3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

Recepción: 20 de marzo de 2015
Aceptación: 24 de marzo de 2015
Publicación: 26 de marzo de 2015

GESTIÓN DE LA IDENTIDAD BIOMÉTRICA EN LAS ORGANIZACIONES

BIOMETRIC ID MANAGEMENT ON ORGANIZATIONS

Julián Felipe Micolta-López [1]

Raúl Fco. Oltra Badenes [2]

1. Ingeniero de Telecomunicaciones. Especialista en Consultoría de Integración de las TIC en las Organizaciones (ITIO). Pre Sales Engineer. Westcon Group. Colombia. E-mail: julianmicolta04@hotmail.com
2. Doctor Ingeniero Industrial. Departamento de Organización de Empresas. Universitat Politècnica de València. España. E-mail: rauloltra@doe.upv.es

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

RESUMEN

Actualmente las grandes empresas cuentan con un complejo esquema de organización, donde sus departamentos se vuelven críticos y transversales a toda la base de negocio y a los objetivos de la organización. La cantidad de clientes internos y/o externos involucrados en los procesos crece de tal manera, que la empresa pierde el control de su dimensionamiento trayendo consigo consecuencias, traducidas como reducción de la productividad y pérdidas económicas. En el presente artículo se mostrarán algunas aplicaciones de la gestión de la identidad biométrica que pueden subsanar, mitigar o controlar debilidades en el desarrollo de algunos procesos que son intrínsecos a cualquier organización.

ABSTRACT

Currently the big companies have a complex organizational scheme where departments become critical and transversal to all business core and the organization objectives. The amount of internal and/or external clients involved in processes grows such that the company loses control of its sizing, bringing consequences translated as reduced productivity and economic losses. In this article some applications of biometric identity management that can cure, mitigate or control weaknesses in the development of some processes that are intrinsic to any organization are shown.

PALABRAS CLAVE

Organización; clientes; procesos; productividad; biométrica

KEYWORDS

Organizations; clients; processes; productivity; biometric

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

INTRODUCCIÓN

Actualmente las grandes empresas cuentan con un complejo esquema de organización, donde muchos de sus departamentos se vuelven críticos y transversales a toda la base de negocio y al objetivo de la organización. En algunos casos es tanta la cantidad de personas internas o externas involucradas en los procesos, que la empresa pierde el control de su dimensionamiento trayendo consigo grandes consecuencias, traducidas generalmente como reducción de la productividad o simplemente en pérdidas económicas.

En el presente trabajo se mostrarán algunas de las aplicaciones de la gestión de la identidad biométrica que pueden ayudar a subsanar, mitigar o controlar debilidades en el desarrollo de algunos procesos que son intrínsecos a cualquier organización, como lo son áreas seguras, control de acceso a terceros, generación de bases de datos de alto flujo de clientes, entre otros.

En primera medida será necesario contextualizar al lector sobre el significado de la gestión de la identidad biométrica. Para ello se describirá su funcionamiento, los elementos que intervienen, los parámetros de medición y sus aplicaciones.

A continuación se enunciarán las ventajas y desventajas orientadas siempre al desarrollo de las organizaciones y su implementación de las TIC como la que se muestra en el presente trabajo.

Finalmente se expondrán las conclusiones y casos de éxito de empresas que han implementado en alguna medida la gestión de la identificación biométrica como ayuda al desarrollo de sus actividades y procesos.

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

GESTIÓN DE LA IDENTIDAD BIOMÉTRICA

¿QUÉ ES BIOMETRÍA?

Este concepto proviene de las palabras griegas Bios (vida) y Metrón (Medida). De esta manera es posible inferir que el concepto de Biometría hace referencia al estudio de la medición de los aspectos biológicos de cualquier ser, en este caso específico, humanos (Wikipedia 2011).

En la actualidad el concepto de biometría se utiliza para referirse al estudio de los métodos automáticos para el reconocimiento único de personas basado en uno o más rasgos conductuales o rasgos físicos intrínsecos. Por lo tanto es bastante común escuchar el término "biometría informática". Dicho término combina las diversas técnicas matemáticas, estadísticas y de inteligencia artificial para aplicar la autenticación e identificación de personas, principalmente en sistemas de seguridad informática.

