Seguridad física en instalaciones de importancia crítica

White Paper 82

Revisión 2

Por Suzanne Niles

> Resumen Ejecutivo

La seguridad física –controlar el acceso del personal a las instalaciones – es un factor crítico para conseguir los objetivos de disponibilidad del centro de datos. A medida que las nuevas tecnologías, como la identificación biométrica y la gestión remota de datos de seguridad, estén más ampliamente disponibles, la seguridad tradicional de tarjetas y guardas será sustituida por sistemas de seguridad que ofrezcan con total certeza una identificación y un seguimiento de la actividad humana en y alrededor del centro de datos. Antes de invertir en equipos, los gestores de TI deben evaluar cuidadosamente sus necesidades específicas de seguridad y determinar las medidas de seguridad más apropiadas y rentables para sus instalaciones. En este documento se presenta una descripción general de los principios de la identificación personal y también se describen los elementos y procedimientos básicos utilizados en los sistemas de seguridad.

Contenido

haga clic en una sección para saltar a ella

Los documentos técnicos de APC by Schneider Electric son ahora parte de la biblioteca de documentos técnicos de Schneider Electric producido por Schneider Electric's **Data Center Science Center**
DCSC@Schneider-Electric.com

Schneider Electric

Introducción

Las personas: un riesgo que hay que controlar

Cuando se menciona la seguridad del centro de datos, lo primero que viene a la mente es la protección contra el sabotaje, el espionaje o el robo de datos. Aunque la necesidad de protección frente a intrusos y los daños intencionados que pueden causar es obvia, los peligros de la actividad normal del personal que trabaja en el centro de datos constituyen un mayor riesgo diario en la mayoría de las instalaciones.

Las personas son esenciales para el funcionamiento de un centro de datos, aunque hay estudios que demuestran que son directamente responsables del 60% del tiempo de inactividad del centro de datos por accidentes y errores: procedimientos incorrectos, equipos mal identificados, cosas que se caen o derraman, comandos mal escritos y otros imprevistos de mayor o menor envergadura. Teniendo en cuenta que los errores son inherentes al ser humano, reducir y controlar el acceso del personal a las instalaciones es un elemento crítico de la gestión de riesgos incluso cuando la preocupación por las actividades maliciosas sea leve.

> **Infraestructura física del centro de datos**
>
> La seguridad física es parte de la Infraestructura física del centro de datos (DCPI) porque tiene la función directa de maximizar la disponibilidad del sistema (“tiempo de actividad”). Lo hace reduciendo el tiempo de inactividad por accidentes o sabotaje debido a la presencia de personas no necesarias o malintencionadas.

La tecnología de identificación está cambiando al mismo ritmo que las instalaciones, la información y la comunicación que protege. Con la constante aparición de nuevos equipos y técnicas, es fácil olvidar que el viejo problema que esta tecnología trata de resolver no es técnico ni complicado: mantener a las personas no autorizadas o malintencionadas fuera de los lugares que no les corresponden. Y mientras el primer paso – definir las áreas seguras del emplazamiento y reglas de acceso a las mismas – puede parecer algo complejo, no es intuitivamente difícil: los gestores de TI saben generalmente quién puede estar dónde. El problema está en el segundo paso: decidir la mejor forma de aplicar las imperfectas tecnologías para implementar el plan.

¿Quién eres y por qué estás aquí?

Aunque las nuevas tecnologías de seguridad puedan parecer exóticas e inescrutables – reconocimiento de la huella digital o de la palma de la mano, exploración del iris, tarjetas inteligentes, geometría facial – el objetivo de seguridad subyacente no ha cambiado desde que las personas empezaron a tener cosas que proteger, y es sencillo y conocido para todos nosotros: obtener una respuesta fiable a la pregunta “¿Quién eres y por qué estás aquí?”

La primera parte de la pregunta – “¿Quién eres?” – provoca la mayoría de los problemas al diseñar sistemas de seguridad automatizados. Todas las tecnologías actuales tratan de evaluar la identidad de una forma u otra con diversos niveles de certeza y al coste variable correspondiente. Por ejemplo, una tarjeta es barata pero no ofrece una identificación segura (no se puede estar seguro de quién está utilizándola); una exploración del iris ofrece una identidad muy segura pero es muy caro. Encontrar un compromiso aceptable entre certeza y economía es el objetivo del diseño de un sistema de seguridad.

La respuesta a la segunda parte de la pregunta, “¿Por qué estás aquí?” – en otras palabras, qué haces en este punto de acceso – podría quedar contestada al establecer la identidad (“Es Alicia López, nuestra especialista en cableado; trabaja con los cables: déjala entrar”), pero puede implementarse de diversas formas: El “quién” y “por qué” de una persona pueden combinarse, por ejemplo en la información de la banda magnética de una tarjeta; la identidad de una persona podría recuperar información de un archivo informático que contiene todas

las autorizaciones de acceso; o podría haber distintos métodos de acceso para diversas partes del emplazamiento, diseñados para permitir el acceso con distintos fines. A veces, "¿Por qué estás aquí?" es la única cuestión y "¿Quién eres?" no importa tanto, sobre todo para el personal de reparaciones o de limpieza.

Combinación de conocimientos para encontrar la solución

Los gestores de TI saben el "quién y por qué" de la seguridad en sus instalaciones, pero pueden no estar familiarizados con los detalles de las metodologías actuales o las técnicas para aplicarlas, ni tienen por qué estarlo. Conocen las limitaciones de su presupuesto y saben los riesgos inherentes de los diversos tipos de fallos de seguridad en sus instalaciones.

El consultor del sistema de seguridad, por otra parte, no está al corriente de los pormenores del emplazamiento, pero conoce las capacidades, los inconvenientes y el coste de las metodologías actuales. También tiene experiencia en el diseño de otros sistemas de seguridad y puede ayudar a aclarar, refinar o simplificar los requisitos de "quién y por qué" formulando las preguntas correctas.

Con sus conocimientos combinados, un sistema puede diseñarse de forma que se equilibren los requisitos de acceso, el riesgo aceptable, los métodos disponibles y las limitaciones de presupuesto.

Definición del problema

Áreas seguras: ¿cuáles necesitan protección?

El primer paso para diseñar un plan de seguridad es precisamente trazar un plano del emplazamiento físico e identificar las áreas y los puntos de entrada que necesitan distintas reglas de acceso o **niveles de seguridad**.

Estas áreas pueden tener límites concéntricos:

- Perímetro del emplazamiento
- Perímetro del edificio
- Área de ordenadores
- Salas de ordenadores
- Racks de equipos

O pueden tener límites contiguos:

- Áreas de visitantes
- Oficinas
- Salas de servicios públicos

"Seguridad física" también puede significar...

Seguridad física también puede hacer referencia a la protección contra catástrofes (incendios, inundaciones, terremotos, atentados con bomba) o averías de los servicios públicos (interrupción del suministro eléctrico, fallo del HVAC). Aquí solo se refiere a la protección contra la intrusión humana.

Las áreas concéntricas pueden tener métodos de acceso distintos o cada vez más restrictivos, y ofrecer una protección añadida llamada **seguridad escalonada**. Con la seguridad escalonada, una área interior está protegida tanto por sus propios métodos de acceso como por los de las áreas que la rodean. Además, toda violación de una área exterior debe enfrentarse a otra prueba de acceso en el siguiente perímetro interior.

