Control de Accesos
Elementos de Identificación

Ing. Luis Cosentino
Consultor Independiente
lcosentino@fibertel.com.ar

Diseñada como una ayuda para técnicos, instaladores y estudiantes, ofrecemos a nuestros lectores una serie de conceptos y fundamentos sobre el control de accesos, sus elementos y funciones. Un detallado estudio de mercado y un ejemplo de diseño son los complementos de esta obra que seguramente será de suma utilidad para nuestros lectores.

Indice

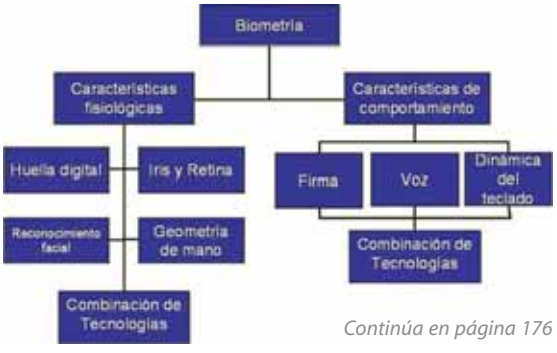
En el número anterior (*Elementos de identificación, Cap. V, 2da. Parte; RNDS nº47*) se describieron las ventajas y desventajas de los diferentes tipos de tarjetas que se utilizan en control de accesos para identificar a sus portadores. El presente artículo cubre los diferentes métodos de identificación basados en tecnología biométrica.

5.3. Lectores Biométricos.
5.3.1. Generalidades. Ventajas y desventajas

Las tecnologías basadas en parámetros biométricos, usualmente denominadas biometrías, parten de la base de reconocer algún parámetro físico o de comportamiento de la persona que lo identifique unívocamente para determinar o verificar su identidad.

Contrariamente a lo que se cree, las tecnologías basadas en parámetros biométricos son bastante antiguas: podría decirse que ya existían los sistemas de geometría de mano y huella digital cuando todavía no se utilizaban *Smartcards* para control de acceso. Lo que sucedió en los últimos años fue una constante baja en los precios de los lectores, lo que está popularizando su uso.

La ventaja principal de estas tecnologías es su alta tasa de identificación de personas y usadas correctamente, prácticamente eliminan la posibilidad de errores. Su principal desventaja, en tanto, radica en que son más lentas, costosas y menos resistentes al vandalismo respecto de las tarjetas de proximidad. Sin embargo, son las tecnologías en las que más se invierte en desarrollo y seguramente en el futuro dominarán el mercado.



Continúa en página 176

Viene de página 172

Cada biometría tiene limitaciones en su rango de aplicabilidad. Por ejemplo, existe entre un 3 y un 5% de personas que o no tienen huellas detectables o sus huellas no se adaptan a los algoritmos de reconocimiento más utilizados.

En países de alto nivel de inseguridad -como el nuestro- no siempre su utilización es una ventaja. Por ejemplo, si se desea disminuir la probabilidad de robo de un vehículo de alta gama puede utilizarse la huella del propietario para ponerlo en marcha. Esto significa que será necesaria esa persona cuando alguien desee robarlo, lo que aumenta el nivel de inseguridad del individuo.

Todo equipo biométrico necesita de un proceso de enrolamiento, es decir que se miden los parámetros de la persona varias veces para generar su "patrón", que será almacenado en la base de datos para luego ser utilizado como el estándar de comparación.

La exactitud de un equipo biométrico se mide fundamentalmente por dos índices: el falso rechazo y la falsa aceptación.

Falso rechazo significa que a la persona enrolada el equipo le está negando el acceso. Este defecto si bien es incómodo no representa un defecto grave para la seguridad del sistema dado que por tratarse de un parámetro biométrico, es posible que la persona pueda haber sufrido algún cambio temporal o algún parámetro ambiental influencie la lectura. Por eso es importante un buen enrolamiento o un sistema que continuamente adapte levemente los parámetros del patrón ante cada medición (sistemas adaptativos).

