UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 1: Anexo Seguridad Lógica y Seguridad Física

Contenido

Anexo Seguridad Lógica

Seguridad Lógica - Identificación y Autentificación

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

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

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

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

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

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

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

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

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
- Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

- Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente. Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Seguridad Lógica - Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- **Todas las anteriores**.

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

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

Seguridad Lógica - Control de Acceso Interno

Palabras Claves (Passwords)

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

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

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la

clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

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

Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

Listas de Control de Accesos

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

Límites sobre la Interfase de Usuario

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

Etiquetas de Seguridad

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

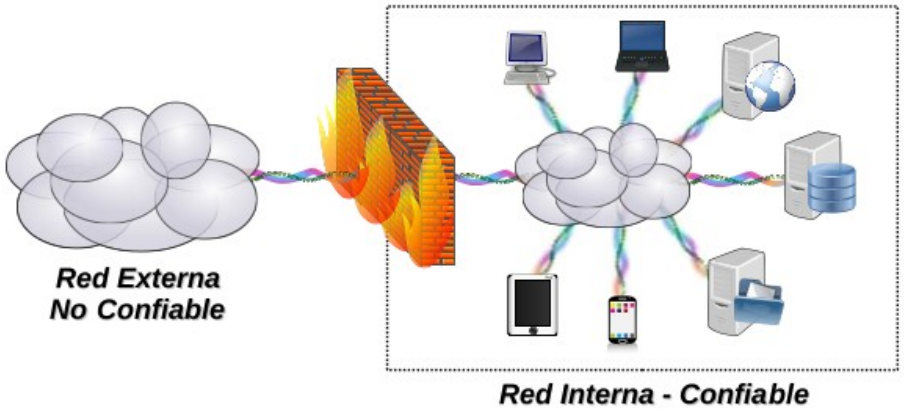
Seguridad Lógica - Control de Acceso Externo

Dispositivos de Control de Puertos

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

Firewalls o Puertas de Seguridad

Es un dispositivo de red que crea una separación entre redes públicas (no confiables) y redes privadas (confiables) mediante el análisis del tráfico de red permitiendo solamente el paso de cierto tráfico entre la red no confiable y la red confiable.



Características básicas

- Son dispositivos de defensa perimetral que separan redes.
- Filtran el tráfico dependiendo de reglas predefinidas.
- No protegen de ataques internos.
- No protegen de accesos no autorizados.
- No protegen de la totalidad de ataques dañinos.

Su funcionamiento se basa en reglas que exceptuan el comportamiento de una condición de general de los siguientes tipos:

- Todo lo que no está expresamente permitido, está prohibido.
- Todo lo que no está expresamente prohibido, está permitido.

Clasificaciones de firewalls

Por tipo o naturaleza

- De tipo software: son componentes lógicos que funcionan en una computadora con 2 ó más NICs.
- Appliances o dispositivos de hardware (a modo de cajas negras) que han sido diseñados para cumplir esta tarea especifica.

Funcionalidades accesorias

Por su ubicación estratégica en la arquitectura de la red y sus sistemas suelen incorporar otras funcionalidades de alcance perimetral a fin de agregar valor al producto. Algunas de ellas son:

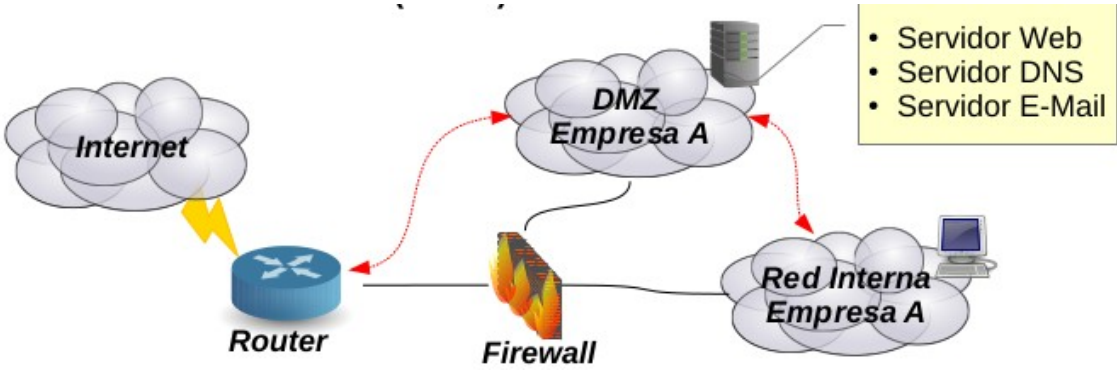
- Punto de conexión de VPNs
- VPN host a red
- VPN red a red
- Escaneo de Virus
- Filtrado de Contenidos / Anti Spam
- Balanceo de carga de Firewalls (BCFW)
- Alta Disponibilidad (AD), cuando se posee mas de un vínculo (agregado de ancho de banda)

