

**UNIVERSIDAD IBEROAMERICANA**  
Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial  
Del 3 de abril de 1981



**“SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS)”**

**TESIS**

Que para obtener el grado de

**MAESTRO EN INGENIERÍA DE SISTEMAS EMPRESARIALES**

P r e s e n t a

**LUIS DANIEL ALVAREZ BASALDÚA.**

Director de la tesis: Maestro Pedro Solares Soto.

Lectores de la tesis:  
Maestro Héctor Manuel Fragoso Trejo.  
Maestro Jorge Rivera Albarrán.

México, D. F.

2005.

# INDICE

<b>Introducción</b> .....	4
<b>Capítulo I.- Planeación de seguridad en redes.</b>	
Planeación de seguridad en redes .....	7
Política de seguridad del sitio .....	7
Planteamiento de la política de seguridad .....	8
Cómo asegurar la responsabilidad hacia la política de seguridad .....	9
Análisis de riesgo .....	10
Identificación de recursos .....	11
Identificación de las amenazas .....	12
Definición del acceso no autorizado.....	12
Riesgo de revelación de información .....	13
Negación del servicio .....	13
<b>Capítulo II.- Uso y responsabilidades de la red.</b>	
Uso y responsabilidades de la red.....	15
Identificación de quien esta autorizado para usar los recursos de la red.....	15
Identificación del uso adecuado de los recursos.....	15
Quién esta autorizado para conceder acceso y aprobar el uso.....	17
Cómo diseñar una política de red .....	19
Determinación de las responsabilidades del usuario .....	20
Determinación de las responsabilidades del administrador de sistemas .....	21
Qué hacer con la información delicada .....	21
<b>Capítulo III.- Políticas de seguridad.</b>	
Plan de accion cuando se viole la politica de seguridad.....	23
Respuesta a las violaciones de la política.....	23
Respuesta a las violaciones de la política por usuarios locales .....	24
Estrategias de respuesta .....	25
Definición de responsabilidades para ser buen ciudadano de internet .....	28
Contactos y responsabilidades con organizaciones externas.....	28
Interpretación y publicación de la política de seguridad .....	29
Identificación y prevención de problemas de seguridad .....	30
Confidencialidad.....	35
Implementación de controles costeables para la política.....	35
Procedimientos de reporte .....	39
Procedimientos de recuperación.....	41
Procedimiento de reporte de problemas para los administradores del sistema .....	44

#### **Capítulo IV.- Auditoria de sistemas.**

Auditoria de Sistemas .....	45
Planeación de la Auditoria en Informática .....	45
Evaluación de Sistemas .....	48
Evaluación del Análisis .....	49
Evaluación del Diseño Lógico del Sistema .....	50
Evaluación del Desarrollo del Sistema .....	55
Control de Proyectos .....	52
Control de Diseño de Sistemas y Programación .....	54
Instructivos de Operación .....	55
Forma de Implementación .....	56
Entrevista a Usuarios .....	56
Controles .....	59

#### **Capítulo V.- Seguridad en centros de cómputo.**

Orden en el Centro de Cómputo .....	69
Evaluación de la Configuración del Sistema de Cómputo .....	70
Seguridad Lógica y Confidencial .....	71
Seguridad Física .....	73
Seguridad en la Utilización del Equipo .....	78
Seguridad al Restaurar el Equipo .....	80
Procedimientos de Respaldo en Caso de Desastre .....	81

#### **Capítulo VI.- Estándares internacionales para tecnologías de la información.**

Marco referencial .....	84
Información .....	88
Recursos de tecnología de la información .....	88
Dominios .....	88
Planeación y organización .....	91
Adquisición e implementación .....	91
Entrega y soporte .....	91
Monitoreo .....	91
Resumen COBIT .....	92
Certificación CISA .....	93
Caso de estudio .....	100
Conclusiones .....	113
Bibliografía .....	114
Anexo 1 .....	115
Anexo 2 .....	115
Anexo 3 .....	116

## INTRODUCCIÓN

---

Los trascendentales cambios operados en el mundo moderno, caracterizados por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoría de sistemas.

Las características que priman en el entorno de cualquier entidad moderna, que incorpore a su gestión las tecnologías de información, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, la contabilidad, y consecuentemente sus resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la auditoría y en especial en la auditoría interna.

Practicar auditorías en una organización en la que el éxito de su gestión depende, como factor crítico, de la eficiente administración de la información y la tecnología de información, en la que los sistemas de gestión y contable han alcanzado un desarrollo tan notable, demanda la introducción de una concepción muy diferente a la que fuera para esta disciplina durante décadas. Tal concepción demanda, la participación inexcusable de la tecnología como herramienta, permitiéndole evolucionar al ritmo de las transformaciones incorporadas a la estructura del registro y del control interno y muy especialmente, para evaluar mediante auditorías a las tecnologías de información, los procedimientos de control específicos, dentro del ámbito de su soporte tecnológico, que a su vez, garantice una información objetiva sobre el grado de cumplimiento de las políticas y normativas establecidas por la organización para lograr sus objetivos.

La auditoría informática tiene como principal objetivo, evaluar el grado de efectividad de las tecnologías de información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la organización, su grado de eficacia, eficiencia, confiabilidad e integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

Su ámbito de acción se centra, en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

La generalizada informatización de los procesos y disciplinas que impactan directamente en la sociedad, en especial las relacionadas con la gestión económica, que hace apenas una década se procesaban manualmente, así como los propios cambios que introduce su tratamiento informatizado, introducen transformaciones sustanciales sobre el concepto tradicional del control interno, la estructura del registro y consecuentemente la práctica de las auditorías.

La auditoría interna, en su desempeño, tiene también la responsabilidad de velar por el adecuado empleo y utilización de los recursos informáticos y por el cumplimiento de la misión que a éstos le ha asignado la organización.

Tal conclusión conduce, a la inexcusable necesidad de practicar “auditorías informáticas”, a partir de un conjunto de técnicas y procedimientos que evalúen los controles internos intrínsecos y específicos de los sistemas de información; en consecuencia, determina, que conceptualmente, no es dependiente ni evoluciona desde la auditoría convencional; sus puntos de partida son esencialmente diferentes ya que no analiza la corrección o incorrección de cuentas contables, sino que constituye un instrumento de control superior para valorar la correcta administración de los recursos de tecnología de información como: datos, aplicaciones, tecnología, instalaciones, y personal para valorar la efectividad de la información que requiere la organización. su concepción se refiere a la integración de las técnicas informáticas y de auditoría para practicar un nuevo estilo de verificación, sobre un ambiente no convencional, con herramientas de punta y con procedimientos inexistentes y que puede definirse como:

“El conjunto de procedimientos y técnicas que evalúan, parcial o totalmente los controles internos de los sistemas de información; la protección de sus activos y recursos; verifica si su explotación se desarrolla con eficiencia, de acuerdo con las políticas y normativas establecidas por cada entidad y valora si se alcanza el grado de organización previsto para el marco donde participa y actúa”.

En correspondencia con la definición que antecede, así como por su finalidad, objetivos y utilidad que le atribuimos, la auditoría informática se clasifica en: auditorías informáticas de seguridad, de redes, de sistemas o aplicaciones, de explotación de los sistemas, de planificación y organización y de gestión de la tecnología para el logro de los propósitos de la organización. Consecuentemente, se han diseñado un conjunto de premisas, principios, y procedimientos para la práctica de estas auditorías.

En cuanto a la seguridad en informática, las computadoras y la Internet son ahora una parte familiar de nuestras vidas. Quizá no las veamos a menudo, pero ahí están; involucradas de alguna manera en la mayoría de nuestras actividades diarias, en los negocios de cualquier empresa, en las instituciones educativas, en las diferentes áreas de gobierno, sin el apoyo de éstas herramientas ninguna de ellas sería capaz de manejar la impresionante cantidad de información que parece caracterizar a nuestra sociedad. Pero también existe una problemática en ellas, la seguridad; para ello se han desarrollado firewalls dispositivos de software que protegen la integridad de las mismas. Cada vez más personas necesitarán conocer el manejo de las computadoras así como las protecciones que día a día se van ofreciendo para garantizarnos la seguridad en el manejo de la información.

Los inconvenientes en cuestión de seguridad no son conocidos por todos los usuarios de la red y por ello no saben como protegerse de dicha vulnerabilidad que tienen cada vez que se conectan a esta red de trabajo.

Convendría hablar un poco de qué se entiende por Seguridad. En esta investigación se entenderá por seguridad en redes, a la protección frente ataques e intrusiones en recursos corporativos por parte de intrusos a los que no se permite acceso a dichos recursos. La seguridad siempre será relativa al tipo de servicios que queremos ofrecer a los usuarios autorizados, según se establece en la política de seguridad de la empresa.

Creo conveniente definir primeramente las partes elementales que se relacionan con la seguridad en informática. En primer lugar tenemos la WAN (World Area Network) es una gran red de cómputo de cobertura mundial y una de las más comunes es Internet. En segundo lugar, está LAN (Local Area Network) que es una red mediana denominada local ya que está limitada a una pequeña área geográfica y normalmente es utilizada por empresas privadas, públicas, educativas, etc. Estas dos redes llegan a interactuar utilizando un conjunto de protocolos de comunicación de datos.

TCP/IP es de los protocolos más comunes. Sus siglas significan Protocolo de Control de Transmisión y Protocolo de Internet (Transmisión Control Protocol / Internet Protocol). Estos protocolos permiten el enrutamiento de información de una máquina a otra, la entrega de correo electrónico y noticias, e incluso la conexión remota.

La idea de este trabajo es que toda persona que se interese en este tema aprenda en forma rápida, simple y a valorar lo importante que es la información, tanto para las grandes como pequeñas y medianas empresas y contar con sistemas de seguridad que alejen visitas de posibles hackers.

# CAPÍTULO I

## PLANEACION DE SEGURIDAD EN REDES

---

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del mismo modo que otros bienes valiosos como la propiedad corporativa y los edificios de oficinas.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de firewall antes de que se haya identificado un problema particular de seguridad de red. Quizá una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de inter redes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.

Si actualmente sus usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También debe tomar en cuenta que la política de seguridad que Usted debe usar es tal, que no disminuirá la capacidad de su organización. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo cual la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

## POLITICA DE SEGURIDAD DEL SITIO

---

Una organización puede tener muchos sitios, y cada uno contar con sus propias redes. Sí la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes. Si esos sitios no están conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad de red. Sin embargo, si los sitios están conectados mediante una red interna, la política de red debe abarcar todos los objetivos de los sitios interconectados.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos relacionados con redes. Algunos, no todos, de esos recursos son los siguientes:

- ✚ Estaciones de trabajo.
- ✚ Computadoras host y servidores.
- ✚ Dispositivos de interconexión gateway, routers, bridges, repetidores.

- ✚ Servidores de terminal.
- ✚ Software para conexión de red y de aplicaciones.
- ✚ Cables de red
- ✚ La información de archivos y bases de datos.

La política de seguridad del sitio debe tomar en cuenta la protección de estos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Este es un punto importante en el que es posible idear una política de seguridad que salvaguarde sus intereses pero que sea dañina para los de otros. Un ejemplo de esto sería el uso deliberado de direcciones IP, detrás del gateway de las firewall que ya estén siendo usadas por alguien más. En este los ataques que se hicieran contra su red mediante la falsificación de las direcciones IP de su red, se desviarán a la organización a la que pertenecen las direcciones IP que usted está usando. Debe evitarse esta situación, ya que su interés es ser un ‘buen ciudadano’ de Internet.

La RFC 1244 aborda con considerable detalle la política de seguridad del sitio. Muchas de las cuestiones de política de seguridad de este capítulo están basadas en las cuestiones planteadas por esa RFC.

## **PLANTEAMIENTO DE LA POLITICA DE SEGURIDAD**

---

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra pérdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ✚ ¿Qué recursos esta usted tratando de proteger?
- ✚ ¿De quiénes necesita proteger los recursos?
- ✚ ¿Qué tan posibles son las amenazas?
- ✚ ¿Qué tan importante es el recurso?
- ✚ ¿Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?
- ✚ Examine periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

La figura siguiente muestra una hoja de trabajo que puede ayudarle a canalizar sus ideas conforme estos lineamientos.

- ✚ La columna “Número de recursos de red” es un numero de red de identificación interna de los recursos que van a ser protegidos (sí se aplica).
- ✚ La columna “Nombre del recurso de red” es la descripción en lenguaje común de los recursos. La importancia del recurso puede estar en una escala numérica del 0 al 10, o en expresiones “Vagas” de lenguaje natural como bajo, alto, medio, muy alto, etcétera.



- ✚ La columna “Tipo de usuario del que hay que proteger al recurso” puede tener designaciones como interno, externo, invitado o nombres de grupos como usuarios de contabilidad, asistentes corporativos, etcétera.
- ✚ La columna “Posibilidad de una amenaza” puede estar en una escala numérica del 0 al 10, o en expresiones “Vagas” de lenguaje natural como baja, alta, media, muy alta, etcétera.
- ✚ La columna “Medidas que se implementarán para proteger el recurso de red” puede tener valores tales como ‘permisos de sistema operativo’ para archivos y directorios; pistas/alertas de auditoría para servicios de red; “routers de selección” y “firewalls” para host y dispositivos para conectividad de red; y cualquier otra descripción del tipo de control de seguridad.

En general, el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Si usted no tiene el conocimiento suficiente de lo que está protegiendo y de las fuentes de la amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

No dude en contar con la ayuda de otros con conocimientos especializados respecto de los bienes de la red y de las posibles amenazas en su contra.

Es importante hacer que en el diseño de la política de seguridad participe la gente adecuada. Quizá usted ya tenga grupos de usuarios que podrían considerar que su especialidad es la implementación de la política de seguridad de red. Estos grupos podrán incluir a quienes están implicados en el control de auditoría, grupos de sistemas de información de universidades y organizaciones que manejan la seguridad física. Si usted desea que la política de seguridad tenga apoyo universal, es importante hacer participar a estos grupos, de modo que usted obtenga su cooperación y aceptación de la política de seguridad de red.

## **COMO ASEGURAR LA RESPONSABILIDAD HACIA LA POLÍTICA DE SEGURIDAD**

---

Un aspecto importante de la política de seguridad de red es asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Es difícil que una política de seguridad se anticipe a todas las amenazas posibles. Sin embargo, las políticas pueden asegurar que para cada tipo de problema haya alguien que lo pueda manejar de manera responsable. Puede haber muchos niveles de seguridad relacionados con la política de seguridad. Por ejemplo, cada usuario de la red debe ser responsable de cuidar su contraseña. El usuario que permite que su contraseña se vea comprometida incrementa la posibilidad de comprometer otras cuentas y recursos. Por otra parte, los administradores de la red y del sistema son responsables de administrar la seguridad general de la red.

## ANÁLISIS DE RIESGO

---

Cuando usted crea una política de seguridad de red, es importante que comprenda que la razón para crear una política es, en primer lugar, asegurar que los esfuerzos dedicados a la seguridad impliquen un costo razonable. Esto significa que usted debe conocer cuales recursos vale la pena proteger, y cuales son más importantes que otros. También debe identificar la fuente de amenazas de la que usted esta protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red, muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas perdidas causadas por los usuarios internos son mucho mayores.

El análisis de riesgo implica determinar lo siguiente:

- ✚ ¿Que necesita proteger?
- ✚ ¿De que necesita protegerlo?
- ✚ ¿Cómo protegerlo?

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida. No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor para usted. En el análisis de riesgo hay que determinar los siguientes dos factores:

1. Estimación del riesgo de perder el recurso ( $R_i$ )
2. Estimación de la importancia del recurso ( $W_i$ )

Puede asignarse un valor numérico como paso para cuantificar el riesgo de perder un recurso. Por ejemplo, puede asignarse un valor de 0 a 10 al riesgo ( $R_i$ ) de perder un recurso, en donde 0 representa que no hay riesgo y 10 representa el más alto riesgo. De igual modo, a la importancia de un recurso ( $W_i$ ) se le puede asignar un valor del 0 al 10, en donde 0 representa que no tiene importancia y 10 representa la máxima importancia. El riesgo evaluado del recurso ser el producto del valor del riesgo y de su importancia (también llamada peso). Esto puede escribirse como sigue:

$$WR_i = R_i * W_i$$

$W_{ri}$  = Riesgo evaluado del recurso "i"

$R_i$  = Riesgo del recurso "i"

$W_i$  = Peso (importancia) del recurso "i"

Considere la figura que se muestra es una red simplificada con un router, un servidor y un bridge.

Suponga que los administradores de la red y del sistema hayan encontrado las siguientes estimaciones del riesgo y de la importancia de los dispositivos de red.

$$R_3 = 10$$

$$W_3 = 1$$

Diagrama de una red simplificada, con evaluaciones de peso Y riesgo. Bridge:

Router

R1=6  
W1=.7

Bridge

R2=6  
W2=.3

Servidor

R3=10  
W3=1

El cálculo de los riesgos evaluados de estos dispositivos se muestra a continuación

Router

$WR1 = R1 * W1 = 6 * 0.7 = 4.2$

Bridge

$WR2 = R2 * W2 = 6 * 0.3 = 1.8$

Servidor

$WR3 = R3 * W3 = 10 * 1 = 10$

La evaluación de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se define en la política de seguridad del sitio. El Servicio de Pesca y Fauna de Estados Unidos ha documentado las cuestiones implicadas en la realización de evaluaciones de amenazas y riesgos. El URL del documento de evaluación de amenazas y riesgos es <http://www.fws.gov/-pullenl/security/rpamp.html>.

Otros factores que hay que considerar al estimar el riesgo de un recurso de red son su disponibilidad, integridad y confidencialidad. La disponibilidad de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo. La integridad de un recurso es la medida de que tan importante es que este o los datos del mismo sean consistentes.

Esto es de particular importancia para los recursos de bases de datos. La confidencialidad se aplica a recursos, tales como archivos de datos, a los cuales se desee restringir el acceso.

## IDENTIFICACIÓN DE RECURSOS

---

Al realizar el análisis de riesgo, usted debe identificar todos los recursos que corran el riesgo de sufrir una violación de seguridad. Los recursos como el hardware son bastante obvios para incluirlos en este cálculo, pero en muchas ocasiones se ignoran recursos tales como las personas que en realidad utilizan los sistemas. Es importante identificar a todos los recursos de la red que puedan ser afectados por un problema de seguridad.

La RFC 1244 enlista los siguientes recursos de red que usted debe considerar al calcular las amenazas a la seguridad general

1. **HARDWARE:** procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers.
2. **SOFTWARE:** programas fuente, programas objeto, utileras, programas de diagnóstico, sistemas operativos, programas de comunicaciones.
3. **DATOS:** durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos, en tránsito a través de medios de comunicación.
4. **PERSONAS:** usuarios, personas necesarias para operar los sistemas.
5. **DOCUMENTACIÓN:** Sobre programas, hardware, sistemas, procedimientos administrativos locales.
6. **SUMINISTROS:** papel, formularios, cintas, medios magnéticos.

## **IDENTIFICACIÓN DE LAS AMENAZAS**

---

Una vez que se han identificado los recursos que requieren protección, usted debe identificar las amenazas a las que están expuestos. Pueden examinarse las amenazas para determinar que posibilidad de pérdida existe. También debe identificar de qué amenazas esta usted tratando de proteger a sus recursos.

## **DEFINICIÓN DEL ACCESO NO AUTORIZADO**

---

El acceso a los recursos de la red debe estar permitido a los usuarios autorizados. Esto se llama acceso autorizado. Una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de cómputo. Este acceso puede tomar muchas formas, como el uso de la cuenta de otro usuario para tener acceso a la red y sus recursos. En general, se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado. La gravedad del acceso no autorizado depende del sitio y de la naturaleza de la pérdida potencial. En algunos sitios, el solo hecho de conceder acceso a un usuario no autorizado puede causar daños irreparables por la cobertura negativa de los medios.

Algunos sitios, debido a su tamaño y visibilidad, pueden ser objetivos más frecuentes que otros. El Equipo de Respuesta de Emergencias de Computo (CERT) ha hecho la observación de que, en general, las universidades de prestigio, los sitios del gobierno y las zonas militares parecen atraer más intrusos. En la sección “Equipo de respuesta de seguridad”, puede encontrarse mayor información acerca de CERT, así como sobre otras organizaciones similares.

## RIESGO DE REVELACIÓN DE INFORMACIÓN

---

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Usted debe determinar el valor y delicadeza de la información guardada en sus computadoras. En el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información específica de un producto representan una ventaja competitiva.

Los hospitales, las compañías de seguros y las instituciones financieras mantienen información confidencial, cuya revelación puede ser perjudicial para los clientes y la reputación de la empresa. Los laboratorios farmacéuticos pueden tener aplicaciones patentadas y no pueden arriesgarse a pérdidas causadas por robos.

A nivel del sistema, la revelación de un archivo de contraseñas de un sistema Unix puede volverlo vulnerable a accesos no autorizados en el futuro. Para muchas organizaciones, un vistazo, a una propuesta o un proyecto de investigación que represente muchos años de trabajo puede darle a su competidor una ventaja injusta.

Muchas veces, la gente supone que los accesos no autorizados de terceros a las redes y computadoras son realizadas por individuos que trabajan por su cuenta. No siempre es así. Los peligros del espionaje industrial gubernamental sistemático son realidades desafortunadas de la vida.

Además, cuando se logra uno de estos accesos no autorizados, por lo general la información fluye por Internet en muy poco tiempo. Hay grupos de noticias y canales de difusión, en Internet (IRC) en los que los usuarios comparten la información que lograron extraer de estas intromisiones.

## NEGACIÓN DEL SERVICIO

---

Las redes vinculan recursos valiosos, como computadoras y bases de datos, y proporcionan servicios de los cuales depende la organización. La mayoría de los usuarios depende de estos servicios para realizar su trabajo con eficacia. Si no están disponibles estos servicios, hay una pérdida correspondiente de productividad. Un ejemplo clásico de esto es el incidente del gusano de Internet, que ocurrió el 2 y 3 de noviembre de 1988, en el que se volvieron inservibles un gran número de computadoras de la red.

Es difícil predecir la forma en que se produzca la negación del servicio. Los siguientes son algunos ejemplos de cómo la negación de servicios puede afectar una red.

- ✚ La red puede volverse inservible por un paquete extraviado.
- ✚ La red puede volverse inservible por inundación de tráfico.
- ✚ La red puede ser fraccionada al desactivar un componente importante, como el router que enlaza los segmentos de la red.

- ✚ Un virus puede alentar o invalidar un sistema de cómputo al consumir los recursos del sistema.
- ✚ Los dispositivos reales que protegen a la red podrán alterar el funcionamiento.

Usted debe determinar que servicios son absolutamente esenciales y, para cada uno de ellos, determinar el efecto de su pérdida. También debe contar con políticas de contingencia para recuperarse de tales pérdidas.

## **CAPÍTULO II**

### **USO Y RESPONSABILIDADES DE LA RED**

---

Existen numerosas cuestiones que deben abordarse al elaborar una política de seguridad:

1. ¿Quién está autorizado para usar los recursos?
2. ¿Cuál es el uso adecuado de los recursos?
3. ¿Quién está autorizado para conceder acceso y aprobar el uso?
4. ¿Quién puede tener privilegios de administración del sistema?
5. ¿Cuáles son los derechos y las responsabilidades del usuario?
6. ¿Cuáles son los derechos y las responsabilidades del administrador del sistema, en comparación con los de los usuarios!
7. ¿Qué hace usted con la información delicada?

### **IDENTIFICACIÓN DE QUIEN ESTÁ AUTORIZADO PARA USAR LOS RECURSOS DE LA RED**

---

Debe hacerse una lista de los usuarios que necesitan acceso a los recursos de la red. No es necesario enlistar a cada usuario. La mayoría de estos pueden dividirse en grupos como usuarios de contabilidad, abogados corporativos, ingenieros, etcétera. También debe tomar en cuenta una clase llamada usuarios externos esta se compone de los usuarios que tengan acceso a su red desde otras partes, como estaciones de trabajo autónomas y otras redes; pueden no ser empleados, o bien, pueden ser empleados que tengan acceso a la red desde sus hogares o durante un viaje.

### **IDENTIFICACIÓN DEL USO ADECUADO DE LOS RECURSOS**

---

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, usted debe establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependen de la clase de usuarios, como desarrolladores de software, estudiantes, profesores, usuarios externos, etcétera. Debe tener lineamientos aparte para cada clase. La política debe establecer que tipo de uso es aceptable y cual es inaceptable, así como que tipo de uso está restringido. La política que usted elabore será la Política de Uso Aceptable (AUP) de esa red. Si el acceso a un recurso de la red está restringido, debe considerar el nivel de acceso que tendrá cada clase de usuario.

