Identificación biométrica

Desde que el hombre comenzó a diferenciarse en sus costumbres y a establecerse como pueblos, nació la necesidad de la identificación de cada uno de sus individuos. Las técnicas fueron cambiando y la tecnología avanzó a pasos agigantados. Hoy, los rasgos y características físicas de una persona pueden ser su "documento de identidad natural". Historia, posibilidades y aplicaciones de la biometría, una ciencia que se perfila como "casi exacta"

En conjunto, la biometría es una serie de métodos de identificación y autenticación de las personas, por medio de alguna de sus características, ya sean fisiológicas o de comportamiento. Ahora bien, ¿qué utilidad puede darse a esa información? ¿Es posible utilizar la tecnología disponible para identificar sin margen de error a un determinado individuo? ¿Cuáles son los diferentes rasgos en los que la biometría puede implementarse para la identificación de una persona? ¿Son todos igual de confiables?

Si desde siempre a una persona se la identificó de alguna manera sin ayuda de la tecnología y nunca se dudó que fuera ella misma, ¿por qué emplear hoy biometría?

Para responder a todos estos interrogantes y ampliar la información sobre esta disciplina, comenzamos por el origen: desde que el hombre se diferenció de los animales por las pisadas.

Quien es quien

Desde el momento en que el hombre comenzó a utilizar su cerebro como fuente de raciocinio e inició su diferenciación, en usos y costumbres, de los animales, necesitó de determinadas herramientas para su identificación. Así, en las primeras civilizaciones el nombre de una persona se asoció a su actividad (José el Carpintero) mientras que su esposa e hijos eran asociados como familia también a través de la actividad del hombre.

Cuando la población comenzó a crecer y diversificarse nombres y actividades comenzaron a ser insuficientes y los países fueron un buen "apellido" hasta que éstos nacieron formalmente.

Un poco más adelante en el tiempo y ya en épocas de la modernidad, al nombre y apellido de cada persona se le adicionó un número, cifra que lo acompañará de por vida en un documento identificatorio.

Más cerca de nuestros días los métodos de identificación fueron evolucionando a tal punto que al documento de identidad se le agregó la fotografía, como complemento visual para una identificación más eficaz de cada persona. Poco antes, en el campo de la autenticación de individuos, comenzaba a ser utilizada la huella digital, una característica personal única para cada ser humano y que se mantiene inalterable a lo largo de toda su vida.

Justamente, de caracteres inalterables, principalmente, es que se nutre la biometría como ciencia para la identificación de las personas.

De la tarjeta al rasgo físico

Hace unos 25 años, a principios de los '80, la tecnología permitió crear dispositivos adicionales de identificación como las tarjetas magnéticas y de proximidad, permitiendo la validación y el

Continúa en página 52

Viene de página 48

acceso "de las tarjetas" pero no de las personas.

Con los años la tecnología fue mejorando y en 1991 la biometría se incorporó al mercado comercial, dejando de ser un producto exclusivo para el uso criminal o proteger información y secretos de Estado.

Como es sabido, cada vez es necesario identificar a las personas con más exactitud y a mayor velocidad. Esto puede lograrse gracias a los avances tecnológicos, que permitió la mejora de los equipos y la baja en los precios.

Los primeros equipos con tecnología biométrica datan de 1992 y fueron los de verificación (1:1), equipos muy costosos (más de cinco mil dólares) en los que el reconocimiento biométrico se realizaba ingresando un PIN y comparando el rasgo biométrico de la persona con el rasgo almacenado en la base de datos.

En los últimos años, los algoritmos biométricos y los procesadores mejoraron y bajaron sus costos, ofreciendo la identificación (1:N) biométrica de las personas, que se realiza utilizando el rasgo biométrico del individuo comparado con toda la base de datos. La gran ventaja de esta variante de la biometría, es que la Persona no necesita ingresar un PIN, no hay errores en el ingreso de los datos, no puede existir un registro duplicado en la base de datos y es más rápida la autenticación.

¿Qué es la biometría?

El concepto estricto de biometría proviene de las palabras bio (vida) y metría (medida), lo cual permite inferir que todo equipo biométrico mide e identifica alguna característica propia, tanto física como de comportamiento, de una persona.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como las huellas digitales.

