CONTROL DE ACCESOS MX

REVISTA DIGITAL

ESPECIALIZADA EN CONTROL DE ACCESOS

www.controldeaccesosmx.com

CONTROL DE ACCESO

"La primera línea de defensa"

Por Rafaela Silva, Security Supplier Relation Manager, Anixter Caribbean & Latin America

Dentro de la tecnología de seguridad electrónica, el control de acceso está en la cima de la pirámide en términos de criticidad, junto con los sistemas de detección y alarma contra incendios. Por ejemplo: Si comparamos el control de acceso con circuito cerrado de televisión o con detección de intrusos, si una cámara o sensor no estuviera funcionando, incluso el usuario común del sistema podría notar este fracaso. Sin embargo, si hay alguna falla de funcionamiento en el control de acceso, se darían cuenta de inmediato, debido a que el usuario no podría entrar en el sitio protegido. Y lo que es peor, ¡no podrá salir! Y en caso de una situación de emergencia como el comienzo de un incendio, esto puede ser crítico.

De ahí la importancia de elegir una solución de control de acceso segura, confiable y estable.

El control de acceso electrónico ha surgido para resolver algunos problemas relacionados con el uso de llaves, cerraduras y cerrojos mecánicos. El uso de la llave metálica convencional, tal y como la conocemos hoy, tiene varios factores negativos. Los principales se discuten a continuación:

- Las llaves pueden ser copiados: Al portar una llave, se puede ir a cualquier cerrajería y solicitar una o más copias;
- No hay un histórico: No es posible saber la fecha y hora en que un portador de una llave entre o salga de un lugar específico, ni el número de veces que lo hizo.
- Pérdida de llaves: Cuando esto ocurre, es necesario el intercambio de juegos de cerraduras y cerrojos para mantener el lugar seguro.
- No hay tiempos de restricción: El portador de la llave puede entrar en el sitio protegido en cualquier día y hora determinada, incluyendo fines de semana y días festivos.
- Gestión de la posesión de llaves: ¿Con quién está cada llave? Esta es una pregunta difícil de responder si no hay un control eficiente de las llaves.
- Llaves Múltiples: Para cada puerta se requiere una llave separada. Esto lleva a que los gerentes tengan que portar diferentes llaves.

El control de acceso electrónico resuelve todos los problemas anteriores. En lugar de una llave de metal, que se puede copiar fácilmente, ahora se utiliza una tarjeta electrónica que puede tener distintos mecanismos de cifrado y protección contra la duplicación, garantizado por los fabricantes. Además, los lectores biométricos pueden ser programados para prevenir que un usuario utilice la tarjeta de otra persona.

Con el control de acceso se puede restringir fácilmente días y horarios de acceso y emitir informes detallados de la actividad del usuario. Una sola tarjeta puede abrir todas las puertas desde que, obviamente, tenga los permisos de acceso para hacerlo.

Hoy en día, con la creciente adopción de equipos tercerizados de seguridad, el control de acceso ha tenido un papel muy importante para las empresas. Como la rotación de este personal de seguridad es alta, el personal de seguridad no es capaz de reconocer a todo el personal y saber si una persona pertenece o no a ese lugar en particular. Con el uso de un sistema de control de acceso electrónico, cada usuario debe utilizar su tarjeta, contraseña o biométrica para entrar en el espacio protegido. Por lo tanto, el criterio de autorización es impersonal, es decir, es realizado de forma automática por el sistema de control de acceso.

La primera variable que se fijará a la hora de elegir un sistema de control de acceso es la tecnología del lector y tarjeta. En la actualidad hay varias tecnologías como código de barras, magnética, Wiegand, Proximidad de 125 Khz, Smart Card (de contacto y sin contacto) y lectores biométricos. Muchas de estas tecnologías ya están obsoletas, y las que todavía están vigentes son: Tarjeta inteligente (Smart Card) con cifrado de clave propia y los lectores biométricos.

El control de acceso es la parte principal de la pirámide de criticidad de sistemas de seguridad. Así que la elección de una solución fiable es clave.

En cuanto a la topología, los sistemas de control de acceso se pueden clasificar como: Autónomo "Stand Alone" Con base en el servidor "Server based" o híbrido con Inteligencia Distribuida. A continuación hay una breve descripción de la operación de cada uno:

Sistemas Autónomos "Stand Alone": Se trata de sistemas que tienen su propia inteligencia y no requieren de software para operar. Toda la base de datos de usuarios y los permisos se almacenan en su memoria interna. Por lo general se trata de sistemas con capacidad limitada y no permiten la administración remota. Pueden ser auditables o no.