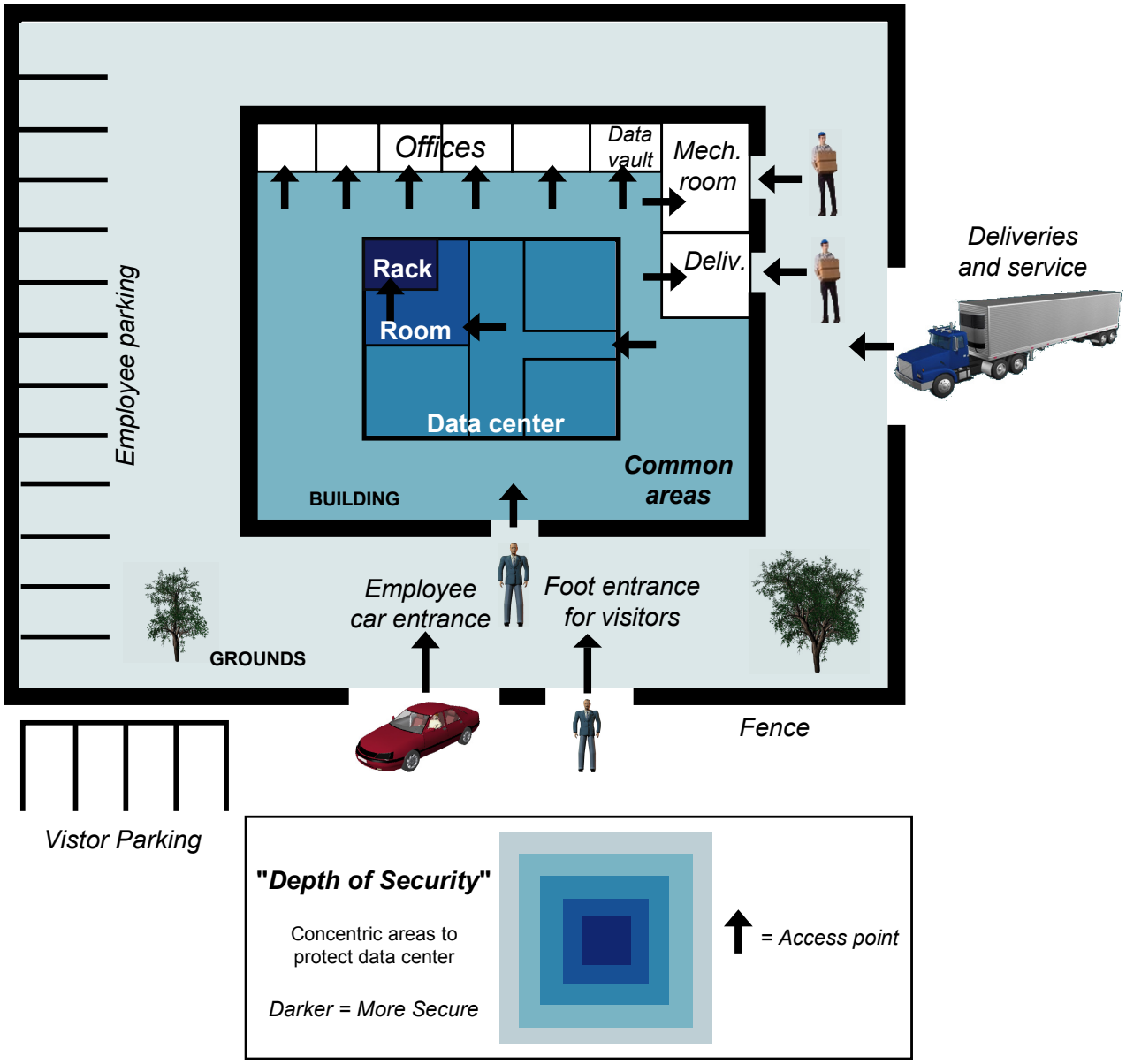


Imagen 1

Plano de seguridad mostrando la "seguridad escalonada"

Seguridad a nivel de rack. La capa de "seguridad escalonada" más interior – incluso más que la propia sala de datos – es el *rack*. Los racks con cerradura no suelen utilizarse (todavía), pero si se utilizan, son la última defensa contra el acceso no autorizado a equipos críticos. Sería muy extraño que, en una sala llena de racks, alguien tuviera que acceder a todos ellos: los racks con cerradura pueden garantizar que solo el personal de servidores pueda acceder a los servidores, que solo el personal de telecomunicaciones pueda acceder a los equipos de telecomunicaciones, etc. Los racks con cerradura "gestionables" que pueden configurarse de forma remota para autorizar el acceso solo cuando es necesario – a personas específicas en momentos específicos – reducen el riesgo de un accidente, sabotaje o instalación no autorizada de equipos adicionales que pudieran causar un aumento potencialmente peligroso del consumo eléctrico y de la temperatura en el rack.

Seguridad de la infraestructura. En el mapa de seguridad, es importante incluir no solo áreas que contengan los equipos de TI funcionales del emplazamiento, sino también áreas que contengan elementos de la infraestructura física que, si se compromete, podría producir tiempos de inactividad. Por ejemplo, el equipo de ventilación, aire acondicionado y calefacción (HVAC) podría apagarse accidental o deliberadamente, las baterías de arranque del generador podrían ser robadas o una consola de gestión del sistema podría inundarse en el caso de que se activaran los aspersores de incendios.

Criterios de acceso: ¿quién puede entrar dónde?

La autorización de una persona para acceder a una área segura puede basarse en distintas categorías. Además de las habituales – identidad y propósito, las dos primeras citadas a continuación – puede haber categorías adicionales que requieran un tratamiento especial, por ejemplo “necesito saber”.

Identidad personal. Algunas personas que son conocidas en el emplazamiento necesitan acceder a las áreas relevantes de su puesto. Por ejemplo, el director de seguridad tendrá acceso a la mayor parte del emplazamiento, pero no a los datos de los clientes almacenados en las instalaciones. El jefe de operaciones informáticas puede tener acceso a las salas de ordenadores y a los sistemas operativos, pero no a las salas de máquinas que contienen las instalaciones eléctricas y de HVAC. El director general de la empresa puede tener acceso a las oficinas del director de seguridad y del personal de TI, así como a las áreas públicas, pero no a las salas de ordenadores ni a las salas de máquinas.

Separación de asuntos

No deje que los detalles de las tecnologías de identificación interfieran en la determinación inicial de los requisitos de seguridad. Primero defina las áreas y los criterios de acceso a las instalaciones y *después* haga el análisis de costes/eficacia/riesgos, considere compromisos e imagine la mejor implementación de tecnología.

Razón para estar ahí. Una persona de reparación de servicios públicos, independientemente de que se llame Juan Pérez o María López, puede tener acceso solo a las salas de máquinas y a las áreas públicas. El equipo de limpieza, cuya composición puede cambiar de un día a otro, podría tener acceso a áreas comunes, pero a ningún otro lado. Un experto en conmutadores de red podría tener acceso solo a racks con equipos de conmutación y no a racks con servidores o dispositivos de almacenamiento. En una instalación de servidores web, el personal de mantenimiento de sistemas de cliente podría tener acceso solo a una “sala de acceso a clientes” donde haya conexiones a su servidor personal con fines administrativos.

Necesito saber. El acceso a áreas extremadamente sensibles puede concederse solo a personas específicas con fines específicos, es decir, si “necesitan saber” y solo mientras tengan esa necesidad.

Aplicación de la tecnología

Métodos de identificación: fiabilidad frente a coste

Los métodos de identificación de personas se dividen en tres categorías generales de fiabilidad – y coste del equipo – en aumento:

- **Qué tienes**
- **Qué sabes**
- **Quién eres**

Qué tienes. *Poco fiable (puede compartirse o robarse)*
Qué tienes es algo que se puede llevar: una llave, una tarjeta o un pequeño objeto (un **testigo**) que puede llevarse puesto o en un llavero. Puede ser tan "tonto" como la típica llave metálica o tan "inteligente" como una tarjeta con un procesador integrado que intercambie información con un lector (una **tarjeta inteligente**). Puede tratarse de una tarjeta con una banda magnética con información personal (como la tarjeta del cajero automático); puede ser una tarjeta o un testigo con un transmisor y/o un receptor que puede comunicarse con el lector a una distancia corta (una **tarjeta** o **un testigo de proximidad**, Mobil Speedpass®, por ejemplo).