Su AUP debe establecer con claridad que cada usuario es responsable de sus acciones. La responsabilidad de cada usuario existe al margen de los mecanismos de seguridad implantados. No tiene caso construir costosos mecanismos de seguridad con firewalls si un usuario puede revelar la información copiando archivos en disco o cinta y poner los datos a disposición de individuos no autorizados.

Aunque parezca obvio, la AUP debe establecer claramente que no está permitido irrumpir en las cuentas o pasar por alto la seguridad. Esto puede ayudar a evitar cuestiones legales planteadas por empleados que pasan por alto la seguridad de la red y después aseguran que no se les informa o capacita adecuadamente acerca de la política de la red. A continuación se muestran los lineamientos que deben escribirse al desarrollar la AUP:

- ✚ ¿Se permite introducirse en las cuentas?
- ✚ ¿Se permite descifrar las contraseñas?
- ✚ ¿Se permite interrumpir servicios?
- ✚ ¿Los usuarios deben suponer que, si un archivo tiene permiso general de lectura, eso los autoriza a leerlo?
- ✚ ¿Debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura?
- ✚ ¿Los usuarios deben compartir cuentas?

A menos que usted tenga requerimientos especiales, la respuesta a estas preguntas, en la mayoría de las organizaciones, debe ser no. Además, quizá usted quiera incorporar en sus políticas una declaración respecto al software registrado y patentado. En general, los procedimientos del uso de red deben ser tales que se dificulte que los usuarios bajen software no autorizado de la red. En la mayoría de los países occidentales, copiar software en forma ilegal está penado por la ley. Las organizaciones grandes tienen políticas muy estrictas respecto a las licencias, debido al riesgo de demandas judiciales y el daño causado por la publicidad de los incidentes.

Muchos productos de software con licencia para redes determinan su uso y restringen el número de usuarios que pueden tener acceso a la red. Sin embargo, algunos acuerdos de licencia quizá requieran que usted vigile su uso para que no se viole el acuerdo.

Quizá se desee incluir información con respecto al software con derechos de autor o con licencia en su AUP. Los siguientes son ejemplos de los puntos que necesita abordar:

- 1 No se puede reproducir el software con derechos de autor y con licencia, a menos que se exprese en forma explícita.
- 2 Indicar métodos de transmitir información acerca de la situación del software con derechos de autor y con licencia.
- 3 Conceda el beneficio de la duda a la precaución. Si tiene dudas, no lo copie.

Si la AUP no establece claramente lo que está prohibido, será difícil demostrar que un usuario ha violado la política. Los miembros de los llamados equipos tigre pueden estar exentos de esta política, ya que son responsables de sondear las debilidades de seguridad de las redes. Debe identificarse claramente a los miembros de los equipos tigre. En ocasiones, quizá se tenga que tratar con usuarios que sean miembros auto designados de estos equipos y que quieran sondear los puntos débiles de la seguridad, con fines de investigación o para demostrar algo.



La AUP debe abordar las siguientes cuestiones acerca de los sondeos de seguridad:

- ✚ ¿Está permitido el vandalismo en el ámbito de usuarios?
- ✚ ¿Qué tipo de actividades de sondeos de seguridad se permiten?
- ✚ ¿Qué controles deben implantarse para asegurar que los sondeos no se salgan de control?
- ✚ ¿Qué controles deben implantarse para proteger a otros usuarios de la red para que no sean víctimas de las actividades de sondeos de seguridad?
- ✚ ¿Quién debe tener permiso de realizar sondeos de seguridad, y cuál es el procedimiento para la obtención del permiso para realizar esas pruebas.

Si quiere permitir sondeos legítimos de seguridad, debe tener segmentos separados de red y hosts en la red para esas pruebas. En general, es muy peligroso probar gusanos y virus.

Si debe realizar esas pruebas, sería tanto hacerlo en una red activa. En cambio, debe aislar físicamente a los hosts y a los segmentos de red que se utilicen para la prueba, y después de cada prueba volver a cargar, por completo y con cuidado, todo el software.

Evaluar los puntos débiles de la seguridad y tomar las medidas adecuadas puede ser eficaz para repeler ataques de hackers. Algunas organizaciones recurren a asesores externos para que evalúen la seguridad de sus servicios. Como parte de esta evaluación, ellos tendrán el derecho de realizar “vandalismo”. La política debe tener margen para estas situaciones.

## **QUIEN ESTA AUTORIZADO PARA CONCEDER ACCESO Y APROBAR EL USO**

---

La política de seguridad de red debe identificar quien esta autorizado para conceder acceso a sus servicios. También se debe determinar que tipo de acceso puede conceder dichas personas. Si no puede controlar a quien se le da acceso a sistema, será difícil controlar quien use la red. Si puede identificar a las personas encargadas de conceder acceso a la red, puede rastrear qué tipo de acceso o control se ha otorgado. Esto es útil para identificar las causas de las fallas de seguridad como resultado de que se hayan concedido privilegios excesivos a ciertos usuarios.

Quizá necesite considerar los siguientes factores al determinar quién conceder acceso a los servicios de la red:

- ✚ ¿Se otorgara el acceso a los servicios desde un punto central?
- ✚ ¿Que métodos se usan para crear cuentas y finalizar accesos?

Si la organización es grande y descentralizada, quizá haya muchos puntos centrales, uno en cada departamento, que sea el responsable de la seguridad de su red departamental. En este caso, se necesitará tener lineamientos globales acerca de los tipos de servicios que se le permitirán a cada clase de usuario. En general, mientras más centralizada este la administración de la red, es más fácil mantener la seguridad. Por otra parte, la administración centralizada puede crear problemas cuando los departamentos deseen tener mayor control sobre sus recursos de red. El grado correcto de centralización o descentralización depender de factores que estén más allá del alcance de este análisis.

Por supuesto, los administradores del sistema necesitaran tener acceso especial a la red, pero quizá haya otros usuarios que requieran de ciertos privilegios. La política de seguridad de la red debe abordar esta cuestión. Una política universal que restrinja todos los privilegios, si bien es más segura, quizá impida que ciertos usuarios legítimos realicen su trabajo. Se necesita un enfoque más equilibrado.

El reto es equilibrar el acceso restringido a los privilegios especiales para hacer más segura la red, con el otorgamiento de acceso a las personas que necesitan esos privilegios para realizar sus tareas. En general, se debe conceder solo los privilegios; suficientes para cumplir con las tareas necesarias.

Algunos administradores de sistemas se van por la vía fácil y asignan mas privilegios de los que necesita el usuario, para que estos no los vuelvan a molestar. Asimismo, el administrador del sistema quizá no comprenda las sutilezas de la asignación de seguridad y se vaya por el lado de conceder más privilegios. La capacitación y la educación ayudan a evitar este tipo de problemas. Las personas que tengan privilegios deben ser responsables y rendir cuentas ante alguna autoridad identificada dentro de la propia política de seguridad. Algunos sistemas podrán tener mecanismos de auditorias personales, que pueden usarse para que los usuarios con privilegios no abusen de la confianza.

### **ADVERTENCIA**

Si las personas a las que les conceden privilegios no son responsables ni rinden cuentas, usted corre el riesgo de crear fallas en el sistema de seguridad y de conceder arbitrariamente los permisos a los usuarios. Por lo general, tales sistemas son difíciles de administrar.

Si existe gran número de administradores de red y de sistemas es difícil llevar la cuenta de que permisos se han concedido para los recursos de la red. Puede seguirse una manera formal de solicitudes de otorgamiento. Una vez que el usuario hace la solicitud y esta es autorizada por el supervisor del usuario, el administrador del sistema debe documentar las restricciones de seguridad o de acceso a las que esta sujeto el usuario.

También debe examinar el procedimiento que seguir para crear cuentas nuevas y asignar permisos. En el caso menos restrictivo, las personas que están autorizadas para otorgar acceso deben poder ir directamente al sistema y crear una cuenta a mano o mediante mecanismos suministra-dos por el proveedor. Estos mecanismos le dan mucha confianza a la persona que los ejecuta, la cual, por lo general, tiene gran cantidad de privilegios, como el usuario raíz (Root) en Unix. En esas circunstancias, necesita seleccionar a alguien confiable para llevar a cabo esa tarea.

Debe elaborar procedimientos específicos para la creación de cuentas. En Unix existen numerosas formas que pueden usarse para crear cuentas. Sin importar el procedimiento que usted decida seguir, este debe estar bien documentado para evitar confusiones y reducir errores. Como resultado de errores cometidas por el administrador del sistema pueden producirse puntos vulnerables en la seguridad. Si tiene procedimientos bien documentados, eso le ayudará a reducir los errores.

## COMO DISEÑAR UNA POLÍTICA DE RED

---

Estos procedimientos también permiten capacitar fácilmente a futuros administradores de sistemas acerca de las peculiaridades de un sistema determinado. Otra cuestión que hay que considerar es seleccionar un procedimiento de creación de cuentas de usuario que sea el más sencillo y fácil de entender. Esto asegura que se cometen menos errores y que sea más probable que lo sigan los administradores del sistema (como debe ocurrir normalmente).

También debe tener una política para seleccionar la contraseña inicial. El momento de otorgar la contraseña inicial es muy vulnerable para la cuenta de usuario. Las políticas como aquellas donde la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco, pueden dejar al descubierto las cuentas. Asimismo, evite establecer la contraseña inicial como una función del nombre de usuario, o parte de este, o alguna contraseña generada por un algoritmo que pueda adivinarse con facilidad. La selección de la contraseña inicial no debe ser tan obvia.

El CERT Equipo de Respuesta a Emergencias de Cómputo (CERT, Computer Emergency Response Team), en avisos publicados calcula que 80 por ciento de todos los problemas de seguridad en redes son creados por contraseñas inseguras.

Algunos usuarios empiezan a usar su cuenta mucho tiempo después de haber sido creada; otros nunca se registran. En esas circunstancias, si no es segura la contraseña inicial, la cuenta y el sistema son vulnerables. Por esta razón, usted debe tener una política para desactivar las cuentas en las que no haya habido acceso durante cierto periodo. El usuario se ve obligado a pedir que se le active su cuenta.

También es un error permitir que los usuarios sigan usando su contraseña inicial en forma indefinida. Si el sistema lo permite, usted debe obligar al usuario a cambiar de contraseña la primera vez que se registre. Muchos sistemas cuentan con una política de caducidad de contraseñas, lo cual es útil para protegerlas. También hay utilerías Unix, que pueden usarse para probar la seguridad de las contraseñas como las siguientes:

Password es una aplicación para analizar contraseñas. Puede encontrarse en <ftp://ftp.dartmouth.edu/pub/security/passwd+.atr>.

Npasswd es un reemplazo compatible para el comando password. Incorpora un sistema de verificación de contraseñas que inhabilita las contraseñas sencillas.

Npasswd puede encontrarse en <ftp://lrtp.usa.edulpub/security/npaccwd.tar.gz>.

## **DETERMINACIÓN DE LAS RESPONSABILIDADES DEL USUARIO**

---

La política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red. La siguiente es una lista de los aspectos que usted puede abordar respecto de las responsabilidades de los usuarios:

1. Lineamientos acerca del uso de los recursos de red, tales como que los usuarios estén restringidos.
2. Que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.
3. Esta permitido que los usuarios compartan cuentas o permitan a otros usar la suya.
4. Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas.
5. Política de contraseña de usuario: con que frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hay al respecto.
6. Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema.
7. Consecuencias para los usuarios que divulguen información que pueda estar patentada. Que acciones legales u otros castigos pueden implantarse.
8. Una declaración sobre la privacidad del correo electrónico (Ley de Privacidad en las Comunicaciones Electrónicas)
9. Una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión.
10. Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

La Asociación de Correo Electrónico (EMA, Electrónica Mail Asociación) recomienda que todo sitio debe tener una política acerca de la protección de la privacidad de los empleados.

Las organizaciones deben establecer políticas que no se limiten a correo electrónico, sino que también abarque otros medios, como discos, cintas y documentos impresos. La EMA sugiere cinco criterios para evaluar cualquier política:

1. ¿La política cumple con la ley y con las obligaciones hacia otras empresas?
2. La política compromete innecesariamente los intereses del empleado, del patrón o de otras empresas.
3. ¿La política es funcional, práctica y de posible cumplimiento?
4. La política aborda apropiadamente todas las formas de comunicación y mantenimiento de archivo en la oficina.
5. ¿La política fue anunciada por anticipado y aceptada por todos los interesados?

## **DETERMINACIÓN DE LAS RESPONSABILIDADES DEL ADMINISTRADOR DE SISTEMAS**

---

Muchas veces, el administrador del sistema necesita recabar información del directorio privado de un usuario para diagnosticar problemas del sistema. Los usuarios, por otra parte, tienen el derecho de conservar su privacidad. Existe, por lo tanto, una contradicción entre el

derecho del usuario a la privacidad y las necesidades del administrador del sistema. Cuando se presentan amenazas a la seguridad de la red, el administrador del sistema tendrá mayor necesidad de recabar información de los archivos, incluidos los del directorio base de los usuarios.

La política de seguridad de la red debe especificar el grado al que el administrador del sistema pueda examinar los directorios y archivos privados de los usuarios para diagnosticar problemas del sistema e investigar violaciones de la seguridad. Si la seguridad de la red esta en riesgo, la política debe permitir mayor flexibilidad para que el administrador corrija los problemas de seguridad. Otros aspectos relacionados que usted debe abordar son los siguientes:

1. Puede el administrador revisar o leer los archivos de un usuario por alguna razón.
2. Los administradores de la red tienen el derecho de examinar el tráfico de la red o del host.
3. Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas.

## **QUÉ HACER CON LA INFORMACIÓN DELICADA**

---

Usted debe determinar que tipo de datos delicados pueden almacenarse en un sistema específico. Desde el punto de vista de la seguridad, la información en extremo delicada, como nóminas y planes, debe estar restringida a unos cuantos hosts y administradores de sistemas.

Para concederle a un usuario acceso a un servicio de un host, usted debe considerar que otros servicios e información se proporcionan y a los cuales el usuario podrá tener acceso. Si el usuario no tiene necesidad de manejar información delicada, no debe tener una cuenta en un sistema que contenga dicho material.

También debe considerar si existe una seguridad adecuada en el sistema para proteger la información delicada. En general, usted no desea que los usuarios guarden información muy delicada en un sistema que usted no planea asegurar bien. Por otra parte, asegurar un sistema puede implicar hardware, software y costos adicionales de administración, por lo cual puede no ser rentable asegurar datos en un host que no sea muy importante para la organización o los usuarios.

La política también debe tomar en cuenta el hecho de que usted necesita decirles a los usuarios que podrán guardar información delicada que servicios son apropiados para el almacenamiento de dichos datos.

## **CAPÍTULO III**

### **POLÍTICAS DE SEGURIDAD**

#### **PLAN DE ACCIÓN CUANDO SE VIOLE LA POLÍTICA DE SEGURIDAD**

---

Cada vez que se viola la política de seguridad, el sistema esta sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando esta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posible. Si la política de seguridad es demasiado restrictiva, o esta explicada inadecuadamente, es muy probable que sea violada o desactivada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que usted establezca deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando usted detecte una violación a la política de seguridad, debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. En este último caso, la violación quizás haya sido efectuada no solo por una persona, sino por un grupo que a sabiendas realiza un acto en violación directa de la política de seguridad. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas que se deben tomar.

Debe llevarse a cabo una investigación para determinar las circunstancias en torno a la violación de seguridad, y cómo y por que ocurrió. La política de seguridad debe contener lineamientos acerca de las acciones correctivas para las fallas de seguridad. Es razonable esperar que el tipo y severidad de la acción dependan de la gravedad de la violación.

#### **RESPUESTA A LAS VIOLACIONES DE LA POLÍTICA**

---

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable del acto. Las violaciones a la política pueden ser cometidas por gran variedad de usuarios; algunos pueden ser locales y otros externos. Los usuarios locales son llamados usuarios internos y los externos, usuarios foráneos. Por lo general, la distinción entre ambos tipos está basada en los límites de red, administrativos, legales o políticos. El tipo de límite determina cual debe ser la respuesta a la violación de la seguridad. Los ejemplos de

respuestas pueden ir desde una reprimenda o advertencia verbal, una carta formal o la presentación de cargos judiciales.

Usted necesita definir la acción según el tipo de violación. Estas acciones requieren ser definidas con claridad, con base en el tipo de usuario que haya violado la política de seguridad de cómputo. Los usuarios internos y externos de su red deben estar conscientes de la política de seguridad.

Si hay usuarios externos que utilicen legalmente la red, es responsabilidad de usted verificar que esas personas conozcan las políticas que se han establecido. Esto es de particular importancia si usted tiene que emprender acciones legales en contra de los transgresores.



Si se ha producido una pérdida significativa, quizá usted tendrá que tomar acciones más drásticas. Si todo esto implica una publicidad negativa, quizás usted prefiera arreglar la falla de seguridad y no emprender acción judicial.

El documento de la política de seguridad también debe contener procedimientos para manejar cada tipo de incidente de violación. Debe llevarse un registro apropiado de tales violaciones, el cual ha de revisarse periódicamente para observar tendencias y tal vez ajustar la política de seguridad para que dicha política tome en cuenta cualquier nuevo tipo de amenaza.

## **RESPUESTA A LAS VIOLACIONES DE LA POLÍTICA POR USUARIOS LOCALES**

---

Se podría tener una violación de la política de seguridad en la que el agresor sea un usuario interno. Esto podrá ocurrir en las siguientes situaciones:

-  Un usuario local viola la política de seguridad de un sitio local.
-  Un usuario local viola la política de seguridad de un sitio remoto.

En el primer caso, debido a que se viola la política de seguridad interna, usted tendrá más control sobre el tipo de respuesta ante esta violación de seguridad. En el segundo caso, un usuario local ha violado la seguridad de la política de seguridad de otra organización.

Esto podrá ocurrir a través de una conexión como Internet. Esta situación se complica por el hecho de que esto implicada otra organización, y cualquier respuesta que usted tome tendrá que discutirse con la organización cuya política de seguridad fue violada por un usuario local de usted. También deber consultar con el abogado de su empresa o con especialistas en seguridad legal de cómputo.

## ESTRATEGIAS DE RESPUESTA

---

Existen dos tipos de estrategias de respuesta ante incidentes de seguridad:

- ✚ Proteja y continúe.
- ✚ Persiga y demande.

Si los administradores de la política de seguridad sienten que la compañía es bastante vulnerable, quizás se decidan por la estrategia de proteger y continuar. El objetivo de esta política es proteger de inmediato a la red y restablecerla a su situación normal, para que los usuarios puedan seguir usándola. Para hacer esto, usted tendrá que interferir activamente con las acciones del intruso y evitar mayor acceso. A esto debe seguir el análisis del daño causado.

En ocasiones no es posible restablecer la red de inmediato a su funcionamiento normal; quizás tenga que aislar sus segmentos y apagar sistemas, con el objeto de evitar más accesos no autorizados en el sistema.

La desventaja de este procedimiento es que los intrusos saben que ya fueron detectados y tomaran medidas para evitar que sean rastreados. Asimismo, el intruso puede reaccionar a su estrategia de protección atacando el sitio con otro método; por lo menos, es probable que el intruso contenga su vandalismo en otro sitio.

La segunda estrategia -perseguir y demandar- adopta el principio de que el objetivo principal es permitir que los intrusos continúen sus actividades mientras usted los vigila.

Esto debe hacerse en forma lo más discreta posible, de modo que los intrusos no se den cuenta de que usted los esta vigilando. Deben registrarse las actividades de los intrusos, para que haya pruebas disponibles en la fase de demanda de esta estrategia. Éste es el enfoque recomendado por las dependencias judiciales y los fiscales, ya que rinde evidencias que pueden usarse para demandar a los intrusos.

La desventaja es que el intruso seguirá robando información o haciendo otros daños, y de todos modos usted estar sujeto a demandas legales derivadas del daño al sistema y la perdida de información.

Una forma posible de vigilar a los intrusos sin causarle daño al sistema, es construir una “cárcel”. Una cárcel, en este caso, se refiere a un ambiente simulado para que lo usen los intrusos, de modo que puedan vigilarse sus actividades. El ambiente simulado presenta datos falsos, pero el sistema esta configurado de tal modo que se registran las actividades del intruso.

Para construir una cárcel, se necesita acceso al código fuente del sistema operativo y alguien interno con talento de programación que sepa simular ese ambiente. Lo mas seguro es construir la cárcel sacrificando una maquina en un segmento aislado de la red, para reducir el riesgo de contaminación hacia otros segmentos y sistemas por las actividades de



los intrusos. También es posible construir la cárcel mediante un ambiente simulado de software; sin embargo, esto es más difícil de preparar.

En un sistema Unix, el mecanismo de root puede ser muy útil para preparar la cárcel. Este mecanismo confina irrevocablemente los procesos a una sola rama del sistema de archivos.

Para todos los fines prácticos, la raíz de esta rama del sistema de archivos parece la raíz del sistema de archivos para el proceso. Este mecanismo evita el acceso a archivos de dispositivo y al archivo de contraseñas reales (/etc/passwd).

Si usted no desea que otros usuarios se conecten con la máquina sacrificada, tendrán que actualizar periódicamente el archivo utmp, que contiene el registro de los usuarios conectados, de modo que la cárcel parezca real. También debe eliminar las utilerías que revelen que la cárcel es un ambiente simulado. Ejemplos de estas utilerías son netstat, ps, who y w.

Alternativamente, usted puede proporcionar versiones falsas de estas utilerías, para hacer que el ambiente simulado parezca real.

#### Arquitectura general de una cárcel (Fig. 1.)

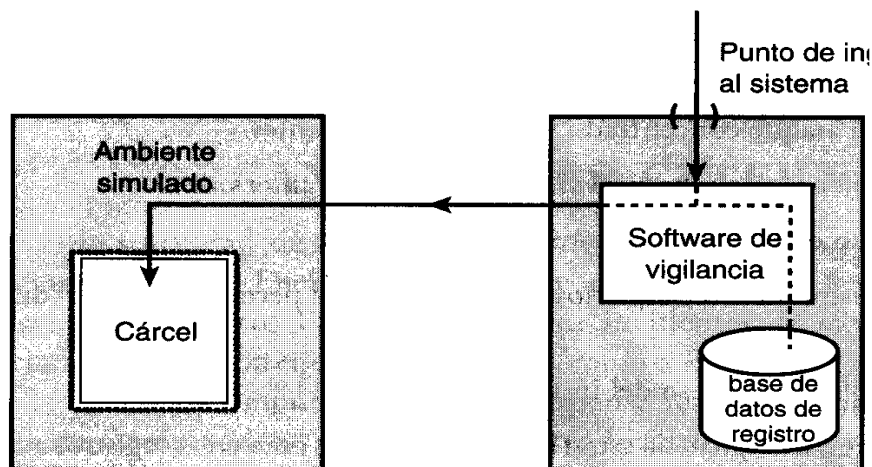


Fig. 1

Una vez que tenga suficientes evidencias contra un intruso, quizá desee demandarlo.

Sin embargo, los pleitos judiciales no son siempre los mejores resultados. Si el intruso es un usuario interno o un invitado, como un estudiante, las acciones disciplinarias adecuadas

pueden ser igualmente eficaces, sin necesidad de los costos adicionales de la demanda judicial y la correspondiente publicidad.

La política de seguridad de red debe contemplar estas opciones y ofrecer lineamientos acerca de cuando deben ejercerse.

La siguiente lista puede usarse como lineamiento para ayudar a determinar cuando el sitio debe usar una política de proteger y continuar, y cuando una de perseguir y demandar.

La estrategia de proteger y continuar puede usarse en las siguientes circunstancias:

- ✚ Si los recursos de la red no están bien protegidos de los intrusos.
- ✚ Si la continua actividad del intruso pudiera resultar en daños y riesgos financieros considerables.
- ✚ Si el costo de la demanda es demasiado elevado, o si no existe voluntad o posibilidad de demandar.
- ✚ Si existen considerables riesgos para los usuarios actuales de la red.
- ✚ Si en el momento del ataque no se conocen los tipos de usuario de una gran red interna.
- ✚ Si el sitio esta sujeto a demandas judiciales por parte de los usuarios. Esto se aplica a las compañías de seguros, bancos, formas de seguridad, proveedores de red, etc.

En las siguientes circunstancias puede seguir la estrategia de perseguir y demandar.

