y recuperación de datos

Los datos son los elementos mas críticos para el negocio y las estrategias de respaldo y recuperación son claves del plan, indican que datos serán respaldados, con que frecuencia, de que manera, como serán recuperados y en que orden. Es importante considerar los factores que influyen en las técnicas de recuperación y respaldo.

✧ Manejo y operación del centro de cómputo alternativo.

Existen diversos factores que se deben tener tomar en cuenta, dependerán de la naturaleza del centro de cómputo alternativo, como se puede ser un centro de cómputo existente o un centro de cómputo nuevo que será construido.

También, es importante considerar en la evaluación las opciones para el centro de cómputo alternativo, el impacto que se tendrán en las actividades de operación, como son. Encender, apagar, reiniciar el equipo, supervisión de la consola, montaje de cintas, impresión, etc.

✧ Descripción de la configuración de la recuperación.

En esta parte el diseño se enfoca en la descripción del centro de cómputo alternativo (ubicación, hardware y software), las conexiones entre el centro de cómputo primario y el alternativo, y la forma en que la red será conectada al centro de cómputo alternativo.

La distancia del centro de cómputos alternativo deberá ser determinada por el análisis de riesgos realizado. Una distancia hasta 20 kilómetros es considerada moderada y presenta ventajas como interconexión con gran ancho de banda, bajo

costo de interconexión, fácil reubicación y actualización en tiempo real en forma remota.

Basados en las aplicaciones y datos que se deben recuperar y en que forma operarán, se deben definir los recursos necesarios de hardware y software.

4. Selección de productos.

La selección de productos consiste en escoger un conjunto de productos que se utilizarán en conjunto para implantar el plan.
La selección del hardware y del software dependerá de la plataforma del centro de cómputo principal. Aunque los requerimientos para el respaldo y recuperación de datos son similares entre plataformas, las herramientas para realizar estas tareas varían, así como la manera en que funcionan.

La selección del centro de cómputo alternativo puede ser la decisión más importante que se tome. Este centro de cómputo no tiene que pertenecer necesariamente a la empresa, se puede utilizar los servicios profesionales de un proveedor o tener un acuerdo con otra organización.

Posteriormente que se han seleccionado los productos, se puede determinar el costo del plan. Este costo debe incluir todos los siguientes componentes del plan:

- Hardware
- Software
- Red
- Centro de cómputo alternativo
- Esfuerzo para la implementación
- Esfuerzo para mantenerlo

Después de estimar el costo del plan, se debe comparar con el riesgo del desastre. El costo del plan debe ser proporcional al costo y riesgo del desastre.

5. Implantación del plan.

Esta etapa para lograr la implantación del plan está compuesta por tres grandes áreas: Establecer el centro de cómputo alternativo, desarrollar e implantar los procedimientos técnicos para apoyar el plan.

I. Establecer el centro de cómputo alternativo.- Las tareas que se necesitan desarrollar, dependerán del tipo de centro de cómputo que se haya seleccionado, podría ser necesario construir y equipar un nuevo centro de cómputo, adquirir o reparar un centro de cómputo existente.

II. Desarrollar procedimientos técnicos.- Nuevos procedimientos tienen que ser creados y los procedimientos existentes deben ser enmendados para asegurar que los procesos críticos del negocio puedan ser recuperados y puedan correr en el nuevo centro de cómputo. Algunos procedimientos pueden ser los relacionados con el respaldo de datos, almacenamiento fuera del centro de cómputo, recuperación de datos, administración de cambios, reglas para el diseño de aplicación y procedimientos de recursos humanos.

III. Desarrollo del plan.- El plan deberá incluir los siguientes puntos:

- Alcance
- Los procesos para reconocer el desastre y la invocación del plan.
- Identificación de los grupos participantes del plan y sus integrantes.
- Descripción de las tareas y responsabilidades de los equipos participantes.
- El responsable del plan.
- Cómo será mantenido el plan.
- Cómo el plan será probado.

En un entorno complejo de cómputo puede ser útil comprar una herramienta para desarrollar el plan para que sirva como apoyo la recopilación de información, entrada de información y para estructurar el plan.

6. Mantener el plan actualizado.

Los cambios en el entorno del procesamiento de datos del centro de cómputo son constantes y algún cambio pudiera convertir el plan obsoleto. Los cambios pueden provenir de los siguientes acciones:

- Desarrollo de nuevas aplicaciones.
- Cambios a la actual configuración del hardware.
- Cambios a la red.
- Cambios en la estructura organizacional.
- Cambios al sistema.
- Cambios al centro de cómputo alternativo.

El coordinador del plan debe documentar los procedimientos para asegurar que las practicas de mantenimiento son adecuadas para sustentar la viabilidad del plan en cualquier momento. La única manera de determinar si se han realizado las actualizaciones es auditar el plan una o dos veces al año.

Una parte importante del plan es probarlo, si no se realiza esta prueba lo más probable es que el plan falle. Probar el plan, es una manera de verificar que los procedimientos de mantenimiento están funcionando.

Cuando sea posible, escoger un centro de cómputo remoto que permita probar el plan dos o cuatro veces al año. Hay dos tipos de realizar la prueba:

1. La prueba activa involucra ir al centro de cómputo alternativo y restaura el sistema y las aplicaciones.
2. La forma pasiva, es una prueba logística, es realizada por un grupo del plan en una sala de conferencias y muestra paso a paso lo que se debe realizar en cada evento del desastre.

6.5 RESPALDO DE INFORMACIÓN

Los sistemas de respaldo y copias de seguridad existen con un solo propósito: recuperar completamente los datos y la información necesaria para hacer funcionar un sistema de computadoras lo más pronto posible en caso de presentarse un siniestro. La información puede ser dañada por los siguientes factores: Errores de programas, errores del software del sistema, fallas de hardware, errores de procedimiento y fallas ocasionadas por el entorno.

Los errores causados por programas, son debidos por "basuras" o errores en la programación que dañan normalmente a la base de datos que el programa está actualizando, sin embargo el daño puede ser mayor si el programa lee registros de otros archivos e intenta actualizarlos. Los programas deben ser desarrollados para reconocer este tipo de situaciones rápidamente y detener su procesamiento. Los programas que afectan a la base de datos deberán tener procedimientos para regresar la base de datos a un previo estado correcto (rollback).