Qué tienes es la forma de identificación menos fiable, ya que no hay garantía de que la esté utilizando la persona correcta: puede ser compartida, robada o perdida y encontrada por otra persona.

Qué sabes . *Más fiable (no puede robarse, pero puede compartirse o escribirse)*
Qué sabes es una contraseña, un código o un procedimiento para algo como la apertura de una cerradura con código, la verificación en un lector de tarjetas o el acceso por teclado a un ordenador. La contraseña/código presenta un dilema de seguridad: si es fácil de recordar, probablemente será fácil de adivinar; si es difícil de recordar, probablemente será difícil de adivinar, pero también es probable que se escriba, reduciendo así su seguridad.

Qué sabes es más fiable que *Qué tienes*, pero las contraseñas y los códigos pueden compartirse y, si se escriben, pueden descubrirse.

Quién eres. *Lo más fiable (se basa en algo que físicamente es único en cada persona)*
Quién eres hace referencia a la identificación por reconocimiento de características físicas únicas: es la forma natural en que nos identificamos unos a otros con certeza prácticamente total. Cuando se realiza (o se intenta) por medios tecnológicos, se llama **biometría**. Se han desarrollado técnicas de identificación biométrica de varias características humanas que se prestan por sí mismas al escrutinio y análisis cuantitativo:

Huella digital
Iris (patrón de colores)
Retina (patrón de vasos sanguíneos)
Voz
Mano (forma de los dedos y grosor de la mano)
Cara (posición relativa de ojos, nariz y boca)
Escritura (dinámica del movimiento del lápiz)

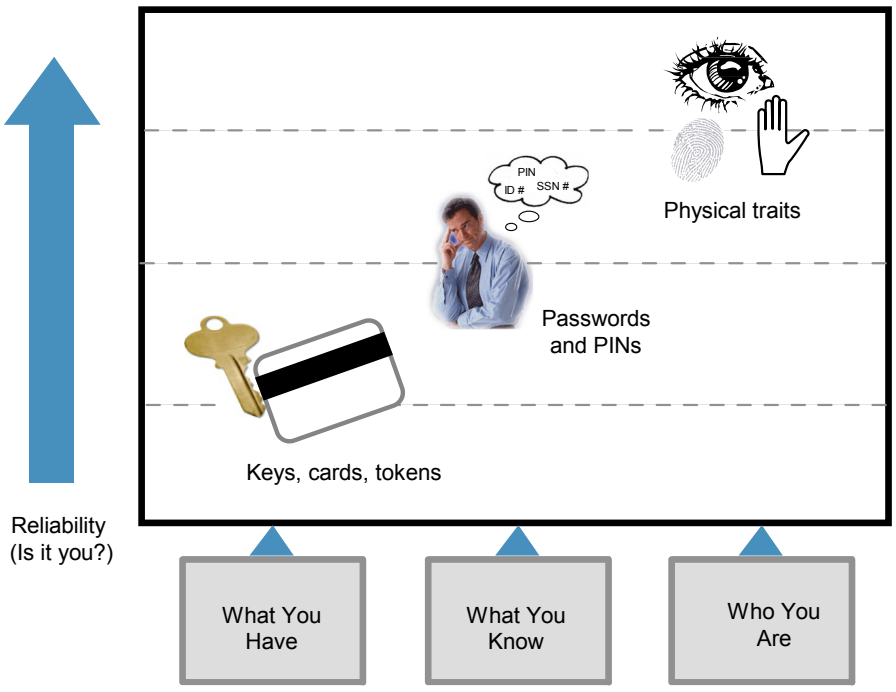


Imagen 2

Qué tienes, qué sabes, quién eres

Los dispositivos biométricos son, por lo general, muy fiables cuando se consigue el reconocimiento: si el dispositivo cree que te reconoce, lo más seguro es que *seas* tú. La principal fuente de fallos de fiabilidad de la biometría no es el reconocimiento incorrecto ni el engaño de un impostor, sino la posibilidad de que un usuario legítimo no sea reconocido ("falso rechazo").

Combinación de métodos para aumentar la fiabilidad

Un esquema de seguridad típico utiliza métodos para aumentar la fiabilidad – y los gastos – progresivamente, de las áreas más exteriores (menos sensibles) a las más interiores (más sensibles). Por ejemplo, la entrada al edificio podría exigir una combinación de tarjeta magnética más código PIN; la entrada a la sala de ordenadores podría exigir teclear un código más una identificación biométrica. La combinación de métodos en un punto de acceso aumenta la fiabilidad en ese punto; la utilización de distintos métodos en cada nivel aumenta significativamente la seguridad en los niveles interiores, ya que cada uno se asegura mediante sus propios métodos más los de los niveles exteriores a los que hay que entrar primero.

Separación de asuntos

No deje que los detalles de las tecnologías de identificación interfieran en la determinación inicial de los requisitos de seguridad. Primero defina las áreas y los criterios de acceso a las instalaciones y *después* haga el análisis de costes/eficacia/riesgos, considere compromisos e imagine la mejor implementación de tecnología.

Gestión del sistema de seguridad

Algunos dispositivos de control de acceso – lectores de tarjetas y escáneres biométricos, por ejemplo – pueden capturar los datos de incidencias de acceso, como la identidad de las personas que pasan y la hora de entrada. Si están en red, estos dispositivos pueden enviar la información a un sistema de gestión remoto de supervisión y registro (quién entra y sale), control de dispositivos (configuración de un bloqueo para permitir el acceso a determinadas personas en determinados momentos), y alarma (notificación de repetidos intentos infructuosos o fallos del dispositivo).

Dispositivos de control de acceso

Tarjetas y testigos: "qué tienes"

Actualmente se utilizan varios tipos de tarjetas y testigos de control de acceso, desde los más sencillos a los más sofisticados, que ofrecen toda una gama de prestaciones en varias dimensiones:

- Capacidad de reprogramación
- Resistencia a la falsificación
- Tipo de interacción con el lector de tarjetas: pasada, inserción, contacto, sin contacto ("proximidad")
- Comodidad: forma física y cómo se lleva
- Cantidad de datos que incluye
- Capacidad computacional
- Coste de las tarjetas
- Coste del lector

Independientemente de lo seguras y fiables que puedan ser por su tecnología, la seguridad ofrecida por estas “cosas” físicas está limitada por el hecho de que no hay garantía de que las esté utilizando la persona adecuada. Por ello es normal combinarlas con uno o más métodos adicionales de confirmación de la identidad, como una contraseña o una identificación biométrica.

La **tarjeta de banda magnética** es el tipo más normal de tarjeta, con una sencilla banda magnética de datos de identificación. Cuando la tarjeta se pasa por un lector, la información que contiene se lee y busca en una base de datos. El sistema es barato y cómodo; el inconveniente es que resulta relativamente fácil duplicar las tarjetas o leer la información que tienen almacenada.

La **tarjeta de ferrita de bario** (también llamada “tarjeta de puntos magnéticos”) es similar a la tarjeta de banda magnética pero ofrece más seguridad sin añadir un coste importante. Contiene una fina lámina de material magnético con puntos redondos dispuestos en un patrón. Más que leerse mediante pasada o escáner, la tarjeta se pone en contacto con el lector.