Las técnicas biométricas se basan en la medida (directa o indirecta) y posterior análisis de uno o un conjunto de rasgos (estáticos y/o dinámicos) del individuo para reconocerlo o verificar automáticamente su identidad. A este conjunto de rasgos también se le conoce como ***indicador biométrico***.

La medición de los rasgos estáticos hace referencia a la anatomía del usuario como las huellas digitales, la imagen facial, la geometría de la mano, los patrones del iris, la retina, etc. Mientras que los rasgos dinámicos miden características del comportamiento dinámico del usuario como patrones de voz, escritura o firma manuscrita, la cadencia del paso, los gestos, etc. (Sánchez Calle 2005).

CARACTERÍSTICAS DE UN SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA

Para la implementación práctica de un sistema de gestión de identificación biométrica, es necesario tener en consideración las siguientes características (Clarke 2009):

1. *Rendimiento:* Hace referencia a la velocidad, robustez y exactitud con que los recursos tecnológicos pueden procesar el tipo de identificación implementada, además, de qué manera los factores operativos o del medio ambiente pueden afectar la exactitud del proceso de identificación y que ventajas existen en lo que refiere a coste-beneficio.
2. *Aceptabilidad:* Que tan dispuestos están los usuarios a facilitar sus datos biométricos en el desempeño diario, o para recibir un determinado servicio, teniendo en cuenta que la implementación de sistemas biométricos podría representar problemas de seguridad para la integridad física del usuario.

3. *Fiabilidad:* Que tan fácil es burlar el sistema que se implemente, mediante falsificación o fraude. El sistema debería ser capaz de identificar si los datos provienen de una fuente viva, debido a que existe la posibilidad de recrear una huella mediante moldes de látex, o la voz, mediante moduladores, entre otros inconvenientes que pueden comprometer la fiabilidad del sistema.

Debido a lo anterior un sistema de gestión de la identidad biométrica debe ser capaz de:

1. Realizar un proceso de identificación de manera rápida y precisa, y con recursos no muy elevados.
2. No ser perjudicial para sus usuarios y ser aceptado por la población a la que está dirigido.
3. Ser lo suficientemente robusto como para evitar cualquier tipo de fraude o falsificación.

ARQUITECTURA GENERAL DE UN SISTEMA DE GESTIÓN DE LA IDENTIDAD BIOMÉTRICA

Los sistemas y dispositivos que permiten la gestión de la identidad biométrica constan generalmente de tres fases o componentes básicos que permiten su funcionamiento (Areitio 2007).

El primer componente se encarga de capturar o adquirir los datos biométricos de un individuo, ya sea de manera análoga o digital, por ejemplo la huella dactilar mediante dispositivos de escaneo o el patrón de la voz con dispositivos capaces de tomar muestras de la voz.

El segundo componente es el encargado de comprimir, almacenar, procesar y comparar los datos previamente capturados, mediante algoritmos matemáticos que garanticen la integridad de la información almacenada y comparada.

El tercer componente básico de un sistema de gestión de identidad biométrica consiste en establecer la interfaz de comunicación entre las aplicaciones y los procesos de la organización, que se encuentren en el mismo o en otro sistema.

De forma conceptual se puede entender la arquitectura de un sistema biométrico como dos instancias o módulos dentro del proceso:

- Módulo de inscripción o enrolamiento
- Módulo de identificación o autenticación

El módulo de enrolamiento se encarga de adquirir y almacenar la información que viene de los indicadores biométricos, con el fin de incluir al individuo dentro de las bases de datos del sistema, las cuales serán utilizadas posteriormente para comparar intentos de acceso o autenticaciones contra el sistema. El proceso de enrolamiento se logra gracias a los

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

dispositivos de captura, como son: lectores de huella, micrófonos, escáner de retina, cámaras de identificación facial, etc.

La información adquirida por los dispositivos de captura, se almacena en las bases de datos con el nombre "template". Este término se utiliza para hacer referencia a toda la información relevante o más representativa del indicador biométrico seleccionado.