En resumen, los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso del reconocimiento de la huella digital, uno de los más extendidos en todo el mundo y el de mayor crecimiento en el mercado desde hace unos años, 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 (template). Pero esto se verá explicado más adelante.

Las aplicaciones de la biometría abarcan un gran número de sectores: desde el acceso seguro a computadores, redes y protección de ficheros electrónicos hasta el control horario y control de acceso físico a una sala de acceso restringido.

Por esta razón, algunos definen a la biometría como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamientos de enfermedades y otros por el estilo.

El cuerpo, tarjeta única

Todos los seres humanos tienen características morfológicas únicas que los diferencian. La forma de la cara, la geometría de ciertas partes del cuerpo como las manos, los ojos y -tal vez la más conocida- la huella digital, son algunos de esos rasgos distintivos que permiten identificar a un individuo a través de una medición biométrica, técnica que se estudia desde hace mucho y es considerada en la actualidad como el método ideal para la identificación de las personas.

Y de entre todas las posibilidades de diferenciación por rasgos, la identificación por medio de huellas digitales constituye una de las formas más representativas de la utilización de la biometría.

¿Cómo se identifica a una persona por medio de sus huellas? Una buena síntesis sería la siguiente: la huella digital está formada por una serie de surcos (montañas y valles) cuyas terminaciones o bifurcaciones son llamados puntos de minucia. A su vez, cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad, previamente asentada en una base de datos de cualquier tipo, de una persona que intenta acceder a un sistema en general.

Origen de la biometría

De ninguna manera la biometría es una técnica futurista, ya que desde hace varios siglos los hombres se han identificado por medio de este sistema. Lo que en realidad está en constante evolución es la tecnología y los sistemas que basan en datos biométricos la identificación de personas.

Está comprobado que en la época de los faraones, en el Valle del Nilo (Egipto), se utilizaban los principios básicos de la biometría para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

Asimismo, abundan las referencias de personas que en la antigüedad han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos y tamaño y composición de la dentadura, entre otros rasgos. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como lo eran sus rasgos físicos.

Una huella está formada por una serie de surcos, Las terminaciones o bifurcaciones de los mismos son llamados puntos de minucia. Midiendo y comparando estos puntos es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

En el siglo XIX, en tanto, comenzaron las investigaciones científicas para poder aplicar la biometría en un sistema de identificación de personas con fines judiciales, investigaciones que produjeron importantes avances y originaron la utilización de los rasgos morfológicos únicos en cada persona para su identificación.

Ya en el siglo XX, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico, nuevos instrumentos aparecen para la obtención y verificación de huellas digitales, a la par que comienzan a utilizarse otros rasgos morfológicos como variantes de identificación. Entre ellos el iris del ojo, el calor facial o la voz.

Continúa en página 56

Viene de página 52

Actualmente la biometría se presenta en un sinnúmero de aplicaciones, demostrando ser el mejor método de identificación humana. Y aunque sus posibilidades de aplicación son diversas, la más extendida hoy, es el control de acceso.

El sistema biométrico

Explicados los orígenes y fundamentos esenciales de la biometría, comenzamos a desarrollar sus alcances, tecnologías y aplicaciones en la identificación de personas destinada al control de accesos y a la seguridad electrónica en general.

La primera pregunta que surge, entonces, es ¿cuál sería la definición de un sistema biométrico?, interrogante que responde **Marcelo Pugliese, de la empresa Biocard**: "*Un sistema biométrico es un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. Para ello utiliza métodos automatizados de identificación y verificación de la identidad de un ser humano viviente basados en sus características fisiológicas y de comportamiento únicas. Los rasgos fisiológicos, estables por naturaleza, incluyen huellas dactilares, silueta de la mano y patrón del iris, mientras que algunos ejemplos de características de comportamiento son la voz y la manera de firmar. Un sistema biométrico es aquel de reconocimiento de patrones que lleva a cabo comparaciones de identidad a la vez que valida las características almacenadas de un individuo contra las que presenta en un ambiente en vivo*".