El software del sistema que fue comprado o desarrollado dentro de las instalaciones pueden tener alguna falla, aún después de haber sido probado extensivamente. Un sistema operativo, un sistema de administración de bases de datos, una utilería para el copiado de archivos puede tener errores. El daño causado dependerá de la naturaleza del software que se esté usando y como se está usando, por ejemplo, un error en el sistema operativo puede causar daño a toda la base de datos, ya que el sistema operativo da servicio a todos los programas; en cambio un error de un programa de las utilerías podría causar solo daño al archivo que utiliza.

A pesar de la alta confiabilidad del hardware pueden ocurrir fallas en el procesador, memoria, terminales, multiplexores, discos, etc., y pueden ocasionar la destrucción de tablas de control de archivos, índices, escritura incorrecta de bloques, etc.

Los errores de procedimiento pueden dañar a los archivos en diversas formas, por ejemplo, un operador puede cargar una versión incorrecta de un programa o montar un archivo incorrecto, los programas pueden ser corridos una secuencia errónea, o usuario puede meter un parámetro incorrecto en el momento de correr una actualización o un archivo maestro puede ser eliminado.

Las fallas del entorno pueden ser ocasionadas por diversos factores, la instalación puede ser inundada, saboteada o destruida por fuego. Las fallas del entorno frecuentemente tienen un amplio impacto sobre los archivos.

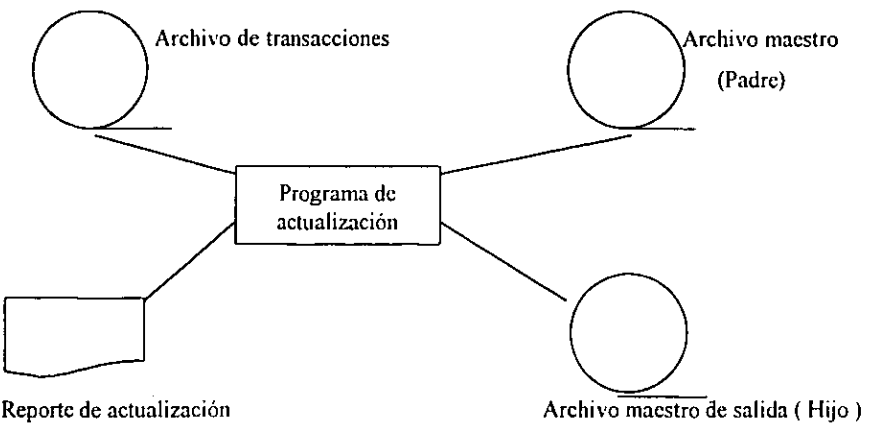
Todas las formas de respaldo y recuperación parten de una versión de la información a un momento dado y una bitácora de transacciones o cambios a la información. Si un programa crea una nueva versión del archivo, la versión previa puede ser utilizada para propósitos de respaldo y el archivo de transacciones usado para el proceso de recuperación. Cuando se actualiza la información, se deberá tomar decisiones sobre la frecuencia en que se realizará el respaldo y la forma en que mantendrá la bitácora [WEBE85]. Algunas estrategias de respaldo y recuperación son las siguientes:

I. Abuelo, padre, hijo.
II. Doble registro.
III. Bitácoras.
IV. Archivo diferenciales.

I. Abuelo, padre, hijo.

La estrategia abuelo, padre, hijo involucra el uso de la versión previa de un archivo maestro y el archivo de las transacciones de actualización para volver a crear el archivo maestro.

La siguiente gráfica muestra el uso de los archivos padre e hijo.



Para utilizar ésta estrategia existen los dos siguientes requerimientos:

1. El archivo maestro de entrada durante una corrida debe mantenerse intacto, los registros cambiados y los que no fueron cambiados deben ser escritos en un nuevo archivo.
2. El archivo de transacciones debe mantenerse intacto.

La re-creación del archivo consiste en volver a realizar la corrida de actualización.

La versión actual del archivo maestro es llamada el hijo; la versión previa padre. El archivo denominado abuelo, es el archivo de entrada para crear al padre. El abuelo es el respaldo para el padre. Si por alguna razón, el padre no puede ser leído, se debe realizar una corrida de actualización para generar al padre. La estrategia de respaldo involucra mantener tres generaciones del archivo maestro y la versión previa del archivo de transacciones. Es importante guardar las copias en diferentes lugares físicos, para que no se pierda toda la información en caso de presentarse una falla provocada por el entorno.

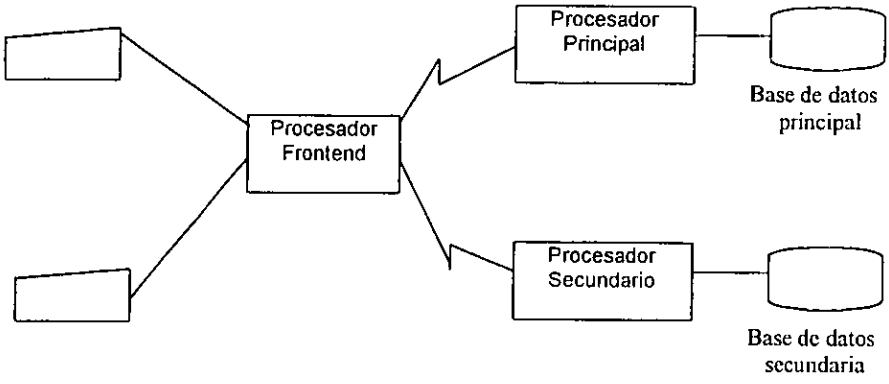
La mayor ventaja de esta estrategia es su sencillez, sin embargo, tiene cuatro desventajas:

1) Impide la actualización en el lugar.
2) Durante la recuperación el archivo no está disponible para otro proceso.
3) Procesos concurrentes no pueden actualizar el archivo y
4) Si el proceso de actualización consume una gran cantidad de recursos y el daño esta localizado, el proceso de recuperación resulta caro. Por los puntos anteriores, la estrategia de respaldo es mas útil para sistemas secuenciales de tipo lote.

II. Doble registro.

La estrategia de doble registro involucra mantener en lugares físicos diferentes dos copias de la información y actualizarlas simultáneamente. Una de las copias debe ser guardada en forma remota para protegerlo contra fallas del medio ambiente. Como una medida de protección contra fallas de hardware un segundo procesador tiene que ser usado. Si una falla ocurre en el procesador principal, se alterna al procesador secundario y a la información duplicada.