El módulo de autenticación en cambio, es el responsable de reconocer los usuarios dentro del sistema biométrico. Este módulo comienza su proceso con la captura de los datos biométricos con ayuda de los dispositivos de captura mencionados anteriormente y convirtiéndolos en formato digital con el fin de que el extractor de características genere un template con los mismos parámetros que se encuentran almacenados en las bases de datos.

Posteriormente este template es enviado al comparador de características, el cual lo confrontará en esquema uno a uno (1:1) o uno a varios (1:N) con los templates de la base de datos para determinar la identidad del individuo.

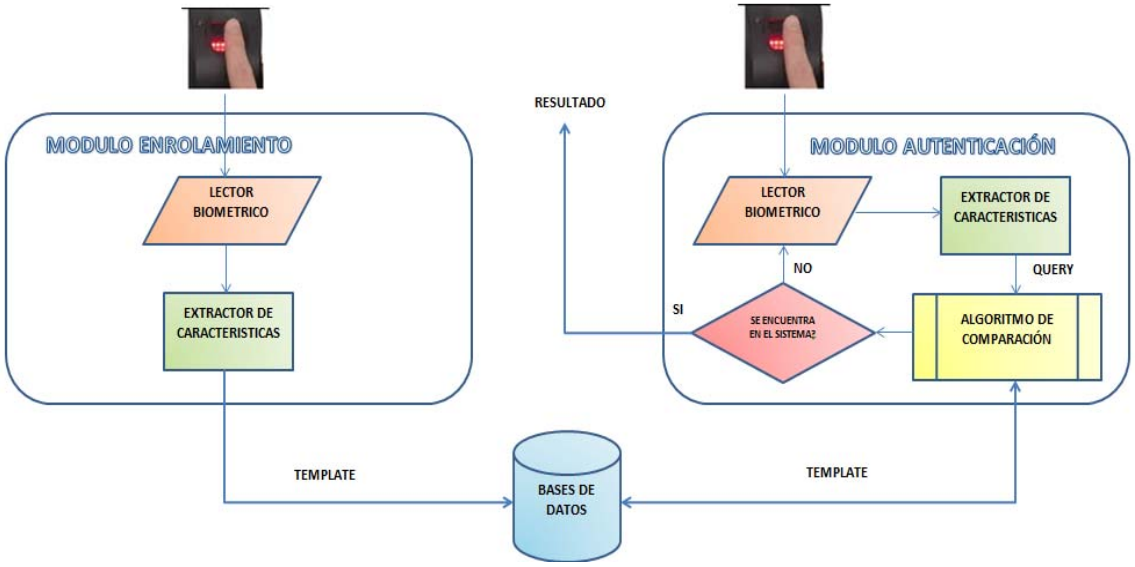

Ilustración 1. Esquema general de un sistema de identificación biométrica (**Fuente:** Propia)

El módulo de autenticación corresponde a la fase operacional del sistema. Dicho de otra manera, opera sobre las inscripciones, configuraciones y políticas ya establecidas.

A continuación se enuncian los dos modos en los que un sistema de gestión de la identidad biométrica puede funcionar en su fase de operación:

1. *Modo de Identificación*: En este modo el sistema tiene la tarea de descubrir un individuo dentro de toda la base de datos del sistema, es decir, debe comparar el template con todos los templates presentes en la base de datos. Esto hace referencia a la configuración 1:N mencionada anteriormente. Este modo de operación responde a lo que sería la pregunta coloquial ¿Quién eres tú?

