CONTROL DE ACCESO

Las barreras perimetrales, los dispositivos de detección de la intrusión, y la iluminación protectora proporcionan medidas de seguridad física; sin embargo, por si solas no son suficientes. Debe establecerse y mantenerse un sistema de control del acceso a fin de precluir el ingreso no autorizado.

La función de un sistema de control de acceso es asegurar que únicamente le sea permitido a personal autorizado estar dentro o fuera un área controlada. El ingreso a una edificación o a cuartos dentro una edificación puede controlarse mediante puertas de cercas con llave, puertas con llave, o especialmente mediante portales (portones) o entradas principales específicamente diseñadas.

Estos medios de control del ingreso pueden implementarse manualmente por los guardias o automáticamente mediante el uso de dispositivos de control del ingreso. **En un sistema manual,** los guardias verifican que una persona se encuentra autorizada para entrar a un área, usualmente comparando la fotografía y las características personales del individuo que solicite ingreso. **En un sistema automatizado,** el dispositivo de control del ingreso verifica que una persona está autorizada para entrar o salir.

El sistema automatizado usualmente va en interface con mecanismos de cerradura de puertas que se abren momentáneamente para permitir el paso. El hardware o accesorios mecánicos (tales como mecanismos de cerradura, cerrojos de activación eléctrica para puertas, y dispositivos especialmente diseñados para portales) junto con el equipo usado para detectar material de contrabando.

Todos los sistemas de control del ingreso controlan la admisión usando una o más de tres técnicas básicas:

1- Algo que una persona conoce
2- Algo que una persona tiene
3- Algo que una persona es o hace

Los dispositivos automatizados de control del ingreso basados en estas técnicas se agrupan en tres categorías — **dispositivos de código, dispositivos tipo credenciales, y dispositivos biométricos.**

Dispositivos de Código: Operan sobre el principio de que una persona a quien se le ha asignado un código, debe ingresarlo en un dispositivo de control del ingreso. Este código deberá coincidir con el código almacenado en el dispositivo y permitir el ingreso. Puede usarse un solo código por todas las personas autorizadas o a cada persona autorizada puede asignársele un código único.

Los códigos individuales usualmente se requieren para el control del ingreso a áreas más críticas. Los dispositivos de código verifican la autenticidad del código ingresado, y cualquier persona que ingrese un código correcto es autorizada para entrar al área controlada. Entre los dispositivos de codificación electrónica se incluyen los teclados electrónicos y los teclados controlados por computador.

Dispositivos de Teclado Electrónico: El teclado de un teléfono común (12 teclas) es un ejemplo de un teclado electrónico. Este tipo de teclado consta de interruptores de pulsado de botones sencillos que, al oprimirse, son decodificados por circuitos lógicos digitales. Cuando se pulsa la secuencia correcta de botones, una señal eléctrica desbloquea la puerta durante unos pocos segundos.

Dispositivos de Teclado Controlado por Computador: Estos dispositivos son similares a los dispositivos de teclado electrónico, excepto que van equipados con un microprocesador en el teclado o en una cubierta separada en un lugar diferente. El microprocesador monitorea la secuencia en la cual las teclas son oprimidas y pueden tener funciones adicionales tales como identificación personal y decodificación digital. Si se ingresa el código correcto y se satisfacen todas las condiciones, una señal eléctrica quitará el seguro de la puerta.

Dispositivos Tipo Credenciales: Identifica a la persona que tenga permiso legítimo para ingresar al área controlada. Un credencial codificada (tarjeta plástica o llave) contiene un código previamente grabado legible por una máquina. Una señal eléctrica desbloquea la puerta si el código pregrabado coincide con el código almacenado en el sistema luego de que se lea la tarjeta. Al igual que los dispositivos codificados, los dispositivos tipo credencial únicamente autentican la credencial, por cuanto se presume que un usuario con una credencial genuina tiene autorización para entrar.

Se emplean diversas tecnologías para almacenar el código sobre o dentro de la tarjeta. Los tipos de tarjetas de mayor uso son los que se describen a continuación:

Tarjeta de Banda Magnética

Se trata de una tira de material magnético localizada a lo largo de uno de los bordes de la tarjeta la cual va codificada con datos (algunos veces encriptados). Los datos son leídos al pasar la tarjeta por una cabeza de lectura magnética.