La siguiente gráfica muestra la operación del registro dual.



Esta estrategia debe ser utilizada en entornos donde la información que se requiere esté siempre disponible, por ejemplo, en los sistemas de reservación en línea, donde el costo de no contar con información disponible excede el costo de contar con recursos duplicados.

Usar la estrategia de registro dual ofrece poca protección contra errores de procedimiento, errores del software del sistema o contra errores de un programa. Por lo que se aplica un segundo respaldo y una estrategia de recuperación debe ser usada para protegerse de este tipo de errores.

III. Bitácoras.

Hay cuatro formas de llevar a cabo esta estrategia:

1. Bitácora de transacciones de entrada.- Requiere volver a procesar las transacciones para la actualización desde el último respaldo hasta el momento en que la información fue dañada. Es necesario tener un identificador de la fecha y tiempo para cada transacción.

2. Bitácora de imágenes del registro cambiado.- Esta estrategia es para facilitar el rollback de la información. Una imagen del registro se guarda en la bitácora antes de que se lleve a cabo la actualización. Cuando se presenta un error de actualización, el rollback ocurre en el punto donde se presentó el error, la bitácora es leída para reemplazar el registro existente.

3. Bitácora de la imagen posterior del registro cambiado.- Está diseñada para facilitar el rollforward de la información. La imagen del registro es copiada en la bitácora después de que fue actualizado, por ejemplo, si un dispositivo físico falla, la recuperación es realizada usando el respaldo más reciente y reemplazar la versión del registro con la imagen tomada de la bitácora que contiene la imagen posterior a la actualización.

4. Bitácora de parámetros de cambio. En ésta opción, los parámetros del cambio son copiados a la bitácora, en ligar de copiar toda la imagen de un registro, solamente el identificador único del registro y el apuntador podrían ser copiados. El proceso de recuperación es más complejo pero menos espacio es consumido por la bitácora.

IV. Archivos diferenciales.

La estrategia de archivos diferenciales facilita las operaciones de respaldo y recuperación, en lugar de aplicar los cambios directamente a la base de datos, los cambios se almacenan en un archivo diferencial y la base de datos se mantiene intacta y el archivo diferencial es guardado en otro dispositivo. El uso de archivos diferenciales tiene varias ventajas:

- Reduce costos de respaldo.- Solamente los archivos diferenciales requieren ser respaldados.
- Facilita el respaldo incremental.
- Permite respaldo en tiempo real y reorganización con actualizaciones concurrentes
- Facilita las operaciones para poner la información en un estado correcto (rollback y rollforward).
- Reduce el riesgo de una seria pérdida de datos.

ALMACENAMIENTO HISTÓRICO

Las empresas también tienen la necesidad de almacenar sus datos por más de dos o tres años o para conservación histórica, que tiene una sola oportunidad de grabarlos, lo que traería implicaciones serias para el tipo medio de almacenamiento que se utilizaría. Los sistemas de respaldo de información no están diseñados para atender éste objetivo, sino el de recuperar los datos de días o semanas después de haberlos almacenado, ante ésta necesidad, las empresas pueden utilizar los productos para archivar y aplicar criterios para seleccionar la información requerida.

Algunos criterios que se pueden aplicar son: El tamaño del archivo, tiempo transcurrido desde la última actualización, directorios o archivos pertenecientes a un usuario, grupo de usuarios o miembros de un proyecto.

El software para gestión documental es un método para archivar algún grupo de documentación definida en la red y permiten una recuperación rápida de documentos mediante criterios de búsqueda que incluyen palabras claves, textos o títulos. Otro método más común de archivar datos de PC, es mediante el uso de una utilería para compresión de datos y posteriormente archivarlos en otro lugar.

6.6 SISTEMA PARA DETECCIÓN DE INTRUSOS

La detección es un componente clave del sistema de seguridad, no importa que tan bien esté protegido un sistema, la seguridad total difícilmente se alcanza y siempre existe alguna persona que intentará encontrar la forma de comprometer el sistema, así es que la detección es la única forma de conocer cuando un sistema ha sido comprometido, ya que si hay algo peor que se cometa una incidente de seguridad, es el de no saber que se ha realizado. La información obtenida del incidente registrado permitirá reconstruir el sistema y tener confianza que la información es íntegra.

El sistema para detección de intrusos no solamente debe notificar los ataques conocidos, también puede buscar nuevos escenario como son actos no usuales o inesperados. El proceso de detección incluye el monitoreo del sistema y la detección de anomalías o de una serie de actividades que indiquen que una intrusión ha ocurrido y ha sido reportada

A menos que esté activado el sistema de monitoreo, los usuarios son los primeros que notarán que el sistema puede tener problemas cuando observe diversos eventos como lentitud, que no tenga espacio o cualquier otra anomalía. En este caso, el reporte se turna a la mesa de reportes y son los primeros para determinar si el sistema ha sido comprometido. Por este motivo, se debe instrumentar en forma conjunta el sistema para detección y los procedimientos para definir tiempos adecuados y la persona para notificar cuando un incidente es detectado y tomar la respuesta apropiada para el incidente de seguridad.

DETERMINACIÓN DE LA GRAVEDAD DE UN INCIDENTE DE SEGURIDAD

La información en los reportes de seguridad muestra actividades debidas a la curiosidad o errores de personas honestas y que no requieren profundizar en su análisis, sin embargo todos los incidentes deben ser registrados y reportados en los resúmenes estadísticos ya que pueden indicar ataques triviales o para identificar si un usuario necesita capacitación.

El volumen de datos en las bitácoras de seguridad requiere que se clasifique la gravedad de los incidentes para facilitar su análisis. Los incidentes que son comunes y detenidos por los controles regulares de seguridad deben ser registrados pero no reportados por ejemplo, el intento de Telnet y que la barrera de seguridad no lo permite, sin embargo, puede haber actividades que deben reportarse inmediatamente, como puede ser un ataque que está en progreso y que cambie inesperadamente un archivo ejecutable.

Para clasificar las alarmas de seguridad se requiere experiencia, sentido común y conocer la infraestructura de cómputo instalado, es fácil identificar las actividades cruciales y las que no son importantes, las actividades intermedias son las que se deben evaluar detenidamente y definir la respuesta adecuada.

