Capítulo 3
Seguridad Informática

En este capítulo se abordan generalidades
de la seguridad Informática,
se identifican los diferentes tipos de seguridad en
informática y las áreas de control crítico,
los principios, propiedades y funciones de la seguridad,
se propone una metodología de seguridad
y por último las responsabilidades del jefe de informática.

Introducción

Uno de los objetivos del centro de cómputo[58] es el procesar los sistemas de información de la empresa en forma tal que se obtengan los resultados esperados de manera confiable, oportuna y con el mínimo de recursos utilizados, para lograr este objetivo se deben considerar algunos aspectos que nos garanticen el procesamiento de datos continuo.

Dado los recursos que se manejan en informática, existe el riesgo de que pueda ocurrir alguna contingencia que impida el logro de ese objetivo, por lo que se debe implementar un programa integral de seguridad.

Para el establecimiento de este programa en los centros de cómputo, primeramente se revisarán los diferentes tipos de seguridad que se pueden reconocer, para estar en posibilidades de desarrollar un método a través del análisis de las áreas de control crítico e identificación de las amenazas potenciales y la evaluación del riesgo.

También es importante obtener el costo-pérdida del recurso Informático, para seleccionar los controles adecuados que se deban implementar y por último se revisaran las funciones y responsabilidades del jefe de informática y del administrador de seguridad.

Fuente: Escamilla Bello Tomás Javier, "<u>Metodología de seguridad avanzada para los sistemas y equipos de cómputo</u>..",
Trabajo recepcional, Facultad de Informática U.V., 1996.

[58] Es una instalación concebida especialmente para albergar computadoras, sus periféricos locales y equipo auxiliar, además áreas de para el personal de servicio.

I.3.1 Generalidades

En términos generales, podemos definir a la seguridad como *la serie de pasos o medidas a realizar para mantenerse a salvo de alguna agresión, desastre o cualquier situación que implique riesgo.* [59]

La seguridad en el área de informática es el *conjunto de medidas, procedimientos y dispositivos adoptados para la protección física del personal, equipo, soporte de información y la confidencialidad e integridad de la misma*. [60]

La seguridad se refiere a todos los controles que nos permiten resguardarnos de algunos problemas que en muchas ocasiones son considerados no evidentes a los ojos de la alta gerencia, pero sin embargo eventualmente pueden tener repercusiones aun más serias que la destrucción misma de los equipos utilizados para proceso de datos.

La seguridad efectiva en informática debe garantizar la prevención y detección de un ataque o accidente, la existencia de medidas claramente definidas para afrontar el desastre cuando ocurra y si existiese una interrupción del procesamiento, reestablecerlo.

Un sistema seguro es aquel del cuál *se tiene siempre e invariablemente un amplio conocimiento de todos sus aspectos y del que han sido previstos los riesgos potenciales que pudieran detener o modificar cualquier procedimiento inherente al mismo.*[61] El conocimiento pleno de un sistema es el resultado del análisis integral en forma periódica del mismo.

Por otra parte, si llegara a presentarse uno o varios agravios en contra de la integridad o consistencia del mismo, éste deberá tener la capacidad suficiente para minimizar sus efectos.

El objetivo final de la seguridad y protección de la información es garantizar la integridad disponibilidad y confidencialidad de la información, no sólo se trata de instalar o implementar protecciones, sino identificar los puntos de riesgo en áreas vulnerables [62] en las que se deberá implementar una serie de controles cronológicos de seguridad efectiva, tomando como base las causas y no los efectos que se presentan.

Existen tres formas básicas de tratamiento de riesgos:
- ✓ Atacarlos
- ✓ transferirlos
- ✓ Aceptarlos

y de acuerdo al tipo de riesgo y su impacto se deberá tomar las medidas y prioridades necesarias.

[59] Diccionario de Reader's Digest
[60] Richard Mosly, Computer and Comunications Security, primera edición pp 92
[61] Eduard R. Buck, Introduction to data & Controls, glosario de términos, segunda edición, pp230
[62] Área vulnerable "*son características que tiene el medio ambiente al permitir una amenaza, la cual, actúa sobre el bien causándole un daño*" Edward R. Buck, .Introducction to data security and controls.

I.3.2 Diferentes tipos de seguridad en informática

Para el establecimiento de un programa integral de seguridad en los centros de cómputo, es indispensable considerar cuatro áreas de oportunidad que son:

- SEGURIDAD FISICA (instalaciones)
- SEGURIDAD LOGICA (Datos, información, software)
- SEGURIDAD CONTRA CONTINGENCIAS (Casos de desastre)
- SEGURIDAD ADMINISTRATIVA (Procedimientos, políticas.)

Seguridad física (instalaciones)

Se refiere a la protección física de las instalaciones y los equipos, al mantenimiento a los circuitos eléctricos a fin de evitar interrupciones de energía, a las protección para todos los puntos de acceso al área, almacenamiento seguro de los dispositivos magnéticos y su protección contra cualquier uso no permitido, daño, pérdida o modificaciones, etc.

Seguridad lógica (datos, información, software)

Se refiere a la seguridad que debe tener el sistema operativo y los sistemas aplicativos, bases de datos y archivos convencionales, deben estar debidamente validados a prueba de errores que se puedan cometer por parte de operadores y usuarios, el acceso a las bibliotecas debe ser restringido solo a personal autorizado, etc.

Seguridad contra contingencias (casos de desastre)

Se refiere a la protección física contra incendios, inundaciones, temblores y sus planes de contingencia, la información, el equipo y el personal deben ser protegidos contra accidentes y desastres naturales.

Seguridad administrativa (procedimientos, políticas.)

Se refiere a la existencia de normas, políticas, procedimientos diseñados para garantizar una seguridad efectiva de los recursos informáticos [63], deben efectuarse prácticas adecuadas de seguridad, las responsabilidades seguridad física deben estar asignadas al personal y deben existir procedimientos de respuesta a emergencia en caso de pérdida total o parcial de la operatividad del centro de cómputo.

[63] Reconoceremos a los Recursos Informáticos como aquellos necesarios para la operación del Centro de Cómputo, llámense personal, hardware, software, mobiliario, insumos, instalaciones, equipo auxiliar, etc.

I.3.3 Áreas de control crítico

La situación de riesgo que deriva de la acción, actitud y circunstancia relacionadas con el personal o agentes externos no es nueva, los daños pueden ser accidentales, deliberados o producto de la negligencia. Los recursos de cómputo deben estar especialmente protegidos contra este tipo de daños.

Los principales elementos de amenaza que afecta el activo informático en cualquier organización son:

- Errores y omisiones
- Incendios
- Inundaciones
- Elementos externos
- Empleados deshonestos
- Sabotaje técnico
- Destrucción de datos negligente o intencional
- Irresponsabilidad
- Falta de capacitación
- Falta de documentación
- Etc...

En la mayoría de los centros informáticos, no se cuenta con normas de seguridad efectivas y mucho menos métodos de seguridad debidamente establecidos, esto trae como consecuencia la implementación de criterios de seguridad poco confiables, parchados y de fácil vulnerabilidad que a largo plazo ocasionan grandes gastos y retrasos en los procesos, es decir se tiene una "seguridad ficticia o falsa".