Sistemas en línea: En esta topología toda la inteligencia está en el servidor que es responsable de la liberación del acceso. Cuando una solicitud de acceso viene a través de un lector (proximidad, magnético, barras, biometría, etc.), se envía a un servidor, que va a revisar el nivel de otorgamiento de autorización, dando o no el acceso y devolviendo el comando de liberación.

Sistemas con Inteligencia Distribuida: En esta topología toda la inteligencia se encuentra en el controlador que es responsable de la liberación de acceso. Tras la liberación, el evento se envía al software en el servidor para el seguimiento y presentación de informes. En caso de pérdida de comunicación con el servidor se libera el acceso y se almacena el evento. A continuación se muestra un diagrama que muestra la topología de un sistema de control de acceso con inteligencia distribuida:

Los sistemas de control de acceso de inteligencia distribuidos son los más recomendables, ya que garantizan un funcionamiento incluso en caso de una caída de la red de comunicación o de fallo del servidor.

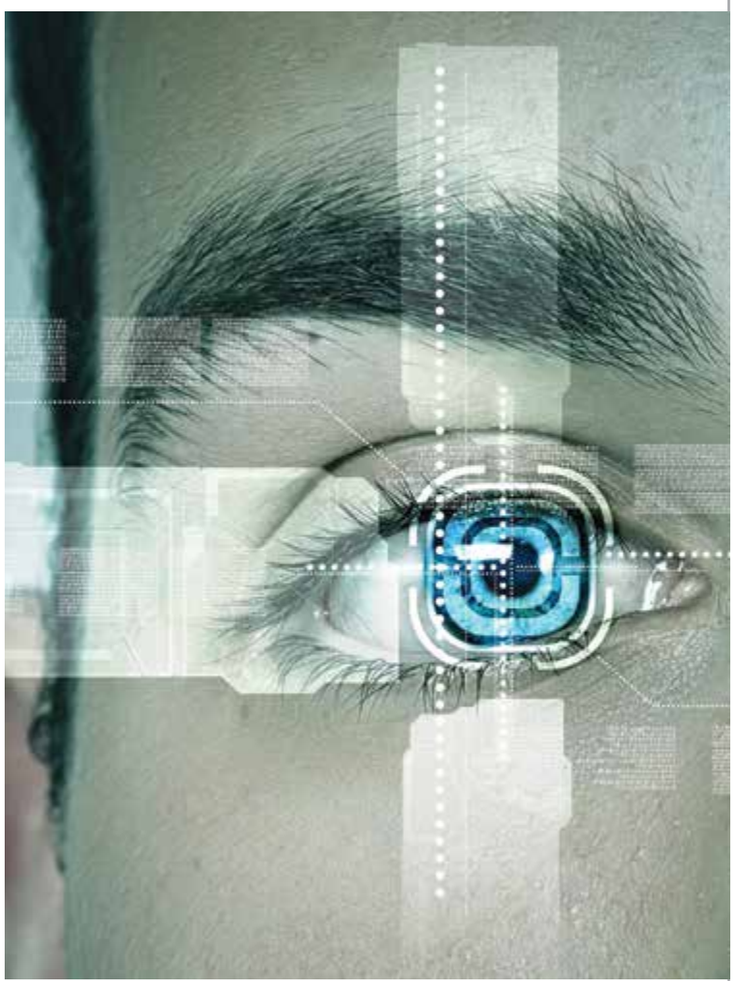
En resumen, a continuación encontramos algunas recomendaciones técnicas para la elección de una solución de control de acceso confiable y seguro:

El sistema de control de acceso debe:

- Tener su funcionamiento basado en la topología: Inteligencia distribuida;
- Permitir la integración con otros sistemas como CCTV, alarma contra intrusos, detección y alarma contra incendios, automatización, etc.;
- Utilizar tecnología de tarjetas inteligentes con cifrado para lectores/tarjetas y/o lectores biométricos en las zonas más restringidas;
- Tener arquitectura IP de comunicación entre los controladores y el software, con cifrado.

Además, es esencial elegir una empresa integradora certificada en la solución y con experiencia en el control de acceso.

Optar por una solución de control de acceso abierta que no se comercialice exclusivamente por una sola empresa. Con esto, el usuario final será libre de cambiar el instalador, en caso de que no esté prestando un buen servicio.