Defensa en profundidad

Usando múltiples tipos de firewalls en serie se puede obtener los beneficios de todos y no ser vulnerable a la debilidad de uno solo. Adicionalmente se debe manejar una administración Centralizada para proveer un único punto de administración para todos los firewalls de la red.

DMZ – Zona Desmilitarizada

Es un área de configuración del firewall con reglas especificas orientada a manejar equipos que deben tener mayor exposición en la infraestructura, como por ejemplo los servidores Web, de Correo y otros.



Tipos de Firewall

Los firewalls pueden clasificarse por su tipo de filtrado en cuatro categorías

1 - Packet filters

Este tipo monitorea las direcciones IP de origen y destino de la conexión, verificando puertos pero no el contenido de la comunicación. Su actividad de filtrado se ejerce en el nivel tres del modelo TCP/IP, correspondiente a **Intenet Protocol (IP)**.

Los ataques de uso frecuente para este tipo son el **spoofing** *(Envió de información con un IP de origen falso)* y el **re-direccionamiento de puertos**.

2 - Circuit Level Gateways

Es un firewall que opera a nivel de la capa de sesión del modelo OSI o la capa TCP de TCP/IP, permitiendo conexiones a través de él y creando un circuito para monitorear la conexión con una verificación de contenido limitada.

3 - Application Level Gateways

Son conocidos con el nombre de proxies, siendo conceptualmente similares a los Circuit Level Gateways, con la diferencia de que son específicos para cada aplicación/protocolo. El firewall comienza una conexión en nombre del usuario y puede filtrar la aplicación si se configura el firewall para que espere solo cierto tráfico.

Como mantiene la conexión en nombre del usuario, produce una gran carga de trabajo. Las aplicaciones, ruteo, browsing y mail necesitan apuntar al firewall ó a una IP (alias) sobre el firewall para poder conectarse. Las conexiones UDP no se pueden manejar fácilmente.

4 - State–Full Multilayer Inspection

Combina los tres tipos previos (Packet filters, Circuit Level Gateways y Application Level Gateways). Usa protocolos de control de paso de contenidos a través de reglas de validación.

Entre sus características encontraremos:

- Utiliza algoritmos de identificación de datos y protocolos.
- Guarda una tabla de estado de conexiones que monitorea el estado de las conexiones TCP y permite el tráfico.
- Traduce direcciones.
- Autentica conexiones.
- Permite conexiones UDP a través de reglas y respuestas esperadas.
- Permite armar VPN con datos encriptados

Consideraciones sobre el uso de firewalls

- El mejor firewall no es un producto, es una combinación de factores.
- Un firewall es tan bueno como las políticas que se implementen.
- Se justifica su existencia en la reducción del impacto y/o probabilidad de amenazas que reduzcan el riesgo.
- Debe ser administrado pro-activamente, revisado y actualizado periódicamente
- Se puede implementar una combinación de firewalls.
- Los firewalls ayudan a proteger los recursos, pero son parte de un plan de seguridad general.