Tarjeta Basada en el Efecto Wiegand

La tarjeta basada en el efecto Wiegand contiene una serie de alambres paralelos de diámetro pequeño de aproximadamente media pulgada de largo, incrustados en la mitad inferior de la tarjeta. Los alambres son manufacturados de materiales

ferromagnéticos que producen un cambio agudo en el flujo magnético cuando se exponen a un campo magnético que cambia lentamente. Este tipo de tarjeta es inmune al borrado accidental. La lectora de tarjetas contiene una pequeña cabeza de lectura y un magneto pequeñísimo para suministrar el campo magnético aplicado. Usualmente no requiere fuente de energía externa.

Tarjeta de Proximidad

La tarjeta de proximidad físicamente no es insertada en una lectora; el patrón codificado sobre la tarjeta es detectado cuando la tarjeta se coloca a varias pulgadas de la lectora. Se usan varias técnicas para codificar las tarjetas. Una técnica acude al uso de cierto número de circuitos eléctricamente sintonizados incrustados dentro de la tarjeta. Los datos se codifican variando las frecuencias resonantes de los circuitos sintonizados. La lectora contiene un transmisor que continuamente hace un barrido a través una rango especificado de frecuencias y un receptor detecta el patrón de frecuencias resonantes contenidas en la tarjeta. Otra técnica usa un circuito integrado incrustado en la tarjeta para generar un código que puede magnéticamente o electrostáticamente acoplarse a la lectora. La energía eléctrica requerida para activar los circuitos incrustados puede proporcionarla una pequeña batería empotrada en la tarjeta o mediante acoplamiento magnético de la energía de la lectora.

Tarjeta Láser

La tarjeta de memoria óptica, comúnmente denominada tarjeta láser, emplea la misma tecnología desarrollada para la grabación de discos de video y audio para aplicaciones como el entretenimiento. Los datos se graban en la tarjeta mediante el quemado de orificios microscópicos (usando un láser) sobre una película fina que recubre la tarjeta. Los datos se leen usando un láser para detectar los lugares en donde se hicieron dichos orificios. La tarjeta láser típica puede contener varios megabytes de información sobre el usuario.

Tarjeta Inteligente

Una tarjeta inteligente es aquella que tiene incrustado un microprocesador, memoria, circuitos de comunicación, y una batería. La tarjeta contiene contactos en sus bordes que hacen posible que la lectora se comunique con el microprocesador. La información sobre control del ingreso y otros datos pueden almacenarse en la memoria del microprocesador.

Código de Barras

Un código de barras consta de barras de color negro impresas en papel blanco o cinta, el cual puede fácilmente leerse con un escáner óptico. Este tipo de

codificación no es ampliamente usado para el aplicaciones como el control del ingreso debido a que puede fácilmente duplicarse. Es posible ocultar el código aplicando una mascarilla opaca sobre éste. En este método, se usa un escáner de IR para interpretar el código impreso. Para el caso de áreas que necesiten un nivel de seguridad bajo, el uso de códigos de barras puede proporcionar una solución costo-efectiva para el control del ingreso. Las tiras codificadas y las mascarillas opacas pueden adherirse a las insignias de ID existentes, solucionando la necesidad del completo reemplazo de las insignias.

Dispositivos Biométricos

La tercera técnica básica usada para controlar el ingreso se fundamenta en la medición de una o más características físicas o personales de un individuo. Debido a que la mayoría de los dispositivos de control del ingreso se basan en esta técnica que acude a la medición de características biológicas, tales dispositivos comúnmente se conocen con el nombre de dispositivos biométricos. Características tales como las huellas digitales, geometría de la mano, impresiones de la voz, la escritura a mano, y los patrones de los vasos sanguíneos retinianos se han venido utilizando para controlar el ingreso. Típicamente, en los individuos objeto de identificación, se efectúan varias mediciones de referencia de la característica física seleccionada y luego se almacenan en la memoria del dispositivo o sobre una tarjeta. Posteriormente, cuando la persona intenta el ingreso, se compara un escaneo de dicha característica con la plantilla que se tiene de los datos de referencia. Si se encuentra una coincidencia, se concederá el ingreso. En lugar de verificar un artefacto, como por ejemplo un código o una credencial, los dispositivos biométricos verifican una característica física de una persona, proporcionando así una forma de verificación de la identidad. Debido a esto, los dispositivos biométricos con frecuencia se les conoce como dispositivos de verificación de la identidad personal. A continuación se describen los dispositivos biométricos más comunes.

Huellas Digitales

Los dispositivos de verificación de huella digital usan una de dos técnicas. La primera es el reconocimiento del patrón de líneas, círculos, y tendencias de la huella digital referenciadas, la cual es almacenada en una representación digitalizada de la imagen y luego comparada con la huella digital de la persona que intente entrar. La segunda técnica consiste en la comparación minuciosa, lo que significa que las terminaciones y puntos de terminación de las crestas y valles de la huella digital en referencia son comparados con las de la huella digital de la persona que intente ingresar.