- ✚ Si los recursos del sistema están bien protegidos.
- ✚ Si el riesgo de la red es incrementado por los disturbios creados por las intrusiones presentes y futuras.
- ✚ Si se trata de un ataque concentrado y ya ha ocurrido antes.
- ✚ Si el sitio es muy notorio y ha sido víctima de ataques anteriores.
- ✚ Si el hecho de no demandar acarrear más intrusiones.
- ✚ Si el sitio esta dispuesto a arriesgar los recursos de la red permitiendo que continúe la intrusión.
- ✚ Si puede controlarse el acceso del intruso.
- ✚ Si las herramientas de vigilancia están bien desarrolladas para crear registros adecuados y recabar evidencias para la demanda.
- ✚ Si cuenta con personal capacitado interno para construir rápidamente herramientas especializadas.
- ✚ Si los programadores, administradores del sistema y de la red son tan listos y conocedores acerca del sistema operativo, utilerías del sistema y los sistemas para que valga la pena el juicio.
- ✚ Si la administración de la empresa tiene disposición a demandar.
- ✚ Si los administradores del sistema saben que tipo de evidencias presentar en un juicio y pueden crear los registros adecuados de las actividades del intruso.
- ✚ Si hay contactos establecidos con agencias judiciales conocedoras.
- ✚ Si existe un representante del sitio versado en las cuestiones legales relevantes.
- ✚ Si el sitio esta preparado para las posibles acciones legales que emprendieran los usuarios si sus datos o sistemas se vieran comprometidos durante la demanda.
- ✚ Si se dispone de buenos respaldos.

## **DEFINICION DE RESPONSABILIDADES PARA SER BUEN CIUDADANO DE INTERNET**

---

Internet es una asociación cooperativa y se espera que los sitios que tengan redes conectadas a ella sigan reglas de buen comportamiento hacia los otros sitios. Esto es similar al funcionamiento de una sociedad moderna exitosa. Su política de seguridad debe contener una declaración que especifique que los intentos deliberados de violar las redes de otro sitio constituyen una violación de la política de la compañía.

También debe definir que tipo de información debe difundirse. Quizás sea más económico publicar documentos acerca de la organización en un servidor FTP. En este caso, debe decidir que tipo y que cantidad de información deber difundirse.

## **CONTACTOS Y RESPONSABILIDADES CON ORGANIZACIONES EXTERNAS**

---

La política de seguridad de red debe definir los procedimientos para interactuar con organizaciones externas. Dichas organizaciones podrían incluir dependencias judiciales, especialistas legales, otros sitios afectados por incidentes de violación de seguridad, organizaciones externas con equipos de respuesta, como el Equipo de Respuesta a Emergencias de Computo (CERT, Computer Emergency Response Team) y la Capacidad de Asesoría en Incidentes de Computadoras (CIAC, Computer Incident Advisory Capability) y, de ser necesario, agencias de noticias.

Debe identificarse a las personas autorizadas para tener contacto con estas organizaciones. Usted debe identificar a más de una persona en cada área para cubrir situaciones en las que la persona designada no se encuentre. Entre las cuestiones que usted debe abordar están las siguientes:

- ✚ Identificar “los tipos de relaciones publicas” de quienes están versados para hablar con la prensa.
- ✚ ¿Cuándo debe ponerse en contacto con dependencias judiciales locales y federales, como con las dependencias investigadoras?
- ✚ Qué tipo de información puede ser divulgada.

Deben seguirse ciertas reglas respecto al manejo de pruebas durante la investigación.

De no seguirse estas reglas, se podría perder el caso. En consecuencia, es esencial que usted se ponga en contacto con las autoridades de su país, encargadas de delitos de cómputo y pedirles que lo ayuden para planear la investigación. Muchas dependencias judiciales ofrecen capacitación en manejo de pruebas y hay compañías que ofrecen servicios en el área de investigación.

## INTERPRETACIÓN Y PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD

---

Es importante identificar a las personas que interpretan la política. Generalmente no es aconsejable que sea una sola persona, ya que podrá no estar disponible en el momento de la crisis.

Se puede designar a un comité, pero también se recomienda que no este constituido por muchos miembros. De vez en cuando, se convocar al comité de política de seguridad para interpretar, repasar y revisar el documento.

Una vez que se haya redactado la política de seguridad y se haya alcanzado el consenso en sus puntos, el sitio debe asegurarse de que la declaración de política se divulgue y discuta ampliamente.

Podrán utilizarse listas de correo o una pagina web interna. Puede reforzarse la nueva política mediante educación interna, como seminarios de capacitación, sesiones informativas, talleres, reuniones personales con el administrador, o todo esto dependiendo del tamaño de la institución y de las necesidades existentes.

Implementar una política de seguridad efectiva es un esfuerzo colectivo. Por lo tanto, debe permitirse que los usuarios comenten la política durante cierto tiempo. Será conveniente que se organizaran reuniones para obtener comentarios y asegurarse de que la política se entienda correctamente. Esto también puede ayudarle a aclarar el texto de la política y evitar ambigüedades e inconsistencias.

Las reuniones deben estar abiertas a todos los usuarios de la red y a los miembros de la administración de alto nivel, quienes pueden ser necesarios para tomar decisiones globales cuando surjan preguntas importantes. La participación y el interés de los usuarios aseguran que la política se comprenda mejor y que será más probable que se siga.

Si los usuarios sienten que la política reduce su productividad, se les debe permitir que argumenten el porque. Si es necesario, habrá que agregar recursos adicionales a la red para asegurarse de que los usuarios puedan realizar su trabajo sin pérdida de productividad. Para crear una política efectiva de seguridad, usted necesita lograr un delicado equilibrio entre protección y productividad.

En ocasiones, los nuevos programas son recibidos con entusiasmo al principio, cuando todos están conscientes de la política. Con el tiempo, empero, existe la tendencia a olvidar el contenido.

Los usuarios necesitan recordatorios periódicos. Asimismo, cuando llegan usuarios nuevos a la red, estos necesitan conocer la política de seguridad.

Los recordatorios periódicos (debidamente programados) y la capacitación continua acerca de la política, incrementan las posibilidades de que los usuarios sigan dicha política de

seguridad. Debe incluirse la política de seguridad en el paquete de información de los usuarios nuevos. Algunas organizaciones requieren que cada usuario de la red firme una declaración en la que se especifique que han leído y comprendido la política. Si posteriormente se necesita emprender acción legal contra un usuario por graves violaciones de seguridad, esta declaración firmada le ayudará a entablar exitosamente la demanda.

## IDENTIFICACIÓN Y PREVENCIÓN DE PROBLEMAS DE SEGURIDAD

---

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente como deben protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deben implementarse para evitar problemas de seguridad.

La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad.






Antes de establecer los procedimientos de seguridad, debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo.

En muchas ocasiones es tentador empezar a implementar procedimientos como el siguiente, sin haber definido la política de seguridad de la red: “Nuestro sitio necesita ofrecer a los usuarios acceso telnet a los hosts internos y externos, evitar acceso NFS a los hosts internos, pero negarlo a los usuarios externos, tener tarjetas inteligentes para registrarse desde afuera, tener módems de contestación de Llamada...”

Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas tengan más protección de la que necesitan, y que otras áreas más importantes no tengan suficiente protección.

Establecer una política de seguridad eficaz requiere considerable esfuerzo. Se necesita cierto esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario para que los usuarios de la red la entiendan adecuadamente.

Además de realizar el análisis de riesgo de los recursos de la red, usted debe identificar otros puntos vulnerables. La siguiente lista es un intento de describir algunas de las tareas más problemáticas. Esta lista lo puede orientar en la dirección correcta, pero de ningún modo esta completa, ya que es probable que su sitio tenga algunos puntos vulnerables particulares.

-  Puntos de acceso
-  Sistemas configurados inadecuadamente
-  Problemas de software
-  Amenazas internas
-  Seguridad física

A continuación presentamos una explicación de estos aspectos.

## PUNTOS DE ACCESO

Los puntos de acceso son los puntos de entrada (también llamados de ingreso) para los usuarios no autorizados. Tener muchos puntos de acceso incrementa los riesgos de seguridad de la red.

La figura 2 muestra una red simplificada de una organización en la que existen varios puntos de ingreso a la red. Los puntos de acceso son el servidor terminal y el router del segmento A de la red. La estación de trabajo del segmento A tiene un módem privado, que se usa para conexiones telefónicas. El host B de segmento B de la red también es un punto de ingreso a este segmento. Ya que el router une los dos segmentos de la red, cualquier intruso puede usar estos puntos de acceso en cada segmento de la red para penetrar a la red completa.

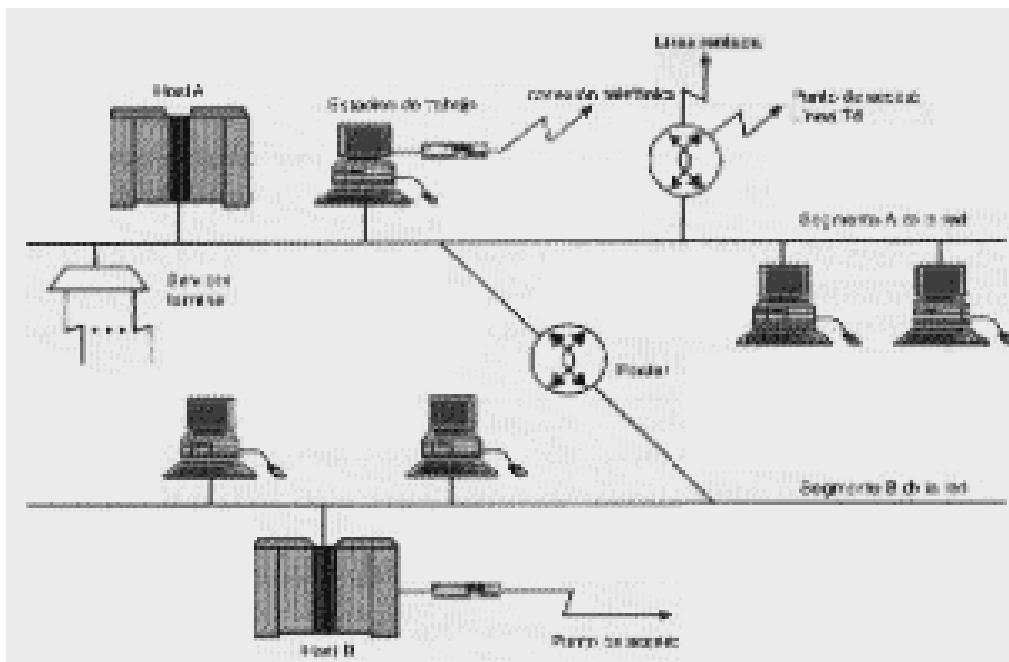


Fig. 2

Se puede asegurar los puntos de acceso en la figura, pero es fácil que se olvide de la estación de trabajo del segmento A, que iba a ser usada para conexiones telefónicas al exterior, quizá para simples boletines electrónicos.

Considere la siguiente situación: el usuario de la estación de trabajo del segmento A puede tener una cuenta con un proveedor de acceso a Internet. Suponga que este usuario utiliza una conexión de Protocolo Internet de Línea Serial (SLIP, Serial Line Internet Protocol) o

de Protocolo de Punto a Punto (PPP, Point to Point Protocol) para acceder a este proveedor de acceso a Internet.

Si el software TCP/IP que este usuario ejecuta en la estación de trabajo está configurado también como router es posible que un intruso tenga acceso a toda la red. Así mismo, si en la estación de trabajo se habilita un protocolo de enrutamiento como el protocolo de información de enrutamiento (RIP, Routing Information Protocol) o el de Abrir Primero la Ruta más Corta (OSPF, Open, Shortest Path First), la estación de trabajo puede exponer a la red interna a ataques basados en los protocolos de enrutamiento.

Observe que quizá el usuario no haya habilitado deliberadamente a la estación de trabajo como router el sistema operativo de la estación de trabajo podría estar habilitado como router en forma predeterminada. Este es el caso de muchos sistemas Unix, así como de los paquetes TCP/IP para DOS y Windows. Aún cuando la estación de trabajo haya sido configurada adecuadamente por el personal de la red, el usuario podrá conectar su computadora laptop a la red y usar un módem para tener acceso telefónico al proveedor de acceso a Internet. Si el usuario estuviera utilizando acceso telefónico (también llamado cuenta shell), donde el usuario ejecuta software de emulación de terminal en la estación de trabajo y no software TCP/IP, quizás no producirá daños. Sin embargo, si el usuario empleara una conexión SLIP o PPP, creara otro punto de acceso sin darse cuenta, el cual podrá pasar inadvertido para el personal de administración de la red.

Esto podrá representar un riesgo para la seguridad de toda la red. Puede evitarse la situación de la figura anterior si la política de seguridad de la red le informa al usuario que están prohibidas las conexiones privadas a través de las estaciones de trabajo individuales. Esta situación también subraya la importancia de tener una política de seguridad en la que se define con claridad la política de uso aceptable para la red.

Si quiere conectarse a Internet, debe tener por lo menos un vínculo con redes fuera de la organización. El vínculo de red hace disponibles numerosos servicios de red, tanto dentro como fuera de esta, y cada servicio es susceptible de ser comprometido.

Los servidores terminales pueden representar un riesgo si no están protegidos adecuadamente. Muchos de los servidores terminales que hay en el mercado no requieren ningún tipo de autenticación. Pregúntele a su distribuidor acerca de la capacidad de autenticación del servidor terminal. Los intrusos pueden utilizar a dichos servidores para disfrazar sus acciones, marcando al servidor terminal y teniendo acceso a la red interna. Si el servidor terminal lo permite, el intruso puede tener acceso a la red interna desde dicho servidor, y después utilizar telnet para salir de nuevo, lo que dificulta rastrearlo. Asimismo, si el intruso lo utiliza para atacar a otra red, parecer que el ataque se origina en la red de usted.

Según su configuración, las líneas telefónicas pueden dar acceso tan solo a un puerto de conexión de un solo sistema. Si esta conectada a un servidor terminal, la línea de telefónica puede dar acceso a toda la red. Como se menciona al explicar la figura 3.6, una línea telefónica en una estación de trabajo que ejecute software TCP/IP puede dar acceso a toda la red.

## SISTEMAS MAL CONFIGURADOS

Cuando los intrusos penetran en la red, por lo general tratan de alterar el funcionamiento los hosts del sistema.

Los blancos preferidos son los hosts que actúan como servidores telnet. Si el host esta mal configurado, el sistema puede ser alterado con facilidad. Los sistemas mal configurados son responsables de numerosos problemas de seguridad de red.

## ANTECEDENTES DE LA SEGURIDAD EN REDES

Los modernos sistemas operativos y su software correspondiente se han vuelto tan complicados, que entender cómo funciona el sistema no solo es un trabajo de tiempo completo, sino que requiere conocimientos especializados. Los distribuidores también pueden ser responsables de la mala configuración de los sistemas. Muchos distribuidores envían los sistemas con la seguridad totalmente abierta. Las contraseñas de cuentas importantes pueden no estar establecidas, o usar combinaciones de contraseñas y logins fácilmente descifrables. El libro *The Cuckoo's Egg*, de Cliff Stoll, narra la historia real de una cacería global de un espía de computadoras y menciona cómo el intruso obtuvo el acceso a los sistemas mediante una combinación de logins y contraseñas como 'Sistema / administrador "campo / servicio", etcétera.

## PROBLEMAS DE SOFTWARE

Al aumentar la complejidad del software, también aumenta el número y la complejidad de los problemas de un sistema determinado. A menos que se encuentren formas revolucionarias de crear software, éste nunca estar por completo libre de errores. Las fallas de seguridad conocidas públicamente se vuelven métodos comunes de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida (como es la de Unix), el intruso puede usar los puntos débiles del código de software que se ejecuta en modo privilegiado para tener acceso privilegiado al sistema. Los administradores de sistemas deben estar conscientes de los puntos débiles de sus sistemas operativos y tienen la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se descubran esos problemas. También usted debe tener la política de reportar al proveedor los problemas cuando se encuentren, de modo que pueda implementarse y distribuirse la solución.

## AMENAZAS INTERNAS

Por lo general, los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario interno decide alterar el funcionamiento la red, puede representar una considerable amenaza a la seguridad de la red. Si usted tiene acceso físico a



los componentes de un sistema, este es fácil de alterar el funcionamiento. Por ejemplo, pueden manipularse fácilmente las estaciones de trabajo para que otorguen acceso privilegiado. Puede ejecutarse fácilmente decodificación de protocolo y software de captura para analizar el tráfico de protocolo. La mayoría de los servicios de aplicación estándar TCP/IP como telnet, rlogin y ftp, tienen mecanismos de autenticación muy débiles, en los que las contraseñas se envían en forma clara. Debe evitarse el acceso a estos servicios desde cuentas privilegiadas, ya que esto puede comprometer fácilmente las contraseñas de dichas cuentas.

## SEGURIDAD FÍSICA

Si la computadora misma no está físicamente segura, pueden ignorarse fácilmente los mecanismos de seguridad del software. En el caso de las estaciones de trabajo DOS (Windows ni siquiera existe un nivel de contraseña de protección. Si se deja desatendida una estación de trabajo Unix, sus discos pueden ser cambiados o si se deja en modo privilegiado, la estación está por completo abierta. Asimismo, el intruso puede parar la máquina y regresarla a modo privilegiado, y después plantar programas tipo caballo de Troya, o tomar cualquier medida para dejar al sistema abierto para ataques futuros.

Todos los recursos importantes de la red, como las backbones, los vínculos de comunicación, los hosts, los servidores importantes y los mecanismos clave deben estar ubicados en una red físicamente segura. Por ejemplo, el mecanismo de autenticación Kerberos requiere que su servidor está físicamente seguro. Físicamente seguro significa que la máquina está guardada en una habitación o colocada de tal modo que se restrinja el acceso físico a ella.

En ocasiones no es fácil asegurar físicamente las máquinas. En esos casos, debe tenerse cuidado para no confiar demasiado en esas máquinas. Usted debe limitar el acceso desde máquinas no seguras hacia las más seguras. En particular, usted no debe permitir acceso a hosts que usen mecanismos de acceso confiable como las utileras Berkeley-r\* (rsh, rlogin, rcp, rexec).

Aún cuando la máquina está segura físicamente, debe tener cuidado en quién tiene acceso a ella. Las tarjetas electrónicas “inteligentes” para tener acceso a la habitación en la que están aseguradas las máquinas pueden limitar el número de personas con acceso y proporcionar un registro de la identidad y hora de las personas que entraron en la habitación. Debe establecerse en la política que los empleados con acceso no podrán introducir a otras personas en la sala segura cuando está abierta la puerta, aun cuando se conozca la identidad de esas personas.

Si usted permite que entre alguien junto con una persona autorizada, no podrá llevar un registro adecuado de quién y cuando entre en la habitación.

Recuerde que el personal de mantenimiento y limpieza del edificio quizá tenga acceso a la sala de seguridad. Asegúrese de tomar esto en cuenta al diseñar el sistema de seguridad.

## **CONFIDENCIALIDAD**

---

La confidencialidad puede definirse como el hecho de mantener las cosas ocultas o secretas. Esta es una consideración muy importante para varios tipos de datos delicados.

Las siguientes son algunas de las situaciones en las que la información es vulnerable de ser divulgada:

- ✚ Cuando la información está almacenada en un sistema de cómputo.
- ✚ Cuando la información está en tránsito hacia otro sistema en la red.
- ✚ Cuando la información está almacenada en cintas de respaldo.

El acceso a la información que está almacenada en una computadora está controlado mediante los permisos de archivo, las listas de control de acceso (ACL) y otros mecanismos similares.

La información en tránsito puede protegerse mediante la encriptación o los gateways de las firewalls. La encriptación puede usarse para proteger la información en las tres situaciones. El acceso a la información almacenada en cintas puede controlarse mediante la seguridad física; como puede ser, guardar las cintas en una caja de seguridad o en una red inaccesible.

## **IMPLEMENTACIÓN DE CONTROLES ECONÓMICOS VIABLES PARA LA POLÍTICA**

---

Deben seleccionarse los controles y los mecanismos de protección de modo que estos puedan hacer frente adecuadamente a las amenazas detectadas en la evaluación de riesgos. Estos controles deben implementarse en forma económicamente viable. Tiene poco sentido gastar grandes cantidades de dinero y sobreproteger y restringir el uso de un recurso, si específico el riesgo de exposición.

El sentido común es, en muchas ocasiones, una herramienta muy eficaz para establecer la política de seguridad. Si bien son impresionantes los elaborados planes y mecanismos de seguridad, estos pueden ser bastante costosos. En ocasiones, el costo de esta implementación está oculto. Por ejemplo, usted podría implementar una solución de seguridad mediante software gratuito, sin tomar en cuenta el costo de administrar ese sistema y mantenerlo actualizado.

Además, si la solución de seguridad es muy elaborada, puede ser difícil de implementar y administrar. Si la administración constituye un paso único, los comandos para administrar tal sistema pueden ser fáciles de olvidar.

También debe mantener la perspectiva de que, por muy elaborada que sea la solución, una contraseña débil o robada puede comprometer a todo el sistema.

A continuación damos algunos lineamientos para implementar controles costeadles para la política.

### SELECCIÓN DE CONTROLES RELACIONADOS CON LAS POLÍTICAS

Los controles que usted seleccione serán la primera línea de defensa en la protección de su red. Estos controles deben representar con precisión lo que usted intenta proteger, tal como está definido en la política de seguridad. Si las intrusiones externas son una gran amenaza contra su sistema, quizá no sea económicamente emplear dispositivos biométricos para autenticar a los usuarios internos. En cambio, si la amenaza mayor a sus sistemas es el uso no autorizado de los recursos de computadora por los usuarios internos, usted necesitar establecer buenos procedimientos de contabilidad automatizados. Si la amenaza principal a la red son los usuarios externos, usted tendrá que construir routers de selección y firewalls.

### USO DE ESTRATEGIAS DE RESERVA

Si el análisis de riesgo indica que proteger un recurso es vital para la seguridad de la red, necesitará usar diversas estrategias para hacerlo, lo cual le da a usted la seguridad de que, si una estrategia falla o es alterada, otra puede entrar en acción y seguir protegiendo el recurso de la red.

Puede resultar más económico y sencillo usar varias estrategias, de fácil implementación pero eficaces, que seguir una sola estrategia complicada y sofisticada. Este último es el principio del todo o nada. Si el mecanismo elaborado es vencido, no hay ninguno de reserva que proteja al recurso.

Ejemplos de controles sencillos son los módems de devolución de llamada, que pueden usarse en combinación con mecanismos tradicionales de conexión. Esto puede reforzarse con tarjetas inteligentes y autenticadotes manuales de un paso.

### DETECCION Y VIGILANCIA DE ACTIVIDADES NO AUTORIZADAS

Si ocurre una intrusión o un intento de intrusión, debe detectarse tan pronto como sea posible.

Usted puede implantar varios procedimientos sencillos para detectar el uso no autorizado de un sistema de cómputo. Algunos procedimientos se basan en herramientas proporcionadas con el sistema operativo por el proveedor. También se dispone públicamente de tales herramientas en Internet.

## INSPECCIÓN DEL USO DEL SISTEMA

El administrador del sistema puede realizar periódicamente la inspección. Si no, puede usarse software elaborado con este fin. La inspección de un sistema implica revisar varias de sus partes y buscar cualquier cosa que sea inusual. En esta sección se explican algunas de las formas para hacer esto.

La inspección debe hacerse con regularidad. No es suficiente hacerla cada mes o cada semana, ya que esto provocaría una brecha de seguridad que no sería detectada en mucho tiempo.

Algunas violaciones de seguridad pueden detectarse unas cuantas horas después de haberse cometido, en cuyo caso no tiene sentido la inspección semanal o mensual. El objetivo de la inspección es detectar la brecha de seguridad en forma oportuna, de modo que se pueda reaccionar adecuadamente a ella.

Si usted utiliza herramientas de inspección, debe examinar periódicamente la información de estas. Si los registros son voluminosos, tal vez necesite usar los scripts awk o perl para analizar la información. Estas herramientas también están disponibles para sistemas que no son Unix.

## MECANISMOS DE INSPECCIÓN

Muchos sistemas operativos almacenan la información de conexiones en archivos de registro especiales. El administrador del sistema debe examinar regularmente estos archivos de registro para detectar el uso no autorizado del sistema. La siguiente es una lista de métodos que puede utilizar en su sitio.

Puede comparar las listas de los usuarios que estén conectados en ese momento con los registros de las conexiones anteriores. La mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días.

- ✚ Una cuenta que muestre actividad fuera del horario “normal” del usuario debe inspeccionarse de cerca. Quizá un intruso este usando esa cuenta. También puede alertarse a los usuarios para que observen el último mensaje de conexión que aparece al momento de hacer su primera conexión. Si notan algún horario inusual, deben avisarle al administrador del sistema.
- ✚ Muchos sistemas operativos llevan registros de contabilidad para efectos de cobranza. También pueden examinarse esos registros para detectar cualquier pauta desacostumbrada de uso del sistema. Los registros de contabilidad inusuales pueden indicar una penetración ilegal en el sistema.
- ✚ El sistema operativo quizá tenga también utilerías de registro de conexión, como el syslog usado en Unix. Deben revisarse los registros producidos por dichas herramientas para detectar cualquier mensaje de error desacostumbrado producido por el software del sistema. Por ejemplo, un gran número de intentos fallidos de conexión en un periodo corto puede indicar que alguien está tratando de adivinar

contraseñas. También debe inspeccionar el número de intentos de registro de conexión en las cuentas delicadas como root, sysadm, etcétera.

