

Sistemas de Control de Accesos

por Gau Barrera

© 2003 HD Corp.



El negocio de los Sistemas de Control de Accesos dista mucho de estar agotado. Sus aplicaciones en seguridad y control son habituales en muchos de los aspectos de la vida diaria de nuestra sociedad y éste ha sido un respaldo decisivo a la hora de marcar el crecimiento de su segmento de mercado.

He aquí una enumeración de las ventajas de estos sistemas. Hablan los proveedores.

Encarar un informe de negocios siempre es un reto. Un negocio suele resultar de la buena aplicación de un sinfín de variables. Y muchas de esas variables dependen del mercado al que nos estemos refiriendo. Claro que si hablamos de Control de Accesos, la apreciación cambia considerablemente, ya que en los últimos años este rubro de la seguridad electrónica se ha mantenido y crecido aún con la crisis del 2001 de manera formidable.

Pero si bien el rubro es conocido y su difusión ha sobrepasado el ambiente de la comercialización de elementos de seguridad, para instalarse en la sociedad como artículos necesarios de prevención y control delictivo, es pre-

ciso, antes de ahondar en la faz comercial de este rubro, definir al menos acotadamente qué es un sistema de control de accesos...

“Un sistema de control de acceso se utiliza para: restringir o controlar el acceso o egreso de personal, vehículos o materiales a una o varias áreas, mediante el uso de barreras físicas, personal de seguridad o dispositivos electrónicos y mecánicos”- es la medida de definición de **G. López de la empresa Protek**.

“Lo primero a tener en cuenta es que debe combinar hardware con software y permitir conectar múltiples accesos entre sí (conexión en red) para

ser controlados y comandados desde una PC. Todo aquello que no contemple estas mínimas características no podrá ser denominado control de accesos. Se lo podrá identificar como Abrepuertas, con o sin software, pero Abrepuertas al fin”- acentúa la diferencia **M. Galdi de la firma SG Systems**.

J. Godoy de la compañía Diastec, siendo un poco más extenso, nos dice: *“Se define como control de accesos a los instrumentos, equipamiento, normas y recursos asignados a la identificación de personas y a la restricción de sus atribuciones destinados a preservar los activos y la confi-*



Continúa en página 80

Viene de página 76

dencialidad dentro de una empresa. El control de accesos registra fecha y hora de todos los eventos y transacciones de manera que permita una auditoría posterior. Estos sistemas deben proveer tres elementos: autenticación, autorización y administración de los datos que maneja. 'Autenticación' se refiere a que el usuario acredite ser quien dice que es, mediante los métodos del sistema (credenciales, biometría, etc.). La 'autorización' permite que el usuario autenticado, acceda a los recursos. Finalmente, la 'administración' permite el alta, la baja, modificaciones de usuarios y atribuciones. La función primaria de un sistema de control de accesos es preservar y proteger la confidencialidad, integridad y disponibilidad de bienes, sistemas y recursos".

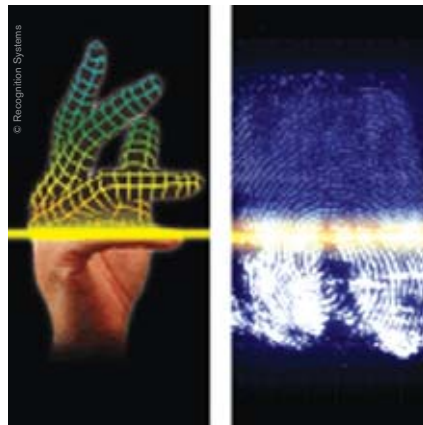
Siguiendo esta línea de razonamiento, no se debe descuidar el hecho que el control debe verificarse en un tiempo administrativamente prudencial. No resultaría útil un sistema que requiera 10 verificaciones para acceder a un recurso, así como tampoco el que las requiera para recursos que no son utilizados por nadie. El ideal, es aquel que le permita a la Dirección determinar quién puede o no acceder, leer, escribir, ejecutar, modificar la situación de bienes y sistemas, basado en el rol del individuo o grupo de individuos dentro de la organización que se tratare.