El control de acceso es la parte principal de la pirámide de criticidad de sistemas de seguridad. Así que la elección de una solución fiable es crítica. El uso de tecnologías de control de acceso ha crecido enormemente en los últimos años. Sin embargo, existen en el mercado muchas soluciones que no cumplen con los requisitos mínimos de seguridad, confiabilidad y estabilidad que estos sistemas requieren.

CONTROL DE ACCESOS
en oficinas bancarias

Las continuas fusiones entre entidades financieras, la reducción del número de oficinas de atención al público y el cambio en su modelo, unido a las nuevas formas de delito, obligan a los bancos a extremar la seguridad de las oficinas adaptándose a la evolutiva normativa vigente. Estas entidades están obligadas por ley a contar con medidas específicas de seguridad – que pasan tanto por su protección tecnológica como por el diseño de sus instalaciones, un exhaustivo mantenimiento de sus sistemas y la obligatoriedad de tener un director de seguridad que vele por su correcta implementación.

Los riesgos en las sucursales de banca han ido cambiando con los años: si hasta ahora los atracos en horario de atención al público eran los peligros más frecuentes, últimamente están proliferando los “atracos a la espera”, consistentes en realizar un butrón para esperar dentro de la oficina la llegada del primer empleado que cuenta con las claves para desbloquear la caja fuerte. A éstos, hay que sumar el fraude tecnológico que sigue en aumento y se puede llevar a cabo sin la intromisión física en las oficinas.

Incremento de la seguridad para el acceso a la cámara acorazada

En espacios que requieran una seguridad especial, como las cámaras acorazadas, se puede requerir el acceso por doble custodia que implica la presentación de 2 tarjetas de usuarios autorizados dentro del horario especificado, o doble custodia con escolta, en la que uno de los dos usuarios autorizados ha de tener el nivel de escolta, o bien asignar calendarios de apertura y cierre.

Control remoto del acceso a las cajas de depósitos nocturnos

Asegura que solo los empleados que dispongan de dicho control remoto podrán acceder a la zona donde se resguardan los sobres con dinero en efectivo que los clientes han depositado en las cajas de depósitos mientras la oficina estaba cerrada.

Reducción de costos por pérdidas y duplicados de llaves

Los costos asociados a los cambios de cerraduras y llaves, sumados a los tiempos de improductividad y falta de seguridad que provocan, se solucionan sustituyendo las llaves por tarjetas magnéticas que se pueden dar de baja y reponer de forma rápida con el mínimo costo.

Restringir el acceso por horarios y calendario

Aplicar la restricción en función de los diferentes tipos de usuarios o bien por el nivel de seguridad del área protegida

y los diferentes niveles de puertas asociados a dicha área, pudiendo requerir acceso mediante Nip + Tarjeta, en función del tipo de área, puerta, calendario y horario.

Interbloqueo automático entre cajeros

Configurar el interbloqueo de modo que no se permite la apertura de uno de los cajeros, hasta que todos los demás están cerrados.

Exclusión del acceso externo

Prevenir el acceso externo de los empleados o clientes a la sucursal ante eventos críticos, como un atraco.

Reducción de los costos derivados de la formación del personal

Menos formación del personal en el manejo del sistema de seguridad, al crearse un entorno de seguridad más automatizado.

Incremento de la seguridad de los cajeros

Aumentar la seguridad mediante su conexión automática al cerrar la puerta, la detección del fallo en el cierre de la misma o al exceder el tiempo de apertura programado.

Control automático de los sistemas de esclusas

Este sistema se basa en encadenar dos accesos consecutivos en los que la persona debe acreditarse. La apertura de los accesos es retardada para permitir decidir qué actuación debe realizarse en caso de ataque a la seguridad de la oficina bancaria.

Control del personal

Un control efectivo sabiendo en todo momento quién accedió dónde y cuándo, también impidiendo el acceso a ciertas áreas o a zonas restringidas o con información confidencial.

EL LADO OSCURO DE LAS BARRERAS DE SEGURIDAD: encontrando el equilibrio dispositivos

Por Kurt Measom

Los torniquetes y las puertas giratorias de seguridad están diseñados para funcionar perfectamente y sin problemas, de modo que las personas puedan atravesarlos sin tener que entrar nunca en contacto no deseado con las barreras. Cuando las personas están bien capacitadas, que es un componente necesario para una implementación exitosa, las entradas de seguridad son muy efectivas para mitigar la posible pérdida catastrófica de propiedad, vida, continuidad, etc., como parte de un plan general de seguridad física.

