

CAPÍTULO 2

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar



“Un experto es aquel que sabe cada vez más sobre menos cosas, hasta que sabe absolutamente todo sobre nada.. es la persona que evita los errores pequeños mientras sigue su avance inexorable hacia la gran falacia”

Definición de Webwer—Corolario de Weinberger (Leyes de Murphy)

SEGURIDAD FÍSICA

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la **Seguridad Física** consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”¹. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.1 TIPOS DE DESASTRES

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Entre Ríos, técnicas de seguridad ante terremotos; pero sí será de máxima utilidad en Los Angeles, EE.UU.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

2.1.1 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.

¹ HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. <http://www.kriptopolis.com>

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:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. 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.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
4. Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
5. No debe estar permitido fumar en el área de proceso.
6. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
7. El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

2.1.1.1 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 18° 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).

2.1.1.2 RECOMENDACIONES

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

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.

2.1.2 INUNDACIONES

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

2.1.3 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.

2.1.3.1 TERREMOTOS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

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.

2.1.4 SEÑALES DE RADAR

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

2.1.5 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.

2.1.5.1 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.

2.1.5.2 CABLEADO

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial 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:

1. 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.
2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. 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:

1. 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.
2. 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.

2.1.5.2.1 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.

2.1.5.2.2 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.

2.1.5.3 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.

2.1.5.4 EMISIONES ELECTROMAGNÉTICAS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

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.

2.1.6 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.”²

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.

2.1.6.1 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.

2.1.6.2 TRASTORNOS VISUALES

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

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:

² ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1º Edición. Argentina. 1997. Página 30.

1. Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
2. 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.

2.1.6.3 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:

1. Los efectos fisiológicos inmediatos, caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardíaca, etc.
2. 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.
3. 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.
4. 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.

2.1.6.4 AMBIENTE LUMINOSO

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

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.

2.1.6.5 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.

2.2 ACCIONES HOSTILES

2.2.1 ROBO

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraible y las cintas y discos son fácilmente copiados sin dejar ningún rastro

2.2.2 FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

2.2.3 SABOTAJE

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

2.3 CONTROL DE ACCESOS

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

2.3.1 UTILIZACIÓN DE GUARDIAS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

2.3.1.1 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.

2.3.1.2 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.

2.3.2 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.

2.3.3 UTILIZACIÓN DE DETECTORES DE METALES

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

2.3.4 UTILIZACIÓN DE 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).

2.3.4.1 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.

2.3.4.2 EMISIÓN DE CALOR

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

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

2.3.4.3 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.

2.3.4.4 VERIFICACIÓN DE VOZ

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

La dicción de una (o más) frase es grabada y en el acceso se compara la voz (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.

2.3.4.5 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.

2.3.5 VERIFICACIÓN AUTOMÁTICA DE FIRMAS (VAF)

En este caso lo que se considera es **lo que el usuario es capaz de hacer**, aunque también podría encuadrarse dentro de las verificaciones biométricas.

Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

2.3.6 SEGURIDAD CON ANIMALES

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema. Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

2.3.7 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.

2.3.7.1 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.

2.3.7.2 DETECTOR ULTRASÓNICO

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

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.

2.3.7.3 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:

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

2.3.7.4 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.

2.3.7.5 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.

2.3.7.6 EDIFICIOS INTELIGENTES

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar□ www.cfbsoft.com.ar□
--

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.

2.4 CONCLUSIONES

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad
- descartar falsas hipótesis si se produjeran incidentes
- tener los medios para luchar contra accidentes

Tesis "Seguridad Informática: Sus Implicancias e Implementación". Copyright Cristian F. Borghello 2001 webmaster@cfbsoft.com.ar www.cfbsoft.com.ar
--

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

SEGURIDAD FÍSICA	1
2.1 TIPOS DE DESASTRES.....	2
2.1.1 INCENDIOS	2
2.1.1.1 Seguridad del Equipamiento.....	3
2.1.1.2 Recomendaciones	3
2.1.2 INUNDACIONES	4
2.1.3 CONDICIONES CLIMATOLÓGICAS.....	4
2.1.3.1 Terremotos.....	4
2.1.4 SEÑALES DE RADAR.....	5
2.1.5 INSTALACIÓN ELÉCTRICA	5
2.1.5.1 Picos y Ruidos Electromagnéticos.....	5
2.1.5.2 Cableado.....	5
2.1.5.3 Sistema de Aire Acondicionado	6
2.1.5.4 Emisiones Electromagnéticas.....	6
2.1.6 ERGOMETRÍA	7
2.1.6.1 Trastornos Óseos y/o Musculares	7
2.1.6.2 Trastornos Visuales	7
2.1.6.3 La Salud Mental.....	8
2.1.6.4 Ambiente Luminoso	8
2.1.6.5 Ambiente Climático	9
2.2 ACCIONES HOSTILES	9
2.2.1 ROBO	9
2.2.2 FRAUDE	9
2.2.3 SABOTAJE	9
2.3 CONTROL DE ACCESOS.....	10
2.3.1 UTILIZACIÓN DE GUARDIAS	10
2.3.1.1 Control de Personas	10
2.3.1.2 Control de Vehículos	10
2.3.2 DESVENTAJAS DE LA UTILIZACIÓN DE GUARDIAS	11
2.3.3 UTILIZACIÓN DE DETECTORES DE METALES.....	11

2.3.4 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS	11
2.3.4.1 <i>Los Beneficios de una Tecnología Biométrica</i>	11
2.3.4.2 <i>Emisión de Calor</i>	11
2.3.4.3 <i>Huella Digital</i>	12
2.3.4.4 <i>Verificación de Voz</i>	12
2.3.4.5 <i>Verificación de Patrones Oculares</i>	12
2.3.5 VERIFICACIÓN AUTOMÁTICA DE FIRMAS (VAF)	12
2.3.6 SEGURIDAD CON ANIMALES	13
2.3.7 PROTECCIÓN ELECTRÓNICA	13
2.3.7.1 <i>Barreras Infrarrojas y de Micro-Ondas</i>	13
2.3.7.2 <i>Detector Ultrasónico</i>	13
2.3.7.3 <i>Detectores Pasivos Sin Alimentación</i>	14
2.3.7.4 <i>Sonorización y Dispositivos Luminosos</i>	14
2.3.7.5 <i>Circuitos Cerrados de Televisión</i>	14
2.3.7.6 <i>Edificios Inteligentes</i>	14
2.4 CONCLUSIONES.....	15