Se enumeran ciertos factores críticos que necesitan atención en relación con los sistemas de cómputo, estos factores han sido el origen de muchos problemas de información en la actualidad, inclusive han sido la clave para mejorar el control de las aplicaciones.

- Adecuada identificación de funciones (usuarios, dueños e informática)
- Limitar al mínimo posible los privilegios de acceso.
- Centralización en el control de los cambios al sistema.
- Mantenimiento de librerías [64] en discos y dispositivos magnéticos.
- Establecimiento de una conciencia de seguridad física y de la información
- Plan de recuperación en caso de desastres naturales.
- Fomento de un programa vital de riesgos.
- Control de los programas en etapa de producción y de prueba.
- Empleo de utilerías y rutinas de ayuda en el software.
- Definición de una metodología del desarrollo de sistemas.
- Programa de entrenamiento.
- Monitoreo de personal.
- Identificación de Inventario.
- Pólizas de seguros y contratos.
- Control de la información de Entrada / salida.

[64] Este concepto se refiere a los directorios creados en el disco duro, también se le conoce como biblioteca

Se debe identificar las áreas que han comprobado ser las mas críticas para el control de la información de los sistemas y equipos, es mucho más efectivo asignar recursos al manejo y protección de las áreas identificadas como vulnerables, que el estar haciendo constantes revisiones, análisis de riesgos o diseño de distintos métodos.

Adecuada identificación de funciones

Este factor asegura que exista una adecuada definición de tareas y responsabilidades para el desarrollo de nuevas aplicaciones y para los sistemas en operación, en particular cita autoridades, responsabilidades y el compromiso del personal en el procesamiento de la información. De ser posible cada una de las siguientes funciones deberá ser ejecutada por una persona distinta, alguna de estas funciones son:

- Diseño de aplicaciones.
- Administración de Bases de Datos.
- Control de librerías y archivos.
- Captura.
- Emisión de reportes.
- Distribución de reportes.
- Programación de los sistemas desarrollados.
- Mantenimiento del software desarrollado.

Limitar al mínimo posible los privilegios de acceso

La manera de conducir los privilegios que serán cedidos a cada usuario, puede realizarse por medio de una sencilla pregunta: Si este reporte o archivo no fuera accesible para el usuario, ¿Podría el usuario cumplir con su trabajo?. Siempre deberá pensarse en el mínimo de privilegios que se otorgarán al usuario y no en los privilegios que él desea manejar.

Centralización en el control de los cambios del sistema

Este factor es crítico para todos los sistemas y aunque éstos hayan sido diseñados con una alto grado de integridad y control, estas consideraciones y protecciones pueden verse anuladas al presentarse una falla en cualquiera de los cambios a los que sea sometido el sistema.

Cada departamento deberá tener establecido un grupo encargado de controlar todos estos cambios.

La mayoría de los problemas que se presentan en la actualidad son el resultado de "arreglos rápidos" al software, con el objeto de sobre llevar un problema determinado o soportar alguna necesidad determinada, al asumir que están apoyando al usuario pueden crear una ruptura o parche al momento de unir dos segmentos del programa, estas inserciones temporales de código que no han sido previamente autorizadas pueden pasar desapercibidas e introducirse de modo permanente en un programa que no fue concebido de tal manera.

Mantenimiento de librerías en discos y dispositivos magnéticos

En la mayoría de las organizaciones actuales la información almacenada en dispositivos magnéticos representa un recurso que garantiza el mantener en operación a dicha compañía, si se perdiera el acceso a estos recursos muy probablemente no podría sobrevivir, todas las organizaciones deben poseer procedimientos que les permitan tener el control de sus inventarios de librerías de información.

Establecimiento de una conciencia de seguridad física y de la información

La mayoría de las empresas que dependen de sus sistemas se preocupan por la seguridad solo en un principio, cuando se implantan los sistemas, es cuando proporcionan cierta orientación y entrenamiento a su personal, sin embargo, no existe un seguimiento de aquella primera introducción, por lo que el empleado al paso del tiempo olvida el objetivo de las normas de seguridad y aun estas mismas. Cada organización debe de tener un programa de seguridad que le permita revisar la continua responsabilidad con respecto a la seguridad en los sistemas.

Plan de recuperación en caso de desastres naturales

El propósito de estos planes es programar los pasos a seguir en caso de desastre con objeto de garantizar la continuidad de las operaciones de la empresa. Estos planes son medidas que deberán ser tomadas para restablecer la capacidad operativa de la organización en el menor tiempo posible, estos desastres comprenden catástrofes mayores como terremotos, huracanes, inundaciones, etc.

Fomento de un programa vital de registros

Con el fin de proteger la información, los datos se deberán clasificar de acuerdo al nivel que ocupan dentro de las necesidades de la empresa, la siguiente clasificación podría ser utilizada:

- Registros vitales, la pérdida de estos registros podrá terminar con la organización misma, esta información a menudo no es recuperable y es información con carácter de disponibilidad inmediata para que la organización se mantenga en operación.

- Registros esenciales, la pérdida de esta información podría ciertamente tambalear la capacidad de operación de la organización, la empresa no se vendría abajo, sin embargo, su nivel de operación seria gravemente afectado.

- Registros importantes, la pérdida de esta información causa inconvenientes, sin embargo rara vez podrá ser el origen de rupturas en la capacidad operativa de la empresa.

- Registros útiles, la pérdida de esta información produce apenas pequeñas perturbaciones en la empresa, generalmente son vistas como no esenciales y puede darse el caso de que no se presente la necesidad de tener que recuperarlos

Control de los programas en etapa de producción y de prueba

El control de las librerías de prueba y los programas en prueba del área de desarrollo de sistemas del centro de cómputo, es clave en el manejo de la integridad y seguridad de los sistemas, entiéndase como producción todos los sistemas y las aplicaciones que ya han sido probados, aprobados y hechos parte de la operación de la organización.

Empleo de utilerías y rutinas de ayuda en el software

Todas las utilerías que permitan añadir, borrar, modificar y copiar información deberán estar bajo completo control, el uso indiscriminado de tales utilerías permitiría a las personas cometer actos deshonestos motivados por intereses personales o por venganza.

Definición de una metodología del desarrollo de sistemas

El área de desarrollo de nuevas aplicaciones del centro de cómputo debe contar con una metodología para el ciclo de vida de desarrollo de sistemas que norme la secuencia lógica, los controles que se deban considerar en su administración y las actividades que se deriven en base a la naturaleza del proyecto.

Programas de entrenamiento

La mayoría de los problemas en los sistemas de procesamiento de datos son debido a errores u omisiones humanas, y puede decirse que la causa es originada por la falta de entrenamiento del personal. Cada organización deberá revisar los planes de capacitación de su personal con el objeto de lograr la máxima eficiencia en todas sus funciones.

Monitoreo de personal

Es importante tener siempre presente que la información de la empresa puede verse amenazada en un momento dado por directivos, usuarios o cualquier persona que tenga un nivel preferencial y privilegios de acceso a la información, para los administradores de bases de datos y el personal de informática siempre existirá la probabilidad de accesar a los sistema sin ser detectados. La mayoría de las aplicaciones son vulnerables a su propio personal.

Identificación de inventario

Muchas organizaciones no poseen registros de los activos que representan el software y la información almacenada dentro de sus inventarios, todas las rutinas que hayan sido desarrolladas por sus programadores deberán ser declaradas como propiedad de la compañía, no se puede pensar en algún grado de protección o de seguridad si no se tiene bien definido los recursos de la organización.