En general es conveniente exagerar la clasificación de la gravedad y con la experiencia bajar el nivel de clasificación a un nivel adecuado. Los nuevos incidentes deben ser investigados y clasificados apropiadamente; los dueños de la información, personal que desarrolla las políticas y administradores de sistemas deben participar en el proceso de clasificación de la gravedad de los incidentes.

Para proteger al sistema de los riesgos más probables, es necesario identificar lo que sería de interés de los atacantes por ejemplo, la información de la empresa puede ser de interés para la competencia, la información personal, médica o financiera, el acceso a una red con grandes privilegios puede ser muy poderoso. Es importante proteger al sistema de atacantes internos y externos.

Una forma de proteger a un sistema de atacantes internos, quienes son usuarios válidos del sistema es mediante el establecimiento de controles para validar la integridad del sistema y su información.

Es necesario que exista una supervisión de las actividades en el sistema para identificar procesos que no están autorizados para correr dentro del sistema o para identificar operaciones sospechosas por ejemplo, los datos de la empresa pueden ser copiados hacia un sistema externo

por diferentes medios como FTP o correo electrónico, para tener una pista de las actividades realizadas, es necesario que se registren en la bitácora las conexiones que salen de la empresa para identificar quien hizo la conexión, donde se conectó y cuantos datos fueron transferidos. Un empleado que transfiere a la competencia mediante correo electrónico un archivo de 500 Megabytes debe considerarse como sospechoso.

Un tratamiento para los atacantes externos es el de mantenerlos fuera del sistema, una forma de conseguirlo es definiendo un perímetro de seguridad donde la información pueda fluir de manera segura, éste perímetro incluye al hardware (computadoras, servidores, impresoras, etc.), localidades físicas (edificios, tableros, cables, etc.) y software (que tipo de software y que datos puede utilizar).

SOFTWARE PARA DETECCIÓN DE INTRUSOS.

Una pieza clave para mantener el sistema seguro es el sistema para detección de intrusos. Las actividades que deberá realizar éste software son supervisar la integridad del sistema y las actividades que pueden ser consideradas sospechosas.

El software de detección deberá ser flexible para poder ajustar la configuración al nivel de detalle deseado y deberá detectar los incidentes con rapidez para facilitar una pronta notificación y respuesta.

También, se debe contar con herramientas para establecer medidas de seguridad preventivas y reactivas. Las medidas preventivas son procesos que se anticipan a un evento relacionada con la seguridad antes de que se convierta en problema. Las herramientas para medidas preventivas incluyen al software que apoyan a los usuarios para generar buenos passwords o para cifrar el trafico en la red. La mayoría de las herramientas de seguridad son medidas preventivas y para que sean eficientes deben ser corridas con un calendario irregular para reducir la certeza que tiene el intruso para cometer sus ataques.

Las medidas reactivas reportarán los ataques que se han cometido o que se están cometiendo. Estas medidas reactivas son procesos que regularmente supervisan el sistema y reportan comportamientos anormales, también pueden ser procesos que buscan actividades que corresponden al perfil de un ataque definido.

Los procesos pueden ser monitores en tiempo real que reportan inmediatamente actividades sospechosas o procesos en lote que corren periódicamente y revisan la bitácora para determinar y reportar actividades sospechosas. Los reportes que se emitan servirán para determinar como se realizaron los ataques, como cerrar las brechas o donde establecer una trampa en tiempo real para atrapar al intruso en el siguiente ataque.

6.7 BARRERA DE SEGURIDAD

Cuando una red es conectada a Internet las amenazas existentes en la red cambian y la organización puede extender sus políticas de seguridad en informática. El uso de una barrera de seguridad es una herramienta útil para disminuir las amenazas que provienen de redes externas a la organización.

El objetivo principal de una barrera de seguridad es proteger una red de otra, muchas personas utilizan la barrera de seguridad como un término genérico que describe un amplio rango de funciones que incluyen la arquitectura de los dispositivos que protegen a la red, también lo utilizan para describir casi cualquier dispositivo de seguridad de red, como puede ser un dispositivo de cifrado, un enrutador de selección o una compuerta a nivel de aplicación.

Las tareas principales de una barrera de seguridad son:

- Permitir el paso exclusivamente al tráfico autorizado conforme a las políticas.
- Control de acceso basado en las direcciones del emisor o receptor.
- Control de acceso basado en el servicio requerido.
- Validación de virus en los archivos de entrada.

Los mecanismos más importantes de una barrera de seguridad son el filtrado de paquetes y compuerta de aplicación, frecuentemente también proveen el servicio de autentificación.

El filtrado de paquetes permite el paso través de la barrera de seguridad solamente a cierto tipo de paquetes, un protocolo de red envía paquetes desde la dirección fuente a la dirección destino, la información relevante del paquete está incluida en su encabezado. El criterio que utiliza para el filtrado puede incluir cualquier información en el encabezado, para TCP/IP utiliza el encabezado del IP que contiene la fuente y dirección del host de destino, el identificador del puerto de destino, el número de puerto puede ser usado para filtrar paquetes basados en la aplicación, ya que las redes que utilizan TCP/IP usan número de puertos fijos para las aplicaciones. El filtrado de paquetes refuerza el control acceso, también las siguientes políticas:

- Permitir correo electrónico en dos formas, servicios de directorio y Telnet, y inhabilitar cualquier otro servicio.
- Permitir la comunicación solamente con un conjunto designado de servidores.
- Inhabilitar el tráfico entrante a un conjunto designado de puertos, porque proveen servicios de alto riesgo.

Los enrutadores (routers) frecuentemente se usan para construir una barrera de seguridad para el filtrado de paquetes, son transparentes para el usuario y pueden direccionar un paquete, de ésta manera el tráfico de un usuario remoto pasa a través de una compuerta que realiza una autentificación y auditoria antes de permitir al usuario remoto acceder al host.

La compuerta de nivel de aplicación usa una capa superior del protocolo de información e implementa servicios de seguridad adicionales, así también, aplica políticas más complejas. Está implementada típicamente en uno o más hosts, e involucra software desarrollado por la organización. La compuerta ejecuta programas para cambiar la dirección de los paquetes de aplicación, denominados apoderados que controlan el acceso a servicios como Telnet y FTP.

Una desventaja de la compuerta a nivel de aplicación, es la incompatibilidad con el cifrado que se realiza en la capa de transporte o de red. La compuerta necesita buscar información del protocolo en la capa de aplicación, por lo que tendría que descifrar y volver a cifrar.