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

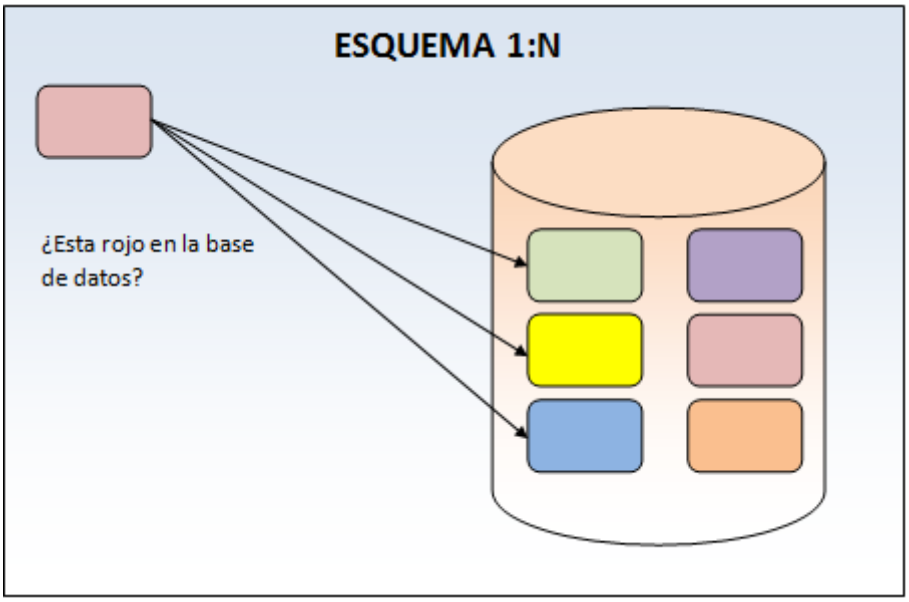

Ilustración 2. Esquema de comparación 1:N (**Fuente:** Propia)

2. *Modo de Verificación*: Poniendo como ejemplo que una persona digita su número de identificación como información adicional al momento de realizar el proceso de autenticación, no será necesario hacer un barrido de comparación de templates en toda la base de datos, sino únicamente con los templates relacionados con ese número de identificación. Lo que lleva al otro tipo de configuración mencionado anteriormente, comparación 1:1. En palabras más sencillas el sistema responde a la pregunta ¿Eres tú quien dices ser?

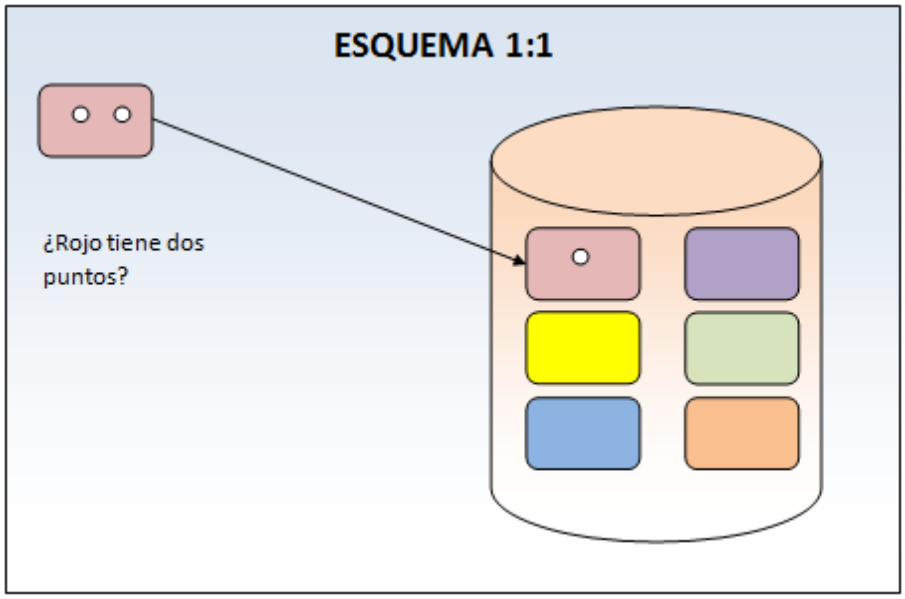

Ilustración 3. Esquema de comparación 1:1 (**Fuente:** Propia)

A rasgos generales, se puede decir que es más difícil diseñar un sistema que funcione bajo el modo de operación de identificación, debido a que es necesario tener bases de datos extensas y un nivel de procesamiento elevado. Pero sus prestaciones, por lo menos en entidades financieras, son excelentes para evitar fraudes como la suplantación de identidad.