Pólizas de seguros y contratos

La gerencia deberá contratar pólizas de seguro para todos los recursos informáticos dada su gran vulnerabilidad, además de pactar contratos legales que especifiquen claramente las responsabilidades del personal de informática y otras empresas relacionadas con los servicios de venta y soporte técnico de hardware, software, además servicios de consultorías, desarrollo de sistemas, programación, Internet, tiempos compartidos, etc. Deberán ser revisados en cada punto de su contenido.

Control de la información de entrada / salida

Todos los sistemas deberán contemplar algún tipo de control y validación de la información que se introduce en el sistema, así como de la que es solicitada, la asignación de la responsabilidad de recibir, transferir y monitorear toda la información que se vaya a introducir o a obtener del sistema es una manera de lograr la integridad de la información.

Los quince puntos anteriores han probado ser algunos de los factores más críticos y problemáticos dentro de un centro de cómputo con respecto a la seguridad y control de la información, antes de iniciar cualquier estudio o solicitar la implantación de alguna técnica de seguridad es conveniente revisar los factores anteriores con el objeto de tener una visión más amplia que le permitirá atacar los puntos más vulnerables sin temor a desperdiciar recursos.

I.3.4 Principios, propiedades y funciones de la seguridad en la informática.

Fuente: Leonardo H. Fine, "Seguridad en centros de cómputo, políticas y procedimientos", 2ª Ed. Trillas, México, 1995.

En informática seguridad es:

> "L*a protección de la información sobre accesos no autorizados, modificaciones y/o algún tipo de destrucción ya sean estos accidentales ó intencionales*".

Es bueno el poder entender los fundamentos de seguridad antes de emprender algún tipo de planeación, diseño, o revisión de cualquier sistema de información.

Principios Básicos.

> "*Debe existir una adecuada separación en la asignación de tareas y responsabilidades en los diferentes departamentos de informática en las diversas empresas*".

A continuación se enumeran otros principios, los cuales toman siempre como base el anterior:

- Segregación de tareas

Significa el separar las actividades de un proceso determinado entre varias personas. Un ejemplo sería que la persona encargada de capturar la información no deberá también tener asignada la función de verificarla, un programador no deberá manejar un código propio, sino el normativo de la institución.

Al momento de llevar a la práctica este principio los errores de transposición podrán ser identificados antes de incluirlos al sistema y las personas podrán descubrir algún intento de accesar las funciones de las cuales solamente ellos son responsables.

- Limitación del acceso a la información sensitiva.

Llámese información sensitiva a aquella que al ser expuesta puede influir en la postura de alguna situación de negligencia. Es posible que la información pueda carecer de significado alguno por sí misma, pero la combinación de varios datos podrían darle el carácter de información sensitiva.

Por ejemplo, un operador no debe estar autorizado para ver los salarios de los empleados de la organización, sin embargo el mismo empleado puede tener acceso a otros datos de empleados y estadísticas y de alguna manera podría inferir cual es el salario de alguno de ellos. Por esto se tiene que poner especial atención a este tipo de combinaciones que tienen cierta probabilidad de ser alcanzadas y exponer un tercer tipo de información que cree mantener bien restringida.

- Ocultar y transformar información.

No deberá permitirse que los empleados puedan situarse en posiciones tentativas en las cuales tengan la capacidad de transformar y de ocultar información para su propio beneficio. Existen procesos en los sistemas que pueden resultar muy vulnerables para un operador que con el paso del tiempo logran dominar sus puntos de control.

Existen diversas causas como el ocio, el allegarse un recurso económico extra al vender copias de información ya procesada o ser el proveedor de información a personas no autorizadas o lo que aún es peor, podría modificar archivos con información vital como nombres de clientes, comisiones, etc.

Funciones de los sistemas

Una estrategia para alcanzar las propiedades de auditabilidad, integridad y controlabilidad es la implantación de controles funcionales para el dominio de cada interfase. Las funciones son descritas en la secuencia en las que son diseñadas dentro de un sistema.

1. **IDENTIFICACIÓN:** La función de identificación nos permite establecer como su nombre lo dice, identificadores (nombres, símbolos) para cada usuario y cada recurso del sistema identifica a los usuarios, hardware, software y demás recursos disponibles para el sistema.

2. **AUTENTIFICACIÓN:** Esta función se encarga de reunir evidencias para cumplir con un determinado nivel de riesgo, para que la exigencia de identidad sea valida, esto puede ser llevado a cabo mediante comparaciones de algo que el individuo sepa, tenga, sea o pueda hacer y que sea factible de ser comparado. Por ejemplo:

Algo que él sepa: PASSWORD	Un código o palabra que solamente él y el sistema conozcan.
Algo que él posea: FOTO DE IDENTIFICACIÓN	Alguna foto personal que pueda ser comparada con una imagen de la misma persona almacenada en memoria.
Algo que él sea: APARIENCIA FÍSICA	Una comparación de cuerpo entero en base a un sistema óptico.
Algo que él pueda hacer: SU FIRMA.	Toda firma posee un estilo único que es susceptible de ser analizado por computadora.

3 **AUTORIZACIÓN:** El único propósito de la función de autorización es establecer quién y qué le esta permitido con respecto a un recurso determinado, esta función generalmente relaciona a un usuario con un recurso a través de ciertas reglas definidas para su autorización.

Esto significa que la autorización establece reglas que restringen a los usuarios a llevar acabo solo acciones predefinidas en el recurso accesado, todos los usuarios sin excepción deberán tener una autorización explícita de la gerencia para accesar los recursos. Un ejemplo típico son los permisos que se definen en el sistema operativo UNIX.

4 **DELEGACIÓN:** Para poder mantener y aplicar la función de autorización, es necesario delegar, esta función determina quién y bajo que circunstancias, podrá ejercitar o cambiar las reglas de autorización.

En los pequeños sistemas, esta tarea puede ser llevada a cabo por el administrador de seguridad, en sistemas muy grandes que poseen una compleja estructura de usuarios, recursos, ubicaciones y actividades puede requerir de un sofisticado mecanismo de delegación que les permita el manejo para actualizar las reglas de autorización en tiempos reales para necesidades reales.

Muchos de los sistemas que se encuentran actualmente en el mercado están diseñados para que solamente el operador designado o controlado pueda cambiar identificadores de operación.

5 **SEGUIMIENTO:** Después de la identificación, autentificación, autorización y delegación, el siguiente paso es el seguimiento de todas las actividades significativas, provee registros escritos del uso de los recursos del sistema.

Ofrece beneficios mayores al permitir reconstruir información, hacer respaldos y recuperaciones, puntualizar la contabilidad, seguir pistas e identificaciones, ganar visibilidad y ver que ésta sucediendo. Los sistemas nunca deberían ser diseñados sin tener la capacidad de hacer seguimiento (quién y qué capturó, donde, porqué y cómo), es la manera más efectiva para monitorear la operación, objetivos, reglas y estándares de ejecución.

6 **RECONOCIMIENTO:** Es necesario que alguien revise el seguimiento, monitoré las variaciones de actividades con respecto al uso, contenido y comportamiento esperado, en realidad lo que se busca con esta función es llegar más allá del seguimiento, informando a la gerencia o jefatura de todo tipo de irregularidades de cualquier comportamiento inesperado, es entonces cuando la jefatura deberá tomar las acciones correctivas pertinentes.