Cuando se desea construir una barrera de seguridad es importante que se definan los recursos y servicios de la red que se desean proteger, para lograrlo es importante elaborar un documento que describa los objetivos de seguridad en la red de la organización.

Las organizaciones pueden elegir el método más adecuado para construir una barrera de seguridad, pueden utilizar los recursos de programación y financieros para desarrollar una barrera de seguridad con un método propio, o pueden utilizar productos existentes y personalizarlos para proteger la red de la organización.

Una barrera de seguridad se coloca entre la red interna confiable y la red externa no confiable, permite supervisar y rechazar el tráfico de red al nivel de aplicaciones, en el modelo OSI (Open Systems Interconnection) la barrera de seguridad puede operar en las capas de red y transporte, en éste caso examina los encabezados de IP y de TCP de paquetes entrantes y saliente, y rechazan o pasan paquetes con bases en las reglas de filtración de paquetes.

El servidor de base dual es un tipo de barrera de seguridad que se puede utilizar, es una máquina con dos interfaces para red, este tipo de barrera de seguridad procesa los paquetes conforme a las políticas de seguridad, por ejemplo si se implementó la política "Lo que no está permitido expresamente, está prohibido", entonces el tráfico de la aplicación no puede cruzar la barrera de seguridad a menos que el emisor de aplicación esté ejecutándose y que se haya configurado en la máquina de la barrera de seguridad [SIYA97].

Un cliente de la red interna puede acceder los servicios de Internet mediante una cuenta de entrada directa a la barrera de seguridad, sin embargo ésta conexión directa puede comprometer la seguridad de la barrera de seguridad, frustrando el propósito de proteger la red interna, el acceso debe ser a través de la consola o del acceso remoto seguro. El administrador de seguridad deberá prohibir la creación de cuentas de acceso directo a la barrera de seguridad. Solo se debe utilizar la barrera de seguridad para autentificar usuarios, para permitir que sus sesiones pasen a través de ella.

Los hosts de base dual frecuentemente están construidos en sistemas UNIX adaptados, por lo que se deben tomar las consideraciones necesarias para configurar adecuadamente la barrera de seguridad, por ejemplo, además de inhabilitar el envío de IP, se deberán eliminar los programas que pueden ser peligrosos en manos de un intruso, eliminar herramientas de programación, eliminar los permisos a los programas SUID (Set UserID) y SGID (Set GroupId) que no se requieran porque permiten un status de superusuario, utilizar particiones especiales para el caso de intrusión, eliminar cuentas especiales y de sistemas innecesarias, eliminar servicios de red que no sean necesarios, modificar los scripts de inicio del sistema para evitar la inicialización de programas innecesarios [SIYA97].

Otra configuración para una barrera de seguridad incluye un enrutador (router) que realiza el filtrado de paquetes y provee la interfaz con Internet y un servidor de bastión para la seguridad de la red. El enrutador manda todo el tráfico de entrada al host de bastión, donde se realiza la evaluación del control de acceso antes de que los paquetes sean pasados a los nodos de la red interna y el enrutador solo acepta paquetes del host de bastión.

La separación del filtrado de paquetes de otras tareas realizadas por la barrera de seguridad, permite tener un enrutador menos complejo y obtener un mejor rendimiento, porque el hardware puede ser optimizado para tareas de direccionamiento y un mayor grado de aseguramiento para su seguridad.

La implantación de una barrera de seguridad se puede realizar mediante paquetes comerciales, por lo que es conveniente hacer un reconocimiento o inventario del hardware y software, así como la capacitación necesaria para implantar los productos.

6.8 POLÍTICAS

Las políticas de seguridad son el conjunto de leyes, reglas y prácticas que regulan cómo una organización administra, protege y distribuye los recursos para lograr sus objetivos de seguridad. Las políticas de seguridad en informática para una organización, especifican las propiedades de seguridad de sistemas y las responsabilidades del personal en materia de seguridad, sirven para guiar el diseño de los puntos de seguridad en los sistemas computarizados. Una efectiva política de seguridad está orientada a proteger la inversión y los activos de una organización.

Las políticas deben considerar las amenazas sobre los bienes informáticos y especificar de qué se debe proteger la organización y qué medidas de seguridad adoptará para protegerse.

Se han desarrollado políticas y modelos para las propiedades de seguridad (confidencialidad, integridad y disponibilidad), de las cuales, la propiedad de confidencialidad ha recibido la mayor atención, las políticas y modelos para la integridad son menos desarrolladas y los modelos para la disponibilidad están en sus inicios.

Desarrollar políticas de seguridad implica realizar un conjunto de preguntas sobre los recursos que se les permitirá a los usuarios y qué recursos tendrán que restringirse debido a los riesgos a que están expuestos. Las políticas que se desarrollen deberán tomar en cuenta los derechos actuales de los usuarios y que no impidan la realización efectiva de su trabajo que se les han encomendado.

Las políticas deberán desarrollarse para ser aceptadas y aplicables en toda la organización y sobre todos sus bienes informáticos.

Para definir una política de seguridad, significa elaborar procedimientos y planes para proteger los recursos informáticos contra pérdida y daño. Para elaborar la política se deberá realizar los siguientes puntos:

- Identificar los recursos que se quieren proteger.
- Identificar de qué se necesita proteger.

- Estimar la posibilidad de que las amenazas se puedan materializar.
- Conocer la importancia de los recursos.
- Revisar medidas de protección económicas y oportunas que se puedan implantar.
- Revisar periódicamente las políticas de seguridad.

Es importante la participación de gente adecuada para el diseño de la política, si no se tiene el conocimiento suficiente de lo que se desea proteger y de las fuentes de la amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad. El grupo se puede integrar con personal de los usuarios, de sistemas de información, asesores de seguridad física y de auditoría. Las políticas deben asegurar que todos conozcan su propia responsabilidad para mantener la seguridad y que para cada problema exista alguien que lo pueda manejar de manera responsable.

Cuando se desarrolla una política de seguridad se debe asegurar que los esfuerzos dedicados a la seguridad sean costeables, esto implica que se debe conocer los recursos que valen la pena proteger y que recursos son más costeables que otros, también es necesario identificar las amenazas de las que se deben proteger los recursos. El análisis de riesgos ayudara determinar los siguientes puntos:

- Qué se necesita proteger.
- De qué se necesita proteger.
- Cómo protegerlo.