Existen diferentes tecnologías que se utilizan, entre ellas podemos mencionar a las tarjetas, las contraseñas, las llaves encriptadas, etc. Mención aparte merecen los sistemas de identificación de patentes automotrices y los biométricos como huella digital, reconocimiento de voz, escaneo del iris, geometría de mano, etc. Estos sistemas tienen la ventaja de que el usuario no puede extraviar u olvidar su identificación personal.

Finalmente, las organizaciones que adopten un sistema de control y acceso, deben apoyarlo con políticas integrales de seguridad bien documentadas y auditadas, dado que al tratarse de información sensible para los individuos (y la comunidad en su conjunto), la documentación de respaldo debe ser cuidadosamente preservada y su acceso limitado.

Pero si nuestra búsqueda nos lleva a requerir una definición un poco más

técnica, la palabra de **D. Schapira de la empresa Codas**, parece ser la adecuada: "Un sistema de control de acceso se compone de los paneles controladores (que se interconectan entre sí para ampliar el número de puertas a controlar), el software de administración y los distintos periféricos tales como cerraduras, sensores y elementos de identificación. Un punto importante a tener en cuenta, es la tecnología de identificación a utilizar. En la actualidad, la identificación de las personas a controlar puede hacerse básicamente mediante dos métodos: tarjetas o



la ventaja que poseen los sistemas de identificación biométrica es que el usuario NO puede extraviar u olvidar su identificación personal

credenciales o a través del reconocimiento de una característica física de los individuos (dispositivos biométricos). Asimismo, hay aplicaciones que utilizan ambos métodos en forma complementaria. Dentro de las tecnologías de identificación por tarjeta podemos nombrar la de código de barras, banda magnética y proximidad, siendo esta última la adoptada mayoritariamente en la actualidad. En el caso de los dispositivos de identificación biométrica, los más comunes son los de identificación por huella digital o geometría de mano, aunque también existen otros métodos como reconocimiento del iris, de la voz, etc.".

Determinamos entonces que un

Control de Accesos es un sistema que nos permite controlar todas las entradas y salidas desde un único puesto de control informático. Autorizar o denegar el acceso a una zona restringida, como también establecer bandas horarias y feriados y visualizar y ordenar la información de eventos sucedidos.

"Ahora bien, una vez identificado lo que es un control de accesos los diferenciaremos por sus prestaciones o categorías: 1º) 'pequeña empresa', que contempla estas mínimas características pero son de baja memoria de eventos, usuarios y accesos y no contemplan la interconexión con sistemas de software de enriquecimiento de información, como ser: Control de Asistencia y Presentismo o Liquidador de Sueldos. 2º) 'mediana empresa', que permite interconexión con estos sistemas pero que los mismos deberán ser de la misma empresa que comercializa el control de accesos, no estando preparado para conectarse (ya sea en tiempo real o no) con otros sistemas estándar o puntuales de enriquecimiento de información. 3º) 'grupo empresario', alta memoria de eventos, usuarios y accesos, con interconexión con sistemas de software de enriquecimiento de información pero que deberán ser de la misma empresa que comercializa el control de accesos. 4º) 'corporativo', alta memoria de eventos, usuarios y accesos, con interconexión con cualquier tipo de sistemas de software de enriquecimiento de información (en tiempo real) estándar o puntuales"- específica **M. Galdi de SG Systems**.

Veamos ahora...

Otras tecnologías aplicadas

"En realidad, si entendemos este concepto en términos muy amplios," reflexiona **E. Meuer de la compañía Tekhnosur**, "podemos decir que la biometría se practica desde el principio de los tiempos, y de hecho, nosotros mismos la practicamos muchas veces a lo largo del día, casi sin darnos cuenta. Por ejemplo, cuando descolgamos el teléfono y escuchamos la voz de nuestro interlocutor, nuestro cerebro trata de comprobar si esa voz se parece a cualquiera de las muestras que



Tekhnosur S. A.
Sistemas y Soluciones Informáticas

Viene de página 80

tiene almacenadas en su memoria y que ha ido recopilando a lo largo de nuestra vida. Si nuestro cerebro encuentra similitudes suficientes entre alguno de sus recuerdos y lo que está escuchando en ese momento, entonces reconocemos a la persona que nos ha llamado. Si no, asumimos que estamos ante alguien a quien no conocemos. Del mismo modo, los animales reconocen a otros animales por características biométricas tales como el olor, el tacto o el timbre de la voz.