Podría confundirse el objetivo de esta función con la de seguimiento, sin embargo, la anterior se limita a la capacidad de registrar las operaciones y esta última se refiere a las acciones de deslindar responsabilidades y revisar oportunamente aquellos registros con el objeto de preparar las acciones correctivas a la brevedad posible

I.3.5 Metodología de seguridad

Fuente: Escamilla Bello Tomás Javier, "Metodología de seguridad avanzada para los sistemas y equipos de cómputo..", Trabajo recepcional, Facultad de Informática U.V., 1996.

- ◊ Identificación de amenazas potenciales
- ◊ Definición de los puntos de control (PC) de un sistema
- ◊ Identificación de problemas potenciales
- ◊ Mapeo de los problemas potenciales
- ◊ Limitación y análisis del riesgo
- ◊ Técnica para obtener el costo / pérdida
- ◊ Controles Básicos
- ◊ Selección de Controles

Identificación de amenazas potenciales.

"*Se consideran amenazas potenciales a toda clase de información que sea expuesta como consecuencia de cualquier tipo de acción mal intencionada*" [65]

[65] Information System Security, Fisher Royal P.1994 IBM Corporation pp 34

Amenaza : *"Es un aspecto del medio ambiente la cual, cuando se da una oportunidad podría causar daño a un evento que actúa sobre un bien"* [66]

Una manera de identificar estas posibles amenazas es mediante un análisis de amenazas:

> "*Que se encarga de identificar causas que pueden causar daño y ataque a algunos medidas importantes que amenazan la misión de una organización* " [67]

En este análisis se irá haciendo una lista que incluya todas las cosas indeseables que pudieran ocurrirle a la información, ciertamente prevalece la incertidumbre de sí estaremos ya incluyendo todas las posibles amenazas contra la información y aún más, dentro de las que hemos identificado, ¿se encuentran las más críticas?

Por lo tanto, todo lo indeseable que pueda ocurrirle a la información que se encuentra residente en el departamento de informática puede ser agrupado dentro de los seis siguientes puntos:

" IDENTIFICACIÓN DE AMENAZAS POTENCIALES"

A
REVELACIÓN ACCIDENTAL se refiere a la revelación de información de manera involuntaria

- **A1.** Información entregada al usuario incorrecto.
- **A2.** Password que se difunden a personal no autorizado.
- **A3.** Copias inservibles que aprovechan terceras personas para intereses personales.
- **A4.** Información desplegada y abonada en el monitor.
- **A5.** Consulta de información no resguardada.

[66] Diccionario Enciclopédico Larousse Plus, Agrupación Editorial S.A.1999
[67] Edward R. Buck, Introduction To Data Security & Controls Second, pp 23

B
MODIFICACIÓN ACCIDENTAL
Cambios involuntarios en la información

- **B1.** Errores de transposición.
- **B2.** Mala operación del hardware.
- **B3.** Mala operación del software.
- **B4.** Duplicación.
- **B5.** Utilización de diferentes versiones de programas.
- **B6.** Mal llenado de los formatos o cálculos erróneos.

C
DESTRUCCIÓN ACCIDENTAL
pérdida de información por causas involuntarias

- **C1.** Causas naturales (incendio, huracán, …).
- **C2.** Escribir sobre un archivo en buen estado.
- **C3.** Dispositivos de almacenamiento dañados.
- **C4.** Pérdida de algún mensaje
- **C5.** Pérdida de información imputable al equipo o a la corriente eléctrica.
- **C6.** Pérdida o extravío de documentos fuente o listados finales.

D
REVELACIÓN INTENCIONAL
difundir la información en forma consciente

- **D1.** Retención de copias del papel carbón de la impresora.
- **D2.** Vender información.
- **D3.** Irrumpir en un archivo.
- **D4.** Accesar información clasificada.
- **D5.** Distribuir o proporcionar información a personal no autorizado.

E
MODIFICACIÓN INTENCIONAL
alterar la información en forma consciente

- **E1.** Copiar un archivo.
- **E2.** Alterar un archivo.
- **E3.** Borrar un archivo.
- **E4.** Sustituir información.
- **E5.** Retener información.

F
DESTRUCCIÓN INTENCIONAL
desaparecer la información en forma consciente

- **F1.** Alborotos.
- **F2.** Sabotaje.
- **F3.** Ocultamiento.
- **F4.** Robo.
- **F5.** Uso de elementos dañinos como pueden ser imanes, explosivos, etc.

Definición de los puntos de control (PC) de un sistema

Es conveniente la utilización de ocho pasos básicos[68] para controlar la información de cualquier tipo de sistema de cómputo, estos pasos se encuentran redactados en una forma muy general con el objeto de que puedan ser aplicados a cualquier sistema que procese información.

PC1: RECOPILACIÓN DE INFORMACIÓN (USUARIO).
ETAPA CLIENTE - USUARIO.
Creación manual y transportación de la información, es aquí donde se concibe la información del sistema que se va a utilizar (mesa de control), incluye cualquier método o manera por el cual sea concebida.

[68] Un estudio multimillonario realizado en Estados Unidos, conocido como el proyecto "SAFE" sugiere estos ocho pasos básicos.

PC2: ENTRADA DE LA INFORMACIÓN (CONTROL Y ENLACE).

ETAPA USUARIO - CAPTURA.

Incluye todos los movimientos manuales de documentación fuente del PC1 hacia el área donde serán procesados.

PC3: CODIFICACIÓN DE LA INFORMACIÓN (BATCH).

ETAPA CAPTURA.

Controla la conversión de la información física en códigos preestablecidos capaces de ser admitidos por la computadora, estas conversiones incluyen codificaciones solicitadas por cada tipo de sistema.

PC4: TRANSMISIÓN DE LA INFORMACIÓN (INPUT).

ETAPA CAPTURA - INTERACTIVA.

La información es llevada al lugar indicado para su procesamiento, la información será transmitida electrónicamente o transportada manualmente.

PC5: PROCESAMIENTO DE LA INFORMACIÓN.

ETAPA DE PROCESO.

Incluye la ejecución de los programas de aplicación para la obtención de los procesos y por ende los cálculos o salidas esperadas, este es el único punto en el que generalmente se busca mantener el control, sin embargo cualquier carencia de controles adecuados en alguno de los puntos anteriores atentará en algún grado la integridad de la información en esta etapa.

PC6: TRASLADO DE LA INFORMACIÓN PROCESADA (OUTPUT).

ETAPA DE CONTROL Y ENLACE.

Este punto cubre aquellos sistemas en los cuales la información no entregada instantáneamente al solicitante (proceso en línea), la información del PC5 es retenida en algún sitio esperando ser recogida o transmitida.

PC7: USO DE LA INFORMACIÓN.

ETAPA USUARIO - PROCESO.

Este punto contempla el control del uso que se le da a la información durante los procesos, además su posible retención y confidencialidad. Es común que pueda encontrarse en forma o estado de fácil recuperación (respaldos o copias), es aquí donde debe darse énfasis al control de su disponibilidad y uso.

PC8: DISPOSICIÓN DE LA INFORMACIÓN.

ETAPA USUARIO - CLIENTE.