Los riesgos se deberán clasificar por nivel de importancia y gravedad de la pérdida y se deberá realizar el análisis para llegar a situaciones donde el gasto originado por las medidas de protección sea menor que lo que se desea proteger. Algunos factores que se deben considerar para estimar el riesgo de un recurso son: Estimación del riesgo de perder el recurso, estimación de la importancia del recurso, disponibilidad, integridad y confidencialidad del recurso.

Los recursos que se deben considerar durante el análisis de riesgos son:

- Hardware.- Procesadores, tarjetas, estaciones de trabajo, computadoras personales, impresoras, líneas de comunicación, terminales, enrutadores.
- Software.- Programas fuentes, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
- Datos.- Manejados durante la operación, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos, en tránsito a través de medios de comunicación.
- Personas.- Usuarios, operadores, etc.
- Documentación.- Correspondientes a los programas, hardware, sistemas y procedimientos administrativos, etc.
- Suministros.- Papel, formularios, cintas y medios magnéticos, etc.

Una vez redactada la política, es importante que se discuta por todo el grupo involucrado para llegar a un consenso y pasar a la implantación. La participación y el interés por parte de los usuarios asegurarán que la política se comprenderá mejor y será más probable que se siga.

Después que una política de seguridad se ha implementado, algunos usuarios tienen la tendencia a violarla, en algunos casos éstas violaciones son evidentes, sin embargo algunas violaciones pasan inadvertidas por lo que se debe considerar los controles necesarios en los procedimientos de seguridad para reducir al mínimo que no se detecte una infracción de seguridad.

Cuando se detecte una violación a la política de seguridad, se deberán determinar las causas y que tipo de personal la realizó para tomar las acciones correspondientes. Estas acciones requieren ser definidas con claridad y con base en el tipo de usuario que haya realizado la violación. La política debe contener procedimientos para manejar cada tipo de incidente de violación, indicar el registro de violaciones y la periodicidad de la revisión de violaciones para observar tendencias.

Ante los incidentes de seguridad se pueden tomar dos tipos de respuesta:

- Proteger y continuar.- El objetivo es proteger inmediatamente los recursos, restablecer a la situación normal y continuar con el servicio.
- Perseguir y demandar.- Consiste en vigilar en la forma más discreta posible las actividades de los intrusos, registrar las actividades para tener pruebas en una demanda judicial.

En los proyectos de seguridad, es importante considerar los modelos de seguridad, los cuales sirven para tres propósitos básicos, el primer propósito provee un marco de trabajo para el entendimiento de concepto, frecuentemente a través de diagramas o gráficas; el segundo propósito es proveer una representación sin ambigüedades, en la mayoría de los casos una representación formal de una política general de seguridad; el tercer propósito es el de expresar la política reforzada por un específico sistema automatizado.

Los modelos de seguridad capturan las políticas de seguridad para las propiedades de confidencialidad y para la integridad, algunos modelos aplican en entornos que son estáticos (Bell-LaPadula) y otras consideran cambios dinámicos en los derechos de acceso (Muralla China). Los modelos formales de seguridad como el modelo de Bell-LaPadula tienen un papel importante en las evaluaciones para asegurar un alto nivel de seguridad, los modelos informales como el de Clark-Wilson son más descriptivos para expresar políticas de seguridad.

El modelo Bell-LaPadula fue desarrollado para el diseño de sistemas operativos seguros para entornos multi-usuario y captura los aspectos de confidencialidad para el control de acceso, los permisos de acceso son definidos mediante una matriz de control de accesos y niveles de seguridad.

El modelo de Harrizon-Ruzzo-Ulman considera políticas para cambiar los derechos de acceso o para la creación y eliminación de sujetos y objetos, y define un sistema de autorizaciones.

El modelo Clark-Wilson considera los requerimientos de seguridad en aplicaciones comerciales, estos requerimientos están orientados a la integridad de datos y prevenir modificación no autorizada de datos, fraudes y errores.

6.9 PRINCIPALES ORGANIZACIONES DE SEGURIDAD EN INFORMÁTICA

Las siguientes organizaciones están orientadas a la seguridad en informática, se encargan de desarrollar estándares, responder a incidentes y a promover las tecnologías de seguridad en informática.

1) Association for Computing Machinery (ACM)

   http://www.comp.org.acm

   Es la organización internacional científica y educativa más grande y más antigua, publica una variedad de revistas y periódicos, tiene capítulos locales y grupos de especial interés.

2) American Society for Industrial Security (ASIS).

   http://www.webplus.net.infoinc/asis/

   Asociación profesional para gerentes de seguridad.

3) Computer Emergency Response Team (CERT).

   cert@cert.sei.cmu.edu

   Establecida en 1988 por DARPA para orientar investigaciones de usuarios de Internet.

4) Computer Operations, Audit, and Security (COAST).

   http://www.cs.purdue.edu/coast/coast.html

   Laboratorio de investigación en seguridad informática dentro del departamento de ciencias de la computación de la universidad de Purdue, trabaja en conjunto con investigadores e ingenieros de grandes compañías privadas y con departamentos del gobierno, enfocan su investigaciones en necesidades del mundo real.

5) Computer Professionals for Social Responsibility (CPSR).

   http://www.cspr.org/

   Asesores expertos que proveen al público y personas que desarrollan políticas, asesoramiento del poder y problemas de la tecnología de la información.

6) Computer Security Institute (CSI).

http://www.gocsi.com/csi

Instituto que ofrece entrenamiento específico para profesionales en seguridad en informática, provee educación con ejemplos prácticos para proteger los activos informáticos de una organización. CSI es la industria líder en entrenamiento orientado a habilidades para practicantes de seguridad en informática.

7) DOE's Computer Incident Advisory Capability (CIAC).

http://ciac.llnl.gov/ciac/

Departamento del gobierno de los Estados Unidos que proporciona servicios de seguridad en informática a empleados y contratistas de Departamento de Energía. Tiene varias listas de correo para publicaciones electrónicas.

1. - CIAC-BULLETIN.- Consejos, información de tiempo crítico, boletines e información importante sobre seguridad informática.
2. - CIAC-NOTES.- Colección de artículos de seguridad en informática.
3. - SPI-ANNOUNCE.- Actualizaciones de software Security Profile Inspectos (SPI), nuevas características, distribución y disponibilidad.
4. - SPI-NOTES.- Discusiones de problemas y soluciones relacionadas con el uso de productos SPI.