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

Las prestaciones a nivel de hardware y a nivel de software son menos exigentes en un sistema diseñado para realizar verificación biométrica, y por ello, su implementación y administración es menos costosa, reflejado también por sus prestaciones limitadas de seguridad ya que el usuario debe darse a conocer antes de ingresar sus características biométricas, facilitando la suplantación de identidad y la existencia de duplicidad de la información como por ejemplo ID's diferentes con los mismos templates, por otra parte existe la posibilidad del extravío del ID o PIN asignado al usuario haciendo que el acceso a los servicios prestados por la plataforma sea negado.

TASA DE ACEPTACIÓN Y MEDICIÓN DE UN INDICADOR BIOMÉTRICO

Los templates brindan información que permite partir la base de datos en dos grupos grandes, de acuerdo a los patrones particulares que estas almacenan de cada indicador biométrico. Estos grupos, que de ahora en adelante se llamaran "clases", al momento de ser generados, reducen los rangos de búsqueda de templates dentro de la base de datos. Por ejemplo los patrones de huellas dactilares se pueden clasificar como se muestra en la siguiente figura.

Ilustración 4. Patrones de Huellas dactilares (**Fuente:** http://juanpa007.obolog.com)

Sin embargo, los templates que pertenecen a la misma clase (por ejemplo, en el caso de las huellas dactilares, dos huellas que pertenezcan a la clase de "arco llano") también presentan diferencias entre ellas, estas diferencias se conocen como "variaciones intraclase".

Que existan variaciones intraclase implica que la identidad de una persona se puede establecer solo con un cierto nivel de confianza. Las decisiones tomadas por los sistemas biométricos se encuentran casi que a un nivel de "verdadero o falso", en este caso, usuario autorizado o impostor. Pero además, el sistema arrojará cuatro tipos de respuesta, las cuales se enuncian a continuación:

1. Un usuario autorizado es aceptado
2. Un usuario autorizado es rechazado
3. Un usuario impostor es aceptado
4. Un usuario impostor es rechazado

De lo anterior se observa que los resultados 1 y 4 son respuestas correctas y las esperadas por todos los sistemas biométricos, mientras que los resultados 2 y 3, son los resultados erróneos que no se esperan que sean arrojados por el sistema biométrico.

El grado de confianza asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de usuarios autorizados e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos posibles tasas de error (Morales Cabello 2000):

- *Tasa de falsa aceptación (FAR: False Aceptation Rate):* Hace referencia a la frecuencia relativa con la que un impostor es aceptado como un usuario autorizado.
- *Tasa de falso rechazo (FRR: False Reject Rate):* Hace referencia a la frecuencia relativa con que un usuario autorizado es rechazado como si fuera un impostor.

Estos indicadores son funciones que proporcionan información sobre el grado de seguridad deseado. Por lo general, el resultado de un proceso de verificación o de identificación, será un valor real normalizado entre cero (0) y uno (1), lo cual indicará el "grado de parentesco" o la correlación entre las características que ha proporcionado el usuario y las que se encuentran almacenadas en la base de datos del sistema.

A modo de ejemplo, si en un sistema de control de acceso se exige un elevado valor del grado de parentesco (cercano a 1), entonces pocos o ningún impostor será aceptado pero de la misma manera muchos usuarios autorizados también serán rechazados por el sistema. Si por el contrario el grado de parentesco es cercano a cero muchos impostores serán aceptados en el sistema y una muy pequeña fracción de usuarios autorizados serán rechazados.

Con este ejemplo se quiere dar a entender la estrecha relación que existe entre los indicadores FAR y FRR, y que son además inversamente proporcionales, lo que quiere decir que una FRR baja entregara una FAR alta y viceversa, tal y como se muestra en la siguiente figura.