Diagrama 1

El lado oscuro de las barreras: Contacto

Sin embargo, ahora hay algo en qué pensar antes de instalar cualquier tipo de entrada de seguridad. Todos los tipos de entradas automáticas tienen barreras que se mueven: estas se balancean, giran, deslizan o caen. Cuando las personas atraviesan barreras movibles, existe la posibilidad de contacto y lesiones potenciales.

La buena noticia es que las entradas de seguridad de hoy vienen equipadas con tecnología de sensores avanzada que se coloca estratégicamente para evitar el contacto. Sin embargo, la verdad es que las personas pueden caminar directamente hacia las barreras o pueden moverse tan rápida e impredeciblemente que los sensores no pueden responder lo suficientemente rápido.

Como ocurre el contacto de barrera

¿Cómo sucede el contacto?

A veces las personas se distraen o se apresuran, y pueden presentar su licencia de conducir en lugar de su tarjeta de proximidad y caminar directamente hacia las barreras. O bien, están hablando por teléfono o enviando mensajes de texto y no viendo lo que hacen las barreras: en una puerta giratoria de seguridad, una persona está en el teléfono y entra en el siguiente compartimiento de la puerta después de un usuario autorizado; la puerta siente que es un intruso y deja de girar y el usuario se pega en el vidrio del ala de la puerta.

Un lector de tarjetas altamente encriptado tarda una fracción de segundo más de lo previsto para leer las credenciales de alguien. La barrera también tardará una fracción de segundo más en abrirse, y la persona puede caminar y pegarse en la barrera antes de que realmente se abra.

Si una persona se apresura en un carril de torniquete óptico para ir detrás de un usuario autorizado, podría haber contacto dependiendo del tiempo. La barrera puede simplemente cerrarse justo en frente de ellos o pueden acercarse a ellos desde los lados (barreras deslizantes).

Estas cosas pasan. Entonces, ¿qué puede hacer usted al respecto?

Balanceando la seguridad, la protección y el flujo de usuarios

El contacto de barreras es algo que claramente desea evitar, pero ¿cómo? La clave es encontrar un equilibrio entre la seguridad y el nivel de seguridad que necesita, así como un nivel de flujo de usuarios de la entrada que funcione para usted. Si observa el diagrama 1, verá que describe la relación entre seguridad, protección y flujo de usuarios cuando se trata de implementar una entrada de seguridad. Usted querrá encontrar su "punto óptimo" donde dirigir los tres al mejor grado posible; esto se muestra con el punto donde los círculos se superponen.

Aquí hay algunos ejemplos extremos que describen las partes externas de cada círculo en el diagrama:

- **Si usted solo deseara la Seguridad:** las barreras solo se moverían muy lentamente y nunca tocarían a un usuario. Se equivocarían por precaución y se abrirían, incluso para los intrusos, para evitar el contacto.
- **Si usted solo deseara la Protección:** entonces las barreas se cerrarían sin importar lo que impidiera que la gente entrara. La gente podría verse afectada y el flujo de usuarios probablemente sería más lento debido a un mayor número de usuarios rechazados.
- **Si usted solo deseara el Flujo de Usuarios:** entonces la gente podría volar a través de las entradas y nunca habría una acumulación, pero alguien podría salir lastimado o entrar sin que lo vieran.

Con un análisis cuidadoso de sus necesidades, puede encontrar el mejor equilibrio entre la seguridad, la protección y el flujo de usuarios. Si bien todos son importantes, cada implementación es única y hay productos y configuraciones específicas que funcionan mejor para optimizar cada situación. Sobre todo, siempre que sea posible, capacitar al personal sobre el uso correcto de las entradas de seguridad puede ayudar a minimizar los errores que podrían causar cualquier problema, permitiéndole maximizar los tres factores importantes.

INTERTRAFFIC MÉXICO
se asocia con ITS México

De izquierdo a derecha: Laura Barrera (Tarsus Mexico), Ing. José C. Azcárate Beltrán (ITS México), Editha Hoogenberg- Derksen (Intertraffic Mexico / RAI Amsterdam)

Nos complace anunciar nuestra nueva alianza con ITS México. Gracias a esta asociación podremos agregar un valor extra tanto a nuestra exposición como a nuestro programa de conferencias. Estamos muy contentos de combinar nuestras fortalezas, conocimientos y contactos. Juntos aceleraremos la transición de la movilidad en Latinoamérica. ITS México será parte de nuestro Consejo Consultivo y del jurado del Intertraffic Award Latin America.