- ✚ Muchos sistemas operativos tienen comandos, como el ps de Unix, que enlistan los procesos que se están ejecutando en ese momento. Pueden usarse estos comandos para detectar si los usuarios están ejecutando programas a los cuales no están autorizados, así como para detectar programas no autorizados que quizá hayan sido iniciados por un intruso.
- ✚ Pueden usarse los gateways de las firewalls para crear un registro del acceso a la red. Esta debe inspeccionarse con regularidad. Más adelante se explican con detalle las firewalls.
- ✚ Si usted tiene recursos especiales que desee inspeccionar, puede construir sus propias herramientas con las utileras estándar del sistema operativo. Por ejemplo, puede combinar los comandos **ls** y **find** de Unix en un script de shell para revisar las configuraciones de propiedades y permisos privilegiados de archivo. Puede guardar la salida de esta actividad de inspección en listas que se pueden comparar y analizar mediante herramientas comunes de Unix como diff, awk o perl. Las diferencias en los permisos de archivos importantes pueden indicar modificaciones no autorizadas en el sistema.

## HORARIO DE INSPECCIÓN

Los administradores del sistema deben inspeccionar con frecuencia y regularidad a lo largo de todo el día. Puede resultar muy fastidioso inspeccionar por horarios fijos, pero pueden ejecutarse comandos de inspección a cualquier hora, en los momentos desocupados, por ejemplo, cuando usted está hablando de negocios por teléfono.

Si ejecuta los comandos de inspección con frecuencia, se familiarizará rápidamente con la información normal de estas herramientas de inspección. Esto le ayudará a detectar la información inusual. Es posible intentar automatizar este proceso ejecutando herramientas de búsqueda sobre la información, y se pueden buscar ciertos patrones fijos, pero generalmente es difícil detectar toda la información inusual causada por la intrusión en el sistema. El cerebro humano sigue siendo mejor que la mayoría de los programas para detectar sutiles diferencias en los registros de inspección.

Si ejecuta diversos comandos de inspección a diferentes horas del día, será difícil que un intruso prediga sus acciones. El intruso no puede saber cuándo el administrador correrá el comando de inspección para desplegar a los usuarios conectados, por lo que corre mayor riesgo de ser detectado. Por otra parte, si el intruso sabe que todos los días, a las seis de la tarde, el sistema se revisa para ver que todos se hayan desconectado, esperará a que concluya esta revisión antes de conectarse.

La inspección es útil, pero también puede ser alterada. Algunos intrusos pueden darse cuenta de los mecanismos estándar de registro de conexiones que se usen en el sistema y pueden tratar de desactivarlos. La inspección periódica puede detectar a los intrusos, pero no ofrece ninguna garantía de que el sistema está a salvo. No es un método infalible para detectar a los intrusos.

## PROCEDIMIENTOS DE REPORTE

---

En caso de que se detecte algún acceso no autorizado, debe haber procedimientos para reportar este acceso y a quién será informado. Además, su política de seguridad debe cubrir los siguientes aspectos:

- ✚ Procedimientos de administración de cuentas
- ✚ Procedimientos de administración de configuración
- ✚ Procedimientos de recuperación
- ✚ Procedimiento de reporte de problemas para los administradores del sistema

### PROCEDIMIENTOS DE ADMINISTRACION DE CUENTAS

Cuando se crean cuentas de usuario, debe tenerse cuidado en no dejar ninguna laguna de seguridad. Si el sistema operativo se esta instalando desde los medios de distribución, debe examinarse que la contraseña no tenga cuentas privilegiadas que usted no necesite.

Algunos vendedores de sistemas operativos proporcionan cuentas para los ingenieros de servicio de campo y servicios de sistemas. Estas cuentas o no tienen contraseña o son de dominio publico. Si usted necesita estas cuentas, debe darles una contraseña nueva; si no, debe eliminarlas o desactivarlas. En general no hay ninguna razón para permitir cuentas que no tienen una contraseña establecida.

Las cuentas sin contraseña son peligrosas aun cuando no ejecuten intérpretes de comandos, como la cuenta que existe tan solo para ver quién esta conectado en el sistema. Si estas no están establecidas correctamente, puede comprometerse la seguridad del sistema. Por ejemplo, si no se establece adecuadamente el usuario anónimo de una cuenta FTP a cualquier usuario le estar permitido el acceso al sistema para recuperar archivos. Si se cometen errores al establecer esta cuenta, e inadvertidamente se concede el permiso de escritura al sistema de archivos, un intruso puede cambiar el archivo de contraseñas o destruir el sistema.

El recurso shadow password se utiliza por primera vez en el System V, pero hay otros sistemas Unix que cuentan con el, como SunOS 4.0 y superior, y el 4.3BSD Unix Tahoe. El archivo shadow password permite que la forma encriptada de las contraseñas esta oculta para los usuarios no privilegiados. El intruso, por lo tanto, no puede copiar el archivo de contraseñas y tratar de adivinarlas.

Su política también debe incluir los procedimientos para llevar cuenta de quién tiene cuenta privilegiada, como raíz en Unix y MAINT en VMS. En Unix, si usted conoce la contraseña raíz (Root), puede usar el comando **su** para usurpar privilegios de raíz. Si se descubre la contraseña en forma inadvertida, el usuario puede conectarse con su cuenta personal y usurpar privilegios de raíz. Por lo tanto, usted debe implantar una política que obligue a los usuarios privilegiados a cambiar de contraseña a intervalos periódicos.

Asimismo, cuando un usuario privilegiado abandone la organización, se le debe avisar a usted para que cambie la contraseña de las cuentas privilegiadas.

Además deben cambiarse las cuentas de usuario de quienes salgan de la compañía.

Los servicios de red deben someterse a un estrecho escrutinio. Muchos proveedores proporcionan archivos de permisos de red predeterminados, que suponen que todos los hosts externos son confiables. Éste no es el caso cuando se está conectado a una red como Internet.

Los mismos intrusos recaban información acerca de los puntos vulnerables de sistemas en particular. En ocasiones hacen circular sus descubrimientos en revistas clandestinas, como las siguientes:

-  2600 Magazine
-  Phrack
-  Computer Underground Digest

Ciertos administradores de sistemas deberían suscribirse a tales publicaciones, para mantenerse adelante de los intrusos.

## PROCEDIMIENTOS DE ADMINISTRACIÓN Y CONFIGURACIÓN

Usted debe mantener actualizadas las versiones del sistema operativo y de utileras importantes.

Por lo general, los puntos débiles de los sistemas anteriores son bien conocidos y es probable que el intruso se dé cuenta de los problemas de seguridad. Desgraciadamente, las nuevas versiones del software, si bien arreglan algunos problemas de seguridad, en muchas ocasiones crean otros.

Por esta razón es importante sopesar los riesgos de no actualizarse con la nueva versión del sistema operativo y dejar descubiertas lagunas de seguridad, contra el costo de actualizarse con un nuevo software.

Aunque puede confiarse en la mayoría de los proveedores en el envío de sus actualizaciones, muchas organizaciones dependen del bienestar del software público desarrollado para cierta actividad dentro de su compañía. Muchas empresas de *software* envían su producto con PGP u otras firmas digitales para demostrar que nadie ha alterado su software.

Tripwire es una herramienta que ayuda a administradores de sistemas y usuarios a inspeccionar cualquier cambio en un conjunto designado de archivos. Usado con archivos de sistema en forma regular (es decir, diario), Tripwire puede notificar al administrador

acerca de archivos alterados o manipulados, de modo que puedan tomarse medidas de control en forma oportuna.

Tripwire puede encontrarse en el siguiente URL:

<ftp://ftp/nordu.net/net-Working/security/tools/tripwire/tripwire-1.2.tar.gz>.

Por lo general, puede confiarse en la mayoría de los proveedores, en el sentido de que las nuevas versiones del software arreglen problemas de seguridad anteriores y no generen otros más grandes. Otra complicación es que la nueva versión puede quebrantar software de aplicación del que dependan los usuarios. Quizá tenga que coordinar la campaña de actualización con más de un proveedor.

También se pueden recibir soluciones a través de las listas de correo en la red. Usted debe tener personal competente que examine con cuidado estas soluciones a los problemas y que las implante sólo si son seguras.

Como regla, usted no debe instalar una solución si no conoce las consecuencias de tal solución. Siempre es posible que los autores de la solución tengan un código no evidente que les permita acceso no autorizado a su sistema.

## **PROCEDIMIENTOS DE RECUPERACIÓN**

---

Siempre que instale una nueva versión del sistema operativo, usted no sólo debe hacer respaldo de la imagen binaria del kernel del sistema operativo, sino también de los archivos usados para compilar y configurar dicho sistema. Lo mismo es válido para todo el software de aplicación y de red.

Los respaldos del sistema de archivos son como una póliza de seguros. No sólo lo protegen en caso de fallas del disco y de otras partes del hardware, sino también contra eliminaciones accidentales y como medida de reserva cuando el sistema es penetrado. Si usted sospecha que alguien ha irrumpido en su sistema, quizá tenga que restablecerlo desde el respaldo para protegerse de los cambios que pudiera haber hecho el intruso. Si usted no puede detectar cuándo ocurrieron los cambios no autorizados, tendrá que examinar numerosos respaldos. Si no cuenta con una buena copia del software del sistema, ser difícil determinar cómo deben de ser los datos y los archivos del sistema.

Los respaldos diarios, así como los de incremento, pueden ser útiles para ofrecer la historia de las actividades del intruso. Al examinar los respaldos anteriores, puede determinar cuándo se penetró por primera vez en el sistema. Aún cuando hayan sido borrados los archivos del intruso, usted podrá verlos en las cintas de respaldo.



Cuando busque rastros de archivos intrusos, debe buscar nombres de archivo que normalmente no aparecerían en el listado del directorio. En los sistemas Unix, a los intrusos les gusta guardar datos en archivos cuyo nombre empieza con punto (.) o que tengan caracteres no desplegables. Estos archivos son más difíciles de detectar.

Usted debe decidir la estrategia de respaldo, lo cual implica la combinación de los siguientes métodos:

- ✚ Respaldo total
- ✚ Respaldo de nivel 1
- ✚ Respaldo de nivel 2
- ✚ Respaldo personalizado

En los sistemas Unix, al respaldo total también se le llama de nivel 0. En estos sistemas, el respaldo de nivel I respalda todos los archivos que han sido modificados desde el último respaldo de nivel 0. En general, un respaldo de nivel N respalda todos los archivos modificados desde el último respaldo de nivel N-1. En el caso de utileras de respaldo, como dump, el respaldo de nivel N respalda todos los archivos modificados desde el último respaldo N-1 o inferior.

Se puede usar un número arbitrario de niveles, pero en general no tiene sentido, pues se dificulta seguir la pista de los respaldos. Los niveles de respaldo numéricos tienen soporte con comandos de respaldo de tipo BSD, desde el nivel 0 al nivel 9, pero esta idea puede usarse con cualquier sistema y usted quizás tenga que llevar la cuenta a mano. En BSD de Unix el programa de respaldo es dump, y los archivos que se han respaldado en un nivel específico se guardan en el archivo /etc/dump/dates.

En el respaldo total (nivel 0) se respaldan todos los datos, sin importar cuando hayan sido modificados, ni aun cuando no lo hayan sido. Un ejemplo de esto son todos los directorios y archivos de un sistema de archivos. Después de haber respaldado los datos, se elimina el bit de archivero en todos los archivos respaldados.

La estrategia de respaldo total es la más exhaustiva de todas, ya que respalda todos los archivos sin importar si estos fueron modificados o no desde el último respaldo. Si embargo, debido al gran volumen de datos que pueden requerir respaldo, es la más lenta de las estrategias.

En el respaldo de nivel 1 se respaldan todos los archivos que se hayan modificado desde el último respaldo total (de Nivel 0). Esto significa que todos los archivos que hayan sido respaldados en el 1º respaldo de nivel 1 lo serán también en el siguiente respaldo de nivel 1, junto con aquellos que se hayan modificado desde el 1º respaldo de nivel 1. Este proceso continúa con cada respaldo de nivel 1 y puede esperarse que, en cada proceso, aumente el número de archivos respaldados.

Existe una lamentable confusión de términos para referirse al respaldo de nivel 1. En los sistemas Unix el respaldo de nivel 1 es llamado respaldo incremental. En muchos sistemas

no Unix (Sistemas operativos DOS / WINDOWS / PC para LAN) este nivel es llamado respaldo diferencial. El término respaldo incremental en muchos sistemas no Unix significa algo por completo diferente. Para evitar confusiones, usted debe establecer claramente en su política que definición está siguiendo.

Para obtener un registro completo de las versiones más actualizadas de los archivos, usted debe empezar con el respaldo completo más reciente (Nivel 1) y agregar a éste los archivos del respaldo de Nivel 1 más reciente. Esto es respaldo más reciente = último respaldo total más  $\Delta_d$ , donde el  $\Delta_d$  es el respaldo de nivel 1 más reciente.

Ya que el último respaldo de nivel 1 contiene todos los archivos modificados desde el último respaldo total, usted podrá restaurar los datos con tan solo 2 juegos de cintas: una para el respaldo total y otra para el último respaldo de nivel uno.

Si los datos en uno de los últimos respaldos de nivel 1 están corrompidos, usted tendrá que acudir a su reserva del penúltimo respaldo diferencial. Por otra parte, si está corrompido algún dato de otra cinta de respaldo de nivel 1, no importa en tanto que estén bien los datos en el más reciente respaldo diferencial.

Si por cierto tiempo no se ha hecho ningún respaldo total, y ha habido muchos cambios en el archivo, en cada respaldo de nivel 1 tenderá a crecer el tamaño de los datos que requieran respaldo.

Si se han modificado todos los archivos la sesión de respaldo de nivel 1 será igual que la del respaldo total. Esto suele no ser el caso, ya que la mayoría de los sistemas contienen una mezcla de programas y de datos y los programas de archivos suelen no modificarse.

En muchos sistemas no Unix se utiliza el término respaldo incremental para referirse al respaldo de todos los archivos que hayan sido modificados desde el último respaldo (de nivel 0 ó 1). Esto es como el respaldo de nivel 2 en los sistemas Unix. Los archivos que no se hayan modificados no se respaldarán. Para obtener un registro completo de las versiones más actualizadas de los archivos, usted empezaría con el respaldo total más reciente, y agregaría los cambios registrados en cada sesión de respaldo incremental. Esto es:

$$\begin{aligned} \text{Respaldo más reciente} &= \text{último respaldo total} + \Delta_1 + \Delta_2 + \Delta_n \\ &\quad \text{Último respaldo total} + \Delta_i \quad (i = 1^a \text{ } n) \end{aligned}$$

Donde cada  $\Delta_i$  es un respaldo incremental.

El respaldo incremental contiene la historia secuencial de los archivos que se han modificado.

Esto significa que, para restaurar los datos usted necesita el último respaldo total y todos los respaldos incrementales posteriores. Si los datos en una de las cintas de respaldo están corrompidos, quizás no pueda restaurarlos. La excepción a esto son las situaciones en las que los respaldos incrementales posteriores tienen los archivos que están inaccesibles en las cintas corrompidas. En este caso, usted podrá restaurar esos datos a partir de las cintas posteriores.

El respaldo personalizado le da el control completo de los archivos que se respaldarán. Usted puede incluir o excluir ciertas partes de la estructura de directorios que serán respaldado, o seleccionar diferentes tipos de elementos de datos que serán respaldados. Los respaldos personalizados son útiles cuando usted quiere respaldar en forma selectiva unos cuantos archivos y directorios y no esperar al respaldo programado.

## **PROCEDIMIENTO DE REPORTE DE PROBLEMAS PARA LOS ADMINISTRADORES DEL SISTEMA**

---

Ya se abordó el tema de los procedimientos para que los usuarios reporten problemas. Los administradores del sistema deben contar con un procedimiento definido para reportar los problemas de seguridad. En grandes instalaciones de red, esto puede hacerse mediante una lista de correo electrónico que contenga las direcciones de correo electrónico de todos los administradores de la organización. En algunas organizaciones se forma un equipo de respuesta que ofrece un servicio de emergencia.

## CAPÍTULO IV

### AUDITORÍA DE SISTEMAS

---

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

#### PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

---

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- ✚ Evaluación de los sistemas y procedimientos.
- ✚ Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

#### INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

## ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar:

A nivel del área de informática:

Objetivos a corto y largo plazo.

Recursos materiales y técnicos:

- ✚ Solicitar documentos sobre los equipos, número de ellos, localización y características.
- ✚ Estudios de viabilidad.
- ✚ Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- ✚ Fechas de instalación de los equipos y planes de instalación.
- ✚ Contratos vigentes de compra, renta y servicio de mantenimiento.
- ✚ Contratos de seguros.
- ✚ Convenios que se tienen con otras instalaciones.
- ✚ Configuración de los equipos y capacidades actuales y máximas.
- ✚ Planes de expansión.
- ✚ Ubicación general de los equipos.
- ✚ Políticas de operación.
- ✚ Políticas de uso de los equipos.

Sistemas

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- ✚ Manual de formas.
- ✚ Manual de procedimientos de los sistemas.
- ✚ Descripción genérica.
- ✚ Diagramas de entrada, archivos, salida.
- ✚ Salidas.
- ✚ Fecha de instalación de los sistemas.
- ✚ Proyecto de instalación de nuevos sistemas.
- ✚ En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

- ✚ No tiene y se necesita.
- ✚ No se tiene y no se necesita.

Se tiene la información pero:

- ✚ No se usa.
- ✚ Es incompleta.
- ✚ No esta actualizada.
- ✚ No es la adecuada.
- ✚ Se usa, está actualizada, es la adecuada y está completa.

En el caso de No se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- ✚ Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- ✚ Investigar las causas, no los efectos.
- ✚ Atender razones, no excusas.
- ✚ No confiar en la memoria, preguntar constantemente.
- ✚ Criticar objetivamente y a fondo todos los informes y los datos recabados.

### PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- ✚ Técnico en informática.
- ✚ Experiencia en el área de informática.
- ✚ Experiencia en operación y análisis de sistemas.
- ✚ Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en el anexo 1, el figura el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoría lo podemos llevar mediante el anexo 2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes. Como ejemplo de propuesta de auditoría en informática véase el anexo 3.

## EVALUACIÓN DE SISTEMAS

---

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

- ✚ ¿Cuáles servicios se implementarán?
- ✚ ¿Cuándo se pondrán a disposición de los usuarios?
- ✚ ¿Qué características tendrán?
- ✚ ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

- ✚ ¿Qué aplicaciones serán desarrolladas y cuando?
- ✚ ¿Qué tipo de archivos se utilizarán y cuando?
- ✚ ¿Qué bases de datos serán utilizarán y cuando?
- ✚ ¿Qué lenguajes se utilizarán y en que software?
- ✚ ¿Qué tecnología será utilizada y cuando se implementará?
- ✚ ¿Cuántos recursos se requerirán aproximadamente?
- ✚ ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

- ✚ ¿Qué estudios van a ser realizados al respecto?
- ✚ ¿Qué metodología se utilizará para dichos estudios?
- ✚ ¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

- ✚ ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
- ✚ ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, con que se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el estudio de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad.

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

## EVALUACIÓN DEL ANÁLISIS

---

En esta etapa se evaluarán las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

Se deberá evaluar la planeación de las aplicaciones que pueden provenir de tres fuentes principales:

- ✚ La planeación estratégica: agrupadas las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la dependencia, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
- ✚ Los requerimientos de los usuarios.



- ✚ El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.

La situación de una aplicación en dicho inventario puede ser alguna de las siguientes:

- ✚ Planeada para ser desarrollada en el futuro.
- ✚ En desarrollo.
- ✚ En proceso, pero con modificaciones en desarrollo.
- ✚ En proceso con problemas detectados.
- ✚ En proceso sin problemas.
- ✚ En proceso esporádicamente.

Nota: Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la dependencia.

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

Se debe evaluar la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse.

Con la información obtenida podemos contestar a las siguientes preguntas:

- ✚ ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
- ✚ ¿Puede ser simplificado para mejorar su aprovechamiento?
- ✚ ¿Se debe tener una mayor interacción con otros sistemas?
- ✚ ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
- ✚ ¿Está en el análisis la documentación adecuada?

## EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

---

En esta etapa se deberán analizar las especificaciones del sistema.

¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia y ocurrencia de los datos, el proceso y salida de reportes?

Una vez que hemos analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión. Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

- ✚ Entradas.
- ✚ Salidas.
- ✚ Procesos.
- ✚ Especificaciones de datos.
- ✚ Especificaciones de proceso.
- ✚ Métodos de acceso.
- ✚ Operaciones.
- ✚ Manipulación de datos (antes y después del proceso electrónico de datos).
- ✚ Proceso lógico necesario para producir informes.
- ✚ Identificación de archivos, tamaño de los campos y registros.
- ✚ Proceso en línea o lote y su justificación.
- ✚ Frecuencia y volúmenes de operación.
- ✚ Sistemas de seguridad.
- ✚ Sistemas de control.
- ✚ Responsables.
- ✚ Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- ✚ Manual del usuario.
- ✚ Descripción de flujo de información y/o procesos.
- ✚ Descripción y distribución de información.
- ✚ Manual de formas.
- ✚ Manual de reportes.
- ✚ Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:

En el procedimiento:

- ✚ ¿Quién hace, cuando y como?
- ✚ ¿Qué formas se utilizan en el sistema?
- ✚ ¿Son necesarias, se usan, están duplicadas?
- ✚ ¿El número de copias es el adecuado?
- ✚ ¿Existen puntos de control o faltan?

En la gráfica de flujo de información:

- ✚ ¿Es fácil de usar?
- ✚ ¿Es lógica?
- ✚ ¿Se encontraron lagunas?
- ✚ ¿Hay faltas de control?

En el diseño:

- ✚ ¿Cómo se usará la herramienta de diseño si existe?
- ✚ ¿Qué también se ajusta la herramienta al procedimiento?

## EVALUACIÓN DEL DESARROLLO DEL SISTEMA

---

En esta etapa del sistema se deberán auditar los programas, su diseño, el lenguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones. Al tener un proceso distribuido, es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza. Las características que deben evaluarse en los sistemas son:

- ✚ Dinámicos (susceptibles de modificarse).
- ✚ Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo)
- ✚ Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- ✚ Accesibles (que estén disponibles).
- ✚ Necesarios (que se pruebe su utilización).
- ✚ Comprensibles (que contengan todos los atributos).
- ✚ Oportunos (que esté la información en el momento que se requiere).
- ✚ Funcionales (que proporcionen la información adecuada a cada nivel).
- ✚ Estándar (que la información tenga la misma interpretación en los distintos niveles).
- ✚ Modulares (facilidad para ser expandidos o reducidos).
- ✚ Jerárquicos (por niveles funcionales).
- ✚ Seguros (que sólo las personas autorizadas tengan acceso).
- ✚ Únicos (que no duplique información).

## CONTROL DE PROYECTOS

---

Debido a las características propias del análisis y la programación, es muy frecuente que la implantación de los sistemas se retrase y se llegue a suceder que una persona lleva trabajando varios años dentro de un sistema o bien que se presenten irregularidades en las que los programadores se ponen a realizar actividades ajenas a la dirección de informática.

Para poder controlar el avance de los sistemas, ya que ésta es una actividad de difícil evaluación, se recomienda que se utilice la técnica de administración por proyectos para su adecuado control.

Para tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan debe ser revisado periódicamente (semanal, mensual, etc.) para evaluar el avance respecto a lo programado. La estructura estándar de la planeación de proyectos deberá incluir la facilidad de asignar fechas predefinidas de terminación de cada tarea. Dentro de estas fechas debe estar el calendario de reuniones de revisión, las cuales tendrán diferentes niveles de detalle.

### CUESTIONARIO

1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?
5. Escribir la lista de proyectos a corto plazo y largo plazo.
6. Escribir una lista de sistemas en proceso periodicidad y usuarios.
7. ¿Quién autoriza los proyectos?
8. ¿Cómo se asignan los recursos?
9. ¿Cómo se estiman los tiempos de duración?
10. ¿Quién interviene en la planeación de los proyectos?
11. ¿Cómo se calcula el presupuesto del proyecto?
12. ¿Qué técnicas se usan en el control de los proyectos?
13. ¿Quién asigna las prioridades?
14. ¿Cómo se asignan las prioridades?
15. ¿Cómo se controla el avance del proyecto?
16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?
17. ¿Cómo se estima el rendimiento del personal?
18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?
19. ¿Qué acciones correctivas se toman en caso de desviaciones?
20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos?  
Enumérelos secuencialmente.  
( ) Determinación de los objetivos.  
( ) Señalamiento de las políticas.  
( ) Designación del funcionario responsable del proyecto.  
( ) Integración del grupo de trabajo.  
( ) Integración de un comité de decisiones.  
( ) Desarrollo de la investigación.  
( ) Documentación de la investigación.  
( ) Factibilidad de los sistemas.  
( ) Análisis y valuación de propuestas.  
( ) Selección de equipos.
21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen

con los objetivos para los cuales fueron diseñados?