El reto de la tecnología biométrica radica en conseguir que las máquinas puedan llevar a cabo esas operaciones de reconocimiento que son en apariencia tan simples y que lo hagan de forma rápida y libre de errores”-

Pero dotar a las máquinas de esas capacidades de identificación efectiva, así como ocurre con otras capacidades humanas, tales como el lenguaje, se ha revelado como una tarea muy compleja.

Aún así, los últimos avances en las investigaciones y el desarrollo de nuevas tecnologías informáticas dieron excelentes resultados en algunos productos como los reconocedores de huellas digitales, de geometría de manos, los escáneres de iris y más recientemente, el reconocimiento de caras.

Estas ideas fabulosas de las películas de ciencia ficción han pasado de la pantalla, al catálogo de muchos fabricantes.

“La biometría es una tecnología basada en el reconocimiento de una característica física e intransferible de las personas. Los sistemas biométricos incluyen un dispositivo de captación y un software que interpreta la muestra física y la transforma en una secuencia numérica única. En el caso del reconocimiento de la huella digital, se ha de tener en cuenta que en ningún caso se extrae la imagen de la huella, sino una secuencia de números que la representan. Esto además sirve para que nadie que opere con estos sistemas guarde un registro “fotográfico” de las huellas digitales con la posibilidad de reproducirlas para otros usos. El dispositivo capta la mues-

TeknoSur S. A.
Sistemas y Soluciones Informáticas

tra y el software biométrico transforma los puntos característicos de esta muestra, en una secuencia numérica a través de un al-

goritmo matemático que no tiene inversa. Es por este motivo por el que la tecnología biométrica es el sistema de seguridad más fiable en la actualidad. Esta secuencia numérica, llamada patrón de registro, queda almacenada en una base de datos segura y servirá para las siguientes comparaciones cada vez que la persona autorizada desee acceder al sistema”-

Los sistemas biométricos tienen como principal ventaja con respecto a los sistemas tradicionales basados en contraseñas o tarjetas, una mayor seguridad y comodidad.

El acceso a través de la biometría no depende de algo que “sabemos” o que



El sistema de lectura de patentes permite controlar vehículos en plena vía pública a una velocidad de hasta 170 km./h

“tenemos” y que nos pueden robar o copiar; depende de lo que “somos”, es decir, nuestras características físicas.

Otra ventaja es que es insignificante el costo de mantenimiento, ya que no necesita de la impresión de tarjetas nuevas o perdidas y el costo de implementación de este tipo de tecnología se ha reducido mucho más a raíz de su popularidad y aceptación.

El estado actual de las investigaciones biométricas permite augurar un próspero futuro en el mediano plazo, dado que la proyección de su inserción en el mercado jugará un papel relevante en lo que a seguridad informática se refiere. La creación de un

DNI digital basado en biometría, la generalización de hardware biométrico en los equipos informáticos o la utilización de biometría en los cajeros automáticos, son una pronta realidad en nuestras vidas.

“Aquellas empresas que opten por estas soluciones con premura, estarán en una clara situación de ventaja competitiva con respecto a las que se limiten a actuar como meros espectadores”- finaliza E. Meuer de la compañía Tekhnosur.

Existe también, probado en Argentina desde hace un año, un sistema de lectura de patentes de automóviles desarrollado en el país, que incluso se combina con el sistema biométrico mencionado de huella digital del conductor, *“es un excelente sistema para controlar y administrar el acceso de vehículos a predios y verificar la circulación por rutas y calles”- puntualiza C.*



Edjen de la firma Vision Robot, *“se ha usado para generación automática de cédulas de infracción a partir de fotografías de multas y para ordenar el acceso a lugares restringidos; en una versión portátil para policías de caminos, se ha usado para encontrar vehículos con pedido de captura en rutas en forma automática, entre un millón de patentes y en pocos segundos. Para cálculo automático y sin ticket de facturas de estacionamiento; para entradas a estacionamiento de espectáculos, hoteles, etc.*

El sistema es tan bueno y seguro como lo es el método de una chapa patente para verificar la identidad de un vehículo, con sus pros y sus contras”-

Este sistema no requiere intervención humana ni acción de parte del conductor o poseedor del vehículo. Sin dispositivos a instalar en el auto, ni ninguna limitación. Permite el control de gestión o logística con solo agregar la placa patente como un dato más a la base.