En general, todos los sistemas de control de acceso, utilicen tecnología biométrica, lectura de tarjetas o cualquier otra técnica se compone, básicamente, de elementos periféricos, centrales de control inteligentes y software de control mientras que cada sistema, a su vez, pueden ser clasificados según su nivel de "inteligencia" en centralizados y distribuidos.

Respecto a esta clasificación, **Roberto Ingham, de Cronos**, explica que en los sistemas de control de accesos biométrico distribuidos, "*la ventaja que ofrecen es que al distribuir la inteligencia, cada acceso tiene todos los permisos de acceso y horario en su propio controlador. Es decir que al momento que el lector biométrico hace su reconocimiento, el resultado es inmediatamente analizado y procesado en tiempo real sin tener que consultar pesadas bases de datos de un servidor*".

Por otra parte, los periféricos asociados a la central de control son precisamente los que interactúan con el usuario. Por ejemplo el molinete, la barrera -en el caso de un control de accesos vehicular-, el lector biométrico y los sensores de apertura o de cierre, entre otros.

Finalmente, el software es el que actualiza a los controladores dando alta, baja y modificaciones de los permisos de acceso y horarios. Desde el soft, que posee las herramientas adecuadas, se generan reportes de eventos y hasta de las personas presentes en el establecimiento en un determinado momento.

Los rasgos distintivos

Como se dijera anteriormente, hay una serie de rasgos físicos y características de la conducta de una persona que pueden ser "medidos" o clasificados a través de un sistema biométrico.

Cada uno de esos rasgos tiene las siguientes particularidades:

De características físicas:

• **Huella digital:** Una huella está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados puntos de minucia y cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

• **Lectura del iris:** El iris tiene cerca de 260 características únicas e irrepetibles en otra persona. Para la digitalización del iris, se utiliza un CCD que capta una foto infrarroja del ojo y para su identificación se expone el ojo a un escaneo con láser.

• **Reconocimiento facial:** Busca obtener la capacidad de identificar y memorizar características genéricas del rostro de las personas por sobre la cuantificación de los rasgos. Permite determinar la identidad de una persona, al comparar una imagen de su cara con imágenes de referencia almacenadas en una base de datos. Esta se realiza analizando elementos estructurales presentes en las caras. Una vez obtenidos los rasgos característicos, se comparan con los previamente almacenados y el resultado de la comparación verifica o descarta la identidad de la persona.

• **Geometría de la mano** y de la estructura venosa: Se sustenta en el perfilado de la imagen de la mano sobre un escáner óptico. Sobre este perfil se determina un conjunto de parámetros que resultan temporalmente estables en cada mano.

De características de la conducta

• **Reconocimiento de firma:** Se realiza un modelado estadístico de las trayectorias de la firma. Hay dos opciones: On-line, que se obtiene en el momento de la realización u Off-line, en la que se analiza la imagen producida. En ambos casos se debe contar con DB con varias muestras de cada individuo.

• **Reconocimiento de la voz:** La voz se produce cuando pasa aire a través de las cuerdas vocales, ocasionando su vibración. La tensión de las cuerdas determinan los tonos (frecuencia). La configuración de las cavidades acústicas (tracto vocal) determinan el timbre (formantes), permitiendo diferenciar los sonidos mediante analizadores especiales de sonidos.

• **Dinámica del teclado:** Los movimientos de tecleado tienen diferentes frecuencias en tiempos y presión. Esto permite formar patrones para usarlos como elementos de identificación.

El iris tiene cerca de 260 características únicas e irrepetibles en otra persona. Para la digitalización del iris, se utiliza un CCD que capta una foto infrarroja del ojo y para su identificación se expone el ojo a un escaneo con láser.

En la implementación de un sistema de identificación biométrico, además, hay que tener en cuenta el nivel de intrusión o invasión que produce en los individuos, que puede convertirlos en reacios a su identificación

Acerca del nivel de invasión y aceptación por parte de las personas en someterse a un control biométrico de identificación, el ingeniero **Eduardo Santarcieri, IT Manager de Miatech** explica que "*cuando contamos con el*

Continúa en página 60

Viene de página 56

individuo en forma presencial, la huella dactilar e iris aportan gran fiabilidad, pero exigen alta cooperatividad, mucho más cuando se trata de lectura del iris. Exponer algo tan sensible y vital como el iris al escaneo de un láser para ser leído y analizado, da miedo. Puede que virtualmente sea improbable, pero esta sensación de inseguridad que nace de una improbable pero no imposible falla que pueda dañarnos algo tan importante como la vista solo para una función de identificación, es real".