De análisis SÍ ( ) NO ( )

De programación SÍ ( ) NO ( )

Observaciones

22. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.

## **CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN**

---

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela desde el análisis hasta la programación y sus objetivos son los siguientes:

**ETAPA DE ANÁLISIS** Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

**ETAPA DE DISEÑO** Descubrir errores, debilidades, omisiones antes de iniciar la codificación.

**ETAPA DE PROGRAMACIÓN** Buscar la claridad, modularidad y verificar con base en las especificaciones.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan: si se descubren en el momento de programación será más alto que si se detecta en la etapa de análisis. Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones de los sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

El siguiente cuestionario se presenta como ejemplo para la evaluación del diseño y prueba de los sistemas:

1. ¿Quiénes intervienen al diseñar un sistema?

- Usuario.
- Analista.
- Programadores.
- Operadores.
- Gerente de departamento.
- Auditores internos.
- Asesores.
- Otros.

2. ¿Los analistas son también programadores?

SÍ ( ) NO ( )

3. ¿Qué lenguaje o lenguajes conocen los analistas?
4. ¿Cuántos analistas hay y qué experiencia tienen?
5. ¿Qué lenguaje conocen los programadores?
6. ¿Cómo se controla el trabajo de los analistas?
7. ¿Cómo se controla el trabajo de los programadores?
8. Indique qué pasos siguen los programadores en el desarrollo de un programa:

- Estudio de la definición ( )
- Discusión con el analista ( )
- Diagrama de bloques ( )
- Tabla de decisiones ( )
- Prueba de escritorio ( )
- Codificación ( )
- ¿Es enviado a captura o los programadores capturan? ( )
- ¿Quién los captura? \_\_\_\_\_
- Compilación ( )
- Elaborar datos de prueba ( )
- Solicitar datos al analista ( )
- Correr programas con datos ( )
- Revisión de resultados ( )
- Corrección del programa ( )
- Documentar el programa ( )
- Someter resultados de prueba ( )
- Entrega del programa ( )

9. ¿Qué documentación acompaña al programa cuando se entrega?

Difícilmente se controla realmente el flujo de la información de un sistema que desde su inicio ha sido mal analizado, mal diseñado, mal programado e incluso mal documentado. El excesivo mantenimiento de los sistemas generalmente ocasionado por un mal desarrollo, se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del mismo, sin que se haya establecido un plan de prueba del sistema para medir su grado de confiabilidad en la operación que efectuará. Para verificar si existe esta situación, se debe pedir a los analistas y a los programadores las actividades que están desarrollando en el momento de la auditoría y evaluar si están efectuando actividades de mantenimiento o de realización de nuevos proyectos. En ambos casos se deberá evaluar el tiempo que llevan dentro del mismo sistema, la prioridad que se le asignó y cómo está en el tiempo real en relación al tiempo estimado en el plan maestro.

## INSTRUCTIVOS DE OPERACIÓN

---

Se debe evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación, y el contenido mínimo de los instructivos de operación se puedan verificar mediante el siguiente cuestionario.

El instructivo de operación deberá comprender:

- Diagrama de flujo por cada programa. ( )

- ✚ Diagrama particular de entrada/salida ( )
- ✚ Mensaje y su explicación ( )
- ✚ Parámetros y su explicación ( )
- ✚ Diseño de impresión de resultados ( )
- ✚ Cifras de control ( )
- ✚ Fórmulas de verificación ( )
- ✚ Observaciones ( )
- ✚ Instrucciones en caso de error ( )
- ✚ Calendario de proceso y resultados ( )

## FORMA DE IMPLEMENTACIÓN

---

La finalidad de evaluar los trabajos que se realizan para iniciar la operación de un sistema, esto es, la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema etc.

Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:

Prueba particular de cada programa ( )

Prueba por fase validación, actualización ( )

Prueba integral del paralelo ( )

Prueba en paralelo sistema ( )

Otros (especificar)\_\_\_\_\_

## ENTREVISTA A USUARIOS

---

La entrevista se deberá llevar a cabo para comprobar datos proporcionados y la situación de la dependencia en el departamento de Sistemas de Información.

Su objeto es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y de los sistemas en operación.

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de los usuarios, tanto de los más importantes como de los de menor importancia, en cuanto al uso del equipo.

Desde el punto de vista del usuario los sistemas deben:

- ✚ Cumplir con los requerimientos totales del usuario.
- ✚ Cubrir todos los controles necesarios.
- ✚ No exceder las estimaciones del presupuesto inicial.
- ✚ Serán fácilmente modificables.

Para que un sistema cumpla con los requerimientos del usuario, se necesita una comunicación completa entre usuarios y responsable del desarrollo del sistema.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por la computadora, estableciéndose los riesgos de la misma y la forma de minimizarlos.

Para ello se debieron definir los controles adecuados, estableciéndose además los niveles de acceso a la información, es decir, quién tiene privilegios de consulta, modificar o incluso borrar información.

Esta etapa habrá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en informática, para comprobar que se logro una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información. Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información.

- ✚ Descripción de los servicios prestados.
- ✚ Criterios de evaluación que utilizan los usuarios para evaluar el nivel del servicio prestado.
- ✚ Reporte periódico del uso y concepto del usuario sobre el servicio.
- ✚ Registro de los requerimientos planteados por el usuario.

Con esta información se puede comenzar a realizar la entrevista para determinar si los servicios proporcionados y planeados por la dirección de Informática cubren las necesidades de información de las dependencias.

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?

Si ( ) No ( )

¿Por que?

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?

Deficiente ( )

Aceptable ( )

Satisfactorio ( )

Excelente ( )

¿Por que?

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?

No las cubre ( )

Parcialmente ( )

La mayor parte ( )

Todas ( )

¿Por que?

4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?

Generalmente no existe ( )

Hay ocasionalmente ( )

Regularmente ( )

Siempre ( )

¿Por que?



5. ¿Son entregados con puntualidad los trabajos?  
 Nunca ( )  
 Rara vez ( )  
 Ocasionalmente ( )  
 Generalmente ( )  
 Siempre ( )  
 ¿Por que?
6. ¿Que piensa de la presentación de los trabajadores solicitados al departamento de cómputo?  
 Deficiente ( )  
 Aceptable ( )  
 Satisfactorio ( )  
 Excelente ( )  
 ¿Por que?
7. ¿Que piensa de la asesoría que se imparte sobre informática?  
 No se proporciona ( )  
 Es insuficiente ( )  
 Satisfactoria ( )  
 Excelente ( )  
 ¿Por que?
8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza?  
 Nula ( )  
 Riesgosa ( )  
 Satisfactoria ( )  
 Excelente ( )  
 Lo desconoce ( )  
 ¿Por que?
9. ¿Existen fallas de exactitud en los procesos de información?  
 ¿Cuáles?
10. ¿Cómo utiliza los reportes que se le proporcionan?
11. ¿Cuáles no Utiliza?
12. De aquellos que no utiliza ¿por que razón los recibe?
13. ¿Que sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte?
14. ¿Se cuenta con un manual de usuario por Sistema?  
 SI ( ) NO ( )
15. ¿Es claro y objetivo el manual del usuario?  
 SI ( ) NO ( )
16. ¿Que opinión tiene el manual?
- NOTA: Pida el manual del usuario para evaluarlo.
17. ¿Quién interviene de su departamento en el diseño de sistemas?
18. ¿Que sistemas desearía que se incluyeran?
19. Observaciones:

## CONTROLES





---

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

- a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.
- b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.
- c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.
- d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

### CONTROL DE LOS DATOS FUENTE Y MANEJO CIFRAS DE CONTROL

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al:

-  Suprimir u omitir datos.
-  Adicionar datos.
-  Alterar datos.
-  Duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que solo puede hacer todos lo anterior y además puede realizar bajas.

NOTA: Debido a que se denomina de diferentes formas la actividad de transcribir la información del dato fuente a la computadora, en el presente trabajo se le denominará captura o captación considerándola como sinónimo de digitalizar (capturista, digitalizadora).

Lo primero que se debe evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, para lo cual se puede utilizar el siguiente cuestionario:

1. Indique el porcentaje de datos que se reciben en el área de captación
2. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:  
Número de folio ( ) Número(s) de formato(s) ( )  
Fecha y hora de Nombre, Depto. ( )  
Recepción ( ) Usuario ( )  
Nombre del documento ( ) Nombre responsable ( )  
Volumen aproximado Clave de cargo  
de registro ( ) (Número de cuenta) ( )  
Número de registros ( ) Fecha y hora de entrega de  
Clave del capturista ( ) documentos y registros captados ( )  
Fecha estimada de entrega ( )
3. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:  
Firmas de autorización ( )  
Recepción de trabajos ( ) Control de trabajos atrasados ( )  
Revisión del documento ( ) Avance de trabajos ( )  
fuente (legibilidad, verificación de datos completos, etc.) ( )  
Prioridades de captación ( ) Errores por trabajo ( )  
Producción de trabajo ( ) Corrección de errores ( )  
Producción de cada operador ( ) Entrega de trabajos ( )  
Verificación de cifras Costo Mensual por trabajo ( )  
de control de entrada con las de salida. ( )
4. ¿Existe un programa de trabajo de captación de datos?
  - a) ¿Se elabora ese programa para cada turno?  
Diariamente ( )  
Semanalmente ( )  
Mensualmente ( )
  - b) La elaboración del programa de trabajos se hace:  
Internamente ( )  
Se les señalan a los usuarios las prioridades ( )
  - c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?
5. ¿Quién controla las entradas de documentos fuente?
6. ¿En que forma las controla?
7. ¿Que cifras de control se obtienen?  
Sistema Cifras que se Observaciones  
Obtienen
8. ¿Que documento de entrada se tienen?  
Sistemas Documentos Depto. que periodicidad Observaciones  
proporciona  
el documento
9. ¿Se anota que persona recibe la información y su volumen?  
SI NO
10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?  
SI NO

11. ¿Se verifica la cantidad de la información recibida para su captura?  
SI NO
  12. ¿Se revisan las cifras de control antes de enviarlas a captura?  
SI NO
  13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?  
SI NO
  14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?
  15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?
  16. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?
  17. ¿Existe un registro de anomalías en la información debido a mala codificación?
  18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?
  19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?
  20. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?
- 
21. ¿Se controlan separadamente los documentos confidenciales?
- 
22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?
- 
23. ¿Existe un registro de los documentos que entran a capturar?
- 
24. ¿Se hace un reporte diario, semanal o mensual de captura?
- 
25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?
  26. ¿Se lleva un control de la producción por persona?
  27. ¿Quién revisa este control?
  28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

### CONTROL DE OPERACIÓN

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de computo?  
SI ( ) NO ( )
2. ¿Están actualizados los procedimientos?  
SI ( ) NO ( )

3. Indique la periodicidad de la actualización de los procedimientos:

Semestral ( )

Anual ( )

Cada vez que haya cambio de equipo ( )

4. Indique el contenido de los instructivos de operación para cada aplicación:

Identificación del sistema ( )

Identificación del programa ( )

Periodicidad y duración de la corrida ( )

Especificación de formas especiales ( )

Especificación de cintas de impresoras ( )

Etiquetas de archivos de salida, nombre, ( )

archivo lógico, y fechas de creación y expiración

Instructivo sobre materiales de entrada y salida ( )

Altos programados y la acciones requeridas ( )

Instructivos específicos

a los operadores en caso de falla del equipo ( )

Instructivos de reinicio ( )

Procedimientos de recuperación para proceso de

gran duración o criterios ( )

Identificación de todos los

dispositivos de la máquina a ser usados ( )

Especificaciones de resultados

(cifras de control, registros de salida por archivo, etc. ) ( )

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?

SI ( ) NO ( )

6. ¿Son suficientemente claras para los operadores estas órdenes?

SI ( ) NO ( )

7. ¿Existe una estandarización de las ordenes de proceso?

SI ( ) NO ( )

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.

SI ( ) NO ( )

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?

Primero que entra, primero que sale ( )

se respetan las prioridades, ( )

Otra (especifique) ( )

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?

SI ( ) NO ( )

11. ¿Quién revisa este reporte en su caso?

12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

14. ¿Cómo se actúa en caso de errores?

15. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes?

16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?
17. ¿Puede el operador modificar los datos de entrada?
18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?
19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?
20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?
21. ¿Las intervenciones de los operadores:  
 Son muy numerosas? SI ( ) NO ( )  
 Se limitan los mensajes esenciales? SI ( ) NO ( )  
 Otras (especifique) \_\_\_\_\_
22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?  
 SI ( ) NO ( )
23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?
24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?  
 SI ( ) NO ( )
25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?  
 Si ( )  
 por máquina ( )  
 escrita manualmente ( )  
 NO ( )
26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.
27. ¿Existen procedimientos para evitar las corridas de programas no autorizados?  
 SI ( ) NO ( )
28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.
29. Verificar que sea razonable el plan para coordinar el cambio de turno.
30. ¿Se hacen inspecciones periódicas de muestreo?  
 SI ( ) NO ( )
31. Enuncie los procedimientos mencionados en el inciso anterior:
32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?  
 SI ( ) NO ( )
33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?  
 SI ( ) NO ( )  
 ¿Cómo? \_\_\_\_\_
34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.
35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?  
 SI ( ) NO ( )

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?  
SI ( ) NO ( )
37. ¿Durante cuanto tiempo?
38. ¿Que precauciones se toman durante el periodo de implantación?
39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.
40. ¿Se catalogan los programas liberados para producción rutinaria?  
SI ( ) NO ( )
41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.
42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.
43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?  
SI ( ) NO ( )
44. Indique como está organizado este archivo de bitácora.
- Por fecha ( )
  - Por fecha y hora ( )
  - Por turno de operación ( )
  - Otros ( )
45. ¿Cuál es la utilización sistemática de las bitácoras?
46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?
47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.
48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?  
SI ( ) NO ( )
49. ¿Cómo se controlan los procesos en línea?
50. ¿Se tienen seguros sobre todos los equipos?  
SI ( ) NO ( )
51. ¿Conque compañía?  
Solicitar pólizas de seguros y verificar tipo de seguro y montos.
52. ¿Cómo se controlan las llaves de acceso (Password)?.

### CONTROLES DE SALIDA

1. ¿Se tienen copias de los archivos en otros locales?
2. ¿Dónde se encuentran esos locales?
3. ¿Que seguridad física se tiene en esos locales?
4. ¿Que confidencialidad se tiene en esos locales?
5. ¿Quién entrega los documentos de salida?
6. ¿En que forma se entregan?
7. ¿Que documentos?
8. ¿Que controles se tienen?
9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

10. ¿Se destruye la información utilizada, o bien que se hace con ella?

Destruye ( ) Vende ( ) Tira ( ) Otro \_\_\_\_\_

## CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas. Además se deben tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

## CONTROL DE ALMACENAMIENTO MASIVO

### OBJETIVOS

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:

Aire acondicionado ( )

Protección contra el fuego ( )

(señalar que tipo de protección) \_\_\_\_\_

Cerradura especial ( )

Otra

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?

SI ( ) NO ( )

(señalar de que tipo) \_\_\_\_\_

3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?

Número de serie o carrete ( )

Número o clave del usuario ( )

Número del archivo lógico ( )

Nombre del sistema que lo genera ( )

Fecha de expiración del archivo ( )

Fecha de expiración del archivo ( )

Número de volumen ( )

Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?

SI ( ) NO ( )



6. ¿Que tan frecuentes son estas discrepancias?

---

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI ( ) NO ( )

¿Cómo?

---

9. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

Otro (especifique) \_\_\_\_\_

11. Este almacén esta situado:

En el mismo edificio del departamento ( )

En otro lugar ( )

¿Cual?

---

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI ( ) NO ( )

15. ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?

SI ( ) NO ( )

16. ¿Se realizan auditorías periódicas a los medios de almacenamiento?

SI ( ) NO ( )

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI ( ) NO ( )

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?

SI ( ) NO ( )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI ( ) NO ( )

21. ¿Se lleva control sobre los archivos prestados por la instalación?

SI ( ) NO ( )

22. En caso de préstamo ¿Con que información se documentan?

Nombre de la institución a quien se hace el préstamo.

✚ Fecha de recepción ( )

✚ Fecha en que se debe devolver ( )

✚ Archivos que contiene ( )

- Formatos ( )
- Cifras de control ( )
- Código de grabación ( )
- Nombre del responsable que los presto ( )
- Otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?

SI ( ) NO ( )

26. ¿La operación de reemplazo es controlada por el cintotecario?

SI ( ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

SI ( ) NO ( )

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?

SI ( ) NO ( )

29. ¿Estos procedimientos los conocen los operadores?

SI ( ) NO ( )

30. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL ( ) ANUAL ( )

SEMESTRAL ( ) OTRA ( )

31. ¿Existe un responsable en caso de falla?

SI ( ) NO ( )

32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?

SI ( ) NO ( )

34. ¿Lo conoce y lo sigue el cintotecario?

SI ( ) NO ( )

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO ( )

¿Con qué frecuencia?

## CONTROL DE MANTENIMIENTO

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente mas caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es “por llamada”, en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como “en banco”, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cual de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).
2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo?  
SI ( ) NO ( )
3. ¿Se lleva a cabo tal programa?  
SI ( ) NO ( )
4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?  
SI ( ) NO ( )
5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?  
SI ( ) NO ( )
6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-  
SI ( ) NO ( )  
¿Cual?
8. ¿Cómo se notifican las fallas?
9. ¿Cómo se les da seguimiento?

## CAPÍTULO V

### SEGURIDAD EN CENTROS DE CÓMPUTO

#### ORDEN EN EL CENTRO DE CÓMPUTO

---

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:  
Semanalmente ( ) Quincenalmente ( )  
Mensualmente ( ) Bimestralmente ( )  
No hay programa ( ) Otra (especifique) ( )
2. Existe un lugar asignado a las cintas y discos magnéticos?  
SI ( ) NO ( )
3. ¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo?  
SI ( ) NO ( )
4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?  
SI ( ) NO ( )
5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?  
SI ( ) NO ( )
6. Indique la periodicidad con que se limpian las unidades de cinta:  
Al cambio de turno ( ) cada semana ( )  
cada día ( ) otra (especificar) ( )
7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?  
SI ( ) NO ( )
8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?  
SI ( ) NO ( )
9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?  
SI ( ) NO ( )
10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

## EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO

---

Los objetivos son evaluar la configuración actual tomando en consideración las aplicaciones y el nivel de uso del sistema, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las políticas seguidas por la unidad de informática en la conservación de su programoteca.

Esta sección esta orientada a:

- a) Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual o de comparar la capacidad instalada con los planes de desarrollo a mediano y largo plazo.
- b) Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.
- c) Evaluar la utilización de los diferentes dispositivos periféricos.

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo?

¿Con poco uso? SI ( ) NO ( )

¿Ocioso? SI ( ) NO ( )

¿Con capacidad superior a la necesaria? SI ( ) NO ( )

Describe cual es \_\_\_\_\_

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro mas lento y de menor costo?

SI ( ) NO ( )

3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado?

SI ( ) NO ( )

4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado.

---

5. ¿El sistema de cómputo tiene capacidad de teleproceso?

SI ( ) NO ( )

6. ¿Se utiliza la capacidad de teleproceso?

SI ( ) NO ( )

7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso?

SI ( ) NO ( )

8. ¿Cuántas terminales se tienen conectadas al sistema de cómputo?

9. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?

SI ( ) NO ( )

10. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente

para atender el proceso por lotes y el proceso remoto?

SI ( ) NO ( )

## SEGURIDAD LÓGICA Y CONFIDENCIAL

---

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado "“virus” de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

- ✚ Elementos administrativos
- ✚ Definición de una política de seguridad
- ✚ Organización y división de responsabilidades
- ✚ Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- ✚ Prácticas de seguridad del personal
- ✚ Elementos técnicos y procedimientos
- ✚ Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- ✚ Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- ✚ El papel de los auditores, tanto internos como externos
- ✚ Planeación de programas de desastre y su prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- ✚ Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- ✚ Identificar aquellas aplicaciones que tengan un alto riesgo.
- ✚ Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- ✚ Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- ✚ La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo, se debe preguntar lo siguiente:
  - Que sucedería si no se puede usar el sistema?
  - Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riesgo.
- ✚ La siguiente pregunta es:
  - ¿Que implicaciones tiene el que no se obtenga el sistema y cuanto tiempo podríamos estar sin utilizarlo?
  - ¿Existe un procedimiento alternativo y que problemas nos ocasionaría?
  - ¿Que se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medidas preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

Hay que tener mucho cuidado con la información que sale de la oficina, su utilización y que sea borrada al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

- ✚ Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.
- ✚ Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.
- ✚ Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- ✚ Especificar la aplicación, los programas y archivos.
- ✚ Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- ✚ Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.

- ✚ En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.
  - El personal que prepara la información no debe tener acceso a la operación.
  - Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.
  - Los operadores no deben tener acceso restringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.
  - Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

## **SEGURIDAD FÍSICA**

---

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Entre las precauciones que se deben revisar están:

- ✚ Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- ✚ En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- ✚ En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.
- ✚ Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- ✚ Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- ✚ También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- ✚ Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
- ✚ Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.



Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?  
SI ( ) NO ( )
2. ¿Existen una persona responsable de la seguridad?  
SI ( ) NO ( )
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?  
SI ( ) NO ( )
4. ¿Existe personal de vigilancia en la institución?  
SI ( ) NO ( )
5. ¿La vigilancia se contrata?
  - a) Directamente ( )
  - b) Por medio de empresas que venden ese servicio ( )
6. ¿Existe una clara definición de funciones entre los puestos clave?  
SI ( ) NO ( )
7. ¿Se investiga a los vigilantes cuando son contratados directamente?  
SI ( ) NO ( )
8. ¿Se controla el trabajo fuera de horario?  
SI ( ) NO ( )
9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.  
SI ( ) NO ( )
10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?  
SI ( ) NO ( )
11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
  - a) Vigilante? ( )
  - b) Recepcionista? ( )
  - c) Tarjeta de control de acceso ? ( )
  - d) Nadie? ( )
12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?  
SI ( ) NO ( )
13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?  
SI ( ) NO ( )
14. El edificio donde se encuentra la computadora esta situado a salvo de:
  - a) Inundación? ( )
  - b) Terremoto? ( )
  - c) Fuego? ( )
  - d) Sabotaje? ( )
15. El centro de cómputo tiene salida al exterior al exterior?  
SI ( ) NO ( )
16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.
17. ¿Existe control en el acceso a este cuarto?
  - a) Por identificación personal? ( )
  - b) Por tarjeta magnética? ( )

- c) por claves verbales? ( )  
d) Otras? ( )
18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?  
SI ( ) NO ( )
19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?  
SI ( ) NO ( )
20. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?  
SI ( ) NO ( )
21. ¿Existe alarma para
- a) Detectar fuego (calor o humo) en forma automática? ( )  
b) Avisar en forma manual la presencia del fuego? ( )  
c) Detectar una fuga de agua? ( )  
d) Detectar magnéticos? ( )  
e) No existe ( )
22. ¿Estas alarmas están
- a) En el departamento de cómputo? ( )  
b) En la cintoteca y discoteca? ( )
23. ¿Existe alarma para detectar condiciones anormales del ambiente?
- a) En el departamento de cómputo? ( )  
b) En la cintoteca y discoteca? ( )  
c) En otros lados ( )
24. ¿La alarma es perfectamente audible?  
SI ( ) NO ( )
25. ¿Esta alarma también está conectada
- a) Al puesto de guardias? ( )  
b) A la estación de Bomberos? ( )  
c) A ningún otro lado? ( )
- Otro \_\_\_\_\_
26. Existen extintores de fuego
- a) Manuales? ( )  
b) Automáticos? ( )  
c) No existen ( )
27. ¿Se ha adiestrado el personal en el manejo de los extintores?  
SI ( ) NO ( )
28. ¿Los extintores, manuales o automáticos a base de TIPO SI NO
- a) Agua, ( ) ( )  
b) Gas? ( ) ( )  
c) Otros ( ) ( )
29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?  
SI ( ) NO ( )
30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?  
SI ( ) NO ( )

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause mas daño que el fuego?  
SI ( ) NO ( )
32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego?  
SI ( ) NO ( )
33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
- Corte la acción de los extintores por tratarse de falsas alarmas? SI ( ) NO ( )
  - Pueda cortar la energía Eléctrica SI ( ) NO ( )
  - Pueda abandonar el local sin peligro de intoxicación SI ( ) NO ( )
  - Es inmediata su acción? SI ( ) NO ( )
34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?  
SI ( ) NO ( )
35. ¿Sabes que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?  
SI ( ) NO ( )
36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?  
SI ( ) NO ( )
37. ¿Existe salida de emergencia?  
SI ( ) NO ( )
38. ¿Esta puerta solo es posible abrirla:
- Desde el interior ? ( )
  - Desde el exterior ? ( )
  - Ambos Lados ( )
39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?  
SI ( ) NO ( )
40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?  
SI ( ) NO ( )
41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
- Evitando artículos inflamables en el departamento de cómputo? ( )
  - Prohibiendo fumar a los operadores en el interior? ( )
  - Vigilando y manteniendo el sistema eléctrico? ( )
  - No se ha previsto ( )
42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?  
SI ( ) NO ( )
43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?  
SI ( ) NO ( )

44. ¿Se controla el acceso y préstamo en la
- Discoteca? ( )
  - Cintoteca? ( )
  - Programoteca? ( )
45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.
46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?  
SI ( ) NO ( )
47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.
48. ¿Se tienen establecidos procedimientos de actualización a estas copias?  
SI ( ) NO ( )
49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:  
0 1 2 3
50. ¿Existe departamento de auditoria interna en la institución?  
SI ( ) NO ( )
51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?  
SI ( ) NO ( )
52. ¿Que tipos de controles ha propuesto?
53. ¿Se cumplen?  
SI ( ) NO ( )
54. ¿Se auditan los sistemas en operación?  
SI ( ) NO ( )
55. ¿Con que frecuencia?
- Cada seis meses ( )
  - Cada año ( )
  - Otra (especifique) ( )
56. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
- Usuario ( )
  - Director de informática ( )
  - Jefe de análisis y programación ( )
  - Programador ( )
  - Otras ( especifique) \_\_\_\_\_
57. ¿La solicitud de modificaciones a los programas se hacen en forma?
- Oral? ( )
  - Escrita? ( )
- En caso de ser escrita solicite formatos,
58. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?  
SI ( ) NO ( )
59. ¿Existe control estricto en las modificaciones?  
SI ( ) NO ( )
60. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?  
SI ( ) NO ( )
61. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?  
SI ( ) NO ( )
62. Se verifica identificación:
- De la terminal ( )

- b) Del Usuario ( )
- c) No se pide identificación ( )
- 63.¿Se ha establecido que información puede ser acezada y por qué persona?  
SI ( ) NO ( )
- 64.¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?  
SI ( ) NO ( )
- 65.¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?  
SI ( ) NO ( )
- 66.¿Existen controles y medidas de seguridad sobre las siguientes operaciones?  
¿Cuales son?
- ( )Recepción de documentos\_\_\_\_\_
  - ( )Información Confidencial\_\_\_\_\_
  - ( )Captación de documentos\_\_\_\_\_
  - ( )Cómputo Electrónico\_\_\_\_\_
  - ( )Programas\_\_\_\_\_
  - ( )Discotecas y Cintotecas\_\_\_\_\_
  - ( )Documentos de Salida\_\_\_\_\_
  - ( )Archivos Magnéticos\_\_\_\_\_
  - ( )Operación del equipo de computación\_\_\_\_\_
  - ( )En cuanto al acceso de personal\_\_\_\_\_
  - ( )Identificación del personal\_\_\_\_\_
  - ( )Policia\_\_\_\_\_
  - ( )Seguros contra robo e incendio\_\_\_\_\_
  - ( )Cajas de seguridad\_\_\_\_\_
  - ( )Otras (especifique)\_\_\_\_\_

## SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

---

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

- 1) Se debe restringir el acceso a los programas y a los archivos.
- 2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
- 3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
- 4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
- 5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
- 6) Se deben monitorear periódicamente el uso que se le está dando a las terminales.
- 7) Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.