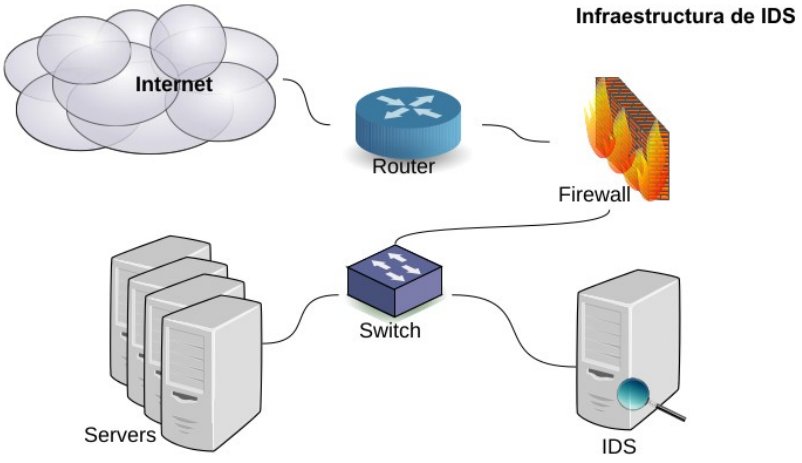
Firewalls Personales

Son dispositivos lógicos (software) que se instalan en la propia terminal y permiten aplicar filtros a la información de red correspondiente a cada interfaz y/o aplicación. Pueden utilizarse como un complemento al firewall de red, con el fin de prevenir ataques internos y actualmente se encuentran disponibles en la mayoría de los sistemas operativos.

IDS – Sistema de Detección de Intrusiones

Es un elemento que detecta, identifica y responde a actividades no autorizadas o anormales (Denning,1987).

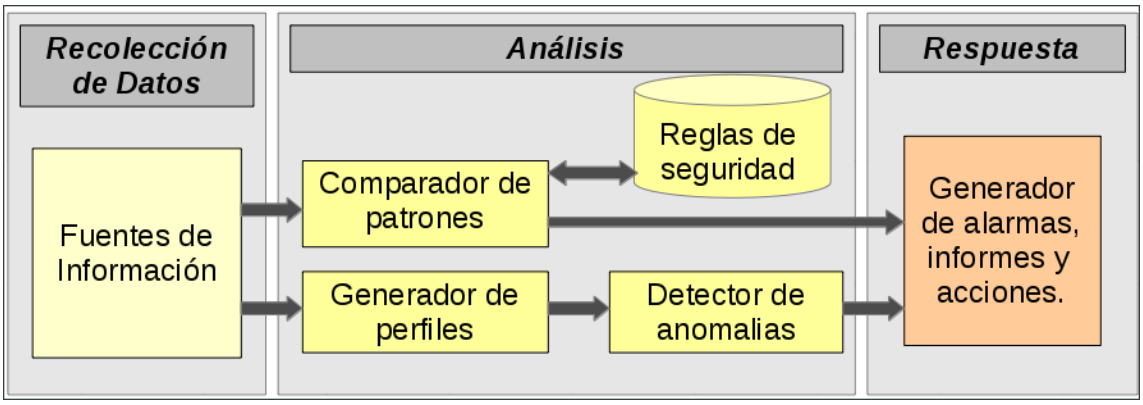
Intrusión: Conjunto de acciones que intentan comprometerla integridad, confidencialidad o disponibilidad de un recurso (Anderson, 1980).



Modelo de Funcionamiento General

El modelo de funcionamiento general de un IPS consta de las siguientes tres fases:

1. Recolección de datos: Registros de auditoría, de sistemas, de aplicaciones, de sistemas de archivos, de paquetes de red, etc.
2. Análisis: de usos indebidos, de anomalías.
3. Respuesta: activa, pasiva



Clasificaciones

Los IDS pueden tipificarse en dos grandes grupos por su fuente de datos

1 - HIDS (Sistema de Detección de Intrusiones de Maquina). Utilizan los registros de auditoría, Registros del sistema, Registros de aplicaciones (Servidor Web, FTP, etc.), sistema de archivos.

Ejemplos: Tripwire, Prelude, Imsafe, GFI, LANguard, S.E.L.M .

2 - NIDS (Sistema de Detección de Intrusiones de Red) y NNIDS (Sistema de Detección de Intrusiones de Nodo de Red). Utilizan paquetes de red (TCP,UDP,IP,...), con posibilidad de utilizar agentes (IDS Distribuido).

Ejemplos: Snort, Bro, Prelude, Suricata.

En relación a su metodología de análisis hay dos grandes grupos:

1 – Por detección de uso indebido, en este caso se utilizan los datos de auditoria para pre-establecer un perfil del sistema y declarar un estado de alerta cuando las actividades del sistema no se ajusten a dicho perfil.

Ejemplos: Snort, Bro

2 – Por detección de anomalías: Se utilizan los datos de auditoria para generar un perfil del sistema de forma dinámica y ante una desviación estadística entre dicha información y el comportamiento actual se declara el estado de ataque.