Geometría de la Mano

Varios dispositivos se encuentran a disposición los cuales usan la geometría de la mano para efectos de la verificación personal. Estos dispositivos usan una variedad de mediciones físicas de la mano, tales como la longitud de los dedos, la curvatura de los dedos, el ancho de la mano, la separación entre dedos, y la transmisividad de la luz a través de la piel a fin de verificar la identidad. Se encuentran a disposición unidades tanto bidimensionales como tridimensionales.

Patrones Retinianos

Este tipo de técnica se basa en la premisa de que el patrón de los vasos sanguíneos de la retina del ojo humano es exclusivo para un individuo. Si bien el ojo debe enfocarse hacia un blanco visual, un haz de luz IR de baja intensidad escanea un área circular de la retina. La cantidad de luz reflejada por el ojo es registrada a medida que el haz progresa alrededor de la ruta circular. La luz reflejada es modulada por la diferencia en la reflectividad entre el patrón de los vasos sanguíneos y el tejido adyacente. Esta información luego se procesa y convierte en una plantilla digital que será almacenada como si fuera la firma del ojo. Puede permitirse el uso de lentes de contacto por los usuarios; sin embargo, si deberán quitarse los anteojos.

Combinaciones de Dispositivos

Frecuentemente, un sistema automatizado de control del ingreso emplea combinaciones de los tres tipos de dispositivos de control del ingreso. La combinación de dos dispositivos diferentes puede significativamente mejorar el nivel del sistema de seguridad. En algunos casos, tal combinación de dispositivos da lugar a la reducción de los tiempos de verificación.

Pautas Para la Aplicación

La función primaria de un sistema automatizado de control del ingreso es permitir que el personal autorizado entre a un área controlada o salga de ésta. A continuación se describen aspectos importantes a tener en cuenta por el diseñador.

Inscripción. Todos los sistemas de control del ingreso deben proporcionar un medio de registrar, actualizar, y suprimir información acerca de los individuos autorizados en los archivos de la base de datos del sistema. Esto usualmente se realiza con una estación exclusivamente dedicada a la inscripción / borrado de personas autorizadas y visitantes, directamente conectada a la unidad de procesamiento central. Cuando se usen dispositivos del tipo de credenciales, deberá proporcionarse a todos los usuarios autorizados una apropiada credencial.

También deberá suministrarse un medio para des-inscribir (borrar) rápidamente una persona sin tener recuperar su credencial. Al usar dispositivos biométricos, se necesitará un equipo adicional para la inscripción.

Técnicas de control del ingreso. Algunas funciones del control del ingreso exigen hardware adicional, mientras que otras se pueden ejecutar con el software. Aquellas acciones ejecutadas con software requieren que se encuentre a disposición la apropiada base de datos en cada estación de ingreso/salida afectada por tales acciones. Típicamente, entre tales técnicas se incluyen:

- Zonas de área.
- Zonas de tiempo.
- Zonas de equipo.
- Anti-pass back (Regreso restringido).
- Recorrido de guardias.
- Control de Ascensores
-

Alarmas. Pueden usarse varios tipos de alarmas con un sistema de control del ingreso. Estas alarmas deben anunciarse tanto audible como visualmente en el centro de seguridad.

1-Negación del ingreso. La mayoría de los dispositivos de control del ingreso son configurados de modo que permitan al usuario tres intentos de ingreso. Si se efectúan más de tres intentos no exitosos de ingreso durante un período de tiempo predeterminado, el dispositivo generará una alarma. También se generará una alarma si se usa una credencial inválida o se detectan intentos de ingreso que violen las exigencias específicas de área, de tiempo, o del personal de seguridad.
2-Fallas en la comunicación. Esta alarma es generada cuando se detecta una pérdida en la comunicación entre el procesador central y el equipo local.
3-Entrada principal abierta. Si una puerta de la entrada principal queda abierta por un tiempo más prolongado respecto del tiempo pre-establecido, se generará una alarma.
4-Coacción. Esta alarma se genera cuando se ingresa un código anti-coacción en un teclado.
5-Guardia vencido. Est**a** alarma anti-coacción se genera cuando se determina que un guardia de seguridad ha sido vencido en un punto de chequeo durante una ronda predefinida de guardias.
6-Manipulación no autorizada del software. Este tipo de alarma se genera cuando se detecta que personas no autorizadas intentan invocar ciertos comandos del sistema o intentan modificar los archivos de la base de datos.