La **tarjeta Weigand** es una variante de la tarjeta de banda magnética. La tarjeta lleva incrustada una serie de hilos especialmente tratados con una firma magnética única. Cuando la tarjeta se pasa por el lector, hay una bobina de detección que detecta la firma y la convierte en una cadena de bits. La ventaja de este complejo diseño es que las tarjetas no pueden duplicarse; el inconveniente es que tampoco pueden reprogramarse. Con esta tecnología, la tarjeta no necesita estar en contacto directo con el lector; por ello, el cabezal del lector puede estar encapsulado: ideal para su instalación en exteriores. A diferencia de los lectores de tarjetas de proximidad y las tarjetas de banda magnética, a los lectores Weigand no les afectan las interferencias de radiofrecuencia (RFI) ni los campos electromagnéticos (EMF). La robustez del lector combinada con la dificultad para duplicar la tarjeta hace que el sistema Weigand sea extremadamente seguro (dentro de los límites de un método “qué tienes”), pero también es más caro.

La **tarjeta de código de barras** lleva un código de barras que se lee al pasar la tarjeta por el lector. Este sistema es muy barato, pero muy fácil de engañar: una simple fotocopiadora puede duplicar lo suficientemente bien el código de barras como para engañar al lector. Las tarjetas de códigos de barras son buenas para requisitos de seguridad mínimos, especialmente los que exigen un gran número de lectores en el emplazamiento o donde hay un tráfico intenso atravesando un punto de acceso determinado. No es tanto un sistema de seguridad como un método barato de *control* de acceso. (Se dice que el acceso mediante código de barras solo sirve para “dejar fuera a las personas honestas”.)

La **tarjeta de sombra de infrarrojos** mejora la escasa seguridad de la tarjeta de código de barras colocando el código de barras entre capas de plástico PVC. El lector pasa la luz infrarroja por la tarjeta y la sombra del código de barras es leída por los sensores del otro lado.

La **tarjeta de proximidad** (también llamada “tarjeta prox”) es un paso adelante en la comodidad comparada con las tarjetas que deben pasarse por el lector o tocarlo. Como su nombre indica, la tarjeta solo necesita “aproximarse” al lector. Esto se consigue utilizando tecnología RFID (identificación por radiofrecuencia), que suministra energía a la tarjeta a través del campo electromagnético del lector de tarjetas. El diseño más conocido funciona a una distancia de unos 10 cm del lector; otro diseño – la llamada **tarjeta de vecindad** – funciona a una distancia de hasta un metro.

La **tarjeta inteligente**, el desarrollo más reciente de tarjetas de control de acceso, se está convirtiendo rápidamente en el método elegido para las nuevas instalaciones. Es una tarjeta con un chip de silicio incorporado para el almacenamiento y/o el cálculo de datos integrado. Los datos se intercambian con el lector por contacto del chip con el lector (tarjeta inteligente de *contacto*) o por interacción con el lector a una distancia, utilizando la misma tecnología que las tarjetas de proximidad y vecindad (tarjeta inteligente *sin contacto* o de *proximidad*).

El chip, que tiene aproximadamente 1,25 cm de diámetro, no tiene que por qué estar necesariamente en una tarjeta: puede estar integrado en una identificación fotográfica, montado en un llavero o llevarse como un botón o una joya (como el iButton®). El término general para los objetos que llevan un chip así es *soporte inteligente*.

Las tarjetas inteligentes ofrecen una amplia flexibilidad en el control de acceso. Por ejemplo, el chip puede incluirse en otros tipos de tarjetas para mejorarlas e integrarse en sistemas ya existentes, o puede almacenarse en el chip la huella digital o el iris del titular para la verificación biométrica en el lector de tarjeta, lo que eleva el nivel de identificación de "qué tienes" a "quién eres". Las tarjetas inteligentes sin contacto que tienen el alcance de "vecindad" ofrecen la mayor comodidad para el usuario: transacciones que duran medio segundo sin tener que sacar la tarjeta de la cartera.

Teclados y cerraduras con código: "qué sabes"

Los **teclados** y **las cerraduras con código** se utilizan ampliamente como método de control de acceso. Son fiables y fáciles de usar, pero su seguridad está limitada por la naturaleza de las contraseñas, que pueden compartirse o adivinarse. Tienen botones como los del teléfono, donde los usuarios marcan un código: si el código es exclusivo de cada usuario, se denomina código de acceso personal (PAC) o número de identificación personal (PIN). El *teclado* generalmente implica la capacidad de aceptar múltiples códigos, uno por cada usuario; la *cerradura con código* normalmente hace referencia a un dispositivo que solo tiene un código que utilizan todos.

El nivel de seguridad de los teclados y cerraduras con código puede aumentarse cambiando periódicamente los códigos, lo que requiere un sistema para informar a los usuarios y comunicar los nuevos códigos. Las cerraduras que no cambian de código deben sustituirse periódicamente si el desgaste de las teclas permite detectar el código. Como con las tarjetas de acceso, la seguridad mediante teclado puede aumentarse añadiendo la identificación biométrica para confirmar la identidad del usuario.

Biometría: "quién eres"

La tecnología biométrica se está desarrollando rápidamente, haciéndose mejor y más barata. La verificación biométrica de elevada confianza, especialmente la del reconocimiento de huellas digitales, está entrando en el ámbito de las soluciones de seguridad. Muchos distribuidores suministran una amplia gama de dispositivos biométricos y, en combinación con los métodos tradicionales "qué tienes" y "qué sabes", la biometría puede completar las medidas de seguridad existentes para convertirse en el mejor control de acceso.

¿Por qué no utilizamos *solo* la biometría?

P: Si un punto de entrada utiliza tarjeta, PIN y biometría, ¿por qué no utilizamos solo la biometría?
R: Porque (1) el tiempo de procesamiento biométrico puede ser inaceptable si debe buscarse en una gran base de datos de imágenes de usuarios en lugar de comparar con la imagen de un único usuario, y (2) el riesgo de falso rechazo o aceptación puede reducirse si la imagen se compara solo con un usuario en la base de datos.

Aunque los rasgos biométricos son casi imposibles de falsificar, sigue habiendo un riesgo de identificaciones incorrectas.

La identificación biométrica suele utilizarse no para *reconocer* la identidad buscando en una base de datos de usuario una coincidencia, sino más bien para *verificar* la identidad que primero se establece mediante un método "qué tienes" o "qué sabes": por ejemplo, primero se utiliza una tarjeta/PIN, y después la comprobación de la huella digital verifica el resultado. A medida que aumenta el rendimiento y la confianza en la tecnología biométrica, finalmente puede convertirse en un método autónomo de *reconocimiento* de la identidad y eliminar la necesidad de llevar tarjetas o recordar contraseñas.

Hay dos tipos de fallos en la identificación biométrica:

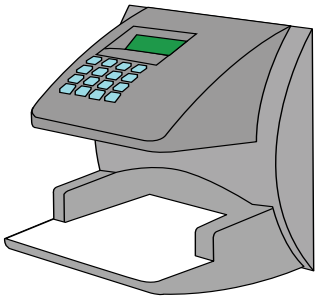
- *Falso rechazo*. Imposibilidad de reconocer a un usuario legítimo. Aunque puede alegarse que tiene el efecto de mantener la área protegida absolutamente segura, es una frustración intolerable para los usuarios legítimos a quienes se les deniega el acceso porque el escáner no los reconoce.
- *Falsa aceptación*. Reconocimiento erróneo, ya sea por confundir a un usuario con otro o por aceptar a un impostor como usuario legítimo.

Los índices de fallos pueden ajustarse cambiando el umbral (“qué grado de exactitud es suficiente”) para declarar una coincidencia, aunque la disminución de un índice de fallos aumentaría el otro.

Los criterios a la hora de elegir una función biométrica son el coste del equipo, los índices de fallos (tanto de falso rechazo como de falsa aceptación) y la aceptación del usuario, que significa qué grado de intrusión, incomodidad o incluso peligro percibe el usuario del procedimiento. Por ejemplo, se considera que los escáneres de retina tienen poca aceptación de los usuarios porque el ojo tiene que estar a una distancia de 2,5 a 5 cm del escáner con un LED dirigido al ojo.

