Una seguridad GLOBAL

La huella digital aplicada a la gestión de identidades

Por Jorge Urios Rodríguez
Front Office Solutions Practice Manager de Getronics Iberia

En los últimos años la Gestión de Identidades se ha convertido en una necesidad dentro del entorno corporativo, donde se tienen que orquestar las funciones de una infraestructura de seguridad global e integrada en el propio *core-business* de la organización, gestionando los usuarios de una manera centralizada, asignando recursos, informes y auditorías de modificaciones y servicios al usuario como la gestión de contraseñas y el ansiado *single sign on* en las aplicaciones. Sin embargo, el eslabón más débil de la cadena sigue en entredicho.

Por todos es conocido el incremento de las partidas de gasto de los departamentos de IT en aumentar la seguridad, sin tener en cuenta que el fallo de una sola password puede comprometer toda la seguridad de los datos de las empresas. La variedad de *passwords* utilizadas en diferentes aplicaciones, su frecuencia de uso y políticas de password difíciles que en lugar de aumentar la seguridad, incrementan el número de llamadas a la *help-desk*, ya sea porque el usuario la ha escrito mal o simplemente por olvido, incrementan los problemas.

Por el contrario, si optamos por un sistema de *single sign on* (sistema de acceso a las diferentes aplicaciones mediante el uso de una única password), a simple vista podría parecer que ya hemos resuelto toda la problemática, pero ¿quién nos asegura que esa persona es la que dice ser y no otra?, ¿Qué ocurriría si dicha *password*, cayera en manos de un "amigo de lo ajeno"? ¿Ha calculado el coste que una brecha de seguridad provocada por el mal uso de una password supondría a su empresa?

Por tanto, está claro que la seguridad basada únicamente en una clave, es insuficiente.

Sistemas de Autenticación

En los últimos años han proliferado en el mercado diferentes sistemas de autenticación, desde los tradicionales lectores de tarjetas hasta los lec-

Métodos de Autenticación	Seguridad	Coste	Conveniencia	Comentarios
Passwords	🔴	🔴	🔴	Compartidas; escritas; fáciles de averiguar
Password Self-Reset	🔴	🔵	🟡	Aumenta los costes de help-desk y no la seguridad
Single Sign-On	🔴	🔵	🔵	Una única password = Única brecha
Smart Card	🔵	🟡	🟡	Fácil compartir/perder
Tokens	🔵	🔵	🔴	Inconveniente; No para uso interno
Autenticación con Huella Digital	🔵	🔵	🔵	**Mejor balance seguridad, coste & conveniencia**

🔵 Positivo 🟡 Neutral 🔴 Negativo

FIGURA 1. Sistemas de Autenticación

tores biométricos.

En la **FIGURA 1** "Sistemas de Autenticación", se puede observar los inconvenientes de los diferentes sistemas autenticación. Como ya hemos comentado el uso de *passwords*, que pueden ser compartidas, escritas o fáciles de averiguar, ponen en riesgo toda la infraestructura informática de la empresa y si optamos por sistemas de pregunta-respuesta para el desbloqueo de *passwords*, o para la generación de una nueva clave, por regla general nos vamos a encontrar con incremento de llamadas y por lo tanto de costes de *help desk* (servicio telefónico de atención al usuario).

El tradicional uso de tarjetas, implica la gestión del ciclo de vida de las mismas, pero quizás el mayor inconveniente es que no se verifica la identidad del usuario, es decir, con el uso de las tarjetas se identifica la persona que accede al sistema, pero en ningún momento se verifica que esa persona es quien dice ser.

El mismo handicap, encontramos con el uso de los *token*, además de que en este segundo caso es necesario disponer de un puerto USB de acceso cómodo para el usuario.

Por último, los sistemas de autenticación biométrica y en particular los lectores de huella digital, parecen posicionarse como la mejor opción de autenticación, ya que reúnen las tres variables clave:

* **Seguridad:** de carácter innato, la huella dactilar.
* **Conveniencia:** facilidad de uso, sólo es necesario posicionar la huella en el lector.
* **Coste:** Reducción exponencial en los últimos años.

