BIOMETRÍA, ¿EL FUTURO DE LA SEGURIDAD INFORMÁTICA?

Areli Ramírez Cabañas
Gerencia de Soluciones Móviles

En la actualidad, la biometría es algo tan común que lo podemos ver en nuestro día a día en dispositivos móviles, acceso a edificios, embajadas, bancos, etc., por lo que empresas de sector privado y público como SURA, HSBC, SAT, SRE, INE están empezando a integrarla como un nuevo método de autenticación para brindar mayor seguridad a los usuarios, dando pie a que los usuarios eviten utilizar contraseñas y patrones para acceder a sus cuentas.

Los expertos en seguridad consideran que las contraseñas en la actualidad empiezan a ser ineficientes, de acuerdo un reciente informe elaborado por el Fondo Monetario Internacional titulado “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment”, los ataques informáticos podrían representar para el sector financiero mundial pérdidas cercanas a los 100 mil millones de dólares.

Como podemos ver, es momento de encontrar un nuevo método de protección de datos y es ahí donde la biometría está acaparando el mercado de la seguridad informática. Sin embargo, ésta conlleva consecuencias que tienen que ser consideradas, como el robo de identidad y la pérdida de privacidad.

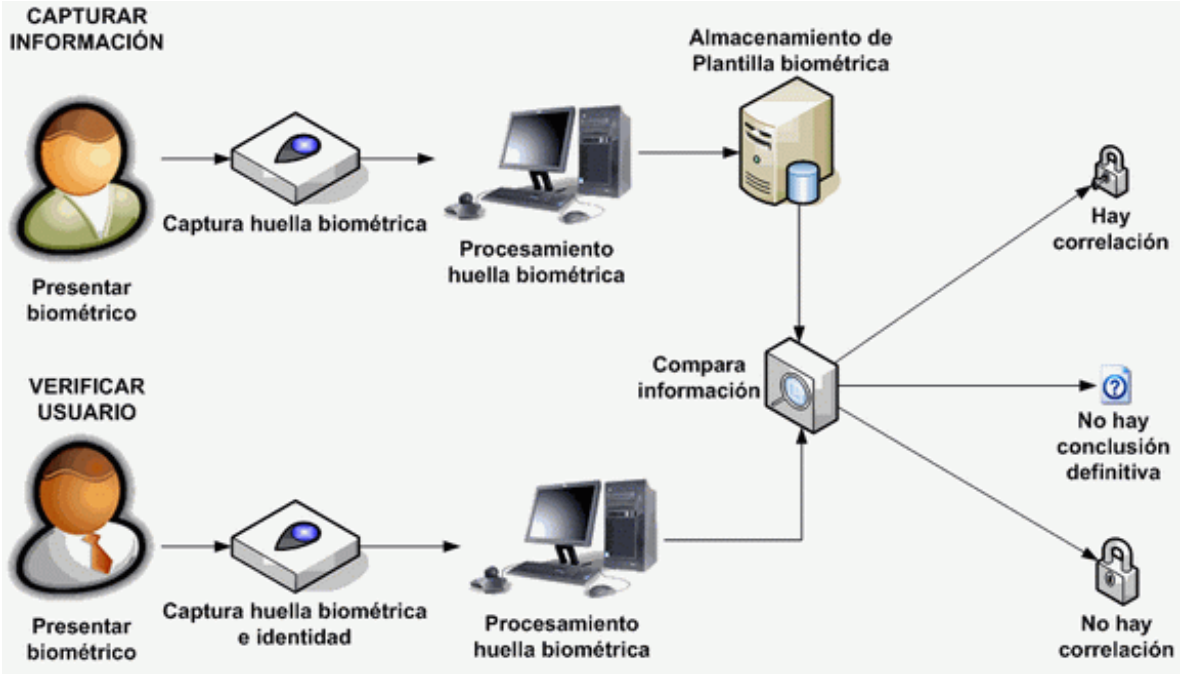
Durante años las empresas han dedicado tiempo, dinero y esfuerzo para proteger el acceso a la información y datos personales de sus clientes mediante métodos como la encriptación o el enmascaramiento de datos. Sin embargo, la seguridad en la vida digital de las personas se encuentra en riesgo ya que, en su mayoría, el acceso a las cuentas se valida mediante contraseñas, las cuales son cada vez más vulnerables.