Imagen 3

Exploración de la mano



Otros elementos del sistema de seguridad

El diseño del sistema de seguridad se centra en dispositivos para identificar y filtrar personas en los puntos de entrada – “control de acceso” – que es todo lo que se necesitaría *si* la identificación tuviera una fiabilidad del 100% y se admitiera una confianza total en las intenciones de las personas admitidas y en la perfección física de paredes, puertas, ventanas, cierres y techos infranqueables. Para cubrir los inevitables fallos por errores o sabotaje, los sistemas de seguridad suelen incorporar métodos adicionales de protección, supervisión y recuperación.

Diseño del edificio

Al construir un nuevo emplazamiento o renovar uno antiguo, puede abordarse el tema de la seguridad física de abajo arriba incorporando características arquitectónicas y de construcción que desanimen o impidan la intrusión. Las consideraciones de seguridad en la estructura y el diseño de un edificio suelen relacionarse con las posibles rutas de entrada y escape, el acceso a elementos de infraestructura crítica, como el cableado y el sistema de HVAC y lugares donde los intrusos puedan ocultarse. Consulte el apéndice para ver una lista de algunas de estas consideraciones de diseño.

Acceso autorizado con y sin cómplice: esclusas

Una laguna frecuente y frustrante de los sistemas de control de acceso seguros puede ser la habilidad de una persona no autorizada para colarse detrás de una persona autorizada (se denomina **colarse con cómplice** cuando la persona autorizada es cómplice, es decir, si sujeta la puerta o **colarse sin cómplice** si la persona no autorizada se cuela sin ser detectada). La solución tradicional es un habitáculo de seguridad denominado **esclusa** con puertas a la entrada y a la salida, y espacio para una sola persona. Las esclusas pueden diseñarse con control de acceso tanto a la entrada como a la salida o solo a la salida, en cuyo caso un intento fallido de salir hace que se cierre automáticamente la puerta de entrada y se envíe una alerta indicando que se ha capturado al intruso. Se puede añadir un suelo detector de pisadas para confirmar que solo hay una persona.

Una nueva tecnología para resolver este problema utiliza una cámara de vigilancia para registrar a las personas según pasan, enviando una alerta si se detecta a más de una persona por entrada autorizada.

Cámaras de vigilancia

Las cámaras fijas pueden utilizarse para cosas tales como grabar matrículas en los puntos de entrada de vehículos o, junto con los sensores de pisadas, grabar a las personas en puntos críticos.

Las cámaras de circuito cerrado de TV (CCTV) – visibles u ocultas – vigilan el interior o el exterior, sirven como medida disuasoria y permiten analizar la grabación después de un incidente. Pueden utilizarse varios tipos de vistas de cámara: fija, giratoria o controlada a distancia. Al colocar cámaras hay que considerar lo siguiente:

- ¿Es importante identificar fácilmente a la persona que se encuentra en el campo de visión de la cámara?
- ¿Solo es necesario determinar si está ocupado el espacio?
- ¿Está vigilando si se retiran los activos?
- ¿Sirve la cámara solo como disuasorio?

Si las señales de CCTV se graban, debe haber procedimientos para solucionar los siguientes problemas:

- ¿Se clasificarán y catalogarán las cintas para su rápida recuperación?
- ¿Se almacenarán las cintas en el emplazamiento o en otro lugar?
- ¿Quién tendrá acceso a las cintas?
- ¿Cuál es el procedimiento para acceder a las cintas?
- ¿Cuánto tiempo se guardarán las cintas antes de ser destruidas?

Se están desarrollando nuevas tecnologías para automatizar el trabajo que tradicionalmente hacen los guardas de seguridad – mirar monitores de TV – mediante la detección por software de los cambios (movimientos) de la imagen en la pantalla

Guardas de seguridad

A pesar de todos los avances tecnológicos en el campo de la seguridad física, los expertos están de acuerdo en que el mejor método para controlar el acceso es un equipo de inspectores de seguridad. Los guardas ofrecen la capacidad de vigilancia de todos los sentidos humanos más la posibilidad de responder con movilidad e inteligencia a incidentes sospechosos, no habituales o desastrosos.

La International Foundation for Protection Officers (IFPO) es una organización sin ánimo de lucro que tiene el objetivo de facilitar la formación y certificación estandarizada de inspectores de seguridad. El *Manual de formación de supervisores de seguridad* es una guía de referencia para los inspectores de seguridad y el personal a su cargo.

Sensores y alarmas

Todo el mundo está familiarizado con los sistemas de alarma tradicionales de casas y edificios: sensores de movimiento, sensores de calor, sensores de contacto (puerta cerrada), y similares. Los sistemas de alarma de los centros de datos podrían utilizar otras clases de sensores: barreras de rayos láser, sensores de pisadas, sensores táctiles, sensores de vibraciones. Los centros de datos también podrían tener algunas áreas en las que se prefiera una alarma silenciosa a una alarma audible con el fin de “pillar in fraganti” a los supuestos delincuentes.

Si los sensores están en red, pueden vigilarse y controlarse de forma remota mediante un sistema de gestión, que también podría incluir datos de movimiento del personal de los dispositivos de control de acceso (consultar sección anterior, **Gestión del sistema de seguridad**).

Visitantes

En el diseño de cualquier sistema de seguridad debe considerarse el control de visitantes. Las soluciones típicas son repartir tarjetas de identificación temporales o tarjetas para áreas de baja seguridad y exigir acompañamiento para áreas de alta seguridad. La presencia de habitáculos de seguridad (para impedir que dos personas traspasen un punto de entrada con solo una autorización) requeriría la posibilidad de cancelación temporal o la emisión de credenciales de visitante que le franqueasen el paso.

El factor humano

La tecnología no puede hacer sola todo el trabajo, sobre todo desde que recurrimos a ella para realizar lo que es esencialmente una tarea humana: evaluar la identidad y las intenciones de las personas. Como las personas son una parte importante del problema de seguridad, también forman parte de la solución: la capacidad y falibilidad de las personas las cualifican no solo como el eslabón más débil, sino también como el apoyo más fuerte.

Las personas: el eslabón más débil

Además de errores y accidentes, en el ser humano hay una tendencia natural hacia la amistad y la confianza. Una persona conocida que entra a las instalaciones puede ser un empleado descontento o un renegado. La tentación de hacer la vista gorda o saltarse los procedimientos con alguien conocido puede tener consecuencias desastrosas: buena parte de los fallos de seguridad vienen de “alguien de dentro”. Incluso los extraños pueden conseguir burlar la seguridad con sorprendente facilidad: la capacidad de un extraño listo para utilizar la astucia y conseguir entrar está tan bien documentada que hasta tiene un nombre: **ingeniería social**. Todo aquel que se encuentre en una área en la que pueda hacerse daño, debe tener formación no solo en los protocolos operativos y de seguridad, sino también de resistencia a las creativas técnicas de ingeniería social.

Las personas: el apoyo más fuerte

La protección contra fallos de seguridad viene normalmente del reconocimiento y la interpretación de factores inesperados: una capacidad que la tecnología no tiene. Si añadimos una resistencia inquebrantable a la manipulación y a los atajos, la presencia humana puede ser un inestimable complemento de la tecnología.

Más allá del personal de alerta, el incomparable valor de los ojos, los oídos, el cerebro y la movilidad del ser humano también cualifica a las personas para considerarlas un elemento dedicado en un plan de seguridad: el guarda de seguridad de toda la vida. La presencia de los guardas en los puntos de entrada y de guardas itinerantes por el exterior y el interior del edificio, aunque resulta cara puede resultar imprescindible si hay un fallo o una violación de la seguridad tecnológica. La pronta respuesta de un guarda cuando “algo no va bien” puede ser la última defensa contra un fallo de seguridad potencialmente desastroso.