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

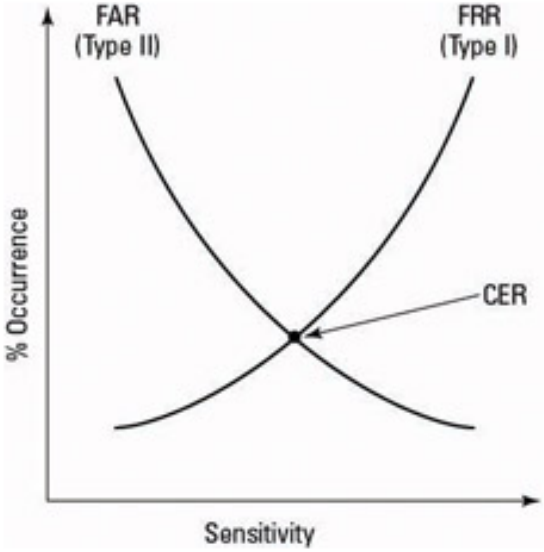

Ilustración 5. Relación FAR y FRR (**Fuente:** http://flylib.com/books/en/2.930.1.46/1/)

En la gráfica anterior, se observa un término nuevo, CER (Crossover Error Rate) el cual indica que el valor de FRR es igual al valor de FAR porcentualmente hablando. Los valores de FRR y FAR son valores variables y pueden ser ajustados modificando las características en hardware o software del dispositivo de captura, lo que aumentará o disminuirá la sensibilidad del sistema. El punto CER, también conocido como tasa de error de inserción, es considerado el indicador o medida más importante en la precisión de un sistema biométrico, ya que proporciona información sobre el punto ideal de sensibilidad para el correcto y equilibrado funcionamiento del sistema (Miller 2004).

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

BIOMETRÍA EN LAS ORGANIZACIONES

A lo largo de la historia, los seres humanos han buscado constantemente la forma de optimizar sus procesos de producción, control, servicios, etc. Inicialmente se buscaba ofrecer la mayor cantidad posible de bienes productos o servicios utilizando cantidades de mano de obra y recursos humanos. Pero con la llegada de las TIC y los altos niveles de competencia empresarial, este enfoque cambió.

Era necesario reducir costos pero además mantener la empresa con los mismos niveles de producción y rendimiento, y es aquí cuando entra en juego la automatización. Esta nueva estrategia permitió que un solo trabajador realizara trabajos que requerían una gran cantidad de personas y con el apoyo de las tecnologías de la información y las comunicaciones, se logró que ese trabajador interactuara con las demás áreas y dependencias, convirtiendo a las empresas en organizaciones totalmente interdisciplinarias.

En este punto, toda empresa, entidad u organización, requiere tener dentro de su estructura funcional un área de TI o TIC, debido a que las tecnologías se han convertido en un elemento transversal y estratégico a todos los elementos misionales de cualquier tipo de organización.

La gestión de la identidad biométrica no es la excepción, puesto que en la mayoría de los casos, debemos identificar los diferentes clientes tanto internos como externos, para mantener el control sobre el crecimiento de la empresa y para generar indicadores de gestión, que permitan ubicar de manera correcta la posición de la empresa ante la competencia.

Por ejemplo, en los sistemas integrados de transporte, las estadísticas más convencionales son la cantidad de personas que ingresan y salen del sistema. Esto permite medir la efectividad y la cantidad de población que moviliza el sistema. Sin embargo las probabilidades de que las estadísticas no reflejen el comportamiento real son bastante altas ya que muchas personas extravían su ticket, olvidan colaborar y guardan el ticket, inclusive existen personas que ingresan al sistema evadiendo el pago. Como se observa el inconveniente es la identificación de los usuarios.

Con la implementación de un sistema biométrico en un sistema de transporte, sería posible saber con certeza cuántos usuarios están usando el servicio, la frecuencia con que ingresan al sistema, cuantas entradas y salidas registran los usuarios reduciendo considerablemente los porcentajes de error en un estudio de la funcionalidad del sistema.

Así como en los sistemas de transporte la gestión de identidad biométrica es completamente aplicable, existen otros ejemplos en los que la biometría ofrecería un sin fin de beneficios, tanto en seguridad, agilidad y funcionalidad como en aumento de la productividad y reducción de costos.