Este aspecto lo amplía **Daniel Arcondo, de Larcon SIA**: "*Cada alternativa tiene diferencias propias de la tecnología asociada pero hay que tener especial cuidado en elegir el método menos invasivo para el usuario. Es más fácil convencer a un usuario para que coloque el dedo o la mano sobre el equipo a que coloque su ojo frente a una luz desconocida, que no sabe si puede ocasionarle daño o no*".

¿Qué son los lectores biométricos?

Los lectores biométricos son sistemas de identificación basados en características biológicas únicas del ser humano, son sistemas que "identifican" una parte del cuerpo humano para posteriormente generar un código único que reconozca las características individuales de la persona. A este tipo de código, que está formado por patrones biológicos, se lo denomina "template".

Al respecto, desde el departamento técnico de **la empresa AdBioTek** explican, que "*la eficacia del sistema biométrico, se basa en el algoritmo utilizado para generar un "template", el cual deberá tener la suficiente complejidad como para que su generación y resguardo consuman pocos recursos del sistema, así como tiempo y espacio en memoria. De la misma manera, debe de ser eficiente a tal grado que, al querer identificar a un individuo, éste sea capaz de reconocerlo sin importar la posición del cuerpo en cada registro, ya que de lo contrario la razón de rechazo falso sería muy alta. Es decir, que un individuo que efectivamente es quien dice ser, tenga que hacer dos o más intentos para que el lector lo reconozca y acepte su entrada*".

Si bien las diferencias quedaron bien establecidas, es importante resaltar que los sistemas biométricos identifican personas y no tarjetas. Al utilizar los lectores de huella digital, por ejemplo, la seguridad de que los datos que se procesan para el control de asistencia son verídicos es absoluta.

Otro aspecto importante, a tener en cuenta en un sistema de identificación de personas basado en la biometría, es que los lectores y software de uso comercial no almacenan "las imágenes de las huellas digitales". Desde el momento del enrolamiento o identificación de la huella digital, se genera un "*template*" -algoritmo codificado- que es almacenado en las bases de datos, siendo imposible generar, desde el algoritmo, la imagen o impresión de la huella digital. Finalmente, es válido aclarar que el éxito de un buen sistema biométrico es el "*enrolamiento*" de datos o alta de la persona al sistema y la identificación posterior, sin la utilización de un pin, como complemento.

La más difundida

De entre todas las tecnologías, la más difundida es sin dudas, es la lectura de la "huella digital", elemento que comenzó a utilizarse en la identificación de personas con fines policiales y luego comenzó a extenderse al ámbito civil.

Luego de un amplio análisis en la identificación de personas, por parte de las empresas dedicadas al rubro, pudo establecerse que la rama de "*huellas digitales*" permite efectuar la identificación de las personas con una relación costo/prestación muy ventajosa, con un nivel de seguridad muy alto, basado en la prevención de fraudes en operaciones que necesitan una identificación positiva de la persona, muy fácil de efectuar cuando se utiliza un password o una tarjeta. Entre las aplicaciones más extendidas se encuentran:

• Protección de información sensible como listados de sueldos o contratos.

• Protección de información estratégica como planes de marketing y operaciones financieras.

• Protección de áreas con elementos fundamentales para el funcionamiento de la empresa, tales como centros de cómputos, cajas de valores o depósito de repuestos.

• Protección de movimiento de materiales de alto valor, entre los que se encuentran los elementos de stock y herramientas con alto valor.

• Control efectivo del personal para evitar pagar erróneamente premios por presentismo y horas extras no trabajadas.

A estos usos se le agregan otras prestaciones. "*La aplicación fundamental es la identificación con total certidumbre, es por ello que estos sistemas son utilizados en lugares donde la seguridad que se requiere es muy alta, como laboratorios, instalaciones militares, bancos o reparticiones gubernamentales*", describe **Adrián Iervasi de Draft.**

La identificación por huella, asimismo, posee notables diferencias respecto de los otros sistemas utilizados.