La información una vez que ha sido utilizada, involucra los medios y lugares de almacenamiento, tiempo de vigencia y seguridad. Este control se da una vez que la información es retirada del dominio del usuario, debe ser inmediatamente retirada y respaldada, destruida o inhabilitada.

Identificación de problemas potenciales.

Una vez que se ha establecido la relación de los ocho puntos de control, el siguiente paso es determinar los problemas específicos a los que puede estar expuesto el proceso en cada uno de los puntos de control.

Se debe recabar información a todas las personas que estén directamente asociadas con los puntos de control y estén consientes del enfoque que aquí se le este dando a la información recabada, las técnicas a ser utilizadas para este objetivo van desde simples entrevistas, aplicación de cuestionarios, auditorías, hasta servicios de consultoría.

El objetivo de la identificación de los problemas potenciales es el definir cuales problemas son los de mayor importancia y la técnica adecuada para esto es aquella que provea esta información de la manera más simple.

Como resultado de esta sesión se obtendrá le siguientes información.

1. Identificación de los puntos específicos de control.
2. Identificación del sistema específico estudiado.
3. Identificación de las amenazas potenciales.
4. Descripción completa de las amenazas en cada punto de control.
5. Documentación de las amenazas ya identificadas.

Mapeo de los problemas potenciales

Una vez definidos y clasificados los problemas potenciales que atacan a nuestros sistemas, se utiliza el mapeo[69] como herramienta para continuar con el proceso. El valor de este mapeo es que nos permite identificar fácilmente las debilidades en cada punto de control, y por ende podemos detectar si alguno de los problemas se repite constantemente en todo el ciclo de vida de la información a través de los diferentes puntos de control, se logra tener una visión general de donde deberán ser aplicados los recursos para obtener un control efectivo.

Si no es posible llevar a cabo un estudio completo de análisis de riesgo a los sistemas de cómputo, por lo menos hasta este punto se podrá visualizar con más certeza los problemas potenciales y no tratar de adivinar.

Una de las limitantes del mapeo es que, no indica cuales son las amenazas más críticas, la agrupación de problemas reiterativos no necesariamente representan el problema potencial, o el que realmente tenga la necesidad de mayor atención y de mayor control por ser el más crítico.

[69] En una hoja dispuesta especialmente para anotar que tipo de problemas potenciales son los que afectan a cada uno de los puntos de control, en forma de matriz de dos entradas.

Puede que existan problemas que ocurra constantemente en uno solo puntos de control, pero que no le cueste a la organización. Si se desea aplicar efectivamente recursos para el control de riesgos de la información, cada una de las amenazas potenciales deberá ser cuantificada.

Limitación del riesgo

RIESGO: "*Condición que puede traer como resultado una pérdida para una organización ".* [70]

Probablemente la llave para la seguridad sea la capacidad para controlar o por lo menos limitar los riesgos, entonces ¿cómo podemos limitar el riesgo?

Nótese que el concepto utilizado es limitar y no eliminar, ya que el único sistema totalmente seguro sería aquel que fuera también inaceptable e inoperable. Desde el momento en que un sistema es abordable, este asume ciertos riesgos.

En los riesgos se debe de:

- Determinar su magnitud.
- Evaluar y/o sugerir los controles indicados para reducirlos.

A continuación se listan algunas maneras en que pueden limitar los riesgos:

LIMITAR LA INFORMACIÓN: Erróneamente se piensa que un servicio de procesamiento de información debe brindar al usuario no solamente lo que realmente necesita, sino también toda aquella información que le pudiera ser de interés.

La información debe ser limitada efectivamente en cuanto a la cantidad, asociación, interpretación y valor unitario, esto limitará el proceso de información de datos individuales en información valiosa y de gran significado.

COMPROMETER AL USUARIO: Cada medida de seguridad implantada en un centro de cómputo representa un obstáculo o una barrera para los usuarios del sistema, al menos esta es la actitud mental que debe prevalecer en los usuarios hasta que estén concientizados de los beneficios que les brinda a cada uno de ellos las diferentes medidas de seguridad.

Por lo que cualquier medida de seguridad implantada debe ser acompañada por una clara y sencilla explicación de los beneficios que otorga al usuario.

[70] Edward R. Buck, Introduction To Data Security & Controls, segunda edición, pp. 24

CONTROL DE LOS DOMINIOS: El riesgo puede ser limitado si las áreas de trabajo se limitan y controlan, estas áreas de trabajo llamadas dominios son definidos con relación a un nivel en particular como lo es el tipo de sistema, de producto o de personal. El nivel de definición del dominio depende del grado de entendimiento y comprensión necesitado para controlar esa área de trabajo; Por ejemplo el área donde el Capturista graba la información para que posteriormente sea procesada es un dominio, el área donde el operador procesa la información es otro dominio, etc.

CONTROLES DE CADA INTERFACE: Después de que ya han sido identificados y definidos los dominios, ya pueden enfocarse las consideraciones hechas para el control de la actividad en cada interfase, es decir, que se deberá decidir que controles serán aplicados al sistema para limitar el riesgo de los movimientos de la información de un dominio a otro.

ASIGNACIÓN DE REFERENCIAS INDIVIDUALES: Para cada actividad que ocurra en el ambiente del sistema, deberá existir un registro[71] permanente disponible para cada evento causante de alguna acción, deberá ser posible rastrear cualquier acción ejecutada en cualquiera de los dispositivos. Con el objeto de limitar los riesgos, el sistema debe ser capaz de señalar eventos anteriores que sean causantes de ciertas acciones y además identificar al responsable directo

MONITOREO DE VARIACIONES: Para poder limitar los riesgos en cualquier sistema es necesario entender lo que es esperado para el sistema y por el sistema, por ejemplo una consulta de información al sistema de nomina realizada a las 3 a.m. o un domingo es ciertamente una práctica anormal. El sistema de control de seguridad debe monitorear y registrar esas incidencias realizadas por personas o por el mismo sistemas.

REPORTAR LAS ANOMALÍAS: No es suficiente con detectar las anomalías en los procesos de la información, también es necesario reportarlos a la persona adecuada para que se aplique la acción precisa, si se quiere limitar el riesgo, algo debe hacerse. La acción puede consistir en no hacer nada o probablemente en aplicar una fuerte medida de corrección, eso dependerá de la gerencia.

[71] Una forma muy útil de llevar a cabo este control es a través de la implementación de bitácoras de control por sistema o proceso de trabajo.

Análisis de riesgos

Los componentes de un análisis de riesgos son:

1. Análisis de los bienes.
2. Análisis de las amenazas.
3. Análisis de la vulnerabilidad.
4. Análisis de evaluación o de valoración.

Los propósitos de un análisis de riesgos son los siguientes:

1. Auxiliar en la identificación de problemas.
2. Asistir en la cuantificación de problemas.
3. Permitir la clasificación por prioridades de los problemas.
4. Servir como base para un análisis de costo / eficiencia.

En resumen, el objetivo de un análisis de riesgos es el cuantificar los problemas potenciales para que sean establecidas las bases para una apropiada selección de costo eficiencia de los controles de seguridad.

El análisis del riesgo deberá aplicarse solo a los problemas que a consideración del responsable representa el riesgo más elevado en términos de frecuencia de la ocurrencia y del costo.