Se puede mediante su utilización, controlar vehículos con restricciones a la circulación en plena vía pública y a una velocidad de hasta 170 Km/h.

“La instalación requiere de algunas placas en la PC (aunque existe una versión sin PC) del puesto de control de acceso y obviamente cámaras. El beneficio es que para sistemas cerrados no requiere instalaciones ni ele-

Continúa en página 88

El negocio de los Sistemas de Control de Accesos

Viene de página 84

mentos a llevar en el vehículo y para sistemas abiertos, no tiene competencia, o sea, donde el vehículo es desconocido o no pertenece a un conjunto limitado de unidades en una flota o country o lo que fuere, como podría suceder en una playa de estacionamiento por horas o en la de un supermercado"- cierra **C. Edjen**.

El mercado de los sistemas de control de accesos

Dado que las aplicaciones más usuales de estos sistemas cubren las áreas de puertas principales de acceso a oficinas o edificios, centros de cómputos, gerencias, puertas de acceso a escaleras, ascensores o a depósitos de materiales y archivos, se hace fácil deducir que sus mayores consumidores son las empresas.

Pero se ha ido viendo con mayor frecuencia desde hace unos años su utilización en countries, barrios cerrados y torres de edificios para controlar la salida y entrada del personal, de los propietarios y sus visitas o de los socios y sus acompañantes; también en estacionamientos, donde su empleo es para el control de entrada y salida de vehículos; en hotelería y edificios reemplazan a la tradicional llave por una tarjeta o un código de identificación.

Existen aplicaciones en unidades carcelarias para control de visitas e incluso se han adoptado en espectáculos deportivos reemplazando la entrada por una tarjeta prepaga.

En un principio, los consumidores de estos sistemas fueron las empresas que deseaban controlar los movimientos del personal en las distintas áreas, así como los movimientos de mercadería o de vehículos, pero actualmente tanto los instaladores como las empresas instaladoras y el público en general han trasladado su uso a prácticamente todos los aspectos de la vida diaria relacionados con el tránsito y control de personas o móviles, así como para el archivo y codificación de historiales basados en los perfiles configurados en la base de datos del sistema.

Todo un mercado. Y si de mercado se trata...

Hablemos de negocios

Si tomásemos un punto de referencia sobre el tema, tendríamos que recurrir a los '90, cuando este tipo de

elementos de seguridad comenzó a desarrollarse sin interrupción; no porque antes no se encontraran en el mercado, sino porque puedo afirmar sin temor a equivocarme que hacia fines de esa década la difusión de sus usos y aplicaciones se convirtió en tema común y de manejo público. Una estadística que se realizó en enero de 2002, arrojaba como resultado que del total del mercado de productos de seguridad electrónica, el 37% lo representaban los productos asociados a los sistemas de control de accesos. Si tomamos como indicador que casi el 40% del mercado está representado por este seg-



El software asociado a estos sistemas le permite restringir accesos por bandas horarias, programar feriados, generar reportes, etc.

mento y que el 60% restante lo ocupan todos los otros ítems del rubro, no hace falta concluir que es el que mejor sobrellevó la crisis del 2001.

En la actualidad, su nivel de intervención en el rubro es amplio y abarcativo. El desarrollo de software y hardware nacional significó para el mercado una nueva ruta de reactivación comercial, y la aplicación de maquinaria y tecnología de última generación trajo emparentado el corrimiento de los márgenes de calidad con orientación a las certificaciones internacionales, como único impedimento para la exportación de desarrollos argentinos. Aun así, en este aspecto queda mucho camino por

recorrer, pero eso no es más que la confirmación del potencial comercial que tiene el rubro.

La relación costo / beneficio está dada por la posibilidad de su interconectividad, de modo de poder ser controlados y comandados desde un solo punto o desde varios y configurarse a elección de la cadena jerárquica de la empresa, personal de seguridad del establecimiento o consorcio del edificio que se trate.

Esto proporciona economía de personal, de estructura y de mantenimiento, y esta relación se torna mucho más ventajosa al tratarse de productos fabricados en el país, que a partir de la devaluación quedaron comparativamente mucho más accesibles que similares equipos importados.