Falsa aceptación significa que una persona es identificada como si fuera otra. Errores de este tipo son graves y destruyen la credibilidad del sistema.

5.3.2. Identificación o verificación

Los parámetros biométricos pueden utilizarse tanto para identificar a una persona dentro de un grupo como para verificar que la persona sea quien dice ser. En términos generales la identificación es la forma más deseada del uso, pero es donde se encuentran las mayores limitaciones. En otras palabras, dado que para aplicaciones de tiempo real todavía los algoritmos están en desarrollo, puede decirse que por el momento es más seguro verificar que identificar.

5.3.2.1. Identificación

Por identificación se entiende al hecho de que el equipo biométrico dispone una base de datos -local o remota- con los parámetros de la población registrada en el enrolamiento y que cuando alguna persona se identifica frente al equipo, éste primero leerá sus parámetros y con esa información buscará en esa base cual de los patrones registrados se le parece más. Una vez ubicado el "patrón más parecido", ese resultado será comparado con el "índice de similitud" previamente definido y si es mayor que el mínimo aceptable, se dará por válida la identificación.

De esta explicación se desprende que los equipos biométricos poseen un parámetro de configuración, que fija ese "límite mínimo de similitud", generalmente denominado *likelihood*. Cuanto más alto sea el *likelihood*, más deberá parecerse la muestra tomada de la persona a la almacenada en el proceso enrolamiento.

En el caso de huella digital, por ejemplo, colocar un *likelihood* alto obliga a que la persona coloque el dedo en la misma posición que lo colocó al enrolar. Por el contrario, bajar demasiado el *likelihood* pone en riesgo la credibilidad del sistema, ya que aumenta la probabilidad de una falta aceptación.

5.3.2.2. Verificación

Se entiende por verificación al hecho de indicarle al equipo la persona se desea identificar y que el sistema compare solamente los parámetros leídos en vivo contra los enrolados para esa persona. De esta forma es posible colocar un *likelihood* mayor que en el caso de identificación, porque sólo se realiza una verificación contra los parámetros indicados.

La verificación es siempre más rápida que la identificación, ya que se efectúa una única comparación. El inconveniente es que siempre necesita de un dispositivo adicional para indicarle cual es la persona que debe usarse como referencia. Para esto se utilizan generalmente 3 métodos:

a- Un teclado para indicarle el número identificatorio de la persona, por ejemplo su número de legajo o documento de identidad

b- Su tarjeta utilizada en control de acceso

c- Una *Smartcard* conteniendo directamente el patrón biométrico deseado y que es leído por el lector previo a la verificación.

5.3.3. Tecnologías de Biometría

Existen varias tecnologías de biometrías con diferentes grados de investigación y/o popularidad. Entre ellas:

• **Geometría de mano:** Es una tecnología bastante antigua, creada y patentada por Recognition Systems, que tuvo un cierto éxito en el mercado e identifica parámetros dimensionales de la mano, que son únicos. Funciona muy bien, sobre todo en lugares donde no se utilizan guantes y es bastante robusta frente al vandalismo. Los motivos por el cual esta tecnología no se popularizó masivamente son estrictamente comerciales: sólo hay un fabricante en el mercado, que además vende sistemas de presentismo y/o control de acceso, lo que hizo que los fabricantes de sistemas de control de acceso no ayudaran a difundirla.

• **Huella digital:** Sin dudas la más popular de todas las biometrías. Existen dos métodos básicos de identificación:

- El utilizado por los organismos de seguridad y gobiernos para la identificación de personas y/o sospechosos de delitos -en términos generales se los denomina AFIS- y parten de la base de tomar una foto de la huella digital para su posterior procesamiento
- Los métodos utilizados en control de acceso, donde la lectora no almacena una foto sino que identifica las denominadas "minucias", que son las bifurcaciones de las nervaduras que tiene la huella digital y con eso hace un mapa de ubicación de las mismas. Este método almacena mucha menor cantidad de información para identificar las diferentes huellas y también utiliza menos capacidad de cálculo en el proceso de comparación para conseguir un resultado.