En la protección contra el daño tanto accidental como deliberado, la contribución humana es la misma: la vigilancia constante y el estricto cumplimiento de los protocolos. Dejando fuera a todo aquel que no es esencial para el funcionamiento de las instalaciones, el resto del personal – bien formado y que respeta prácticas y procedimientos bien diseñados – es el cortafuegos final de un eficaz sistema de seguridad física.

Elección de la solución correcta: tolerancia al riesgo frente a coste

El mejor sistema de seguridad es el que consigue equilibrar por una parte el riesgo y el daño potencial de que haya personas donde no deben y por otra los gastos y molestias de las medidas de seguridad para mantenerlos fuera.

Coste potencial de un fallo de seguridad

Como cada centro de datos tiene sus propias características y su propio potencial de pérdida, la mayoría tienen algo que considerar en las siguientes categorías generales:

- *Pérdida física*. Daños en salas y equipos por accidentes, sabotaje o robo.
- *Pérdida de productividad de TI*. Desviación del personal de sus obligaciones mientras se reparan o sustituyen los equipos, se reconstruyen los datos o se eliminan problemas de los sistemas.
- *Pérdida de productividad corporativa*. Interrupción del negocio por tiempos de inactividad.
- *Pérdida de información*. Pérdida, corrupción o robo de datos.
- *Pérdida de reputación y renombre comercial* . Consecuencias de fallos de seguridad graves o repetidos: pérdida de negocio, caída en la bolsa, pleitos.

Consideraciones para el diseño de sistemas de seguridad

El diseño de sistemas de seguridad puede ser una ecuación compleja con muchas variables. Aunque las estrategias específicas del diseño de sistemas de seguridad están más allá del ámbito de este documento, todo diseño considerará probablemente los siguientes puntos:

- *Coste del equipo*. Las limitaciones del presupuesto normalmente limitan el uso extensivo de equipos de identificación de alta confianza. La solución habitual es implementar una variedad de técnicas apropiadas para los diversos niveles de seguridad.
- *Combinación de tecnologías*. La fiabilidad de identificación en cualquier nivel puede aumentarse combinando tecnologías de bajo coste, teniendo al nivel más interior la protección combinada de todos los demás perímetros concéntricos que lo incluyen.
- *Aceptación del usuario*. (El factor "molestias"). La facilidad de uso y la fiabilidad de la identificación son importantes para evitar que el sistema se convierta en una fuente de frustración y provoque la tentación de transgredirlo.
- *Escalabilidad*. ¿Podrá ampliarse el diseño a medida que aumente la necesidad, la financiación y la confianza en la tecnología?
- *Compatibilidad hacia atrás*. ¿Es compatible el nuevo diseño con los elementos del antiguo sistema existente? Mantener todo o parte de un sistema existente puede reducir enormemente el coste de implantación.

> No se puede comprar la salida

Incluso si el gasto no fuera un problema, cubrir las instalaciones con la máxima seguridad sería, en la mayoría de los casos, inaceptablemente intrusivo y molesto. Deben evaluarse de forma realista las necesidades de todas las áreas que hay que proteger basándose en qué hay dentro y quién necesita acceder

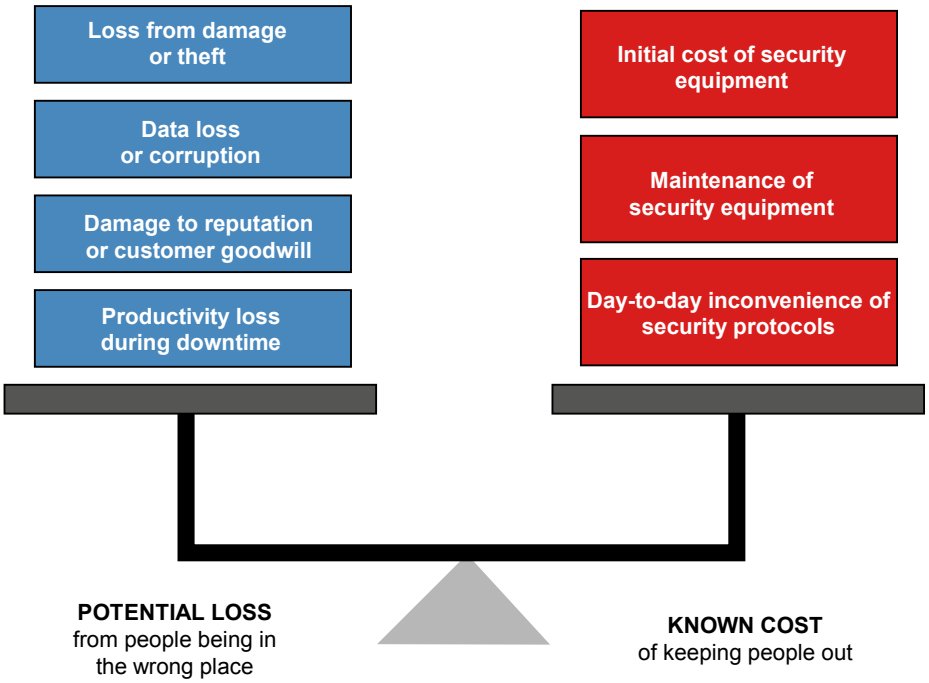


Imagen 4

Equilibrio entre pérdida potencial y coste de seguridad conocido

Conclusión

A medida que proliferan los centros de datos y los sitios de alojamiento web, la necesidad de seguridad física en las instalaciones es exactamente igual de importante que la necesidad de ciberseguridad de las redes. Los intrusos que falsifican su identidad o sus intenciones pueden causar enormes daños, desde la inutilización física de equipos críticos hasta el lanzamiento de ataques de software en un teclado no seguro. Incluso los errores normales del personal bienintencionado suponen una seria amenaza diariamente, y pueden minimizarse limitando el acceso a solo el personal estrictamente esencial.

Hay tecnologías, cada vez menos caras, para implantar amplias soluciones basadas en los principios de identificación **Qué tienes**, **Qué sabes** y **Quién eres**. Combinando una evaluación de la tolerancia al riesgo con un análisis de los requisitos de acceso y tecnologías disponibles, puede diseñarse un sistema de seguridad eficaz que ofrezca un equilibrio realista entre protección y coste.

Acerca del autor

Suzanne Niles es analista de investigación sénior en el Centro científico de centro de datos de Schneider Electric. Estudió Matemáticas en el Wellesley College y se licenció en Informática en el MIT, con una tesis sobre el reconocimiento de caracteres escritos a mano. Suzanne se ha dedicado a la formación durante más de 30 años, utilizando una amplia gama de soportes, desde manuales de software hasta fotografías o canciones infantiles.

Recursos

Presione en el icono para dirigirse al recurso

Selección del emplazamiento para instalaciones de importancia crítica
White Paper 81

Examinar todos los documentos técnicos
whitepapers.apc.com

Examinar todas las herramientas TradeOff Tools™
tools.apc.com

Contacte con nosotros.

Si tiene algún comentario o sugerencia sobre el contenido de este White paper:

Data Center Science Center
DCSC@Schneider-Electric.com

Si es cliente y tiene dudas específicas sobre su proyecto de centro de datos:

Póngase en contacto con su representante de **Schneider Electric**
www.apc.com/support/contact/index.cfm

Apéndice

Enlace al
White Paper 81

Selección del emplazamiento para instalaciones de importancia crítica

Consideraciones de seguridad al diseñar edificios

Al construir un nuevo emplazamiento o renovar uno antiguo, puede abordarse el tema de la seguridad física de abajo arriba incorporando características arquitectónicas y de construcción que desanimen o impidan la intrusión. Las consideraciones de seguridad en la estructura y diseño de un edificio suelen relacionarse con las posibles rutas de entrada y escape, el acceso a elementos de infraestructura crítica, como el cableado y el sistema de HVAC, y lugares donde los intrusos puedan ocultarse.

Para ver las consideraciones de seguridad al elegir el emplazamiento, consulte el documento técnico APC número 81, *Selección del emplazamiento para instalaciones de importancia crítica*.