Para realizar un correcto análisis de los beneficios y las dificultades que pueden surgir al implementar sistemas de gestión de la identidad biométrica en las organizaciones es necesario tener en cuenta algunos factores importantes como lo son; la finalidad, la cantidad

estimada de usuarios, la técnica de identificación empleada, el entorno de "confianza" o "desconfianza" en el que se encuentra, etc. Por este motivo es necesario realizar un análisis de cada caso para saber si es conveniente y rentable establecer un sistema de identificación biométrica en la organización.

La implantación de este tipo de tecnologías sugiere una serie de ventajas y beneficios tanto para entidades públicas como privadas.

BENEFICIOS PARA LAS ORGANIZACIONES

Las entidades tanto públicas como privadas deben ser las encargadas de promover el uso de las nuevas tecnologías de la información y las comunicaciones (TIC's) como la biometría, que tecnológicamente hablando se encuentra suficientemente madura, solo depende de las grandes y medianas empresas para que impulsen su implementación a gran escala.

Para que lo mencionado anteriormente ocurra es necesario que los beneficios potenciales que se pueden obtener de su implantación sean claros y relevantes. A continuación se enunciaran cada una de ellas (ENISE 2010):

- *Aumento de la seguridad*

Una de las ventajas más importantes de la utilización de las técnicas de identificación biométrica, es el aumento considerable de la seguridad, debido a que garantizan que la persona es quien dice ser, es decir, que los rasgos biométricos se encuentran exclusivamente ligados a su legítimo usuario.

Por otra parte, mediante el robo de credenciales, un individuo puede acceder a zonas restringidas o realizar operaciones no permitidas, inculpando a terceros. De la misma manera, es posible que estas credenciales se compartan voluntariamente entre empleados o usuarios.

Tanto el robo como la utilización por parte de diferentes usuarios de las mismas credenciales, se traduce en una enorme brecha de seguridad en las entidades que puede ser evitada. A través de la implementación de sistemas biométricos, se aumenta la seguridad reduciendo la probabilidad de que alguien no autorizado acceda a zonas o aplicaciones restringidas.

- *Reducción de los costos de mantenimiento*

Las técnicas tradicionales (el uso de contraseñas o tarjetas de identificación) generalmente no necesitan de mucha inversión en su implementación. Sin embargo conllevan grandes inversiones y costes elevados ligados a su gestión y mantenimiento diarios. Esta es la consecuencia de uno de los riesgos más evidentes asociados a este tipo de métodos de autenticación: la pérdida, robo o incluso olvido de las credenciales asociadas a un usuario específico.

Sin embargo, en el caso de los sistemas de gestión de la identidad biométrica la inversión inicial puede llegar a ser elevada, sobre todo en el caso de necesitar la adquisición de

hardware y/o software para la adquisición y procesamiento de indicadores biométricos. Pero después de que el sistema se encuentre funcionando y los usuarios estén acostumbrados a usarlo, el costo de mantenimiento es muy reducido ya que no se presentan ninguno de los casos anteriormente mencionados.

Este beneficio es más notorio en tecnologías cuyo coste de implementación es menor, tales como la huella dactilar, el reconocimiento de voz o el reconocimiento facial.

- *Aumento de la eficiencia*

La realización de diferentes procesos de autenticación, controles de acceso e identificación mediante técnicas tradicionales no biométricas supone, en ocasiones, una inversión excesiva de tiempo. Algunas veces, aunque el proceso dure pocos segundos, si es realizado por un gran número de usuarios en un corto periodo de tiempo, puede resultar altamente ineficiente. Esto sucede por ejemplo, en los accesos a grandes edificios de oficinas o en el control fronterizo de un aeropuerto en las horas de máxima afluencia.

- *Reducción de fraude interno*

Uno de los métodos más habituales para cometer fraude interno en empresas y en organismos públicos es la imputación de horas de trabajo inexistentes, en algunos casos, no estando tan siquiera el empleado físicamente en las instalaciones de la entidad. Para ello, se pueden acompañar en sus compañeros que "autentican" en su lugar. Como consecuencia de ello, la empresa estaría remunerando al empleado por horas que, en realidad, el empleado no ha realizado.