El análisis de riesgos puede ser considerado como una guía para el jefe de informática en las diferentes organizaciones donde se procesa la información en forma computarizada o para el responsable de la seguridad, por lo mismo, debe tenerse en cuenta que el tiempo más adecuado para llevar a cabo este estudio es antes de hacer cualquier consideración en la selección de técnicas de control.

El riesgo debe de incluir todos los desastres posibles, la naturaleza de los riesgos se define mediante tres preguntas:

¿ Que desastres son posibles, aunque sea remotamente?

¿ Cuales son los daños si se produce el desastre?

¿ Cuál es la probabilidad de que ocurra el desastre?

Factor clave

El factor clave en la aplicación de un análisis de riesgos es poder alcanzar un alto grado de exactitud, por lo anterior siempre se debe tener en mente que el objetivo primario es obtener información que nos permita clasificar los riesgos en términos de la magnitud del costo de la pérdida y la probabilidad de ocurrencia con una exactitud relativa en un tiempo razonable.

Uno de los problemas que se presentan en estudios de esta naturaleza es que a veces se gasta más en proveer de información a la gerencia que en la aplicación de los recursos para los riesgos encontrados, un estudio detallado y confiable no deberá tomar nunca más de tres o seis semanas.

Un estudio de análisis de riesgos generalmente abarca múltiples áreas y requiere más de una persona para poder ser terminado antes de que se convierta en un estudio obsoleto, por lo tanto, lo más adecuado es formar un equipo para llevarlo a cabo.

Se pueden determinar para un departamento de informática las siguientes áreas de estructuración: [72]

1. Área de recepción de documentos fuentes.
2. Área de captura de información.
3. Área de proceso.
4. Área de Soporte técnico
5. Área de apoyo operativo
6. Área de recepción de documentos finales.

La fórmula para cuantificar los riesgos es la siguiente: **R = P * C**

R = Riesgo, **P** = Probabilidad de que ocurra el riesgo **C** = El costo o la pérdida atribuida al riesgo. (Se debe expresar en pesos perdidos por año).

La probabilidad **(P)** [73] está dada en las veces que se estima podría ocurrir el riesgo en un rango de tiempo. Un modo para determinar el valor del costo **(C)** es relacionar cual de los siguientes tipos de costo se identifican más con el cada uno de los riesgos:

1. - Costo físico del recurso.
2. - Costo de la reparación del recurso.
3. - Costo de reemplazar el recurso
   (Incluye pedidos, transportación é instalación).
4. - Costo de recuperación / reproceso del recurso.
5. - Costo por seguros.

El costo que se asignan a los recursos que podrían ser dañados deberá ser obtenido por el consenso de un grupo de expertos[74] y consiste básicamente en asignar valores subjetivos y preferentemente múltiplos de 10.

[72] Las áreas de estructuración generalmente se definen considerando la estructura orgánica del Centro de Cómputo.

[73] La probabilidad de que ocurra un evento se puede calcular a través de leyes probabilísticas que nos proporcionan el porcentaje de posibilidad de que ocurra un evento con un alto grado de certeza.

[74] Es muy común que en los centros informáticos exista un comité de sistemas o un grupo de control de calidad que integra a todos los jefes de áreas y al personal más experimentado en Informática.

Técnica para obtener el costo / pérdida.

Fuente: Jack R. Meredith, Thomas E. Gibbs PP.,
"Administración de operaciones "

El costo / pérdida es un pronóstico que se realiza y que puede ser:

◊Cualitativo
◊Cuantitativo

La técnica cualitativa es muy subjetiva y combina los pronósticos de varios expertos,[75] y consiste básicamente en reunirlos y dejar que discutan el evento hasta que se produzca un consenso, a este grupo se le da el nombre de panel de consenso. [76] La fuerza del método cualitativo radica en la sencillez que aporta para clasificar los problemas potenciales en un tiempo mínimo.

El siguiente paso en la utilización del método es hacer un análisis mediante la tabulación de los resultados en una tabla que nos permite identificar lo siguiente:

- El problema potencial.
- Los puntos de control (PC1 al PC8).
- Un valor de "R" asignado de acuerdo al costo del riesgo.

La técnica cuantitativa utiliza los valores de los riesgos estimados, en este método se multiplican los valores obtenidos por el valor estimado de la perdida, si por ejemplo el valor estimado fuera de 20,000 y la probabilidad de ocurrencia fuera 1 vez cada dos años (1/2) con una valor igual a 0.5 entonces el valor del riesgo seria de 10,000.

El método cuantitativo nos provee una clara separación de los riesgos, brinda una mejor apreciación con valores más exactos de los riesgos, mediante la utilización de valores más precisos en los costos / pérdida por año, su fuerza radica en una mayor exactitud.

Resumiendo, podemos decir que el método cualitativo ofrece un camino rápido y fácil para cuantificar los riesgos, no requiere de muchos cálculos, desde el momento que no emplea tablas, para determinar los costos. El método cuantitativo hace necesario el hacer algunos cálculos sencillos, sin embargo provee datos de costo / pérdida que representan más claramente el valor de las posibles pérdidas y además provee de una mayor exactitud en los resultados.

[75] A este método se le conoce como DELPHI ó DELFOS
[76] Jack R. Meredith, Thomas E. Gibbs, Administración de operaciones, Ed. Limusa, pp 106

Controles Básicos.

Fuente: Escamilla Bello Tomás Javier, "Metodología de seguridad avanzada para los sistemas y equipos de cómputo..", Trabajo recepcional, Facultad de Informatica U.V., 1996.

El siguiente paso es poder seleccionar el tipo de control adecuado para poder limitar al máximo los riesgos[77] previamente identificados y cuantificados.

Control es la capacidad de ejercer restricciones o influencia directa sobre una situación o evento dado, algunos tipos de controles son activos y otros son pasivos, esto es que algunos controles no requieren ser retroalimentados antes de ponerlos en acción.

Algunos controles relacionados con el procesamiento de la información son activos, es decir, son controles diseñados para operar de alguna manera particular, dependiendo de las condiciones presentadas en un momento determinado.

Por ejemplo, una Password es un control activo, ya que requiere de una comparación de un código autorizado establecido antes de tomar cualquier acción subsecuente. Esta acción puede ser el permitir el acceso, impedir el acceso, monitorear al acceso y aun el tomar alguna medida correctiva contra dicho intento de accesar al sistema.

Los controles son utilizados donde quiera que sean aplicables, en sistemas son aplicables a la entrada, al procesamiento y a la salida de la información, seguridad, medio ambiente, administración, hardware, software, etc., por lo tanto existen literalmente miles de controles que pueden ser utilizados.

Lo que se sugiere y puede ser puesto en práctica inmediatamente es el manejar los tipos de control desde un punto de vista un poco más ordenado, teniendo como base la clasificación de estos.

Los controles se clasifican por su propósito en áreas que son:

1. Prevenir las causas del problema.
2. Detectar las causas del problema.
3. Corregir las causas que propician el problema.

[77] Nótese la palabra "limitar", un riesgo no podría desaparecer a no ser que desparezca el evento.

Todas las áreas de sistemas en el que pueden ser aplicados distintos controles encajan dentro de alguno de los tipos anteriores, la combinación de estos controles permitirá mantener los sistemas seguros.