- Sitúe la puerta del centro de datos de forma que solo quede cerca de la puerta el tráfico que entra y sale del centro de datos.
- Utilice puertas y marcos de acero, con puertas macizas en lugar de huecas. Asegúrese de que las bisagras no pueden quitarse desde el exterior.
- Las paredes del centro de datos deben utilizar materiales más sólidos que los típicos paneles de roca utilizados para las paredes interiores. Pueden incrustarse sensores en las paredes para detectar la manipulación.
- El espacio utilizado para el centro de datos no debe colindar con ninguna pared exterior.
- Deje líneas de visión largas y despejadas para cualquier cámara o puesto de seguridad del centro de datos.
- Utilice barreras para impedir la visión desde el exterior de las entradas y otras áreas comprometidas. Esto evitará la inspección visual de personas que deseen estudiar la disposición del edificio o sus medidas de seguridad.
- Conozca la situación de los conductos de ventilación, las trampillas de servicio, las canalizaciones, los montacargas y otras posibles aberturas que puedan utilizarse para conseguir acceder. Deberán instalarse rejillas antirrobo en todas las aberturas que tengan una anchura superior a 30,5 cm con el fin de impedir la entrada de un ser humano.
- Evite crear espacios que puedan utilizarse para ocultar personas o cosas. Por ejemplo, el espacio que hay debajo de los suelos elevados puede ser un lugar donde ocultarse. Compruebe que estos lugares están bien cerrados y no son fácilmente reconocibles al andar por las instalaciones.
- Instale cerraduras y alarmas de puerta en todos los puntos de acceso del tejado de forma que el personal de seguridad sea informado inmediatamente de un intento de acceso. Evite que haya puntos de entrada en el tejado siempre que sea posible.
- Tome nota de todos los conductos externos de fontanería, cableado, HVAC, etc., y disponga la protección apropiada. Si se dejan a la vista o desprotegidos, estos componentes de infraestructura pueden utilizarse para sabotear las instalaciones sin necesidad de inhabilitar las medidas de seguridad.
- Elimine el acceso a los conductos internos de cableado, fontanería y ventilación dentro de las instalaciones. Puede que el centro de datos sea totalmente seguro, pero si una persona puede acceder desde un pasillo a los conductos de cables de alimentación o de datos, el centro de datos está en peligro.
- Considere la situación del centro de datos dentro del edificio cuando actualice unas instalaciones existentes o construya un nuevo centro de datos dentro de una estructura existente. Evite lugares vulnerables o riesgos provocados por el ser humano. Por ejemplo, evite situar el centro de datos debajo o al lado de las instalaciones de cocina, áreas de fabricación con grandes maquinarias, aparcamientos o cualquier área con mucho tráfico o acceso de vehículos. Cualquier cosa, desde incendios en cocinas a coches bomba o accidentes de tráfico suponen una amenaza.

- Proteja el puesto de supervisión de seguridad central cerrándolo con cristal antibalas.
- Si el centro de datos se encuentra en el interior de su propio edificio, mantenga el exterior despejado. No utilice marcas de identificación, como nombres de empresa o logotipos, que puedan indicar que dentro hay un centro de datos.
- Utilice bolardos de hormigón u otros obstáculos para evitar que vehículos no autorizados se aproximen a una determinada distancia del edificio.

Glosario

En este glosario se definen los términos que aparecen en **negrita**.

Control de acceso

Control de la entrada de personas a edificios, salas y racks, y control del uso de teclados y equipos, mediante el uso de dispositivos automatizados que leen la información almacenada en un objeto, como una tarjeta (**qué tienes**), reciben un código o una contraseña (**qué sabes**) o reconocen un rasgo físico mediante análisis biométrico (**quién eres**).

Punto de acceso

Un lugar dentro del perímetro de una área segura en el que hay una puerta y algún tipo de método de **control de acceso** para filtrar usuarios que intentan entrar en la área.

Disponibilidad

Una predicción calculada de un porcentaje de “autonomía” de la red. Para instalaciones de misión crítica, el objetivo es conseguir los “cinco nueves” o el 99,999%, menos de 5 minutos de inactividad al año.

Tarjeta de código de barras

Un tipo de tarjeta de **control de acceso** que utiliza un código de barras para almacenar información; se lee pasando la tarjeta por un lector.

Tarjeta de ferrita de bario

Un tipo de tarjeta de **control de acceso** que utiliza un patrón de puntos magnéticos para almacenar información; se lee dejando la tarjeta plana sobre un lector. También se llama “tarjeta de puntos magnéticos”.

Cerradura biométrica

Una cerradura que se controla mediante un escáner biométrico.

Biometría

Determinación de la identidad personal utilizando la tecnología para medir rasgos físicos o de comportamiento, por ejemplo, la huella digital.

Cerradura cifrada

Una cerradura que se abre pulsando sus botones en una secuencia específica. Se diferencia de una **cerradura con código** que normalmente solo tiene 4-5 botones, y cada botón solo puede pulsarse una vez. La cerradura cifrada, con botones metálicos, era el precursor mecánico de la cerradura con código electrónico actual con un teclado de tipo teléfono.

Cerradura con código

Una cerradura que se abre tecleando un código en un teclado.

Tarjeta inteligente de contacto

Una tarjeta inteligente que debe ponerse en contacto con el lector. Compárela con **tarjeta inteligente sin contacto**.

Tarjeta inteligente sin contacto

Una **tarjeta inteligente** que utiliza tecnología **RFID** para activar su uso sin contacto físico con el lector. La distancia máxima hasta el lector es de **proximidad** (10 cm) o de **vecindad** (un metro) dependiendo de cuál de las dos normas RFID se use.

Seguridad escalonada

Perímetros concéntricos de seguridad que pueden tener métodos de acceso distintos o cada vez más restrictivos. Una área interior está protegida tanto por sus propios métodos de acceso como por los de las áreas que la rodean y a las que debe entrarse primero.

Geometría facial

Uno de los rasgos físicos que puede medir la tecnología biométrica: la posición relativa de ojos, nariz y boca en la cara.

Falsa aceptación

En identificación biométrica, el resultado erróneo de identificar a alguien que no está en la base de datos de personas conocidas. Es una de las dos formas en que puede fallar la identificación biométrica; la otra es el **falso rechazo**.

Falso rechazo

En identificación biométrica, el resultado erróneo de no identificar a una persona conocida. Es una de las dos formas en que puede fallar la identificación biométrica; la otra es la **falsa aceptación**.

FAR

Índice de falsa aceptación. En un dispositivo biométrico, el porcentaje de lecturas que son una **falsa aceptación**.

FRR

Índice de falso rechazo. En un dispositivo biométrico, el porcentaje de lecturas que son un **falso rechazo**.

Exploración de la mano

Una técnica de identificación biométrica que mide la geometría tridimensional de la mano: forma de los dedos y grosor de la mano.

iButton®

Un microchip similar a los utilizados en las **tarjetas inteligentes** pero incrustado en un botón redondo de acero inoxidable de aproximadamente 1,25 cm de diámetro y que puede ponerse en un llavero o en una pieza de joyería. Los iButtons son extremadamente resistentes, pero (desde mayo de 2004) no están disponibles con tecnología **RFID** para uso sin contacto.

IFPO

International Foundation for Protection Officers. Una organización sin ánimo de lucro fundada con el objetivo de ofrecer formación estandarizada y certificación a los inspectores de seguridad. El Manual de formación de supervisores de seguridad es una guía de referencia para los inspectores de seguridad y el personal a su cargo.

Tarjeta de sombra de infrarrojos

Un tipo de tarjeta de **control de acceso** que tiene un código de barras entre dos capas de plástico. El lector pasa la luz infrarroja por la tarjeta y la sombra del código de barras es leída por los sensores del otro lado.