Esta situación acarrea pérdidas económicas así como posibles perjuicios a la imagen corporativa. El uso de tecnología biométrica para el control de horario de los empleados puede ayudar a prevenir este y muchos tipos más de fraude, verificando mediante diferentes métodos que tanto el tiempo laboral imputado, como el tiempo de trabajo que registra el empleado, es registrado por el empleado correcto y no por alguien que está intentando suplantar su identidad.

- *Mejora de la imagen corporativa*

La implantación de tecnologías de identificación biométrica, supone una mejora de imagen de la seguridad de una entidad, contribuyendo además a que sea más eficiente, más segura y con mecanismos que combatan y eviten cualquier tipo de fraude.

Por este motivo, sumado a las ventajas que se han mencionado anteriormente, se produce una mejora en la opinión general sobre la compañía. De la misma manera, se asocia a la empresa con la innovación, la inversión en investigación y desarrollo y la apuesta por tecnología puntera.

- *Oferta de nuevos servicios*

Los sistemas de gestión de identidad biométrica dan las pautas para nuevas líneas de investigación en entrega de nuevos productos y servicios. Estos productos o servicios se

basan sobre diferentes y diversas aplicaciones en el sector sanitario, el pago mediante dispositivos móviles, control parental, videovigilancia, etc.

3C TIC *(Edición núm. 12)* Vol.4 – Nº 1
Marzo – junio 2015, 57 - 72
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 6529

CONCLUSIONES

La gestión de la identidad biométrica es una fuerte herramienta en el crecimiento económico y tecnológico de cualquier empresa, además de aportar otros beneficios como el control total del personal que aporta o consume los servicios prestados por la entidad.

Gracias al rápido y continuo desarrollo, es más fácil su implementación y combinación con aplicaciones computacionales de cualquier área y nivel. Sin embargo, la sociedad y el mercado no han notado las grandes ventajas y beneficios que pueden obtener, debido al desconocimiento, falta de información e inversión en sus áreas de investigación y desarrollo.

Otro aspecto importante para la adopción de esta tecnología, es el marco regulatorio debido a que las leyes de protección de datos forman la columna vertebral del marco jurídico para su implementación, y no existen estándares internacionales que regulen y controlen la manera en que las empresas deben almacenar la información personal y confidencial de los usuarios.

En muchos países como en Colombia, se están implementando infraestructuras que permitan tanto a entidades públicas como privadas la autenticación contra las bases de datos estatales, con el fin de garantizar el uso de la información, y proteger la información de los ciudadanos.

REFERENCIAS

AREITIO, Javier, Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación [En Línea], País Vasco, [Consultada 18 de Febrero de 2015]. Disponible en: http://www.redeweb.com/_txt/630/52.pdf.

Facultad de Biometría Informática [En Línea], Mexico, [Consulta 18 de Febrero de 2015]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/escaneoretina.html.

CLARKE, Roger, Human Identification in Information Systems: Management Challenges and Public Policy Issues [En Línea], Australia, [consulta 18 de Febrero de 2015]. Disponible en: http://www.rogerclarke.com/DV/HumanID.html.

MILLER, Lawrence, CISSP for Dummies [En Línea], Hoboken, New York EEUU, [consultada 20 de Febrero de 2015]. Disponible en: http://flylib.com/books/en/2.930.1.46/1/.

MORALES CABELLO, Eduardo, Detección automática de vectores de características en huellas dactilares, Universidad de Chile, Chile 2000

SANCHEZ CALLE, Angel, Aplicaciones de la Visión Artificial y Biometría Informática, Universidad Rey Juan Carlos, Madrid 2005

Servicios basados en DNIe (premio ENISE al mejor servicio) [video en línea], León, España, Octubre 2010. Podcast 135 min. [Consulta el 22 de Febrero de 2015]. Disponible en: http://www.webcastlive.es/4enise/index2.htm#ponencia=t33.

Wikipedia: la enciclopedia libre [Wiki en Internet]. St. Petersburg (FL): Wikimedia Foundation, Inc. 2001. [Consulta 18 de Febrero de 2015]. Disponible en: http://es.wikipedia.org/wiki/Biometr%C3%ADa