Viene de página 176

Actualmente no existen normas que regulen estos algoritmos de reconocimiento, por lo que cada fabricante guarda diferente información sobre cada huella y esto hace que sean incompatibles entre sí.

En cuanto a los sensores utilizados para reconocer a la huella digital, existen de diversas tecnologías, siendo los más populares los ópticos, capacitivos y ecográficos. Cada una presenta ventajas y desventajas frente a las demás sobre todo en la relación exactitud/precio/robustez.

Ninguno de los métodos de identificación de huella digital es altamente resistentes al vandalismo y uno de los grandes inconvenientes es que la reparación del daño en el elemento sensor es bastante costoso, por lo que se recomienda utilizarlos en lugares no expuestos a estos inconvenientes. Algo similar ocurre con las inclemencias del tiempo, por lo que se deberán extremar los cuidados si es necesario colocarlos en el exterior y sobre todo expuestos a la intemperie.

• **Reconocimiento facial:** Es una tecnología que año a año mejora en sus resultados y si bien actualmente existen fabricantes que ofrecen soluciones de este tipo, todavía no se consiguen equipos comerciales de bajo costo con prestaciones aceptables de identificación y velocidad. Básicamente identifica y calcula las distancias entre los diferentes «accidentes faciales», de manera de reducir la imagen a un conjunto de coordenadas de puntos significativos.

En cuanto a la compatibilidad de los diferentes fabricantes, la situación es similar a la de las huellas digitales. Se está investigando mucho en el reconocimiento facial de imágenes en vivo, con fines investigación fundamentalmente antiterrorista y aunque se cree que los resultados de estas investigaciones llegarán al campo del control de accesos, hoy los equipos son muy sofisticados y con una gran capacidad de cálculo, cuyos costos todavía son altos para la industria.

• **Reconocimiento de Iris y Retina:** Los equipos de reconocimiento de iris y retina funcionan muy bien, tienen un costo relativamente accesible y no tienen contacto físico con el usuario, por lo que pueden ser ubicados detrás de un vidrio de manera de hacerlos resientes al vandalismo. El inconveniente radica en que no son muy populares, por tratarse de equipos en los que la persona debe «mirar» adentro y si bien su ojo no tiene contacto con ningún elemento, de todas formas suelen generar el rechazo de los usuarios.

• **Reconocimiento de voz:** Esta tecnología se encuentra en una etapa similar al reconocimiento facial y probablemente algún día sean una alternativa válida.

5.3.4. Equipos biométricos como dispositivos periféricos. Integración con sistemas existentes.

Las placas de los controles de accesos tradicionales poseen interfases unidireccionales para la conexión de dispositivos de identificación, dado que históricamente sólo permitían la conexión de lectores de tarjetas o teclados PIN. Cuando un sistema posee varias lectoras biométricas, es esperable que el usuario sólo se enrole una vez y que esta información esté disponible para todas las lectoras que la necesiten. Para eso debe existir una comunicación bidireccional entre las controladoras y los lectores biométricos o al menos entre la base de datos centralizada y dichos lectores.

Al intentar integrar los dispositivos biométricos, deben resolverse dos problemas:

- Como transmitirle al lector biométrico el parámetro almacenado deseado, que se encuentra en una base de datos central.
- Como unificar la información del usuario, asumiendo que todas los accesos no necesariamente tendrán lectores biométricos.

Para contestar adecuadamente estas preguntas debe considerarse también que los fabricantes de equipos control de accesos no son quienes fabrican los lectores de biometrías, por lo que no siempre están totalmente integrados, fundamentalmente en lo relacionado con el mantenimiento de la base de datos. En la práctica, se observan cuatro diferentes situaciones:

1- Los sistemas de control de acceso de gran porte integran las biometrías de terceros fabricantes mediante placas y drivers específicos para ofrecer a sus usuarios una solución integrada única. Sin dudas es la mejor solución pero no siempre está accesible en sistemas medios y pequeños.