Intertraffic México, hace la invitación a su exposición los próximos 12, 13 y 14 de noviembre; este evento tiene como propósito reunir en un mismo lugar a expositores y personas interesadas en movilidad, infraestructura, gestión del tráfico, seguridad y estacionamientos.

En este espacio se podrá hacer intercambio de ideas para que los asistentes mejoren su 'know-how', establezcan negocios rentables y tengan acceso al mercado de movilidad en México.

La invitación está dirigida al público en general, pero principalmente a visitantes con perfil del sector público como la Secretaría de Comunicaciones y transportes, autoridades del transporte público, autoridades del aeropuerto, instaladores de sistemas de gestión de tráfico y de estacionamientos, empresas de mantenimiento de carreteras, operadores de transporte público y privado, entre otros.

Los expositores tendrán un perfil relacionado con la fabricación de equipos y soluciones de gestión de estacionamientos, desarrollo de infraestructura, fabricación de equipo de seguridad de tráfico, instituciones financieras públicas, agencias federales y de gobierno central en busca de inversión privada, integración de sistemas de gestión de tráfico urbano e interurbano, y más.

El evento se llevará a cabo en Centro Banamex de la Ciudad de México ubicado en Av. Del Conscripto 311, Colonia Lomas de Sotelo, en un horario de 12:00 a 19:00 horas. El registro es gratuito y se puede realizar en: https://www.intertraffic.com/es/mexico/

ASIS CAPÍTULO MÉXICO

"Seguridad en parques eólicos"

El pasado 6 de agosto se realizó la reunión mensual de ASIS Capítulo México, en el lugar de costumbre, la Hacienda de Los Morales, en la Ciudad de México.

Alberto Frieddman, director general de PROSA

Pedro Sanabria, presidente del Capítulo, presentó su informe mensual de actividades, en el que destacó el crecimiento constante en el número de socios y los reconocimientos que otorgó ASIS Internacional al equipo del Capítulo México. En esta ocasión se reconoció la labor de Enrique Tapia Padilla, CPP, presidente del Capítulo en 2011.

Para finalizar, Pedro Sanabria, invitó a los asistentes al próximo evento de seguridad integral que se realizará del 13 al 17 de octubre en el centro Citibanamex, el Security Week, lo que antes era el Congreso Latinoamericano de Seguridad ASIS. En esta ocasión, además de las conferencias en diferentes formatos y la zona de la Expo, se busca la realización de sesiones de networking, y generar espacios de aprendizaje y diálogo.

La empresa patrocinadora de la reunión fue Procesos Automatizados, S.A. de C.V. (PROSA), por lo que Alberto Frieddman, director general adjunto de la empresa, dio la bienvenida a los asistentes y realizó una breve reseña de la historia de esa empresa.

Por otra parte, Armando Zúñiga Salinas, director general de Grupo IPS, invitó a los asistentes al Diplomado en Desarrollo de Empresas de Seguridad Exitosas y Sustentables, organizado por Agrupaciones de Seguridad Unidas por México (ASUME), la Universidad Panamericana y el High Potential Development Center. También rifó una beca para ese diplomado.

La conferencia de este mes estuvo a cargo de Eduardo González Martínez, DSI, gerente de seguridad corporativa para Latinoamérica Norte de Siemes Gamesa, y que llevó por título "Seguridad en parques eólicos y los retos sociales que implica".

"En México, los parques eólicos generan el 6% de la electricidad, por eso es vital que los colaboradores conozcan a la perfección las buenas prácticas y la autoprotección, dentro y fuera de los proyectos. La implementación de estudios y de programas de seguridad, así como una mayor concientización social son elementos clave para su seguridad".

Afirmó que el sector busca implementar programas de concientización entre las comunidades e impulsar las actividades económicas de las poblaciones. Los proyectos también tienen el objetivo de tener una mayor capacidad de gestión de seguridad, pues una mala administración puede llevar a la cancelación del proyecto.

Otros retos que enfrenta este sector son de tipo logístico y de transporte para la movilización de materiales de construcción y montaje, desde que llegan a los puertos y hasta su destino final. Actualmente existen 59 parques eólicos en México, distribuidos en Baja California, Zacatecas, Chiapas, Jalisco, Nuevo León, Oaxaca, San Luis Potosí, Tamaulipas y Puebla.

Eduardo González Martínez, DSI, gerente de seguridad para Siemes Gamesa

Pedro Sanabria, Presidente de Asis Capítulo México (izquierda) y Enrique Tapia Padilla, CPP