9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.

10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).

11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.

12) Se debe tener un estricto control sobre el acceso físico a los archivos.

13) En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.

2) Sólo el personal autorizado debe tener acceso a la información confidencial.

3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.

4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- ✚ Equipo, programas y archivos
- ✚ Control de aplicaciones por terminal
- ✚ Definir una estrategia de seguridad de la red y de respaldos
- ✚ Requerimientos físicos.
- ✚ Estándar de archivos.
- ✚ Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

## **SEGURIDAD AL RESTAURAR EL EQUIPO**

---

En un mundo que depende cada día mas de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la

originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo mas rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro.

Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

- ✚ En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
- ✚ Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
- ✚ El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de él reanudar el proceso.
- ✚ Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.
- ✚ Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo.

1) ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?

SI ( ) NO ( )

2) ¿Enuncie los procedimientos mencionados en el inciso anterior?

3) ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?

SI ( ) NO ( )

En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:

1) Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.

2) Los nuevos sistemas deben estar adecuadamente documentados y probados.

3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

## **PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE**

---

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.

Los desastres que pueden suceder podemos clasificar así:

a) Completa destrucción del centro de cómputo,

b) Destrucción parcial del centro de cómputo,

c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)



- d) Destrucción parcial o total de los equipos descentralizados
- e) Pérdida total o parcial de información, manuales o documentación
- f) Pérdida del personal clave
- g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- ✚ La documentación de programación y de operación.
- ✚ Los equipos:
  - El equipo completo
  - El ambiente de los equipos
  - Datos y archivos
  - Papelería y equipo accesorio
  - Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- ✚ Asegurarse de que todos los miembros sean notificados,
- ✚ Informar al director de informática,
- ✚ Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.
- ✚ Determinar el estado de todos los sistemas en proceso,
- ✚ Notificar a los proveedores del equipo cual fue el daño,
- ✚ Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:
  - Elaboración de una lista con los métodos disponibles para realizar la recuperación
  - Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
  - Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
  - Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- ✚ Posponer las aplicaciones de prioridad más baja,
- ✚ Cambiar la frecuencia del proceso de trabajos.
- ✚ Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc. a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- ✚ Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- ✚ Se debe tener documentados los cambios de software.
- ✚ En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- ✚ Configuración de equipos.
- ✚ Configuración de equipos de captación de datos.
- ✚ Sistemas operativos.
- ✚ Configuración de equipos periféricos.

- ✚ Ver anexos al final del documento.

## CAPÍTULO VI

### ESTÁNDARES INTERNACIONALES PARA TECNOLOGÍAS DE LA INFORMACIÓN

---

COBIT es en realidad un acrónimo formado por las siglas derivadas de Control Objectives for Information and Related Technology (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas).

Ahora COBIT es:

Governance indica que el Cobit también incluye directrices gerenciales

Control and

Audit for

Information and

Related Technology (Control y Auditoría para Información y Tecnología Relacionada.)

#### Misión:

Investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnología de información generalmente aceptados para el uso cotidiano de gerentes de empresa y auditores (Fig. 3.)

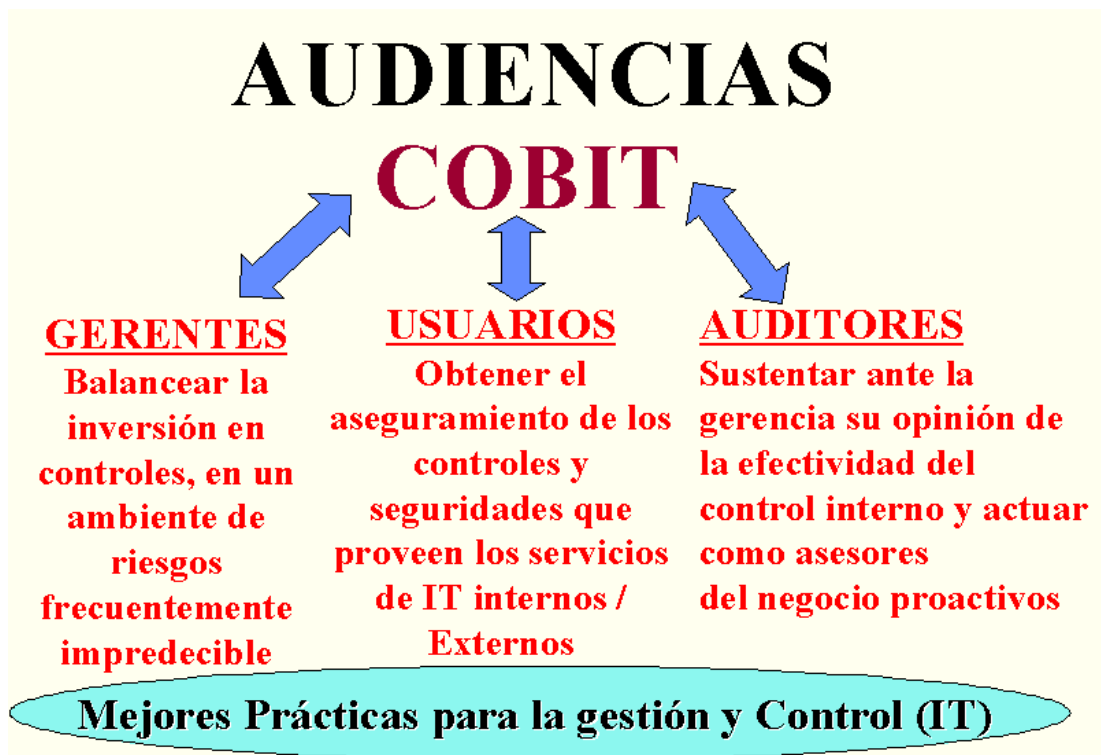


Fig. 3.

La figura 4 nos muestra **los componentes de COBIT**:

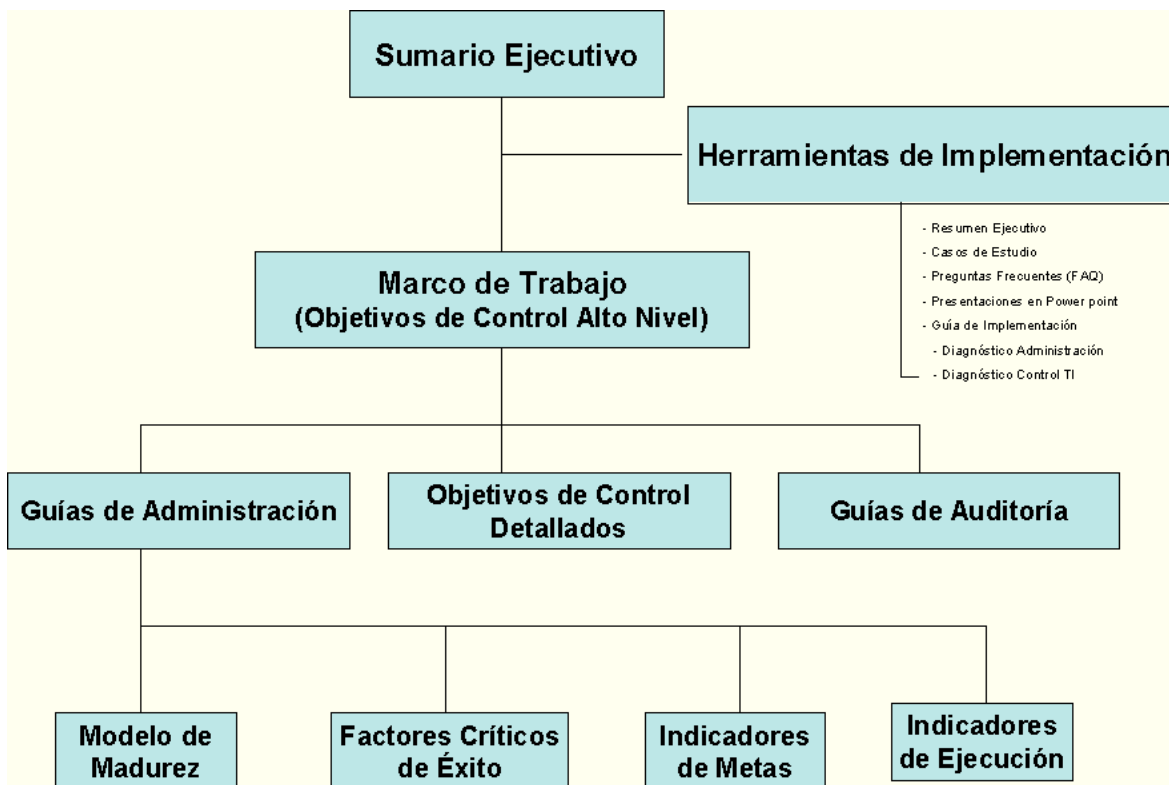


Fig. 4.

#### 1. Marco Referencial (Fig. 5)

El concepto fundamental del marco referencial de COBIT, se refiere a:

- ✚ El enfoque de control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio.
- ✚ La Información es el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

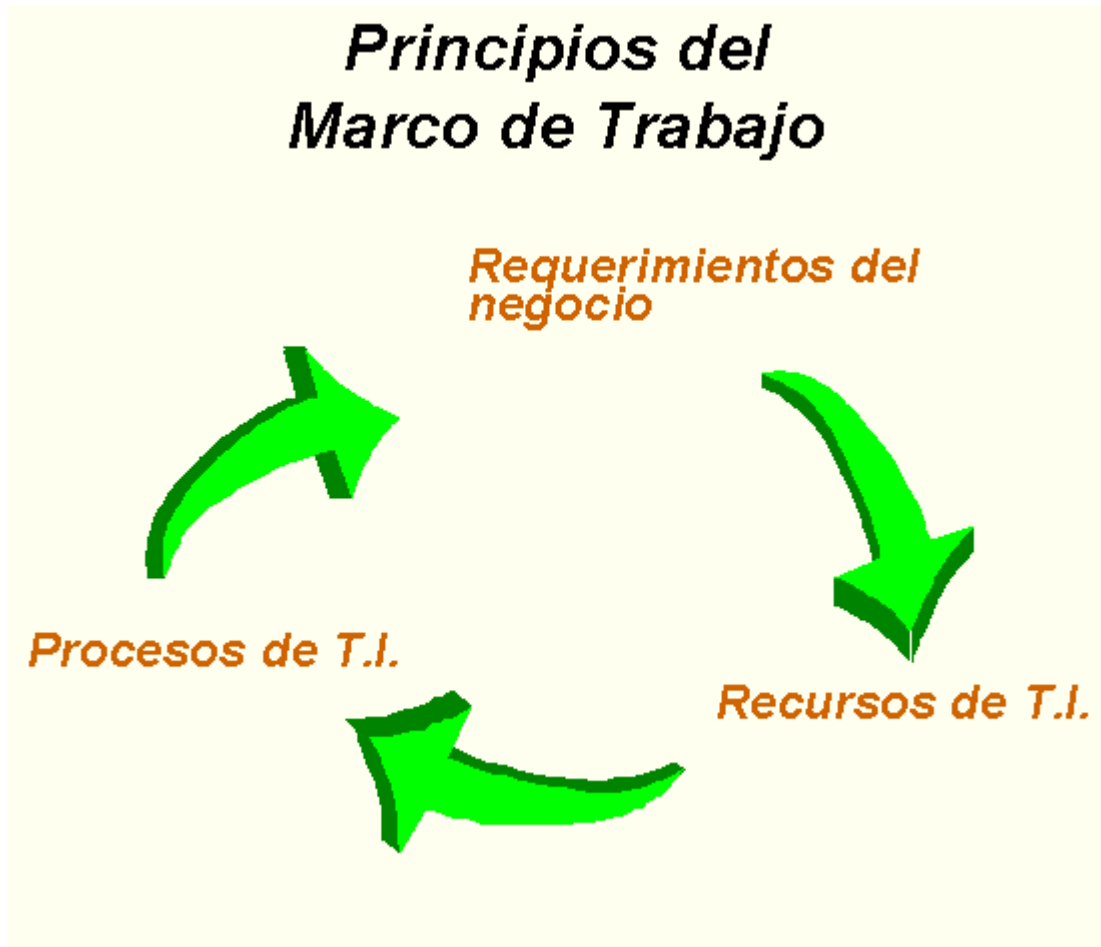


Fig. 5.

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que Cobit hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, Cobit combina principios contenidos en modelos referenciales existentes y conocidos (Fig. 6):

**REQUERIMIENTO DE CALIDAD:** Calidad, Costo, Entrega de Servicio.

**REQUERIMIENTOS FIDUCIARIOS (COSO):** Efectividad y Eficiencia de Operaciones, Confiabilidad de la Información, Cumplimiento de las Leyes y Regulaciones.

**REQUERIMIENTOS DE SEGURIDAD:** Confidencialidad, Integridad, Disponibilidad.

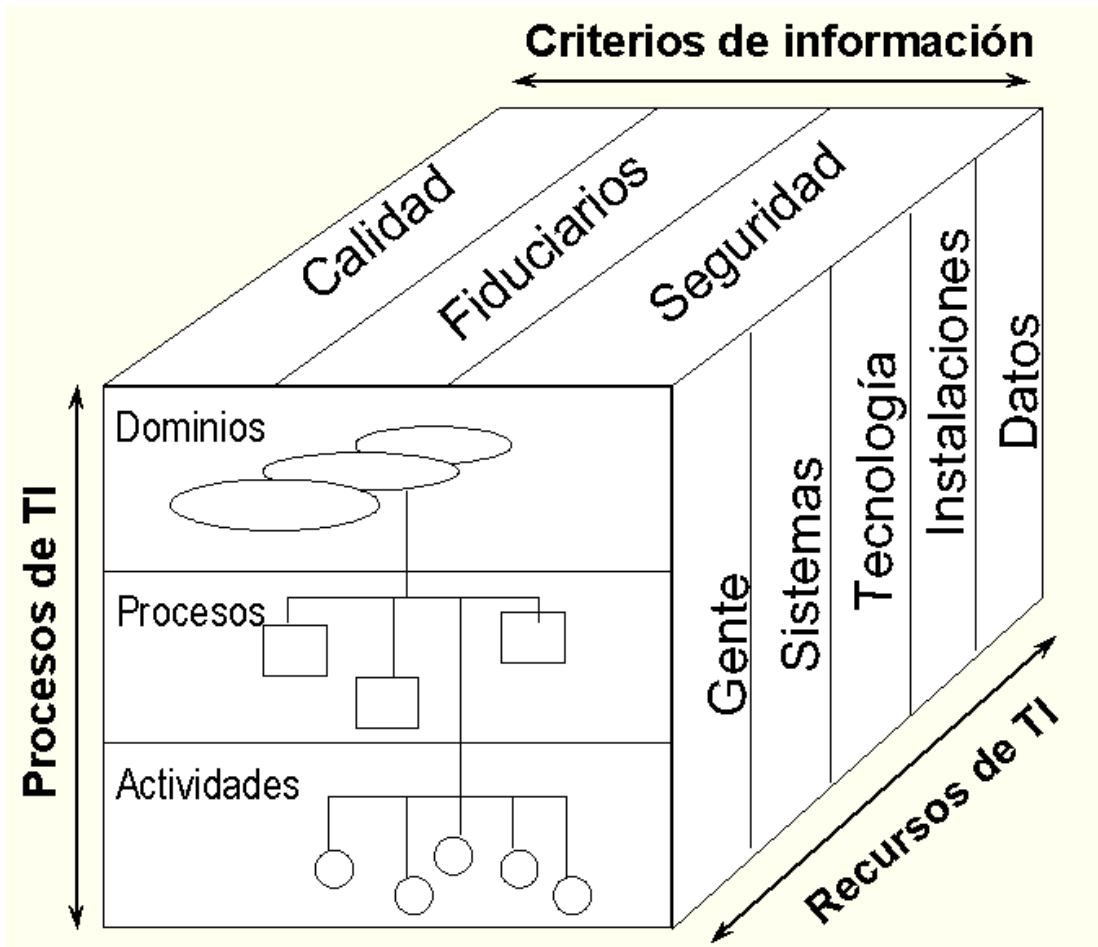


Fig. 6.

Estructura de COBIT (Fig. 7):

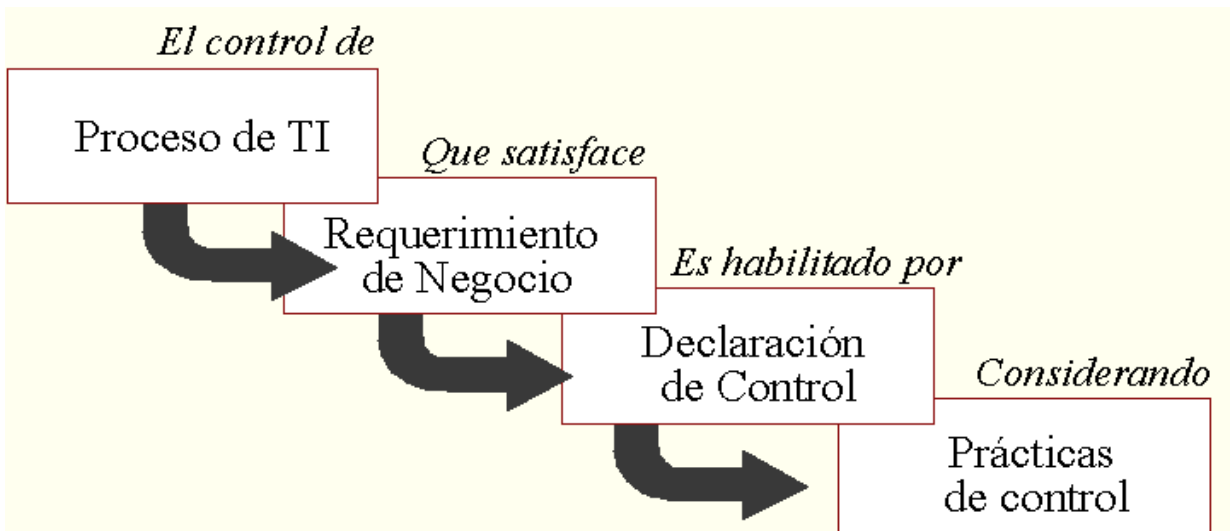


Fig. 7.

## **Información**

- **Efectividad:** La información relevante y pertinente al proceso de negocio existe y es entregada a tiempo, correcta, consistente y de una manera usable.
- **Eficiencia:** Relativo a la entrega de información a través del óptimo (más productivo y económico) uso de los recursos.
- **Confidencialidad:** Relativo a la protección de información sensitiva de acceso y divulgación no autorizada.
- **Integridad:** Relativo a la exactitud y completitud de la información así como a su validez de acuerdo con el conjunto de valores y expectativas del negocio.
- **Disponibilidad:** Relativo a que la información debe estar disponible cuando es requerida por el proceso de negocio y por lo tanto también relativo a la salvaguarda de recursos.
- **Cumplimiento:** relativo al cumplimiento de leyes, regulaciones y acuerdos contractuales los cuales el proceso de negocio debe cumplir.
- **Confiabilidad:** Relativo a que los sistemas proveen a: la gerencia con la información apropiada para ser usada en la operación de la empresa; reportes a los usuarios de la información financiera e información a los organismos reguladores en cumplimiento de leyes y regulaciones.

## **Recursos Tecnología de la Información**

- **Datos** usados en el sentido más amplio (externos e internos, estructurados y no estructurados, gráficos, sonidos, etc.)
- **Sistemas Aplicativos** es entendido como la suma de los procedimientos manuales y de los procedimientos automatizados.
- **Tecnología** se refiere a hardware, Sistemas operativos, Bases de Datos, Sistemas de administración, redes, multimedia.
- **Instalaciones** lugar usado para el propósito de TI. Recursos para albergar y apoyar los sistemas de información.
- **Gente** habilidades, conocimientos y productividad para planear, organizar, adquirir, entregar, mantener y monitorear los sistemas de información y servicios.

## **Dominios**

Se muestran a continuación en las figuras 8, 9, y 10:

## Como se relacionan

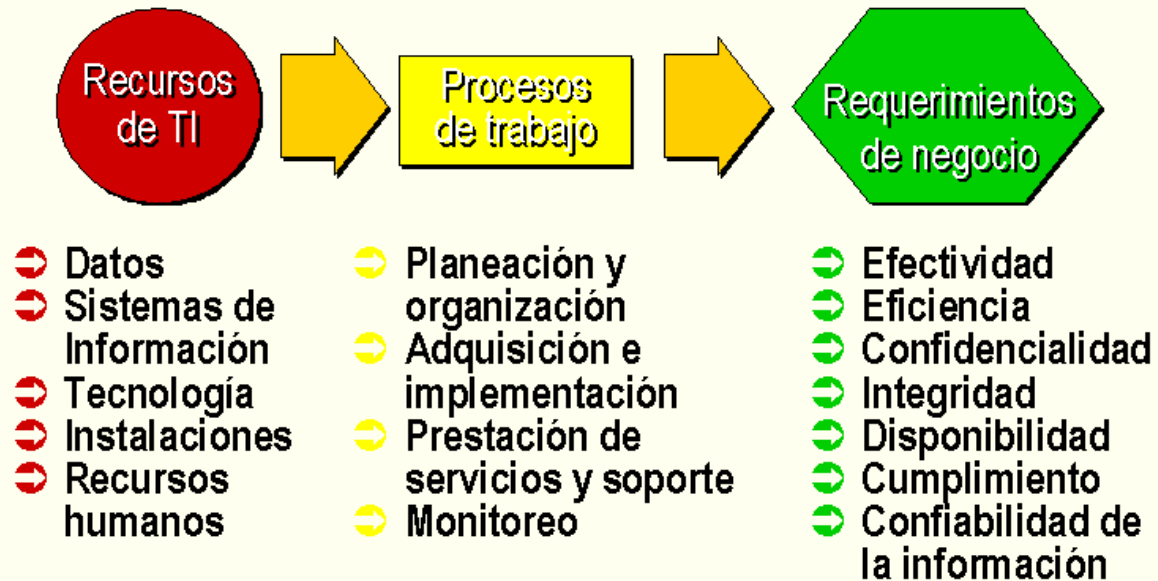


Fig. 8.