Controles preventivos

Toda la información es siempre susceptible de ser alcanzada por amenazas externas (cuales quiera que sean), los controles preventivos ofrecen la primera línea de defensa o barrera contra los casos indeseables que pueden atacar a nuestros sistemas de información, el control preventivo define la mayoría de los intentos de destruir, accesar o modificar accidental o intencionalmente la información, si alguna amenaza o algún riesgo permaneciera vigente ante esta primera defensa, deberá ser detectado y corregido.

Características de los controles preventivos:

1 **Son pasivos**
(no requieren retroalimentación)
- Llave de la terminal.
- Switch de encendido de CPU.

2 **Guían las situaciones hacia un buen manejo**.
- Guías para operar las máquinas.
- Guías para operar el sistema.
- Hojas con formatos previos.
- Programas de entrenamiento.
- Control de prioridades para redes

3 **Solos, no son suficientes**
(Pasan por alto un cierto porcentaje de violaciones).
- Timelock (puede ser modificado por otros).
- Puertas automáticas, que se abran o cierren bajo ciertas condiciones.

4 **Reducen la frecuencia de las amenazas.**
- Inspección a las computadoras.
- Auditorías.
- Monitoreo.

5 **Son ocultos; la gente no esta consciente de su existencia.**

- Sistemas hidratantes contra incendios.
- Extintores automáticos de techo con detectores contra incendios.
- Vidrios contra golpes.
- Circuitos encapsulados
  (cerebros de circuitos cerrados para protección contra intrusos).
- Sistemas infrarrojos, para detección de intrusos.

6 **No son caros y además son muy sencillos**.

- Chapas para puertas.
- Interruptores para emergencia.
- Placas protectoras para objetos.

Controles para detecciones

Estos controles ofrecen la segunda línea de defensa contra cualquier agente externo y se asume que ya han sucedido cosas inesperadas que deben ser detectadas por este segundo tipo de control para la información, un aspecto interesante de este tipo de controles es que raras veces son efectivos por sí mismos, pueden detectar ciertos eventos, sin embargo, mientras no se tome algún tipo de acción correctiva, el riesgo potencial continúa.

Características de los controles para detecciones:

1 **Disparar una alarma.**

- Detectores de humo automáticos.
- Voltímetros y no-breaks con led's de advertencia.
- Beeper al abrir una puerta.

2 **Registro de amenazas presentadas.**

- Impresión de sucesos mediante monitores.
- Contador automático para errores (en aplicaciones software).
- Rutinas de revisión del software.
- Disparador de fotografías para intrusos.

3 **Poner fin a la operación del sistema.**

- Obstruir la computadora.
- Anular la terminal.
- Crear corrida anormal para un programa.

4 **Alertar al personal.**

- Cornetas, sirenas, alarmas.
- Flashes de emergencia.
- Reportes de errores de manera manual.
- Rutinas de revisión capaces de emitir diagnósticos (mediante auditoria).

5 **Están visibles;** la gente los puede utilizar en caso de emergencia (previo entrenamiento)

- Extintores (en caso de fuego).
- Traje contra incendios.
- Peto de asbesto aluminado.
- Caretas de protección contra humos y gases.
- Cintas de emergencia.

Controles correctivos

Los controles correctivos generalmente son implantados a la par por un control del tipo para detecciones, una vez que la incidencia ocurre y ha sido identificada y registrada, es cuando deben tomarse acciones correctivas que detengan el intento de accesar la información.

El propósito de los controles correctivos es emprender alguna acción determinada que corrija cualquier intento o intentos de abordar la información por medios no preestablecidos o regulares, entiéndase por regulares todas aquellas maneras de accesar la información por métodos "ortodoxos" y no a escondidas o mediante el uso indebido de passwords o comandos.

Selección de Controles.

Se sabe que todos los bienes de un centro de información son vulnerables a un sin número de posibles amenazas y el tratar de considerar un control para cada una de ellas sería muy difícil si no es que muy poco práctico. por lo que se tiene la necesidad de clasificar los problemas potenciales tomando como base las causas y no los múltiples efectos que se presentan.

No se debe seleccionar el tipo de control con el objeto de solucionar un problema especifico pues resolverá un problema momentáneo, pero sin embargo, seguiríamos manejando una SEGURIDAD FICTICIA, si por el contrario aplicamos los resultados del estudio realizado, el problema de seleccionar dispositivos y técnicas de control se simplifica grandemente, porque el número de causas identificadas que aquejan a nuestros sistemas es mucho menor y podremos completar el proceso de control de la información dentro de nuestro departamento de informática.

Cabe hacer mención que mediante la selección de controles se pretende reducir o suprimir al máximo los riesgos, pero si los costos de implantación de los mismos son muy altos o se observa que no se esta reduciendo lo suficiente el costo probable de las pérdidas, entonces los controles deberán ser revalorados, teniendo en cuenta la posible aplicación de algunas de las siguientes premisas:

1. Rediseñar por completo los tipos de controles a usar.
2. Revisar los estimados de costo / pérdida de los riesgos.
3. Reducción del costo de los controles.
4. Aumento de la probabilidad de éxito del control.

Para tomar una decisión final se hace necesario analizar los resultados del método, sentido común y razonamiento son ingredientes indispensables que tienen que ser aplicados para la decisión final.

I.3.6 Planes y programas de seguridad

Fuente: Aguilar Castillo Gildardo, "Apuntes para la materia Informática de la Empresa", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998

Los planes y programas constituyen una parte integral directamente relacionada con desastres potenciales y planes de recuperación, los más comúnmente sugeridos para las áreas de informática son:

- ◊ Plan de respaldos
- ◊ Plan de registros vitales
- ◊ Plan de control de accesos
- ◊ Plan de respuestas de emergencias
- ◊ Plan de procesos intermedios
- ◊ Plan de reacondicionamiento
- ◊ Programa de avalúo de riesgo

Plan de respaldos

Debe de existir un plan documentado de respaldo para el procesamiento de trabajos críticos, para casos en que se presente una falla mayor en el equipo o en el software, o de que exista una destrucción permanente o temporal de las instalaciones del centro de cómputo.

El plan de respaldo debe contener:

- ✓ Una prioridad preestablecida para el procesamiento de datos.
- ✓ Debe identificar la producción crítica, los sistemas operativos y los archivos necesarios para recuperación.
- ✓ Debe contener instrucciones para restablecer las comunicaciones.
- ✓ Prever un procesador de respaldo o cualquier otro tipo de recurso de cómputo.
- ✓ Prever que exista más de una fuente de abastecimiento para la recuperación de formas especiales.
- ✓ Debe ser periódicamente probado.
- ✓ Debe considerar los procedimientos manuales relacionados.

Debe existir un método para reiniciar o reprocesar un trabajo después de que se han detectado errores de procesamiento, las fallas del equipo, la recuperación de errores y los procedimientos de reinicio y de alto, deben estar claramente documentados y deben ser revisados periódicamente.

Plan de registros vitales

Su propósito principal es proteger la información y los programas que son esenciales para asegurar la adecuada operación y funcionamiento de la Empresa.

Primeramente los sistemas y datos deberán ser identificados de acuerdo a su grado de importancia (vitales, esenciales, importantes e inútiles), la responsabilidad de determinar cuales registros son vitales es de informática.

1. Identificar aquellos registros vitales para garantizar el procesamiento continuo en la organización.
2. Establecer el modo de protección (respaldo fuera o dentro de la instalación)
3. Desarrollar ciclos de respaldos
4. Establecer el modo para reconstruir registros dentro de tiempos razonables.