8) Forum of Incident Response and Security Teams (FIRST).

http://www.first.org/

Coalición de organizaciones privadas y de gobierno para intercambiar información y coordinar las respuestas a incidentes relacionados con la seguridad en informática. Integra equipos con elementos del gobierno, organizaciones comerciales y educativas, y coordina la prevención de incidentes, una respuesta rápida y promueve el compartimiento de información entre los miembros y la comunidad.

9) High Tech Crime Investigation Association (HTCIA).

http://www.htcia.org/

Asociación que promueve y ayuda el intercambio de información, ideas y conocimiento sobre métodos, procesos y técnicas relacionadas con la investigación y seguridad en tecnologías avanzadas.

10) Institute of Electrical and Electronics Engineers (IEEE).

http://www.ieee.org/

Fundada en 1884 con más de 320,00 miembros que realizan avances revolucionarios en la ingeniería.

11) Information Systems Audit and Control Association (ISACA).

http://www.isaca.org/

Organización profesional internacional para practicantes de auditoria en sistemas, control y seguridad.

12) Information Systems Security Association (ISSA).

http://www.uhas.uh.edu/issa/

Organización internacional de profesionales en seguridad en informática que proporcionan educación.

13) International Information Systems Security Certification Consortium (ISC)2

http://www.utoronto.ca/security/isc2.htm

Corporación establecida para desarrollar un programa de certificación en seguridad en informática.

14) National Computer Security Association (NCSA).

http://www.ncas.com/

Asociación que proporciona información de seguridad, confiabilidad y ética.

15) National Institute of Standards and Technology (NIST).

http://www.nist.gov/itl/div877

Provee guía y asistencia técnica al gobierno y a la industria para la protección de sistemas de información.

16) UniForum

http://www.uniforum.org/

Asociación profesional que ayuda a individuos y organizaciones para incrementar la efectividad de los sistemas de información a través del uso de sistemas abiertos, basados en estándares de industria compartida.

17) USENIX.

http://www.usenix.org

Asociación que brinda apoyo a sus miembros, profesionales y desarrollos técnicos mediante diferentes actividades que incluyen conferencias, tutoriales, publicaciones y participa con ISO, IEEE y ANSI en el desarrollo de estándares.

7. INFORME FINAL DEL DIAGNÓSTICO DE RIESGOS

7.1 FORMATO DEL INFORME FINAL

Al terminar el proceso del diagnóstico de riesgos, se han identificado los activos informáticos que están bajo un riesgo y se ha cuantificado el valor del riesgo asociado, las medidas preventivas han sido identificadas para minimizar el efecto del riesgo y se les ha asignado un costo a dichas medidas.

Cuando el diagnóstico de riesgos está completo, el equipo está preparado para elaborar un reporte que refleje los resultados del trabajo realizado. El reporte del diagnóstico de riesgos, es el medio para presentar a los directivos de la empresa, las observaciones y recomendaciones en materia de seguridad en informática que se pueden implantar en la empresa.

La información presentada servirá a los directivos para tomar decisiones en materia de seguridad en informática con bases bien sustentadas. El reporte se mandará al directivo de la organización para revisión, aprobación y para agilizar las acciones que se deberán tomar.

El formato sugerido para el reporte contiene las siguientes secciones:

1.- Introducción

A. Describe el alcance del diagnóstico de riesgos. Adicionalmente, puede describir las decisiones que delimitan el alcance.

B. Describe el entorno físico del procesamiento de la información

C. Describe las medidas de seguridad que se están aplicando actualmente o que están en proceso de ser implantadas.

2.- Antecedentes

A. Describe las relaciones entre los dueños de la información, custodios y usuarios de la información.

B. Incluye un informe de las suposiciones para el estudio.

3 - Requerimientos y restricciones.

A. Describe trabajos en seguridad en informática que se han realizado previamente

B. Lista los requerimientos y restricciones para el estudio realizado.

4.- Análisis de Riesgos

A. Análisis de las amenazas y vulnerabilidades.

B. Resumen de las observaciones y su probable impacto, identifica los activos informáticos en riesgo, identifica los riesgos, probabilidades de ocurrencia y estimación de la posible pérdida. Los papeles de trabajo no deben ser incluidos.

C. Lista de recomendaciones y estimación del costo de su implantación, descripción de las amenazas y riesgos que pueden ser minimizadas por la recomendación.

5.- Recomendaciones.

A. Lista de recomendaciones por orden de importancia; descripción del impacto de implantar las recomendaciones; descripción del costo-beneficio y de los recursos necesarios para desarrollar, mantener, implantar y mantener recomendaciones.

6.- Resumen

A. Describe las dificultades encontradas durante el trabajo.

B. Describe las técnicas que fueron usadas para conducir el estudio; identifica los elementos de los equipos y los recursos utilizados.

C. Describe brevemente las medidas de seguridad.

Todos los papeles de trabajo generados durante el análisis deben estar organizados y almacenados para apoyar las observaciones y recomendaciones sugeridas, y para trabajos futuros.

El reporte del análisis de riesgos y la documentación generada son considerados como informacion sensitiva por lo que se deben proteger adecuadamente y no se debe distribuir en forma general o indiscriminada.

8. CONCLUSIONES

El dominio de tecnologías de información no es suficiente para realizar el diagnóstico de riesgos en informática en forma satisfactoria, es necesario complementarlo con el conocimiento de políticas, técnicas, modelos y controles de seguridad, así como habilidades administrativas y procedimientos para desarrollar su trabajo.

Los elementos que se exponen resaltan la necesidad de contar con una buena preparación y capacitación continua en seguridad en informática, de saber como planear y organizar la actividad del diagnóstico de riesgos para realizar su trabajo en forma organizada, eficiente y efectiva.

Dominar los elementos propuestos para el diagnóstico de riesgos además de conseguir resultados satisfactorios, tendrá beneficios adicionales, permitirá que la organización identifique y acepte la función de diagnóstico de riesgos; incrementará su participación en forma oportuna dentro de su marco de trabajo y responsabilidades.