Criterios de Desempeño

El desempeño global de un sistema de control del ingreso puede evaluarse examinando la tasa de errores de verificación y el indicador de eficiencia. Un

sistema de control del ingreso puede producir dos tipos de errores —negación del ingreso a una persona que debería haberse admitido o la admisión de una persona que no debería haber sido admitida. Estos son comúnmente denominados **errores de rechazo falso** (errores de tipo I) **y errores de aceptación falsa** (errores tipo II). Aunque un error de rechazo falso no constituye una violación a la seguridad, si crea un problema operacional que debe manejarse mediante un método alternativo. Los errores de aceptación falsa constituyen una violación de seguridad. Idealmente, tanto la tasa de errores de rechazo falso como la tasa de errores de aceptación falsa deberán ser cero. En la práctica, sin embargo, no lo son. En efecto, tales tasas entran en contraposición entre sí. Cuando se ajusta el sistema para reducir la tasa de errores de aceptación falsa, la tasa de errores de rechazo falso usualmente se incrementan.

Las tasas de errores de verificación típicamente se miden en porcentaje (número de errores/número de intentos x 100 %). Estas tasas de error típicamente son muy bajas en el caso de los dispositivos de código y las credenciales, pero podrían incrementarse significativamente si se usan dispositivos biométricos.

El índice de eficiencia es el número de personas que pueden pasar a través de un punto de ingreso en una unidad dada de tiempo y usualmente se expresa en personas por minuto. Este índice tiene que ver con el tiempo requerido para abordar el dispositivo de control del ingreso y para que el dispositivo verifique la información (tiempo de verificación), junto con el tiempo requerido para pasar el punto de ingreso. Típicamente, un individuo puede abordar el dispositivo y pasarlo en 3 - 5 segundos. El tiempo de verificación depende del tipo de dispositivo y puede variar entre 3 y 15 segundos. La Tabla 6-5 proporciona una lista de tiempos de verificación típicos de diferentes tipos de dispositivos de control del ingreso.

Tiempos de Verificación Típicos de Dispositivos de Control del Ingreso

Dispositivo	**Tiempo de Verificación**
Teclado	3 segundos
Lectora de tarjetas	3 segundos
Teclado/lectora de tarjetas	6 segundos
Biométricos/teclado	6 - 15 segundos
Biométricos/ lectora de tarjetas	6 - 15 segundos
Biométricos	2 minutos

Las planillas de control del acceso, el reconocimiento del personal, las tarjetas de identificación, los procedimientos de intercambio de insignias o tarjetas de ID, y las escoltas o acompañamiento del personal contribuye todo a un sistema de control eficaz del acceso.

Áreas Restringidas DESIGNADAS

El jefe de seguridad del sitio es responsable de la designación y establecimiento de las áreas restringidas. Un área restringida es cualquier área que se encuentre sometida a restricciones o controles especiales por razones de seguridad, Las áreas restringidas pueden establecerse para lo siguiente:

- Puesta en práctica de las medidas de seguridad y la exclusión de personal no autorizado.
- Controles intensificados en áreas que requieran protección especial.
- Protección de la información clasificada, o de equipos o materiales cruciales.

Grado de Seguridad

El grado de seguridad y control requeridos depende de la naturaleza, sensibilidad, o importancia del activo objeto de la seguridad. Las áreas restringidas son clasificadas como áreas controladas, limitadas, o áreas de exclusión.

- Un **área controlada** es aquella porción de un área restringida usualmente cercana o circundante a un área limitada o a una de exclusión. El ingreso al área controlada deberá permitirse únicamente al personal que tenga necesidad de acceso. El movimiento de personal autorizado dentro de esta área no necesariamente deberá controlarse puesto que el solo ingreso al área no proporciona acceso al activo a proteger. El área controlada se proporciona para efectos de control administrativo, por razones de seguridad industrial, o como una zona buffer (de retardo) para más seguridad del área limitada o del área de exclusión. El jefe de seguridad deberá ser quien establezca el control del movimiento o tránsito por las diferentes áreas.

- Un **área limitada** es un área restringida de cercana proximidad a un activo a proteger. El movimiento no controlado puede permitir el acceso al activo de interés. Los escoltas u otras restricciones internas pueden impedir el acceso a las áreas limitadas.

- Un **área de exclusión** es un área restringida que contiene un activo a proteger. El movimiento no controlado puede permitir el acceso directo al activo.