Ejemplos: Imsafe, Prelude

En cuanto al modo de respuestas también hay dos grandes grupos

1 - Respuesta pasiva, en este caso se genera un registro de evento o un envió de alerta, como un email, ante la declaración de una situación de ataque.

2 - Respuesta activa, en este otro caso el sistema toma una acción automáticamente para evitar la continuidad del ataque declarado, como por ejemplo cerrar la sesión de un usuario o bloquear la conexión de un intruso.

IPS (Sistemas de Prevención de Intrusiones)

Es el resultado de la combinación de IDS + Firewall en respuesta activa, estos dispositivos Identifican el curso de un ataque y lo bloquean antes de que suceda.

Ej: IntruShield, Hogwash, Radware, Storm watch. ISS, Juniper, Tipping Point (3Com), Cisco, Suricata, etc.

Dispositivos UTM

Son firewalls de red que manejan diferentes servicios en un mismo equipo. Algunos de ellos son:

- Función de un firewall de inspección de paquetes
- Función de VPN (para hacer túneles o redes privadas)
- Antispam (para evitar los correos no deseados o spam)
- Antiphishing (evitar el robo de información)
- Antispyware
- Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías)
- Antivirus de perímetro (evitar la infección de virus informáticos en computadoras clientes y servidores)
- Detección/Prevención de Intrusos (IDS/IPS)

Los dispositivos UTM (Unified Threat Management) son soluciones centrales y fáciles de instalar. Funcionan en forma de sistemas de control de acceso a redes. Algunos UTMs examinan los paquetes desde la capa uno a la siete (del modelo OSI), pero sólo una vez, así se puede implementar una solución de seguridad en tiempo real sin afectar a la performance de la red.

Los UTM se pueden integrar con toda la infraestructura legacy utilizando SOA (Service Oriented Architecture) y otras arquitecturas extensibles .

Usualmente los encontraremos configurados con los siguientes modos:

Modo proxy

Hacen uso de proxies para procesar y redirigir todo el tráfico interno. El firewall UTM hace de cliente y de servidor, y es el intermediario indirecto de las comunicaciones desde y hacia el internet (o otras redes).

Modo Transparente

No redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones hardware pero es la mejor alternativa de UTM.

NGFW - Next Generation Firewalls

La Nueva Generación de Firewalls se basa en la inspección profunda de paquetes, sumada a las tecnologías para evitar intrusiones y de firewalls tradicionales.

El producto ideal es el que combinaría capacidades de firewall a nivel de la red con inspección profunda de paquetes y pueda ir incorporando nuevas características para resolver nuevas amenazas.

Los mayores desafíos a la seguridad se originan en: administración de configuración de la red empresarial; ejecutivos senior que no aplican políticas; el uso de parches como política de actualización; y por último el alto movimiento de los entornos, con su tráfico elevado y complejo en las redes.

Acceso de Personal Contratado o Consultores

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

Accesos Públicos

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

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

Seguridad Lógica - Administración de Seguridad

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

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

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

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

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

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

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

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

Administración del Personal y Usuarios - Organización del Personal

Este proceso lleva generalmente cuatro pasos:

- Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
- Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

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

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

Seguridad física

Seguridad Física - Incendios

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Seguridad del Equipamiento

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Recomendaciones

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

Suministrar información, del centro de computo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento esté consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

Seguridad Física - Condiciones Climatológicas

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

Seguridad Física - Instalación Eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Picos y Ruidos Electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxil o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

Cableado de Alto Nivel de Seguridad

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

Pisos de Placas Extraíbles

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

Sistema de Aire Acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Emisiones Electromagnéticas

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

Seguridad Física - Ergometría

"*La **Ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.*"

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

Trastornos Óseos y/o Musculares

Una de las maneras de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, y esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural.

En el ambiente informático, la operación del teclado es un movimiento repetitivo y continuo, si a esto le sumamos el hecho de trabajar con una distribución ineficiente de las teclas, el diseño antinatural del teclado y la ausencia (ahora atenuada por el uso del mouse) de movimientos alternativos al de tecleado, tenemos un potencial riesgo de enfermedades o lesiones en los músculos, nervios y huesos de manos y brazos.