2- La mayoría de los equipos biométricos que funcionan como periféricos de los sistemas de control de accesos poseen una salida *Wiegand*. De esta forma, cuando se enrola a un usuario se vincula su parámetro biométrico a un número de forma tal que cuando la terminal biométrica identifica fehacientemente a esa persona, emite por su salida *Wiegand* este código previamente asignado. De esta forma, la placa del control de acceso recibe la información de manera similar a si se hubiera pasado una tarjeta, por lo que no es necesaria una integración. Pero integrar la biometría de esta forma hace que se deban tender dos redes: una para el control de acceso y otra para mantener actualizadas las bases de datos de los parámetros biométricos a los lectores. La ventaja es que desde el punto de vista de integración es posible tener reportes consolidados e integrados. Esta solución no es tan buena como la anterior, pero puede utilizarse cualquier equipo biométrico, independientemente de los que son soportados por el fabricante del sistema de control de accesos.

3- No es infrecuente encontrar instalaciones donde el control de acceso funciona de manera independiente en aquellos lugares de alta seguridad o presentismo donde se utilizan biometrías. En este caso existen dos sistemas aislados, cada uno montado en una red propia y que de manera más o menos eficiente se consolidan tanto las bases de datos de usuarios como los reportes. Sin dudas esta es no es la mejor solución desde el punto de vista de integración, aunque a veces ésta no es necesaria. Tal es el caso cuando los lectores biométricos se utilizan solo para el sistema de presentismo y el control de acceso funciona independientemente con tarjetas, los reportes de presentismo no necesitan estar integrados con los de seguridad.

4- La última forma es una variante de la segunda mencionada, pero almacenando el parámetro biométrico en una *Smartcard*. El sistema se basa en almacenar el resultado del enrolamiento en la tarjeta de forma que cuando el usuario se presente frente a un acceso con lector biométrico, primero deberá acercar su tarjeta al lector para que éste extraiga el parámetro biométrico patrón y luego procederá a hacer la comparación 1:1 (verificación) con el parámetro en vivo. Esta solución posee varias ventajas:

- El sistema biométrico funciona siempre en la modalidad de verificación, minimizando el error de falsa aceptación.
- El lector biométrico no necesita de una base de datos propia porque ésta reside en las tarjetas. Es decir, no posee memoria y puede manejar infinitas huellas u otras biometrías.
- La *Smartcard* se puede tener otros usos, por ejemplo como

Continúa en página 184

Viene de página 180

tarjeta de acceso para aquellas puertas donde se coloque una lectora común en lugar de una con lector biométrico

- No existen potenciales conflictos de confidencialidad porque no existe una base de datos centralizada con parámetros biométricos y es cada usuario quien porta la única copia de sus propios parámetros biométricos.

5.3.5. Equipos biométricos como dispositivos autónomos

Casi todos los fabricantes de biometrías incursionaron en el mercado de control de accesos y, fundamentalmente, en el de control de asistencia con equipos propios.

Los equipos ofrecidos por estos nuevos jugadores del mercado generalmente tienen solo identificación biométrica, por lo que se enfocan en soluciones bien específicas. En la gran mayoría de los casos utilizan terminales que se comunican por protocolo TCP/IP para aprovechar las estructuras de redes existentes, simplificando las instalaciones. Por otro lado, ofrecen herramientas para que sus sistemas puedan ser integrados como si fueran un subsistema a una solución mayor que utiliza equipos adicionales.

5.3.6. El futuro de las biometrías

Indudablemente el uso de biometrías permite la identificación robusta de las personas y por tal, los sitios que requieren de mucha seguridad ya los adoptaron definitivamente como la tecnología de acceso. Con las prestaciones actuales de las biometrías se hace difícil vislumbrar el fin de la era de las tarjetas para control de acceso, ya que en toda instalación existen puertas que no necesitan de tanta seguridad y el acceso por biometría es siempre más lento y engorroso.

Dentro de las diferentes tecnologías de biometrías la huella tiene un lugar de privilegio, aunque en el futuro podría ser desplazada por el reconocimiento facial, dada la mayor cantidad de información que una foto entrega respecto de la huella.