La principal diferencia entre los sistemas es el tiempo de respuesta. El sistema de reconocimiento de huella digital, por lo general, tiene la modalidad de uso de 1 a N, lo cual significa que compara la huella contra toda la base de huellas previamente cargadas en el lector, arrojando un resultado de aceptación o rechazo prácticamente al instante *(tiempo menor a 2 segundos)*.

La Geometría de la mano y de la estructura venosa se sustenta en el perfilado de la imagen de la mano sobre un escáner óptico. Sobre este perfil se determina un conjunto de parámetros que resultan temporalmente estables en cada mano.

Otros sistemas, como por ejemplo el de geometría de la mano, requiere de un pin o número de acceso consistente en cinco dígitos que hay que marcar en un teclado previamente y luego el reconocimiento de la imagen de la mano, lo que los hace más lentos (tiempo promedio 5 segundos).

Respecto al reconocimiento del iris, es una tecnología en desarrollo y actualmente muy cara para ser utilizada en sistemas de control horario y de accesos.

Algunas variantes

Como quedó establecido, la identificación de personas, a través de la biometría, por sus huellas digitales es la más utilizada. Pero dentro de esta variante existen diferentes tecnologías.

"*Existen básicamente cuatro tipos de tecnologías para la lectura de huellas dactilares: lectura óptica, por resonancia ultrasónica, lector diferen-*

Continúa en página 64

Viene de página 60

cial capacitivo y por campo eléctrico (RF)", detalla **Carlos Vázquez, Presidente Ejecutivo de Biometrix.**

Dadas las limitaciones de los lectores ópticos para adaptarse a condiciones de trabajo no controladas como la suciedad del área de apoyo o las condiciones de la superficie del dedo, al salir al mercado los lectores capacitivos, fueron rápidamente adoptados para comenzar a migrar los proyectos que ya utilizaban lectores ópticos.

"*Al poco tiempo -continúa Vázquez- se introdujo en el mercado una tecnología que sorprendió por su eficacia y confiabilidad: la tecnología de campo eléctrico, también denominada como de radiofrecuencia (RF)*".

Esta tecnología actúa mediante la aplicación de una pequeñísima señal de radiofrecuencia sobre la superficie de la piel al hacer contacto con el lector, lo que produce un mínimo campo eléctrico que copia la forma de las huellas digitales desde su nacimiento más allá de la piel de la superficie. Las ondas de ese campo eléctrico son "leídas" por 16.000 diminutos sensores integrados al área de apoyo del dedo. Esta tecnología genera de una imagen de alta precisión de la huella digital que prescinde del estado de la capa exterior de la piel (suciedad, transpiración, callos o lastimadura).

El reconocimiento facial se realiza analizando elementos estructurales presentes en las caras. Una vez obtenidos los rasgos característicos, se comparan con los previamente almacenados y el resultado de la comparación verifica o descarta la identidad.

Diferencias

¿Por qué la identificación por huellas digitales está más difundida? Además de los motivos expuestos anteriormente, hay una serie de características, que hacen de los sistemas biométricos de lectura de huellas digitales, los más prácticos y difundidos. Entre ellas:

- *Universalidad:* cualquier persona posee esa característica
- *Unicidad:* la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
- *Permanencia:* la característica no cambia en el tiempo;
- *Cuantificación:* la característica puede ser medida en forma cuantitativa.
- *Backup:* se pueden "enrolar" (dar de alta la huella digital) hasta los 10 dedos, recomendado los "índices o mayores", uno de cada mano.

La identificación de personas mediante sus huellas digitales, además, es quizás la primera técnica que viene a la mente cuando se habla de biometría, ya que es uno de los métodos más utilizados por la ley. Está comprobado que los patrones de las huellas digitales son únicos y se mantienen durante la vida de la persona y en caso de "corte" se vuelven a regenerar. De hecho, son diferentes en cada dedo en ambas manos e incluso entre gemelos idénticos.

También deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella digital, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales.

En la geometría de la mano generalmente están definidos para la mano derecha del individuo, y para realizar su identificación es necesario incorporar un PIN y luego la mano, agregándole de esta manera más tiempo a la hora de efectuar un registro.