En resumen, el lugar de trabajo debe estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variará de acuerdo a los distintos usuarios, lo fundamental en todo esto es que el puesto de trabajo sea ajustable, para que pueda adaptarse a las medidas y posiciones naturales propias de cada operador.

Trastornos Visuales

Los ojos, sin duda, son las partes más afectadas por el trabajo con computadoras.

La pantalla es una fuente de luz que incide directamente sobre el ojo del operador, provocando, luego de exposiciones prolongadas el típico cansancio visual, irritación y lagrimeo, cefalea y visión borrosa.

Si a esto le sumamos un monitor cuya definición no sea la adecuada, se debe considerar la exigencia a la que se someterán los ojos del usuario al intentar descifrar el contenido de la pantalla. Además de la fatiga del resto del cuerpo al tener que cambiar la posición de la cabeza y el cuello para acercar los ojos a la misma.

Para prevenir los trastornos visuales en los operadores podemos tomar recaudos como:

- Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
- Usar de pantallas antirreflejo o anteojos con protección para el monitor, es una medida preventiva importante y de relativo bajo costo, que puede solucionar varios de los problemas antes mencionados.

La Salud Mental

La carga física del trabajo adopta modalidades diferentes en los puestos informatizados. De hecho, disminuye los desplazamientos de los trabajadores y las tareas requieren un menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

Por su parte, la estandarización y racionalización que tiende a acompañar la aplicación de las PCs en las tareas de ingreso de datos, puede llevar a la transformación del trabajo en una rutina inflexible que inhibe la iniciativa personal, promueve sensaciones de hastío y monotonía y conduce a una pérdida de significado del trabajo.

Además, el estrés informático está convirtiéndose en una nueva enfermedad profesional relacionada con el trabajo, provocada por la carga mental y psíquica inherente a la operación con los nuevos equipos.

Los efectos del estrés pueden encuadrarse dentro de varias categorías:

- Los efectos fisiológicos inmediatos, caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardiaca, etc.
- Los efectos psicológicos inmediatos hacen referencia a la tensión, irritabilidad, cólera, agresividad, etc. Estos sentimientos pueden, a su vez, inducir ciertos efectos en el comportamiento tales como el consumo de alcohol y psicofármacos, el hábito de fumar, etc.
- También existen consecuencias médicas a largo plazo, tales como enfermedades coronarias, hipertensión arterial, úlceras pépticas, agotamiento; mientras que las consecuencias psicológicas a largo plazo pueden señalar neurosis, insomnio, estados crónicos de ansiedad y/o depresión, etc.
- La apatía, sensaciones generales de insatisfacción ante la vida, la pérdida de la propia estima, etc., alteran profundamente la vida personal, familiar y social del trabajador llevándolo, eventualmente, al aislamiento, al ausentismo laboral y la pérdida de la solidaridad social.

Ambiente Luminoso

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

Ambiente Climático

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

Seguridad Física - Utilización de Guardias

Control de Personas

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por **algo que posee**, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identification Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.

- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

Las personas también pueden acceder mediante **algo que saben** (por ejemplo un número de identificación o una password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

Control de Vehículos

Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

Desventajas de la Utilización de Guardias

La principal desventaja de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o egresar de la planta con materiales no autorizados. Esta situación de soborno es muy frecuente, por lo que es recomendable la utilización de sistemas biométricos para el control de accesos.

Seguridad Física - Sistemas Biométricos

Definimos a la **Biometría** como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona **por lo que es** (manos, ojos, huellas digitales y voz).

Los Beneficios de una Tecnología Biométrica

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

Emisión de Calor

Se mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

Huella Digital

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

Verificación de Voz

La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de animo y enfermedades de la persona, el envejecimiento, etc.

Verificación de Patrones Oculares

Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

Seguridad Física - Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Barreras Infrarrojas y de Micro-Ondas

Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa.

Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las micro-ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

Detector Ultrasónico

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

Detectores Pasivos Sin Alimentación

Estos elementos no requieren alimentación extra de ningún tipo, sólo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes están incluidos dentro de este tipo de detectores:

- Detector de aberturas: contactos magnéticos externos o de embutir.
- Detector de roturas de vidrios: inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
- Detector de vibraciones: detecta golpes o manipulaciones extrañas sobre la superficie controlada.

Sonorización y Dispositivos Luminosos

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc.

Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

Circuitos Cerrados de Televisión

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

Edificios Inteligentes

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos.

El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.