Plan de control de acceso

Su propósito es permitir solamente las personas autorizadas el acceso a ciertas áreas del centro de cómputo, evidentemente esto puede resolverse mediante guardias o algún mecanismo automático en las puertas como llaves o tarjetas magnéticas.

Se deben elaborar políticas de acceso para en caso de que se tenga la necesidad de que personas ajenas entren a las áreas restringidas.

Plan de respuesta a emergencias

Este plan permite dar respuesta inmediata a cualquier tipo de amenaza, su propósito es limitar los daños críticos que pudieran causar a los recursos y mantener la operación, no es un plan de recuperación, sino de mitigar o evitar pérdidas esenciales para el centro de cómputo cuando ocurra el desastre.

El plan de respuesta a emergencias incluye:

1. Proteger los recursos en el orden de importancia (gente, datos, equipo)
2. Comunicar la alarma a todas las áreas
3. Evacuar y resguardar a las personas
4. Proteger el equipo esencial.....etc.

Este plan tiene la característica que se debe probar, es decir, realizar prácticas regulares sin previo aviso.

Plan de procesamiento temporal

Este plan entrará en vigor durante el periodo existente entre la pérdida de la operatividad del centro de cómputo y el inicio del reacondicionamiento, este plan se activa por el plan de respuesta a emergencias y consiste en la descripción de lo que deberá hacer el personal de procesamiento de datos y la organización misma para recuperar la operatividad pérdida.

1. Definición de las responsabilidades de los usuarios
2. Planes organizacionales alternativos nivel por nivel (proceso, captura...)
3. Planes de acciones individuales
4. Identificación de aplicaciones críticas
5. Identificación de configuraciones críticas
6. Asignación provisional de tareas y responsabilidades
7. Identificar instalaciones alternas dónde procesar
8. Identificar aplicaciones críticas y su puesta en operación

El único plan realmente efectivo es aquel que ha sido previamente simulado y probado periódicamente con personal debidamente entrenado.

Plan de reacondicionamiento

El propósito de este plan es devolverle al departamento de informática la misma capacidad que tuvo antes del siniestro para procesar información.

1. Determinar si el área física aún es reutilizable
2. Identificar sitios alternativos
3. Hacer reasignaciones definitivas al personal
4. Restablecer las comunicaciones
5. Identificar proveedores y reemplazar el equipo dañado
6. Reimplantación de todas las aplicaciones para su proceso

Programa de avalúo de riesgo

El propósito de este programa es el de ayudar a los responsables del centro de cómputo a comprender y a desempeñar sus funciones con relación a la seguridad informática, que el jefe evalúe su postura respecto a la seguridad.

Una herramienta para lograrlo es con la aplicación de las diferentes técnicas de recopilación de información aplicadas a las tres áreas que deben ser controladas.

1. **Seguridad física**
   - Incendios
   - Fugas de agua
   - Temblores
   - Instalaciones
   - eléctricas
   - Intrusos
   - etc.
2. **Controles y procedimientos**
   - Personal
   - Control del
   - procesamiento
   - Procedimientos de
   - respaldo y
   - recuperación
   - Enlace con los
   - usuarios
   - Desarrollo de
   - Aplicaciones
   - etc.
3. **Planes de contingencia**
   - Registros vitales
   - Respuesta a
   - emergencias
   - Procesos
   - intermedios
   - Reacondicionamiento
   - Etc.

La mayoría de los responsables de informática clasificarán bien en las categorías del área 1, sin embargo siempre se pueden hacer mejoras en las áreas 2 y 3, estas áreas son consideradas de alto riesgo y de tomar acciones inmediatas.

I.3.7 Responsabilidades del manejo de la seguridad

Entrenamiento propuesto para el personal

Una de las partes más críticas dentro de la seguridad es la participación y compromiso del personal de informática, “la infraestructura del manejo de la seguridad en computación debe ser consistente con la filosofía de operación, centralización, políticas y guías con implantación de procedimientos detallados” [78]

La selección del entrenamiento de seguridad dependerá de las tareas específicas asignadas para cada individuo, “todo personal debe recibir una sesión inicial y periódica de seguridad en computación y seguridad en el área de informática” [79]

[78] William Heinemann LTD, Seguridad en Centros de Cómputo, Políticas y Procedimientos, pp. 81
[79] Idem.

La responsabilidad del manejo del programa de seguridad en computación debe ser compartida por el Jefe del área de cómputo y el administrador de seguridad.

El jefe del centro de cómputo porque es el responsable directo de los recursos informáticos así que debe evaluar y mantener un excelente nivel de seguridad, a continuación alguna de las políticas a implementar:

- Protección de todos los bienes, incluyendo a los empleados, propiedades físicas y la información relacionada con el comportamiento de la organización.
- Desarrollar prácticas y procedimientos de seguridad.
- Implantación de medidas correctivas al menor índice de variación en las prácticas de seguridad.
- Implementar la metodología informática.

El administrador de seguridad es el responsable de la seguridad física y lógica de las operaciones en un centro de cómputo, obviamente una sola persona no puede realizar tal tarea sola, por lo que la seguridad debe ser ubicada dentro de la organización a nivel staff y cada jefe deberá ser el responsable por su conocimiento, conciencia, autoridad, responsabilidad de los recursos de cómputo que están en su jurisdicción.

A continuación algunas *obligaciones y responsabilidades:*

- Administrar directamente los sistemas de seguridad instalados
- Preparar objetivos para futuros desarrollos de sistemas de seguridad
- Determinar los requerimientos de recursos especiales tales como entrenamiento, equipo.
- Continuas revisiones y evaluaciones de alternativas de seguridad para determinar el curso de acción basado en implicaciones tecnológicas.
- Asegurarse que los proyectos asignados sean compatibles con los de otras áreas para optimizar recursos.

- Coordinarse con el staff para manejar investigaciones de seguridad internas en base a un alto grado de confidencialidad.

- Participar en las pruebas de seguridad y proveer guías y asesorías para facilitar el desarrollo de los programas.

Cualidades del administrador de seguridad, debe ser una persona con talento individual capaz de:

- Reconocer problemas actuales y potenciales de seguridad

- Desarrollar soluciones en un ambiente de constantes cambios tecnológicos

- Manejo de información altamente especializada y confidencial

- Establecimiento de procedimientos y criterios para desarrollar programas futuros

- Mediar los resultados de los estudios de análisis de riesgo

- Iniciativa con dependencia de experiencias pasadas

- Crear soluciones únicas para problemas presentes y posibles problemas futuros

Bibliografía de este capítulo:

1. Escamilla Bello Tomás Javier, "Metodología de seguridad avanzada para los sistemas y equipos de cómputo..", Trabajo recepcional, Facultad de Informática U.V., 1996.
2. Leonardo H. Fine, "Seguridad en centros de cómputo, políticas y procedimientos", 2ª Ed. Trillas, México, 1995.
3. Edward R. Buck., Introducction to data security and controls
4. Fisher Royal P., Information System Security
5. Jack R. Meredith, Thomas E. Gibbs PP., "Administración de operaciones "
6. Aguilar Castillo Gildardo, "Apuntes para la materia Informática de la Empresa", Facultad de Estadística e Informática, Universidad Veracruzana. México, 1998