## Principios de la Infraestructura

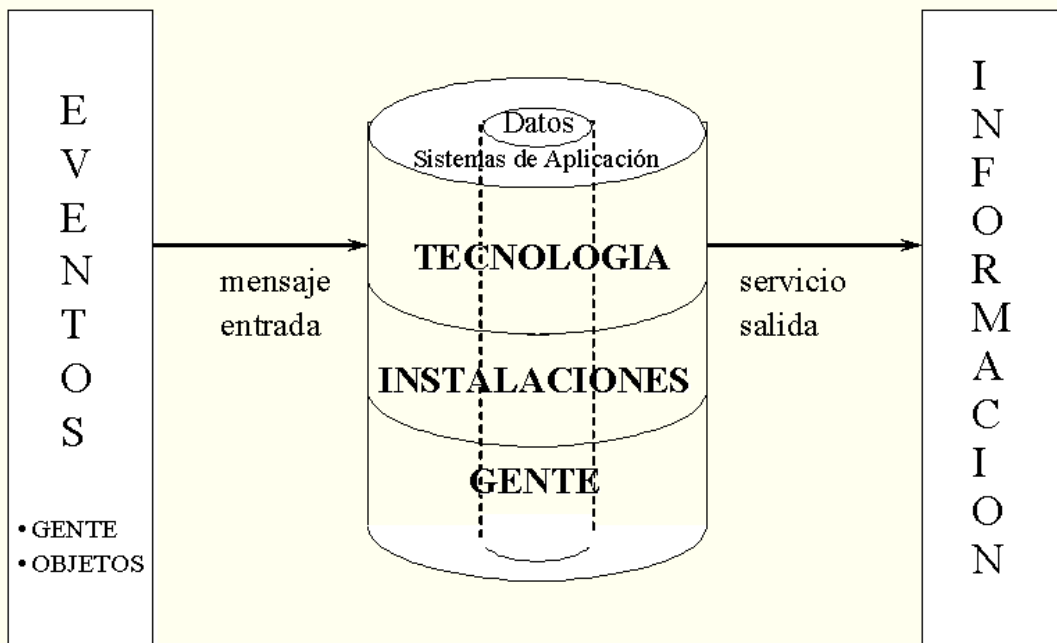


Fig. 9.



# PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINIOS

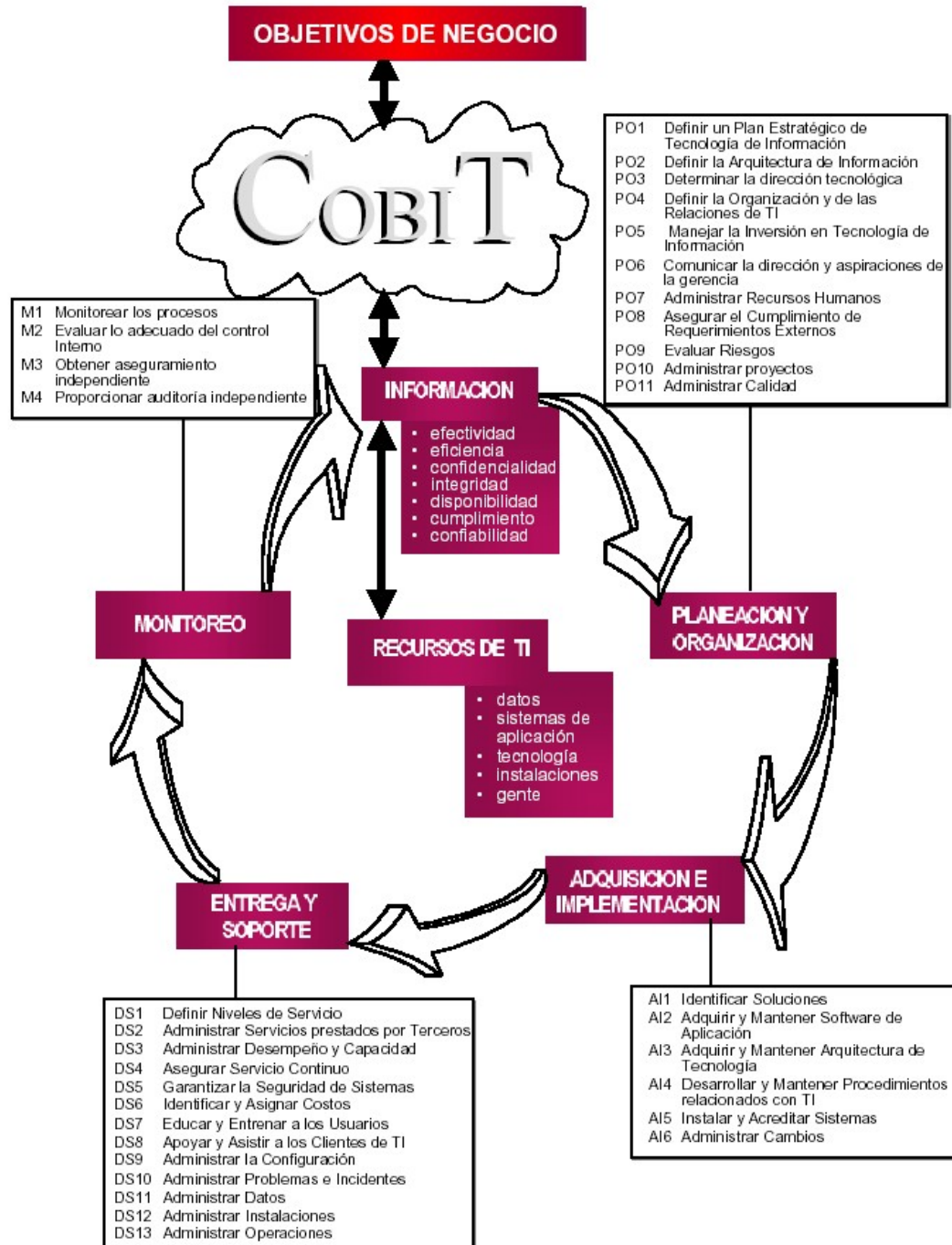


Fig. 10.

## **Planeación y Organización**

- P01 Definir un Plan Estratégico de Tecnología de Información.
- P02 Definir la Arquitectura de Información
- P03 Determinar la Dirección Tecnológica
- P04 Definir la Organización y las relaciones de Tecnología de la Información.
- P05 Administrar la Inversión en Tecnología de Información.
- P06 Comunicar la Dirección y Aspiraciones de Gerencia.
- P07 Administrar Recursos Humanos
- P08 Asegurar el Cumplimiento de requerimientos externos.
- P09 Evaluar Riesgos.
- P010 Administrar Proyectos
- P011 Administrar Calidad

## **Adquisición e Implementación**

- AI1 Identificar Soluciones
- AI2 Adquirir y Mantener Software de Aplicación
- AI3 Adquirir y Mantener Arquitectura Tecnológica.
- AI4 Desarrollar y Mantener Procedimientos relacionados con T.I.
- AI5 Instalar y Acreditar Sistemas
- AI6 Administrar Cambios.

## **Entrega y Soporte**

- DS1 Definir Niveles de Servicio
- DS2 Administrar Servicios prestados por Terceros.
- DS3 Administrar Desempeño y Capacidad.
- DS4 Asegurar Servicio Continuo.
- DS5 Garantizar la Seguridad de Sistemas.
- DS6 Identificar y Asignar Costos.
- DS7 Educar y Entrenar a los Usuarios.
- DS8 Apoyar y Asistir a los Clientes de T.I.
- DS9 Administrar la Configuración.
- DS10 Administrar Problemas e Incidentes
- DS11 Administrar Datos.
- DS12 Administrar Instalaciones.
- DS13 Administrar Operaciones.

## **Monitoreo**

- M1 Monitorear los Procesos.
- M2 Evaluar lo adecuado del Control Interno.
- M3 Obtener Aseguramiento Independiente.
- M4 Proporcionar Auditoría Independiente.



## COMO OBTENER EL RECONOCIMIENTO MUNDIAL CON CISA

La marca de la excelencia para un programa de certificación profesional está en el valor y reconocimiento que se concede al individuo que la obtiene. Desde 1978, el programa de Certified Information Systems Auditor™ (CISA®), patrocinado por Information Systems Audit and Control Association® (ISACA™), ha sido aceptado a nivel mundial como la norma entre los profesionales de auditoría, control y seguridad de SI.

Los conocimientos y prácticas técnicas que CISA promueve y evalúa son las piezas básicas del triunfo en el campo profesional.

Poseer la designación CISA demuestra el nivel de competencia y constituye la pauta para medir la profesionalidad. Con una creciente demanda de profesionales que posean conocimientos y experiencia en auditoría, control y seguridad de SI, la certificación CISA se ha convertido en el programa de certificación preferido por individuos y organizaciones en todo el mundo.

La certificación CISA es sinónima de dedicación al servicio con distinción tanto de la organización como de la industria de auditoría, control y seguridad de SI. Además, ofrece un número de beneficios tanto a nivel profesional como personal.

### Identificación como Profesional Consumado

Obtener la designación CISA coadyuva a asegurar una reputación positiva como profesional cualificado de auditoría, control y/o seguridad en SI. Bien sea que desee mejorar su rendimiento en el trabajo o asegurar un ascenso o una nueva posición, convertirse en auditor CISA lo hará distinguirse de otros candidatos y le dará una ventaja competitiva.

### Las Credenciales que las Empresas demandan

Debido a que el programa CISA certifica individuos que demuestran dominio y maestría en los conocimientos más deseados de hoy en día, las empresas prefieren contratar y conservar aquellas personas que logren y mantengan su designación. La designación CISA asegura a las empresas que su personal ha cumplido con los criterios actuales a nivel de educación y experiencia necesarios para un rendimiento exitoso en el trabajo.

### Reconocimiento a Nivel Mundial

Aun cuando la certificación quizá no sea obligatoria para usted en estos momentos, un número creciente de organizaciones está recomendando a sus empleados que se certifiquen. Para ayudarle a triunfar en el mercado global, es vital que usted seleccione un programa de certificación con base en prácticas de tecnología aceptadas universalmente. CISA provee ese tipo de programa.

El programa CISA está reconocido a nivel mundial, por todas las industrias, como la designación preferida para los profesionales de auditoría, control y seguridad de SI.

### Conviértase en un Nuevo Auditor CISA

El programa CISA está diseñado para evaluar y certificar a los individuos en la profesión de auditoría, control y seguridad de SI que demuestren criterio y habilidades excepcionales.

Para obtener la designación CISA, se requiere que los candidatos:

- Aprueben el examen CISA;
- Cumplan con el Código de Ética Profesional de la entidad Information Systems Audit and Control Association, el cual está incluido en la Guía del Candidato para el Examen CISA y se le entrega a cada candidato que se inscribe; y
- Presenten evidencia de experiencia de trabajo profesional en el campo de auditoría, control o seguridad de sistemas de información (SI) de cinco (5) años como mínimo. Substituciones y excepciones de dicha experiencia pueden obtenerse de acuerdo a lo que se establece a continuación:
  - Un máximo de un año de experiencia en auditoría, control o seguridad de SI puede ser substituido por:
    - un año completo de experiencia en auditoría no relacionada con SI, o
    - un año completo de experiencia en sistemas de información, y/o
    - un grado de Asociado/Técnico (60 créditos universitarios o su equivalente).
  - Dos años de experiencia en el campo de auditoría, control o seguridad de SI pueden ser substituidos por un título universitario o licenciatura (120 créditos universitarios o su equivalente).
  - Un año de experiencia en auditoría, control o seguridad de SI puede ser substituido por cada dos años de experiencia como instructor universitario a tiempo completo en un campo relacionado (es decir, computación, contabilidad, auditoría de SI).

No es aplicable un límite máximo (es decir, seis años de experiencia como instructor universitario equivale a tres años de experiencia en auditoría, control o seguridad de SI).

La experiencia debe haber sido adquirida en el lapso de 10 años previos a la solicitud de certificación o dentro de los cinco (5) años siguientes de la fecha inicial de aprobación del examen. La solicitud de certificación deberá presentarse dentro de los cinco (5) años posteriores a la fecha de aprobación del Examen CISA. Toda la experiencia laboral será verificada en forma independiente con las empresas donde se haya trabajado.

Es importante resaltar que muchas personas deciden tomar el Examen CISA antes de cumplir con los requisitos de experiencia. Esta práctica es aceptable y recomendada, aunque la designación CISA no se concederá hasta que se hayan cumplido todos los requisitos.

### El Examen CISA

El examen CISA se presenta en junio de cada año y consiste en 200 preguntas de selección múltiple, administradas durante una sesión de cuatro horas. El objetivo del examen es comprobar en el candidato el conocimiento, evaluación y aplicación de los principios y

prácticas de auditoría de SI y en áreas de contenido técnico. Estas áreas y sus definiciones son las siguientes:

#### Área Basada en Procesos

■ **Procesos en SI** – Llevar a cabo auditorías de acuerdo con las normas y directrices de auditoría de SI generalmente aceptadas para asegurar que la tecnología de información de la organización y los sistemas empresariales son adecuadamente controlados, vigilados y evaluados.

#### Áreas de Contenido

■ **Gerencia, Planificación y Organización de SI** – Evaluar la estrategia, políticas, normas, procedimientos y prácticas relacionadas para la gerencia, planificación y organización de SI.

■ **Infraestructura Técnica y Prácticas Operacionales** – Evaluar la efectividad y eficiencia de la implantación y gerencia continuada de la infraestructura operacional y técnica de la organización para asegurar que apoyen adecuadamente los objetivos empresariales de la organización.

■ **Protección de los activos de Información** – Evaluar la seguridad lógica, ambiental y la infraestructura de TI para asegurar que satisface los requerimientos empresariales de la organización con el fin de salvaguardar los activos de información contra el uso, divulgación y modificación no autorizados, daño o pérdidas.

■ **Recuperación ante Desastres y Continuidad de Operación** – Evaluar el proceso para desarrollar y mantener planes documentados, comunicados y comprobados para la continuidad de la operación empresarial y el proceso de SI en caso de una interrupción.

■ **Desarrollo, Adquisición, Implantación y Mantenimiento de los Sistemas de Aplicación Empresariales** – Evaluar la metodología y los procesos por los cuales el desarrollo, adquisición, implantación y mantenimiento de los sistemas de aplicación empresariales son llevados a cabo para asegurar que cumplan con los objetivos empresariales de la organización.

■ **Evaluación de Procesos Empresariales y Gerencia de Riesgos** – Evaluar los sistemas y procesos empresariales para asegurar que los riesgos estén administrados y gestionados de acuerdo con los objetivos empresariales de la organización.

Las preguntas del Examen CISA están desarrolladas y mantenidas cuidadosamente para asegurar que se compruebe en forma exacta el dominio del individuo en prácticas de auditoría, control y seguridad de SI. Se requiere una puntuación de escala corregida de 75 puntos para aprobar el examen. Puesto que la designación CISA es reconocida mundialmente, el examen se ofrece en los siguientes idiomas: chino (mandarín simplificado), chino (mandarín tradicional), holandés, inglés, francés, alemán, hebreo, italiano, japonés, coreano y español.

#### Preparación para el Examen CISA

Se puede lograr la aprobación del examen CISA mediante un plan de estudios organizado. Para ayudar a los individuos con el desarrollo de un plan exitoso de estudios, ISACA proporciona varias guías de estudio y cursos de repaso para los candidatos al examen. (Véase también [www.isaca.org/bk\\_cisa.htm](http://www.isaca.org/bk_cisa.htm) para más información.)

- La Guía del Candidato para el Examen CISA se suministra a los individuos después de recibir el formulario y el pago de inscripción para el Examen CISA. Esta guía proporciona un esquema detallado de las áreas de proceso y de contenido cubiertas en el examen, una lista sugerida de materiales de referencia, un glosario de acrónimos utilizados normalmente en el examen y una copia de muestra de la hoja de respuestas utilizada en dicho examen.
- El Manual de Repaso CISA se actualiza en forma extensa cada año para reflejar los principios y prácticas actuales y cambiantes de la industria. Este manual proporciona una guía completa de estudio para ayudar a los individuos a prepararse para el Examen CISA. Incluye una explicación detallada de la estructura y contenido del examen, sugerencias sobre cómo desarrollar un plan de estudios y brinda guía y cobertura del material técnico detallado en las áreas de contenido y proceso del examen. También incluye definiciones actualizadas y ejemplos prácticos, así como referencias a otros materiales de estudio de utilidad y un glosario de términos que se suelen encontrar en el examen. Además incluye preguntas de repaso al final de cada capítulo para familiarizar a los candidatos con la estructura de las preguntas. Este manual puede usarse como documento único para estudio individual o como una guía o referencia para grupos de estudio y capítulos regionales que ofrezcan cursos de repaso a nivel local. (Versión disponible en inglés y español.)
- El Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA consiste de 500 preguntas de estudio de tipo opciones múltiples organizadas en la misma proporción que el “análisis de trabajo” CISA.

Muchos de estos ítems aparecieron en versiones anteriores del Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA, pero han sido rescritas para ser más representativas del tipo de preguntas en el examen real y para brindar mayor claridad o indicar un cambio en la práctica. Además, se han agregado varios ítems nuevos para brindar una cobertura más amplia de los tópicos. Las preguntas están clasificadas de acuerdo con las áreas de proceso y contenido de CISA y se ofrece un modelo de examen. Esta publicación es ideal para usarse en conjunto con el Manual de Repaso CISA. (Versión en inglés.)

- El Suplemento al Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA, desarrollado cada año por ISACA, incluye 100 preguntas, respuestas y explicaciones de muestra nuevas para que los candidatos las usen en la preparación del examen CISA. Se desarrollaron los ítems en el suplemento mediante un proceso similar al usado para la creación de los ítems del examen real. Esta publicación es ideal para usarse en conjunto con el Manual de Repaso CISA y el Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA. (Versión disponible en inglés y español.)
- El CD-ROM de Preguntas, Respuestas y Explicaciones para Repaso CISA consiste de las mismas 600 preguntas, respuestas y explicaciones incluidas en el Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA y en el Suplemento al Manual de Preguntas, Respuestas y Explicaciones para Repaso CISA. Con este producto, los candidatos CISA pueden identificar sus puntos fuertes y débiles realizando distintos exámenes de muestra de longitud variable, y desglosando los resultados por área. También se pueden elegir exámenes de muestra por área para poder concentrar el estudio, un área a la vez, y por otras características de clasificación, tales como la omisión de preguntas contestadas previamente en forma correcta. También se incluyen los artículos de Information Systems Control Journal citados en el Manual de Repaso de CISA (Versión en inglés)

■ Cursos de Repaso CISA a través de los capítulos regionales de ISACA. Los candidatos al examen podrán comunicarse con el capítulo regional ISACA en su área para saber si se está ofreciendo un curso de repaso. Estos cursos muchas veces son impartidos por auditores CISA actualmente certificados quienes presentan y debaten los temas del examen y comparten los secretos de su éxito. La información relativa a los contactos de los capítulos regionales y cursos ofrecidos está disponible en [www.isaca.org/chap1.htm](http://www.isaca.org/chap1.htm) y [www.isaca.org/cisarevw.htm](http://www.isaca.org/cisarevw.htm) respectivamente.

No se establece ninguna confirmación ni garantía por parte de la Junta de Certificación ni de la Information Systems Audit and Control Association en relación con estas u otras publicaciones o cursos de la Asociación que asegure de ninguna forma que los candidatos aprobarán el examen.

## **Mantenimiento de la Certificación CISA**

Una cualidad importante de cualquier designación profesional es un programa de educación continua que el individuo debe seguir para mantener la certificación. Para mantener la certificación CISA, los individuos deben cumplir con una política de educación continua y observar el Código de Ética Profesional de ISACA. Ambos programas ayudan a asegurar que los auditores CISA se mantengan al día con los avances técnicos e industriales y demostrar altos principios profesionales.

La Política de Educación Continua exige que el individuo obtenga y presente un número mínimo de horas de educación continua profesional (CPE en inglés) y pague una cuota de mantenimiento cada año. Además, se debe obtener y presentar un número mínimo de horas CPE durante un período fijo de certificación de tres años. El no cumplir con esta política traerá como consecuencia la revocación de la certificación del individuo.

Durante los últimos cinco años, más del 93 por ciento de todos los auditores CISA han conservado su certificación. Esta es una estadística ejemplar que demuestra el deseo de los auditores CISA de mantener su credencial CISA.

## **Administración y gestión del Examen**

### **Boleto de Admisión**

Aproximadamente de dos a tres semanas antes de la fecha del examen CISA, la agencia que administra las pruebas le enviará un comprobante físico de admisión e ISACA le enviará uno electrónico. Los comprobantes indicarán la fecha, hora de inscripción y la localización de su examen, programa de eventos de ese día y los materiales que usted debe traer para tomar el examen CISA.

Es sumamente importante que usted revise la hora de inscripción y examen específicos indicados en su Comprobante de Admisión. **NO SE ADMITIRÁ A NINGÚN CANDIDATO AL CENTRO DE PRUEBA UNA VEZ QUE EL SUPERVISOR PRINCIPAL COMIENCE LA LECTURA DE LAS INSTRUCCIONES, APROXIMADAMENTE 30 MINUTOS ANTES DE QUE COMIENCE EL EXAMEN.**



Usted puede usar su comprobante de admisión solamente en el centro de prueba designado en su comprobante de admisión.

Usted será admitido al centro de prueba solamente si tiene un Comprobante de Admisión válido y una forma aceptable de identificación. Ejemplos de identificación aceptable podrán incluir los que tengan una fotografía (como pasaportes, licencias de conducir con foto) u otra forma de identificación con su firma e información descriptiva tales como su altura, peso y color de los ojos (como en las licencias de conducir sin foto).

### Vigilancia

Se descalificará a los candidatos a los que se les descubra involucrados en algún tipo de conducta no aceptable (tales como proporcionar o recibir ayuda, utilizar notas, papeles u otro tipo de ayuda), intentando tomar el examen en lugar de otra persona, o llevándose el folleto, hoja de respuestas o notas fuera del aula de la prueba. La agencia que administra las pruebas informará tales irregularidades al Directorio de Certificación.

### Resultados del Examen

#### Recepción del Informe de Calificaciones

Aproximadamente 10 semanas después de la fecha del examen, los candidatos recibirán por correo los informes con las calificaciones. Para garantizar la confidencialidad de las calificaciones, los resultados del examen no se informarán por teléfono, fax ni correo electrónico. Sin embargo, con su consentimiento al ítem número 28 del formulario de inscripción, se le puede enviar por correo electrónico un aviso de examen aprobado/reprobado.

#### Informe de Resultados de su Examen

Los candidatos CISA recibirán un informe indicando la calificación en el examen. Esta calificación es una calificación escalada de uno (1) a cien (100) que se deriva de un proceso aritmético que convierte las calificaciones brutas a calificaciones escaladas en base a los resultados de todos los candidatos que se presentaron al examen y al punto de aprobación. No es un promedio aritmético. El punto de aprobación se deriva de un proceso de igualación usado por la agencia examinadora independiente que compara los resultados del examen actual con los de exámenes anteriores.

Los candidatos que obtengan una calificación de 75 o más aprobarán el examen y pueden entonces solicitar la certificación CISA.

Un candidato que reciba una calificación de 74 o menos deberá volver a realizar el examen. Para ayudar con los estudios futuros, aquellas personas que obtengan una calificación de 74 o menos recibirán un análisis de la calificación, por área de contenido y proceso, el cual se incluirá en la carta con los resultados.

## Tomar de Nuevo el Examen CISA

Los candidatos que reciban una calificación de 74 o menor pueden inscribirse de nuevo para el Examen CISA durante cualquier realización futura del examen.

✚ A continuación se presenta un caso de estudio que nos permite ejemplificar lo que hasta ahora se ha mencionado (Figs. 12 – 21.)

## CASO DE ESTUDIO

---



Fig. 12



Fig. 13.

**Sistemas Inteligentes de México, S. A. de C. V. (SIM)** es una empresa con más de 10 años de experiencia colaborando en tareas como: *Antivirus, FireWall, VPN, Filtrado de Contenido, AntiSpam, Detección de Intrusos (IDS), Voz por IP, Análisis de Vulnerabilidades, Monitoreo de REDES CORPORATIVAS en tiempo real, Consultoría en Seguridad, Servicio de Instalación y Configuración de Linux desde Cero, Capacitación de Seguridad Lógica, Cursos de DISEÑO DE REDES SEGURAS, Capacitación de ( LINUX ), Curso de Linux I Básico, Curso de Linux II Avanzado, Capacitación de Virus, Curso de Taller de Virus en Vivo*, entre otras tareas.