De no contar con directrices para realizar el diagnóstico, se tendrá el riesgo de ejecutar trabajos indebidos con pobres resultados, por ejemplo, el de intentar cubrir áreas que no son de su competencia, ocasionando que confundan su responsabilidades con la de otros departamentos, que lo consideren un elemento que interfiere en las actividades de los usuarios, lo que provocará que no pueda realizar el diagnóstico de riesgos.

En las áreas de participación se describen técnicas, modelos, operaciones, planes o relacionadas con la seguridad en informática, con la finalidad de obtener una mayor perspectiva de las actividades más importantes relacionadas con la seguridad informática, visualizar los retos que le esperan, orientar sus esfuerzos de capacitación para lograr un dominio razonable de las áreas de participación.

Los elementos de evaluación propuestos sirven como guías para integrar una lista de controles de seguridad que deben existir en el área que se desea realizar el diagnóstico, la cual se deberá ajustar

conforme a estándares, prácticas aceptadas, criterio o alcance deseado. En virtud de que las áreas de participación pueden tener una alta relación entre ellas, se deberán seleccionar los elementos de seguridad requeridos conforme al criterio seleccionado para no duplicar esfuerzo.

La coordinación de un trabajo de evaluación requiere de una persona con experiencia para asesorar y organizar al grupo de trabajo y en especial a sus compañeros que tienen menor experiencia, así mismo, presupueste los costos originados por las personas que necesitan entrenamiento.

El desarrollo del diagnóstico de riesgos no se debe dejar en manos de inexpertos, si recomendaciones de baja efectividad se llevan a la práctica los costos pueden ser muy altos y las consecuencias muy graves, la selección de personal deberá ser cuidadosa y considerar a los elementos que tengan el perfil adecuado, que tengan el conocimiento técnico en tecnologías de información, habilidades administrativas para sensibilizarse con las operaciones de las organización, un alto sentido ético para manejar información valiosa para la empresa y conocimiento de estándares para proteger la información.

El grupo encargado de realizar el diagnóstico de riesgos deberá dominar la metodología propuesta para poderla aplicar, durante la aplicación de la metodología se deberá poner en práctica todos los elementos para el diagnóstico de riesgos para obtener resultados satisfactorios.

El informe final se deberá elaborar cuidadosamente, debe ser claro y bien organizado, para que la dirección tenga la información necesaria para la toma de decisiones y apoye la implantación de las medidas de seguridad propuestas. Un informe bien elaborado obtendrá el apoyo de la dirección para continuar realizando diagnósticos de riesgos en informática.

9. BIBLIOGRAFÍA

[CAST95] Castano, Silvana, *Database Security*, ACM Press, 1995.

[COME97] Comer, Douglas E., *Redes de Computadoras Internet e Inter-redes*, Prentice-Hall Hispanoamerica, primera edición, 1997.

[DEMP97] Dempsey, Rob, *Security in distributed computing: did you lock the door?*, Prentice-Hall PTR, 1997.

[FARL98] Farley, Marc, *Guía LAN Times de Seguridad e Integridad de Datos* , Mc Graw-Hil/Interamericana de España, S. A. U., 1998.

[FINE90] Fine, Leonard H., *Seguridad en centros de cómputo: políticas y procedimientos*, México: Trillas, segunda edición, 1990.

[FUST97] Fuster Sabater, Amparo., *Técnicas criptográficas de protección de datos*, RA-MA Editorial, 1997.

[GHOS98] Ghosh, Anup K., *E-Commerce Security: Weak links, best defenses*, John Wiley & Sons, Inc., 1998.

[GOLL99] Gollmann, Dieter, *Computer Security*, John Wiley & Sons Ltd., 1999.

[GRAT98] Gratton, Pierre, *Protección Informática: en datos y programas; en gestión y operación; en equipos y redes; en Internet*, México: Trillas,1998.

[HANC96] Hance, Olivier., *Leyes y Negocios en Internet*, McGraw Hill Interamericana Editores, 1996.

[HUTT95] Hutt, Arthur E., *Computer Security Handbook*, John Wiley & Sons, Inc. third edition, 1995.

[ICOV95] Icove, David., *Computer Crime: A Crimefighter's Handbook*, O'Reilly & Associates, Inc. 1995.

[KOVA97] Kovacich, Gerald L., *The information Systems Security Officer's Guide*, Butterworth-Heinemann, 1997.

[LIDA90] Li, David H., *Auditoria en centros de cómputo: objetivos, lineamientos y procedimientos*, México: Trillas, 1990.

[LIUC97] Liu, Cricket., *Administración de Servicios de Información en Internet*, McGraw Hill Interamericana Editores, S.A. de C.V., 1997.

[MCRA78] Mc Rae, T.W., *Muestreo estadístico para auditoria y control*, primera edición, Editorial Limusa, 1978.

[NEAG97] Neaga, Gregor., *Fire in the computer room, what now ?:disaster recovery, preparing for business survival*, Prentice Hall PTR, 1997.

[OPPL98] Oppliger, Rolf, Sistemas de autentificación para seguridad en redes, RA-MA Editorial, Madrid, España, 1998.

[PIAT98] Piattini, Mario G., *Auditoría Informática: Un enfoque práctico, RA-MA Editorial, 1998.*

[PARK98] Parker, Donn B., *Fighting Computer Crime*, John Wiley & Sons, Inc. 1998.

[PIPK97] Pipkin, Donald L., *Halting the Hacker: a practical guide to computer security*, Prentice Hall PTR, 1997.

[PRES97] Pressman, Roger, *Ingeniería del Software, un enfoque práctico*, Mac Graw Hill/Interamericana de España, S.A. de C.V. 4ta. Edición, 1997.

[ROSA96] Rosales Herrera, Humberto David, *Determinación de riesgos en los centros de cómputo*, México: Trillas, 1996.

[SHAW98] Shaw, Paul, *Managing legal and security risks in computing and communications*, Butterworth-Heinemann, 1998.

[SIYA97] Siyan, Karanjit, *Firewalls y la seguridad en Internet*, Segunda edición, Prentice-Hall Hispanoamericana,S.A., 1997.

[SUMM97] Summers,Rita C. *Secure computing: threats and safeguards*, McGraw Hill Book Co, 1997.

[TANE97] Tanenbaum, Andrew S., Redes de computadoras, 3ª. Edición, Prentice Hall Hispanoamerica, S. A. 1997.

[WEBE85] Weber, Ron , *EDP Auditing Conceptual Foundations and Practice*, third printing, McGraw Hill Book Co., 1985.