Exploración del iris

Una técnica de identificación biométrica que explora el patrón de colores del iris del ojo.

Niveles de seguridad

El rango de protección, de menor a mayor, ofrecido en los perímetros concéntricos – el menos seguro es el perímetro más exterior (como la entrada al edificio) y el más seguro es el perímetro más interior (como el acceso a un rack).

Tarjeta de banda magnética

Tarjeta de banda magnética

Un tipo de tarjeta de **control de acceso** que utiliza una banda magnética para almacenar información; se lee pasando la tarjeta por un lector.

Gestionable

Que puede supervisarse y controlarse a distancia. Los dispositivos de **control de acceso** gestionables pueden comunicarse con un sistema de gestión remoto para *supervisar* (quién entra y sale, y cuándo), *controlar* (configurar el dispositivo para permitir el acceso a determinadas personas en determinados momentos), y *dar la alarma* (notificación de repetidos intentos de acceso infructuosos o fallos del dispositivo).

Gestión

Comunicación automatizada con dispositivos remotos para supervisar, controlar y dar la alarma. Tradicionalmente llamada “automatización de edificios” o “automatización doméstica”, el nuevo término *gestión* hace referencia a la comunicación basada en red con todos los elementos de un centro de datos, incluido el propio equipo de TI (servidores, dispositivos de almacenamiento, telecomunicaciones y dispositivos de red) y la infraestructura física (potencia, refrigeración protección contra incendios y seguridad).

Esclusa

Un habitáculo de tipo burbuja con puertas seguras a la entrada y a la salida, y espacio para una sola persona ente las puertas. Es una solución a los fallos de seguridad denominada **colarse con cómplice** o **colarse sin cómplice**, en los que una persona no autorizada pasa libremente por un punto de acceso detrás de a una persona autorizada que abre la puerta.

DCPI

Infraestructura física del centro de datos. Elementos de la infraestructura física de un centro de datos (distinta de la infraestructura de TI como enrutadores y gestores de almacenamiento) que contribuyen directamente a la **disponibilidad** garantizando un funcionamiento ininterrumpido. DCPI incluye potencia, refrigeración, extinción de incendios y seguridad **física**.

Necesito saber

Un nivel de seguridad muy alto, con acceso limitado a personas que tienen una necesidad específica e inmediata de estar en la área segura (para acceder a un dato particular, por ejemplo), y con acceso solo durante el tiempo en el que existe esa necesidad.

Infraestructura física del centro de datos, consulte DCPI

PAC

Código de acceso personal. Otro nombre para PIN (número de identificación personal). Un código o una contraseña que identifica a un usuario en un **punto de acceso**.

Seguridad física

Protección de instalaciones físicas de accidentes o sabotaje causados por la presencia de personas no autorizadas o malintencionadas. Un sistema de seguridad física siempre incluye dispositivos de **control de acceso** para el filtrado automatizado en los puntos de entrada más un sistema de alarma basado en sensores. La protección adicional puede incluir cámaras de vigilancia y guardias de seguridad. (*Seguridad física* suele utilizarse de forma más general para referirse a la protección de todo tipo de daños físicos, incluido el mal tiempo, terremotos y atentados con bomba. En este documento solo hace referencia a la protección de problemas causados por personas no autorizadas dentro de las instalaciones.)

Colarse con cómplice

Es el fallo de seguridad que se produce cuando una persona autorizada abre una puerta utilizando credenciales legítimas y sujeta la puerta para que pase una persona no autorizada y sin credenciales. (Un fallo similar es **colarse sin cómplice** en el que un usuario no autorizado se cuela inadvertidamente detrás de un usuario autorizado.)

Tarjeta prox

Tarjeta de proximidad

Una tarjeta de **control de acceso** que tiene un transmisor/receptor **RFID** incorporado que le permite comunicarse con un lector a una distancia de un metro.

Tarjeta inteligente de proximidad

Una **tarjeta inteligente** que tiene tecnología **RFID** en su chip, de forma que puede comunicarse con el lector a una distancia de hasta 10 cm. También se llama **tarjeta inteligente sin contacto**.

Exploración retinal

Una técnica de identificación biométrica que explora el patrón de vasos sanguíneos de la retina del ojo.

RFID

Identificación por radiofrecuencia. Comunicación entre tarjeta y lector sin contacto físico. La tecnología RFID es lo que hace que funcionen las **tarjetas de proximidad**, las **tarjetas de vecindad**, y las **tarjetas inteligentes sin contacto**. El chip RFID es alimentado por un campo electromagnético desde el lector, por lo que no necesita batería.

Tarjeta inteligente

Un tipo de tarjeta de **control de acceso** que almacena información en un microchip. El chip no solo almacena datos, sino que puede realizar cálculos e intercambiar datos con el lector. Se lee tocando el lector con la tarjeta para que los contactos eléctricos se alineen; véase también **tarjeta inteligente sin contacto**.

Soporte inteligente

Pequeños objetos de cualquier forma que contienen el mismo tipo de chip utilizado en una **tarjeta inteligente**. Los soportes inteligentes suelen ser objetos pequeños (**testigos**) que pueden ponerse en un llavero o llevarse como una pieza de joyería.

Ingeniería social

El uso de la astucia para manipular a las personas y conseguir que relajen sus procedimientos de seguridad, por ejemplo, que revelen sus contraseñas, dejen las llaves o abran las puertas.

Colarse sin cómplice

El fallo de seguridad que se produce cuando una persona no autorizada se cuela inadvertidamente por un punto de acceso siguiendo a un usuario autorizado por una puerta abierta. (Un fallo similar es **colarse con cómplice**, en el que el usuario autorizado sujeta la puerta para que pase el usuario no autorizado.)

Plantilla

plantilla En **biometría**, una transformación computada de una exploración de escáner; sigue siendo única del individuo pero ocupa mucho menos espacio de almacenamiento. Es la plantilla, no la exploración real, la que se almacena en la base de datos de usuario o en el chip de una **tarjeta inteligente**, para su comparación con una exploración real tomada en un **punto de acceso**.

Umbral

En **biometría**, el parámetro ajustable por el usuario que puede utilizarse para ajustar los dos índices de fallo (**falsa aceptación** y **falso rechazo**). Como representa el “grado de exactitud que es suficiente” para declarar una coincidencia, al disminuir un índice de fallos aumenta el otro.

Testigo

Un pequeño objeto con un microchip que lleva la información de identificación personal. El testigo se pone en contacto con el lector o simplemente se acerca si incluye tecnología **RFID**.

Tarjeta de vecindad

Una tarjeta de **control de acceso** que tiene un transmisor/receptor **RFID** incorporado que le permite comunicarse con un lector a una distancia de un metro.

Reconocimiento de voz

En **biometría**, una representación digital de la voz de un usuario utilizada para compararla con la voz en vivo del usuario en el **punto de acceso**.

Tarjeta Weigand

Un tipo de tarjeta de **control de acceso** que incorpora cables especialmente tratados y magnetizados para almacenar información; se lee pasando la tarjeta por un lector.

Qué tienes

En **control de acceso**, cualquier método de identificación basado en un objeto que uno posee, como una tarjeta o un **testigo**. Es la categoría de identificación menos segura, ya que no hay garantía de que el objeto esté siendo utilizado por la persona correcta.

Qué sabes

En **control de acceso**, cualquier método de identificación basado en algo que uno sabe, como un código numérico o una contraseña. Es más fiable que **qué tienes**, pero pueden revelarse a alguien o escribirse y que alguien los descubra.

Quién eres

En **control de acceso**, cualquier método de identificación basado en un rasgo biológico o de comportamiento único de cada persona. Es la categoría más segura de identificación porque es muy difícil falsificar el rasgo, aunque no es 100% fiable porque existe el riesgo de errores de lectura o interpretación. Otro nombre para este tipo de identificación es **biometría**.