La experiencia de nuestro personal que ha laborado en puestos clave de *Auditoría en Seguridad Informática, Administración de Proyectos, Consultoría y Manejo de Áreas de Negocio*, nos da el conocimiento superior para realizar tareas como *Auditoría Informática, Asesoramiento de Riesgos Informáticos, Pruebas de Intrusión, Análisis Forense, etc.*

Además de esto, **SIM** está especializado en programación de sistemas utilizando tecnologías actuales como *PHP, MySQL, HTML dinámico, etc.*, lo que nos ayuda a proporcionar servicios competitivos en el mercado moderno así como productos de alta calidad.

**SIM** es una empresa que valora y fomenta las relaciones basadas en honestidad y mutuo beneficio con nuestros clientes. Con esto en mente, nuestro personal siempre va más allá de lo requerido, con el fin de brindar el apoyo que las empresas necesitan, ya que queremos ser sus *“Aliados de Negocio”*.

Con nosotros, usted ha encontrado no solo una empresa seria que le brinda los servicios que requiere, con un alto nivel de calidad; sino también ha encontrado un *“socio”* con el que puede contar para todos sus requerimientos de Internet, Desarrollo de Sistemas y más.

**Lic. Luis Díaz Sánchez**  
**Director General**  
**SIM**



Fig. 14.

**>> Misión:**

**SIM** se crea con el fin de proporcionar servicios y productos de seguridad con soluciones de software y hardware dirigidos a empresas de clase mundial.

Su principal objetivo es satisfacer las necesidades de las empresas, tanto en el mercado nacional como en el internacional, apoyados en tecnología de vanguardia.

**SIM** busca la integración de los socios empresariales con sus clientes y proveedores a través de una cultura organizacional que permita asegurar a los empleados una mejor calidad de vida y a sus accionistas la rentabilidad esperada.

Dicha cultura se implanta mediante:

- **Calidad en el servicio**
- **Personal especializado**
- **Trabajo en equipo**
- **Una organización formal**

**>> Visión:**

Proporcionar servicios y productos de seguridad a sus clientes, con soluciones de software y hardware. Orientando todos sus recursos a ser el líder en el mercado nacional e internacional, a través de la consolidación de su negocio y mediante la creación de su propia tecnología.



Fig. 15.



Fig. 16.

### >> **Estrategia:**

En **SIM** la identificación de prioridades se realiza antes de correr cualquier tipo de riesgo.

Los consultores de **SIM** están a la vanguardia en esquemas y estados de seguridad, lo cual nos permite eliminar cualquier riesgo localizado en el sistema de seguridad de su empresa una vez que nuestro equipo evalúa la situación e identifica las fuentes de los mismos.

Si existe la amenaza de riesgos o intentos de daño a la información de los clientes, nuestros especialistas en seguridad están capacitados para responder con un paso adelante evitando cualquier pérdida.

Debido a que cada uno de los clientes tiene diferentes necesidades, **SIM** cuenta con la experiencia para implementar los esquemas de seguridad, realizar penetraciones (pen-test), identificar vulnerabilidades, auditar sistemas, detectar intrusos, monitorear, capacitar, desarrollar políticas y normas, y dar la protección global que requiera su empresa de forma personalizada.

Para garantizar la seguridad de los clientes, todos los empleados de **SIM** están sujetos a un análisis a fondo antes de trabajar en cualquier sección e información, ejerciendo el código de ética de **SIM**.

Nuestra prioridad:

- **Realizar políticas y normas de seguridad**
- **Trabajar en forma global y conjunta con todos los organismos de seguridad**
- **Investigación de nuevas vulnerabilidades**
- **Desarrollo de aplicaciones para la autenticación y confiabilidad de la información**
- **Proporcionar esquemas de seguridad complejos que faciliten la disponibilidad de la información de los clientes**
- **Otras**

Cada una de estas actividades tiene como objetivo garantizar la seguridad de los sistemas de nuestros clientes.



Fig. 17.

**>> Servicios:**

Modelo de Seguridad de la Información.  
Plan de Contingencia Tecnológico.  
Plan de Continuidad Operativa del Negocio.  
Oficial de Seguridad de la Información.  
Charlas de "Evangelización" en Seguridad de la Información.  
Análisis y Evaluación de Site de Contingencias.  
Administración y Gestión en Seguridad de la Información.  
Procedimientos de Procesos de Negocio.  
Análisis y Evaluación de Riesgo Tecnológico.  
Educación en Tecnologías de la Información.



>> *Algunos de nuestros clientes:*



*ARCO IRIS SCHOOL*



Fig. 18.



# Aplicación de las Normas COBIT



Fig. 19.

A continuación, analizaremos como se deberían aplicar las Normas COBIT en una Organización, utilizando para ello la Guía de Auditoria presentada en la pagina Web [www.isaca.org](http://www.isaca.org), la misma indica los pasos a seguir para auditar cada uno de los procesos de TI de la norma. Este reporte lo confeccionamos dándole el formato de un informe de auditoría:

## Informe de Auditoria

- Entidad Auditada: ARCO IRIS SCHOOL
- Alcance de la auditoría: Esta auditoría comprende solamente al área de Recursos Humanos de la Arco Iris School, con respecto al cumplimiento del proceso “Administración de Recursos Humanos” de la norma COBIT.
- Norma Aplicada: COBIT, específicamente el proceso de TI Po7 “Administración de Recursos Humanos”

### • Relevamiento:

Organización: Colegio Privado que brinda un servicio de educación a niños de nivel inicial y primario.

### Objetivos de la Organización:

- Ofrecer el servicio de una excelente educación con orientación bilingüe (Español - Ingles), artística, deportiva y ecológica en forma personalizada a los niños de nivel inicial y primario, y obtener por el servicio un beneficio monetario acorde a las ofertas educativa que brinda la Institución (según si el inscripto participa de escolaridad simple o doble)
- Incrementar cada año el número de inscriptos para obtener mayor rentabilidad y ampliar la comunidad educativa.
- Transmitir a la comunidad en general el perfil institucional y los beneficios que los alumnos obtienen por una educación personalizada.

Departamento de administración de personal: Comprende todo lo relacionado con el desarrollo y administración de políticas y programas que provean una estructura organizativa eficiente, empleados calificados, tratamiento equitativo, oportunidades de progreso, satisfacción en el trabajo y adecuada seguridad de empleo.

Depende de la Gerencia de Administración.

### ***Políticas y estrategias del Departamento de Administración de personal***

Políticas Estrategias Para con el Personal

Objetivo: perfeccionar al personal con el perfil Institucional

Seleccionar docentes que respondan a los requerimientos del proyecto educativo institucional

Realizar durante la selección de personal talleres de capacitación y evaluación de inteligencia emocional y desarrollo de la persona.

Seleccionar docentes con muy buenas referencias

Los docentes de asignaturas especiales (plástica, música, deportes, etc.) deben tener experiencias mínimas en mas de una escuela y estar abalados con referencias por escrito

Respetar las decisiones personales de los docentes y no docentes.

Antes de que un personal forme parte de la institución debe conocer y firmar las Normativas Institucionales donde se especifican todas las medidas, deberes y derechos de todo el personal docente y no docente

La dirección general realiza periódicamente evaluaciones del rendimiento de trabajo individual y grupal mediante entrevistas. (Grupales y personales)

Educativas

Objetivo: Lograr una excelencia educativa

Brindar una educación excelente y personalizada

Confeccionar un PEI (Proy. Educ. Inst.) con los objetivos que cubran las orientaciones Bilingüe, deportiva, ecológica y artística.

Realizar periódicamente talleres de capacitación docente a nivel institucional donde se promueve la inteligencia emocional y el desarrollo personal.

La dirección académica debe evaluar constantemente el trabajo de los docentes y elevar los informes a la dirección general.

Funciones – Subfunciones – Tareas:

1-Realizar el reclutamiento: lograr que todos los puestos estén cubiertos por personal competente que cubran el perfil institucional por un costo razonable.

**a)** Buscar los postulantes (docentes y no docentes)

✓ Análisis de las necesidades del cargo

✓ Desarrollo de especificaciones de trabajo

✓ Análisis de las fuentes de empleados potenciales

✓ Atracción de los posibles postulantes

**b)** Realizar el proceso de selección: Análisis de la capacidad de los aspirantes para decidir cual tiene mayores posibilidades.

✓ Entrevistar los postulantes

✓ Realizar talleres de Pruebas de inteligencia emocional.

✓ Evaluación de los postulantes en base a los resultados de los talleres.

✓ Confección y entrega de los diferentes tipos de contratos de trabajo (contratos temporales, a plazo fijo, contratos de prueba, pasantías, etc.)

**c)** Instrucción y entrega de materiales: Entrenamiento, información y entrega de materiales necesarios a los empleados contratados (o nuevos) para que cumplan sus obligaciones eficientemente.

- ✓ Orientación de los nuevos empleados mediante talleres de capacitación y entrega de documentación con las normativas (reglas con las que se rige la institución)
  - ✓ Seguimiento de la actuación de los empleados (y empleados nuevos también).
  - ✓ Compra de materiales didácticos u otros servicios para entregar a los docentes y así los mismos puedan dictar sus clases eficientemente.
  - d) Despidos:** Terminación legal de las relaciones con los empleados en la forma mas beneficiosa para ellos y el colegio.
  - ✓ Realización de la entrevista de egreso
  - ✓ Análisis de las bajas
  - e) Determinar los servicios sociales para los empleados.**
  - ✓ Determinación de servicio médicos y otros para los empleados (y alumnos) que cubran la seguridad e integridad física del personal dentro de la organización.
  - ✓ Prepara la documentación para la gestión de obras sociales del personal.
- 2-Administrar sueldos y jornales: lograr que todos los empleados estén remunerados adecuada, equitativamente y en tiempo.
- a) Clasificar la posición, responsabilidades y requerimientos de los empleados**
  - ✓ Preparación de las normativas institucionales donde están las especificaciones de trabajo
  - ✓ Revisión periódica y corrección de las normativas.
  - ✓ Fijar los valores monetarios de los puestos en forma justa y equitativa, respecto a otros puestos en el colegio y a puestos similares en el mercado de trabajo.
  - ✓ Efectuar los pagos correspondientes a los sueldos mensuales (el pago y entrega de recibos de sueldo se efectúa en la propia institución)
  - b) Control de Horarios:** Fijación de horas de trabajo y periodos de inasistencia con goce de haberes o sin el, que sean justos tanto para el empleado como para el colegio.
  - ✓ Planificación y administración de políticas sobre horarios de trabajos o inasistencias.
  - ✓ Planificación y administración de planes de vacaciones.
- 3- Promocionar las Relaciones institucionales: Asegurar que las relaciones de trabajo entre la dirección general y los empleados al igual que la satisfacción en el trabajo y oportunidad de progreso del personal, sean desarrollados y mantenidos siguiendo los mejores intereses del colegio y de los empleados. También su función es la de desarrollar proyectos de Relaciones Institucionales con el medio externo (otras instituciones escolares, clubes, etc.)
- a) Realizar negociaciones colectivas:** Lograr concordancia con las organizaciones de empleados reconocidas oficialmente y establecidas legalmente, de la manera que mejor contemple los intereses de la escuela y los docentes.
  - ✓ Negociación de convenios
  - ✓ Interpretación y administración de estos
  - b) Controlar la disciplina del personal**
  - ✓ Fijar reglas de conducta y disposiciones mediante las normativas institucionales
  - ✓ Establecer y administrar las medidas disciplinarias con respecto a inasistencias injustificadas.
  - c) Investigación de Personal:**

- ✓ Investigación de referencias de trabajos anteriores.
- ✓ Confirmar las referencias y otras documentaciones a la administración general.
- ✓ Investigar y verificar la documentación presentada por los empleados que luego conformaran el legajo de los mismos (DNI, títulos oficiales, registración en la Junta de clasificaciones, etc.)

#### 5-Generar Informes

- ✓ Confeccionar todos los informes mensuales, semestrales y anuales con las estadísticas, resúmenes, etc. de las gestiones administrativas del personal.

- **Diagnóstico:**

De acuerdo con el Dominio “Planificación y Organización” y el Proceso “Administración de Recursos Humanos”, nosotros hemos desarrollado un análisis, donde identificamos con que normas esta cumpliendo la organización y con cuales no, a partir de allí definiremos que es lo que la escuela debería hacer para cumplir con las normas COBIT.

### **Conclusiones:**

La organización ARCO IRIS SCHOOL, según nuestro parecer y de acuerdo a lo relevado, creemos que se ajusta bastante bien a las normas COBIT en cuanto al proceso en cuestión, puesto que la misma cumple con las siguientes actividades o tareas del mismo:

Reclutamiento y Promoción personal, ya que la Dirección evalúa regularmente los procesos necesarios para asegurar que las practicas de reclutamiento y promoción de personal tengan excelentes resultados, considerando factores como la educación del personal, la experiencia y la responsabilidad.

Personal Calificado, puesto que se verifica que el personal que lleva tareas especificas este capacitado y para ello se realizan Talleres Docentes.

Entrenamiento de Personal, ya que en cuanto ingresa el personal y durante su permanencia en el establecimiento tiene a su disposición toda la información que necesite, así como también la permanente capacitación. Aunque es importante destacar que no hay un manual de Funciones, ni de Procedimientos, por lo cual los empleados pueden tener dudas con respecto a sus funciones.

Evaluación de Desempeño de los Empleados, ya que el establecimiento implementa un proceso de evaluación de desempeño de los empleados y asesora a los mismos sobre su desempeño o conducta de manera apropiada. Aunque las evaluaciones de rendimiento no están definidas formalmente y por ende se puede llegar a tener problemas por la subjetividad de la persona que esta evaluando el desempeño.

Cambios de puestos y Despidos, puesto que cuando se toman tales acciones se trata de que sean oportunas y apropiadas, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

Es importante destacar que ARCO IRIS SCHOOL tienes dificultados en cuanto a:

Respaldo de Personal, puesto que no cuenta con suficiente personal de respaldo para solucionar posibles ausencias. Tampoco el personal encargado de puestos delicados

como ser el Tesorero toma vacaciones interrumpidas con duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

Procedimientos de Acreditación de Personal, puesto que las investigaciones de seguridad asociada a la contratación no son llevadas a cabo.

**Recomendaciones:**

Por lo tanto, podemos especificar que para que la escuela cumpla con las normas COBIT en cuanto al proceso “Administración de Recursos Humanos” deberá:

- Realizar manuales de funciones, de manera que estén definidos todos los puestos de trabajo y sus correspondientes funciones.
- Realizar manuales de Procedimientos, de manera que los empleados puedan identificar cuales son las tareas que deben realizar de acuerdo a su puesto y funciones.
- Establecer Procedimientos de Acreditación, ya que de lo contrario se pueden tener serios problemas por no haber realizado correctamente las investigaciones de seguridad.
- Proporcionar un entrenamiento “cruzado” de manera de tener personal de respaldo con la finalidad de solucionar posibles ausencias, ya que la escuela no puede contar con suficiente personal por su economía actual.
- Definir y publicar formalmente las evaluaciones de rendimiento, de manera de aplicarlas a la hora de hacer la evaluación de desempeño para evitar problemas con el personal docente y no docente.



Fig. 20.

>> **Contáctenos:**

Mediante e-mail a [sim\\_consultores@sim.com.mx](mailto:sim_consultores@sim.com.mx)



*Sistemas Inteligentes de México S.A. de C.V.*

**Dirección:**

Río Danubio No. 8 Despacho 1

Colonia Cuauhtemoc

Delegación Cuauhtemoc

**Teléfono.:**

5245-1553

*Lic. Luis Diaz Sanchez* ----- [luis.diaz@sim.com.mx](mailto:luis.diaz@sim.com.mx)



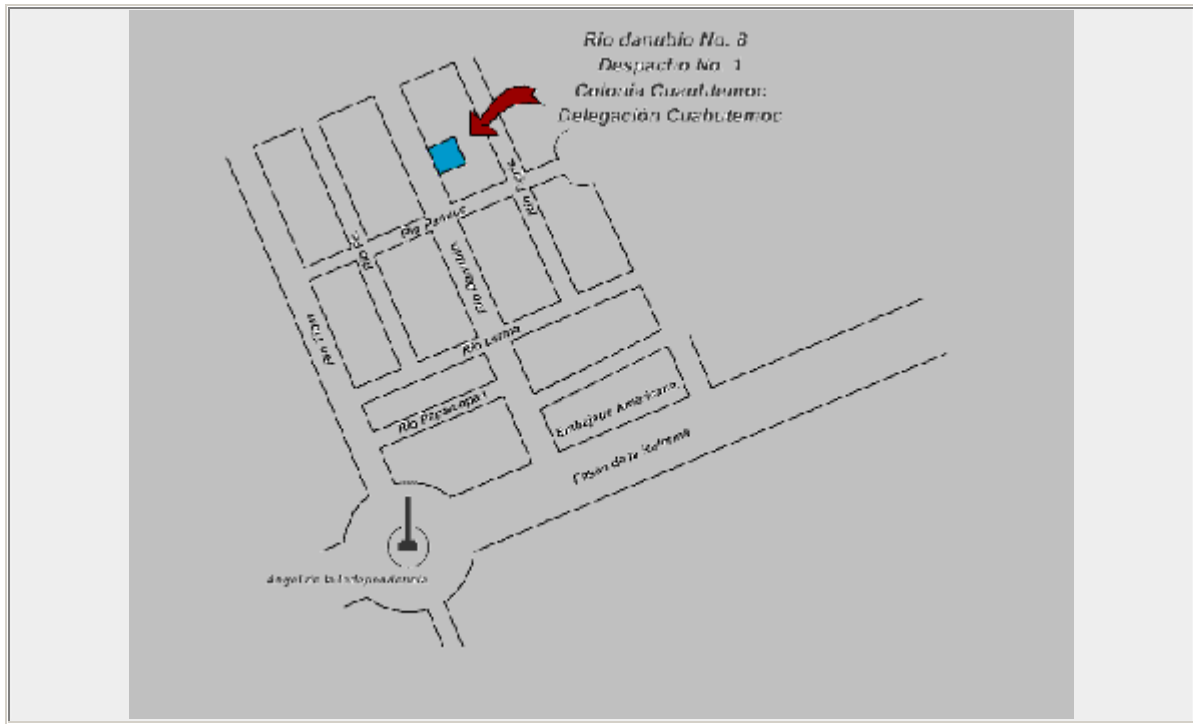


Fig. 21.

## CONCLUSIÓN

---

Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

La sociedad de la información y nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas en las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas, ya sean presentes o futuras.

Los servicios de auditoría comprenden el estudio de los sistemas para gestionar las vulnerabilidades que pudieran estar presentes en los sistemas. Una vez localizadas, las anomalías se documentan, se informa de los resultados a los responsables y se establecen medidas proactivas de refuerzo, siguiendo siempre un proceso secuencial que permita que los sistemas mejoren su seguridad aprendiendo de los errores pasados.

Las auditorías de los sistemas permiten conocer en el momento de su realización cual es la situación exacta de los activos de información, en cuanto a protección, control y medidas de seguridad.

Realizar trabajos de auditoría con cierta periodicidad es necesario para asegurar que la seguridad de la red corporativa es la óptima. El continuo cambio en las configuraciones, la aparición de parches y mejoras en el software y la adquisición de nuevo hardware hacen necesario que los sistemas estén periódicamente controlados mediante auditoría.

Una auditoría de sistemas es una radiografía completa de la situación de éstos. Asegúrese de que está preparado para interconectarse. Audite sus sistemas.



## BIBLIOGRAFÍA

---

- Echenique García, J. A. (1997). Auditoria en Informática. México: Editorial McGraw-Hill.
- Hernández Hernández, E. (1991). Auditoria en Informática. México: Editorial CECSA.
- Fine H., L. (1999). Seguridad en centros de cómputo. México: Editorial Trillas.
- Carballo Pariñas, R. (1981). Auditoria de sistemas. Universidad Iberoamericana, México.
- Bravo González, A. L. (1998). La Información y la auditoria de sistemas. Universidad Iberoamericana, México.
- Camargo Andraca, M. I. G. (1990). Metodología para auditar la seguridad operativa de instalaciones, Hardware y Software en centros de cómputo en México. Universidad Iberoamericana, México.
- Senn, J. (1990). Análisis y Diseño de Sistemas de Información. Traducción de Edmundo Gerardo Urbina Medal. México: Editorial McGraw-Hill.
- Bernal Montañez, R. (1994). Auditoria de los Sistemas de Información. UPV, Valencia España.
- Thierauf, R. (1990). Auditoria Administrativa. México: Editorial McGraw-Hill.
- Instituto Mexicano de Contadores Públicos (2000). Normas y Procedimientos de Auditoria. IMCP, México.
- Etcheverry, S. (2003). COBIT. [En línea]. Disponible. <http://www.unap.cl/~setcheve/cobit/>
- Miro, I. (2005). Seguridad de la Información. [En línea]. Disponible. <http://www.kelssiler.com/>
- Pallavicini, C. (2005). Seguridad Informática. [En línea]. Disponible. <http://www.seguridadinfomatica.cl/empresa.php>

**ANEXO 1**

PROGRAMA DE AUDITORIA EN SISTEMAS
INSTITUCION _____ HOJA No. _____ DE _____ FECHA DE FORMULACION _____

FASE	DESCRIPCION	ACTIVIDAD	NUMERO DE PERSONAL	PERIODO ESTIMADO		DIAS HAB EST.	DIAS HOM. EST.
			PARTICIPANTE	INICIO	TERMINO		

**ANEXO 2**

<p><b>AVANCE DEL CUMPLIMIENTO DEL PROGRAMA DE AUDITORIA EN SISTEMAS</b></p>
<p>INSTITUCION _____ NUMERO _____ HOJA No. _____                  DE _____                  PERIODO QUE REPORTA _____</p>

FASE	SITUACION DE LA AUDITORIA			PERIODO REAL DE LA AUDITORIA		DIAS REALES UTILIZADOS	GRADO DE AVANCE	DIAS HOM. EST.	EXPLICACION DE LAS VARIACIONES EN RELACION CON LO PROGRAMADO
	NO INICIADA	EN PROCESO	TERMINADA	INICIADA	TERMINADA				


## ANEXO 3

### Ejemplo de Propuesta de Servicios de Auditoría en Informática

---

#### I. ANTECEDENTES

Anotar los antecedentes específicos del proyecto de Auditoría.

#### II. OBJETIVOS

Anotar el objetivo de la Auditoría.

#### III. ALCANCES DEL PROYECTO

El alcance del proyecto comprende:

1. Evaluación de la Dirección de Informática en lo que corresponde a:
  - ✚ Capacitación
  - ✚ Planes de trabajo
  - ✚ Controles
  - ✚ Estándares
2. Evaluación de los Sistemas
  - a. Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas)
  - b. Evaluación del avance de los sistemas en desarrollo y congruencia con el diseño general
  - c. Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo)
  - d. Seguridad física y lógica de los sistemas, su confidencialidad y respaldos
3. Evaluación de los equipos:
  - ✚ Capacidades
  - ✚ Utilización
  - ✚ Nuevos Proyectos
  - ✚ Seguridad física y lógica
  - ✚ Evaluación física y lógica

#### IV. METODOLOGIA

La metodología de investigación a utilizar en el proyecto se presenta a continuación:

1. Para la evaluación de la Dirección de Informática se llevarán a cabo las siguientes actividades:
  - ✚ Solicitud de los estándares utilizados y programa de trabajo
  - ✚ Aplicación del cuestionario al personal
  - ✚ Análisis y evaluación de la información
  - ✚ Elaboración del informe
2. Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:
  - ✚ Solicitud del análisis y diseño de los sistemas en desarrollo y en operación
  - ✚ Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)

- ✚ Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)
  - ✚ Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos
  - ✚ Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado
  - ✚ Entrevista con los usuarios de los sistemas
  - ✚ Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario
  - ✚ Análisis objetivo de la estructuración y flujo de los programas
  - ✚ Análisis y evaluación de la información recopilada
  - ✚ Elaboración del informe
3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:
- ✚ Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización
  - ✚ Solicitud de contratos de compra y mantenimientos de equipo y sistemas
  - ✚ Solicitud de contratos y convenios de respaldo
  - ✚ Solicitud de contratos de Seguros
  - ✚ Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad
  - ✚ Visita técnica de comprobación de seguridad física y lógica de la instalaciones de la Dirección de Informática
  - ✚ Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado
  - ✚ Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación
4. Elaboración y presentación del informe final (conclusiones y recomendaciones)

## V. TIEMPO Y COSTO

Poner el tiempo en que se llevará a cabo el proyecto, de preferencia indicando el tiempo de cada una de las etapas, costo del proyecto, personal involucrado, responsabilidades, etc.