Finalmente, en relación con productos de geometría de la mano, lectura del iris o reconocimiento facial las soluciones actuales, son más lentos y tienen un alto costo, tanto en lo referente al equipamiento como en lo que respecta a su implementación.

"*El de huellas digitales, es el sistema más difundido, si bien a veces se dificulta la identificación, según el estado de las huellas dañadas por manejo de materiales abrasivos (construcción), teniendo en estos casos, un porcentaje mayor de rechazo para el enrolado de la huellas digitales. Sin embargo, una de sus principales ventajas es la utilización en lugares de máxima seguridad como control de acceso, ya que todos los sistemas poseen un extremadamente bajo porcentaje de falsa aceptación*", asegura **Gerardo Saavedra, Director de Diastec.**

Control de accesos

El control de accesos, como la aplicación más difundida de la identificación de personas por sus huellas digitales, tiene sus justificativos en las diferencias con las tecnologías tradicionales, como las basadas en la tarjeta. Entre las más expuestas se encuentra, fundamentalmente, el intercambio que existe entre los poseedores de las credenciales, es decir pasarse la tarjeta unos a otros, por lo cual la seguridad se ve ampliamente vulnerada. Si se utiliza la huella digital como medio para registración, ese rasgo es característico y único de esa persona, y no hay forma de que otra pueda registrar en su lugar.

"*La falsa aceptación (confirmar la identidad erróneamente) y el falso rechazo (negar la identidad cuando en realidad debería confirmarla) son variables que presentan resultados distintos según la tecnología y el fabricante, aunque se pueden encontrar habitualmente excelentes índices para la mayoría de las aplicaciones*", asegura **David Walfisch, de Intelektron.**

También, entre las principales diferencias, se encuentran los costos, que no dejan de ser un factor importante. En un sistema con tarjetas, por ejemplo, existe un costo de mantenimiento anual de ese insumo que oscila entre el 10 y el 20% en algunos casos, para la reposición de las mismas, entre pérdidas, "olvidos", roturas y nuevos ingresos. Asimismo, el costo, por ejemplo, de una tarjeta de proximidad todavía está en valores muy altos, y que a la hora del presupuesto total tienen un gran peso sobre éste.

Lo más significativo y diferencial entre una tecnología de huellas digitales y otra de proximidad, entonces, es la seguridad y los bajos costos.

Relación costo/beneficio

A diferencia de otros sistemas de identificación de personas, los sistemas biométricos requieren de una inversión muy pequeña, (no es un gasto) única al adquirir el sistema y adicionan la gran ventaja del mantenimiento cero: no hay que comprar tarjetas, reimprimirlas, vincularlas con las personas, reponer las robadas o extraviadas.

La masificación que están adquirien-

Continúa en página 68

Viene de página 64

do actualmente algunas de las tecnologías de control biométrico, se debe no solamente a sus ventajas operativas, sino también a la drástica disminución de los precios de estos sistemas y por ende, a la posibilidad de acceder a su utilización por un segmento mucho más amplio del mercado.

Desde los fraudes de empleados que "marcan" su asistencia por otros -ya sea para acortar horarios de trabajo o tratarse de los tristemente conocidos "ñoquis"- hasta la sustitución de la identidad de una persona por otra para efectuar transacciones financieras -con las consiguientes consecuencias económicas y crediticias-, los sistemas biométricos reportan beneficios que pagan con creces la inversión efectuada al corto o mediano plazo, hay sistemas biométricos que se "amortizan en el primer mes".

Existen otros puntos, que deben ser tomados en cuenta a la hora de evaluar la instalación de un equipo de identificación basado en rasgos de las personas. Entre ellos la seguridad interna que se adquiere con el sistema, el nivel de satisfacción en relación a lo esperado, el sentirse respaldado desde ámbitos legales y de manejo interno, y por qué no, un mejor aprovechamiento de la fuerza de trabajo con que el cliente cuenta.

Estrategias

Muchas empresas argentinas, están adoptando los sistemas biométricos como una buena opción, para expandir sus negocios y ofrecer a sus clientes un abanico más amplio de soluciones. Cada una de ellas, basadas en distintas estrategias comerciales.