Para aplicaciones como el control de presentismo, la huella digital va ganando terreno rápidamente no solo por evitar el inconveniente de "pasarse la tarjeta" sino que en esos lugares el vandalismo no suele ser importante. El dilema continúa en aquellos lugares donde el presentismo está integrado a un control de accesos y los empleados deberán, igualmente, portar una tarjeta. Últimamente han aparecido en el mercado aplicaciones que integran CCTV con el control de acceso por tarjetas, permitiendo almacenar una imagen en vivo de la persona al instante de fichar, de manera de dejar un registro «biométrico» para evitar el préstamo de tarjeta.

5.3.7. Ejemplos de aplicación

5.3.7.1. Control de asistencia

Si bien este artículo está orientado a control de accesos, el que generalmente depende del departamento de seguridad de las empresas, es indudable que los departamentos de relaciones humanas utilizan tecnologías de identificación para registrar las fichadas del personal y proceder al pago de salarios. Dado que están involucrados dos departamentos, es frecuente encontrar diferentes puntos de vista, lo que algunas veces dificulta la solución.

En términos generales los departamentos de recursos humanos prefieren el uso de biometrías de huella para el registro de ingreso y egreso del personal. Esta preferencia se basa en que:

- Nadie se olvida la huella y por lo tanto no hay problemas relacionados con la logística (reponer tarjetas, sacar fotos, etc.). Eventualmente será necesario repetir el proceso de enrolamiento de algún empleado que presente inconvenientes al momento de realizar sus fichadas.
- El fraude es prácticamente nulo dado que no es posible prestar un parámetro biométrico.

Para el departamento de seguridad, los ingresos basados en biometrías presentan algunos inconvenientes adicionales debido a que:

- Dada la baja velocidad de lectura siempre existirá una concentración de personas en los horarios de entrada y salida, que son justamente aquellos donde se requiere la mayor agilidad porque coinciden con los horarios en los cuales se producen la mayor cantidad de incidentes.
- En empresas de mucho personal es muy difícil recordar a cada uno. Por lo tanto el portar una tarjeta con foto simplifica la identificación.
- El estado de ánimo de un empleado, al que por algún motivo el lector biométrico le rechaza la fichada, suele no ser el más positivo.
- Dada su baja resistencia al vandalismo, los lectores biométricos siempre deben ser objeto vigilancia especial y permanente.

En general, dado que el sistema de asistencia no se utiliza para abrir las puertas sino que solamente registra los ingresos y egresos del personal, es que para este caso se suele instalar sistemas biométricos independientes del sistema de seguridad utilizado, totalmente administrado por el departamento de recursos humanos.

Debe tenerse en cuenta el enrolamiento: si se desea enrolar a las personas en las oficinas del departamento de recursos humanos deberá adquirirse un equipo más para enrolar, o si se utilizará algún equipo para la doble función de enrolamiento y verificación.

5.3.7.2. Ingreso a la sala de servidores

Este es un caso diferente porque se trata de un sistema de control de accesos de una empresa donde se desea colocar accesos por tarjetas para todos los accesos excepto para la sala de servidores, donde se requiere el acceso mediante algún parámetro biométrico para aumentar la seguridad.

En general, las salas de servidores son internas (no tienen problemas de intemperie), está en un lugar controlado (no presentan inconvenientes de vandalismo) por lo que la huella digital suele ser la tecnología adecuada. Como este ingreso será el único de este tipo en toda la instalación, no existe la necesidad de armar una red que permita almacenar la base de datos centralizada. De hecho deberá elegirse un equipo que permita ser utilizado tanto para enrolarse como para su verificación posterior.

Por otro lado, en estos casos solo muy pocas personas tendrán acceso a esta sala, (asumamos que no serán más de 10), por lo que hacer identificación o verificación es prácticamente lo mismo.

La selección debe recaer en un equipo de huella digital que pueda ser utilizado tanto para enrolar como para verificar, con capacidad para al menos 30 huellas (10 personas con 2 dedos por persona y un 50% de reserva) y salida *Wiegand* para ser conectada al control de accesos general y de esta forma unificar tanto el control de la sala de servidores como los reportes que se generen. ■