Por supuesto, existen otros métodos de autenticación biométrica, como pueden ser la lectura de la retina, del iris, el reconocimiento de la voz, de la cara, de las características de la mano,... pero como se puede observar en la **FIGURA 2** "Comparativa de Sistemas de Autenticación Biométrica" la relación coste - seguridad - conveniencia, no es siempre tan positiva.

De la Huella Dactilar a la Huella Digital

La identificación de personas mediante su huella dactilar es una técnica que cuenta ya con casi un siglo de antigüedad. Su amplio reconocimiento, como técnica válida, por los sistemas legales de la mayoría de los países del mundo, y su amplia experiencia, impulsaron hace muchos años a que se desarrollaran sistemas que permitiesen la identificación de las personas de forma automática. En el pasado, tanto por su coste como su aplicación se ha destinado principalmente al uso legal y militar, pero en los últimos años su aplicación en la empresa como medio de autenticarse para acceder al puesto de trabajo o a las aplicaciones ha ido en aumento y ya son más de 1 millón de personas las

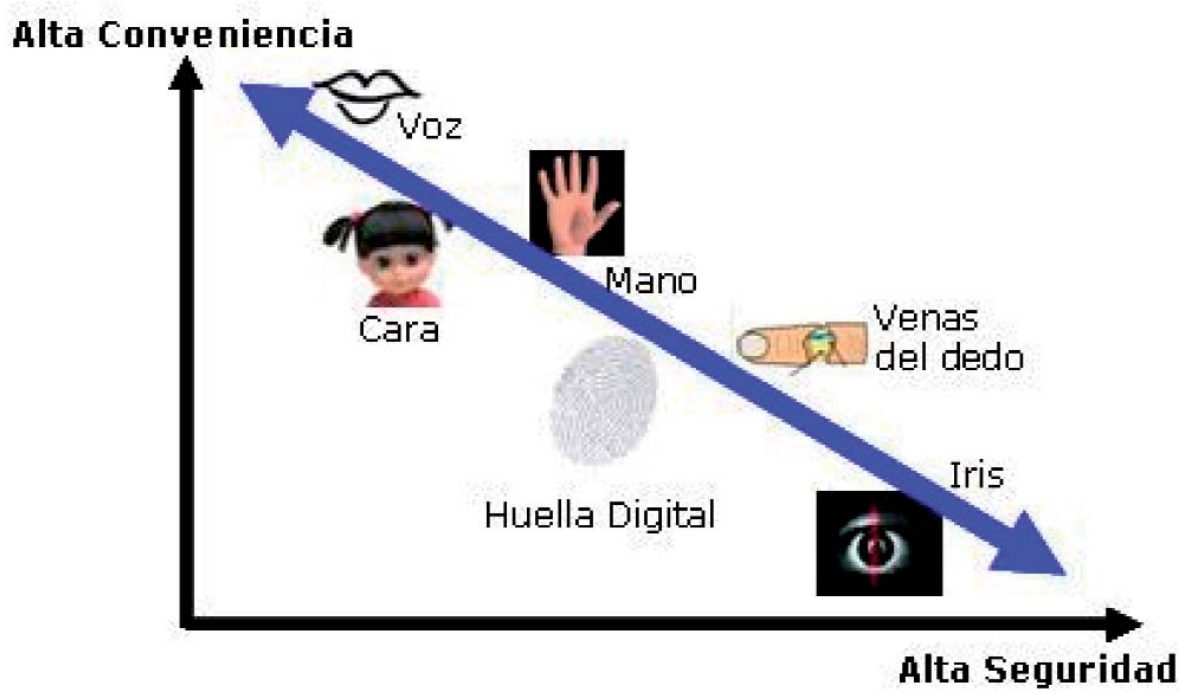

FIGURA 2. Comparativa de Sistemas de Autenticación Biométrica

que lo utilizan en todo el mundo.

En la huella dactilar, podemos observar ciertos puntos característicos, o puntos de minucia, formados principalmente por las crestas y los valles de la huella. Al procesar el lector, dicha huella y mediante la extracción de los puntos de minucia, va a formar lo que se denomina el "*hash* de la huella", es decir, un algoritmo matemático irreversible (con el cual no se puede reconstruir la huella) y unívoco.