Sin embargo, todos los consultados coinciden en que, el primer paso para la captación de clientes, es escuchar atentamente sus requerimientos para poder asesorarlo objetivamente sobre la solución que está buscando y luego determinar si se requiere de un control biométrico y de qué clase.

Asimismo, otro aspecto fundamental, es el servicio de post venta, a través del cual se le brinda al usuario asesoramiento permanente acerca de las posibilidades y ventajas que ofrecen las diferentes tecnologías y sus aplicaciones.

Lo que viene

A la cantidad de posibilidades de identificación de una persona, a través de sus rasgos ya sean físicos o conductuales, hay que agregar nuevas tecnologías que aún están en fase de investigación y desarrollo. Entre ellas, el reconocimiento de acuerdo a la geometría de la oreja.

Actualmente expertos de la universidad de Leicester, Gran Bretaña, están desarrollando esta tecnología que se basa en la toma de fotografías de este órgano para su posterior análisis a través de software y contrastación con una base de datos existente.

La ventaja de este sistema es que es mucho menos agresivo que otros como el escáner de retina, al no existir un contacto físico. Igualmente en el estudio se investiga cual es la distancia máxima a la que podría tomarse la fotografía para realizar una identificación fiable.

La desventaja de este sistema, por otra parte, es la facilidad, dados los avances en maquillaje y cirugía plástica, de engaño al sistema mediante elementos postizos pues, como se dijo, sólo se analiza la forma de la oreja y ningún otro parámetro.

"El estado actual de la investigación de la biometría permite augurar un futuro a medio plazo en el que ésta tomará 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 fenómenos que no tardarán en ser una realidad patente en nuestras vidas", asegura **Eric Meuer, de TekhnoSur.**

La biometría es un campo que está en constante expansión, esperándose que en un futuro sea la forma estándar de sistemas de identificación. Mientras tanto, los desarrolladores seguirán perfeccionando sus productos para intentar solventar uno de los mayores problemas a los que se enfrenta la seguridad biométrica: los falsos positivos y negativos que, aunque han sido reducidos en gran medida, es de vital importancia el "reducirlos al 0%". Y para el éxito de los sistemas biométricos, lo más importante a tener en cuenta, es el "enrolamiento", (alta de la persona al sistema).

Un ejemplo: si usted tiene un documento original de buena calidad y realiza fotocopias del mismo, no notará diferencia entre el original y las copias, o sea que si el enrolamiento se realiza con óptima calidad, no tendrá dificultades en las identificaciones posteriores. En cambio, si UD. saca "fotocopias" de un documento borroso o de mala calidad, o sea si el enrolamiento es de mala calidad, seguramente tendrá problemas en el reconocimiento y falsa aceptación.

Actualmente los niveles standard de un sistema biométrico dicen que puede existir una falsa identificación de uno en un millón.

Estos niveles de seguridad son más que suficientes para una actividad comercial que, en caso de requerir mayor seguridad, puede combinar más de un rasgo biométrico, como la identificación con más de un dedo en forma secuencial.

Tecnología hoy no falta. Sólo resta saber qué nos deparará el futuro en la identificación de personas. Quizá, con el avance constante y el desarrollo de nuevos elementos, para acceder a un sitio controlado biométricamente sólo baste con traspasar una puerta. En el camino, un número "equis" de lectores y sensores habrán determinado, mediante vaya uno a saber qué milagro de la ciencia, que la persona es quien dice ser con sólo "*escanearla al paso*". ☒

Los sistemas biométricos requieren de una inversión pequeña, (no es un gasto) única al adquirir el sistema y adicionan la gran ventaja del mantenimiento cero: no hay que comprar tarjetas, reimprimirlas, vincularlas con las personas, reponer las robadas o extraviadas.

Agradecemos a las siguientes personas y empresas su colaboración en la elaboración de este informe:

Adrian Iervasi **(Draft)**
Carlos Vázquez **(Biometrix)**
Daniel Arcondo **(Larcon SIA)**
David Walfisch **(Intelektron)**
Eduardo Santarcieri **(Miatech)**
Eric Meuer **(TekhnoSur)**
Gerardo Saavedra **(Diastec)**
Marcelo Pugliese **(Biocard)**
Ricardo Becker **(AdBioTeK)**
Roberto Ingham **(Cronos)**