Otra virtud es la de "reutilizar" equipos (lectores, tarjetas, etc.) adquiridos hace algunos años, de los cuales muchos quedaron sin soporte local y utilizarlos con controladores más avanzados, recuperando así parte del capital invertido y ampliando las aplicaciones del sistema ya existente. También es una ventaja presentarle al usuario final una consola de administración de seguridad integrada, desde donde puede supervisar todos los sistemas de seguridad. En algunos sistemas se permite la edición, transferencia, importación y exportación de datos e imágenes en un formato de texto ASCII lo que posibilita el uso de los datos e imágenes con software de terceros.

Y en cuanto a la estrategia comercial necesaria para la venta de estos equipos, no difiere en mucho de cualquier estrategia utilizada para otros equipos relacionados con la seguridad electrónica, es decir, satisfacer la necesidad de protección. Si bien muchas veces resulta difícil establecer una ecuación costo / beneficio que se justifique desde un punto de vista puramente económico, resulta fundamental explicarle al cliente las ventajas que se obtienen al tener un sistema de control de accesos.

Es importante determinar cuáles son las áreas que se deben proteger y con qué grado de seguridad, a los efectos de encarar un buen proyecto. A veces, gracias a la capacidad modular de la mayoría de los sistemas, se puede comenzar con un sistema pequeño para luego ir ampliándolo.

La necesidad de utilizar productos de

Continúa en página 92

El negocio de los Sistemas de Control de Accesos

Viene de página 88

primera marca, con garantía y respaldo técnico local e instalado por profesionales certificados (aunque a veces esto no parezca ser la opción más económica), se impone a la hora de asegurar la venta. O sea, cuantificar las ventajas mencionadas aplicándolas a la realidad del cliente, ya sea una empresa o un negocio dado.

-“Este tipo de productos está dirigido a grandes empresas, con lo cual la venta se realiza a través de canales industriales en los cuales es necesario ofrecer el producto desde el punto de vista costo / beneficio. Demostrar

BOSCH *que el sistema es efectivo y que, además, refuerza la protección de los bienes inmuebles y la administración del personal, es uno de los puntos más importantes a tener en cuenta”- afirma D. Madeo del grupo Bosch.*

-“La implementación de un sistema de control de accesos electrónico aporta diferencias significativas con respecto a los sistemas manuales. Las principales ventajas son: Eliminación de errores en el registro manual de

datos. Eliminación de elementos subjetivos y de complicidad en funciones desempeñadas actualmente por personas. Nivel de seguridad adaptable de acuerdo con el presupuesto, desde las opciones más económicas basadas en identificación por claves y tarjetas, hasta las más sofisticadas basadas en biometría. Esto nos lleva a que la estrategia comercial que empleamos sea la de enunciar la rápida amortización del capital invertido, la disminución de las horas contratadas con las empresas de seguridad física, la disminución de daños, robos y hurtos del capital de la empresa y la eficaz integración con otros sistemas”- resume **D. Arcondo de Larcon Sia.**

■ Conclusiones

En las pequeñas, medianas y grandes empresas su uso está ampliamente difundido, aunque eso no significa que esté ampliamente adoptado, por lo que el negocio de los Sistemas de Control de Accesos desde el punto de vista netamente empresarial, aún tiene territorio por recorrer. Los desarrollos tecnológicos y de seguridad encarados en este aspecto, llevan a hacer evolucionar al rubro y por ende, a ampliar sus horizontes comerciales.

Por otro lado, su funcionalidad y su afortunada incursión en el territorio de la cotidianeidad, le dieron un decisi-

vo ascendente por sobre las cerraduras convencionales, otorgándole al tipo de sistema autónomo, una ventaja taxativa en cuanto a la relación costo / beneficio, en un nicho de mercado tan poco explotado como lo es el de clientes particulares, edificios, barrios cerrados y otros, en donde las posibilidades de vender estos sistemas es mucho mayor que la de no hacerlo.

En conclusión, se dice por ahí que “en la variedad está el gusto”, pero tratándose de sistemas de control de accesos, “en la variedad de aplicaciones está el negocio”.

Agradecemos la colaboración de todos los profesionales que han participado para la realización de este informe.