El *hash* de la huella será almacenado en una base de datos, y cada vez que el usuario acceda al sistema comparará el hash de la huella generado, con éste. Dicha comparativa se puede realizar de dos formas:

1. 1:N - Identificación: El *hash* generado buscará en la base de datos su correspondiente para dar el acceso o denegar la entrada al sistema.

2. 1:1 - Verificación: Antes de posicionar la huella en el lector, introduciremos un ID del usuario (que puede ser su número de empleado, DNI, número de la Seguridad Social,...), de tal manera que al posicionar el dedo sobre el lector y generar el *hash*, lo buscará directamente en la base de datos y comparará si el ID del usuario se corresponde con dicho hash.

Ambas comparativas son igualmente fiables, si bien es cierto que por rapidez y sencillez, cuando hablamos de organizaciones con más de mil empleados tenderemos a sistemas 1:1.

En general hablaremos de dos ratios que podremos regular según nuestro propio interés, el Ratio de Falsa Aceptación FAR (False Acceptance Rate) y el Ratio de Falso Rechazo FRR (False Rejection Rate), que es si cabe más importante que el anterior ya que puede provocar la frustración del empleado.

a) Tasa de Falsa Aceptación F.A.R. (False Acceptance Rate):

* Probabilidad de que un dispositivo biométrico permita entrar a una persona no autorizada

* Debe ser suficientemente baja para que no sea un inconveniente para el usuario.

* La única manera que una persona no autorizada puede tener acceso es si esa persona lo intenta. Por lo tanto, la Tasa de Falsa Aceptación debe multiplicarse por el número de intentos de personas no autorizadas para determinar el número de posibles ocurrencias.

b) Tasa de Falso Rechazo F.R.R. (False Rejection Rate):

* Probabilidad de que un dispositivo biométrico no permita entrar a una persona autorizada

* En muchas ocasiones el permitir entrar a los buenos es tan importante como mantener afuera a los malos.

La Huella Digital y el Directorio Activo

La autenticación mediante la huella digital nos va a proporcionar un ini-

FIGURA 3. **Puntos de Minuncia**

La identificación de personas mediante su huella dactilar es una técnica que cuenta ya con casi un siglo de antigüedad

cio de sesión seguro y fácil para el usuario en el PC, dominios y aplicaciones Web. Esto principalmente se va a traducir en una:

a) En una mayor productividad y cumplimiento de los empleados.

b) Una menor cantidad de llamadas a la *Help Desk*.

c) La desaparición de la necesidad de recordar, actualizar y administrar contraseñas.

Además de proveer un identificador único y que otros no pueden utilizar, es importante destacar el cumplimiento de las principales normativas internacionales: *HIPAA; Sabarnes-Oxley; Acta Gramm-Leach-Bliley; NIST/GSA National Information Assurance Partnership (NIAP);...*

El acceso a Windows, se va a poder realizar sólo con sólo la huella, la huella y/o la utilización de password, y en aquellos entornos de alta seguridad huella y *smartcard*.

Para aquellos pc's genéricos, multi-usuarios, en los que es necesario el acceso continuo y momentáneo al ordenador de distintas personas, y/o en diferentes horarios como puede ser su uso por ejemplo en puestos de atención al cliente en la Administración Pública, en Hospitales, en puestos de *HelpDesk*, en líneas de fabricación, etc. se hace necesario poder controlar dichos accesos y proporcionar al empleado un acceso fácil y cómodo a sus aplicaciones. En este sentido el sistema *Pro Kiosk*, permite la creación de un usuario principal sobre el que se gestionan los privilegios de acceso a las diferentes aplicaciones en función de los privilegios del empleado y sin necesidad de un cambio de sesión, simplemente posicionando el dedo sobre el lector de huella y proporcionado un registro de eventos.

FIGURA 4. GINA Huella Digital

One Touch Sing On, One Touch Unlock y Event Logging

One Touch Sign On, va a proporcionar autenticación a aplicaciones o entornos webs basados en *passwords*, mediante la creación de una plantilla que sustituirá los campos de identificación por el hash de la huella, sin necesidad de desarrollos o *plug-ins* adicionales, gestionado de manera centralizada y disponible para usuarios de Directorio Activo. La creación de la plantilla sólo será necesaria la primera vez que el usuario accede a la aplicación.

Como funcionalidad adicional, el sistema de huella digital nos va a permitir bloquear y desbloquear el equipo simplemente posicionando el dedo registrado en el lector.

Y quizás lo más importante de todo, el sistema de huella digital nos va a proporcionar un *logging* de eventos, o lo que es lo mismo una auditoría exacta de acceso en entornos de pc´s monousuarios y en pc´s compartidos. Todos los eventos en los ordenadores son reproducidos en local y en el visor de eventos de Directorio Activo, usando los Logs de eventos de Windows y con la posibilidad de obtener informes gracias a herramientas como como *Microsoft ACS, Quest Software Reporter*.

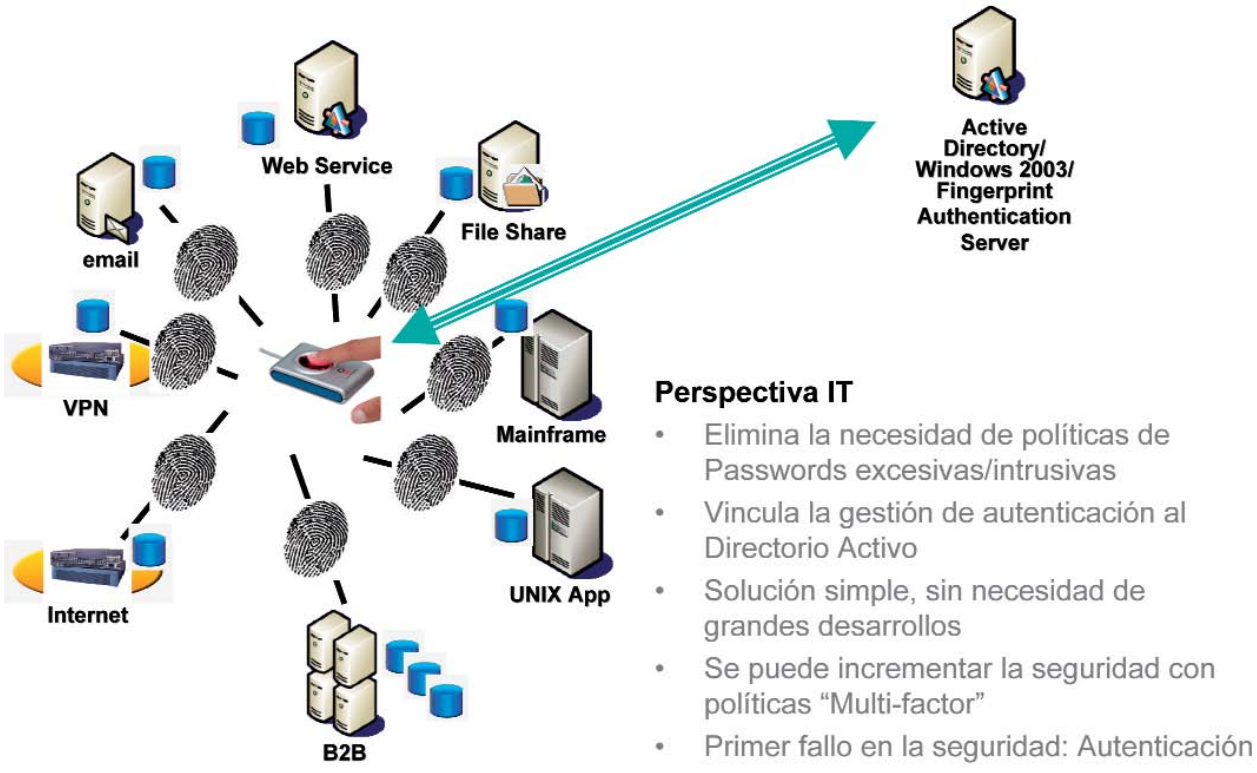

FIGURA 5. Getronics Solution