En la última década, los expertos en seguridad informática han empezado a trabajar en la integración de nuevos métodos de autenticación donde los rasgos de una persona se utilicen como método de identificación. A este método se le conoce como biometría y lo podemos observar en los dispositivos móviles principalmente, ya que la tecnología inteligente de los teléfonos incluye sensores que permiten reconocer la huella y los rasgos faciales de los usuarios.

¿Qué es biometría?

La aplicación de la biometría en el mundo de la tecnología generó un nuevo campo de investigación llamado biometría informática, la cual se enfoca en el análisis y medición de las características fisiológicas y de comportamiento de un individuo mediante el uso de dispositivos biométricos para verificar la identidad de los individuos, un ejemplo, es el proceso que se lleva acabo para verificar la identidad de una persona basado en experiencias de la vida diaria. Cuando vemos la cara de una persona, nuestro cerebro trata de verificar que los rasgos de la persona se encuentren registrados en nuestra memoria. En caso de que el cerebro encuentre coincidencias, nos informa que es una persona que conocemos; en caso de que no encuentre muchas coincidencias, nos informa que es alguien que no conocemos.

Dispositivos Biométricos



En la actualidad existen biométricos especializados en identificar características físicas de las personas (huellas, manos, rostro, iris, retina) y biométricos especializados en características de comportamiento (voz, firma, teclado).

El proceso de identificación que siguen la mayoría de biométricos es:

- Registro de datos
- Procesamiento de los datos
- Almacenamiento
- Autenticación o rechazo

Proceso de identificación de biométricos

Seguridad Biométrica

La seguridad biométrica hasta hace unos años era exclusiva de sectores particulares que podían pagar altos costos por la obtención, mantenimiento e implementación de dispositivos biométricos. En la actualidad, podemos observar que la biometría se presenta en millones de dispositivos electrónicos. Esto ha abierto una brecha para la seguridad informática, la cual ha sido aprovechada por sectores financieros, aeropuertos, instituciones de gobierno como lo son los Afores, empresas de desarrollo de software, entre muchas otras.

Por ejemplo, en aeropuertos de países como Ámsterdam, Reino Unido y cajeros de Canadá se ha empleado el registro de la información del iris (estructura en forma de disco que da el color característico al ojo), para proteger la identidad de las personas.

La biometría ha demostrado ser la manera más confiable para la protección de información sensible y evitar fraudes. Lo cual ha logrado generar la confianza y comodidad suficiente de los usuarios para compartir sus datos biométricos.

Biometría o Contraseña

Son muchas las personas que se sienten cómodas y beneficiadas con el método de desbloqueo de cuentas y dispositivos mediante el uso de la huella dactilar y el reconocimiento facial, ya que les evita estar generando e ingresando nuevas contraseñas y patrones. Sin embargo, los expertos temen que se pierda el concepto de biometría, el cual es autenticar la identidad de una persona (reconocer a una persona a través de sus rasgos físicos con fines que no son exclusivos de la protección de datos) y se empiece a pensar en ella como una clave de acceso (finalidad es proteger datos).

Diferentes conceptos

Una de las mayores diferencias que se plantean en cuanto a la viabilidad de ambos métodos es que la biometría es un método difícil de hackear por basarse en rasgos físico, y una contraseña es más fácil de hackear porque, al ser difíciles de recordar, los usuarios generan contraseñas fáciles de descifrar. Esta gran ventaja también se puede ver como una desventaja porque, en caso de que los datos biométricos de una persona se obtengan, no hay posibilidad de cambiarlos, como se puede hacer con una contraseña. Siguiendo este punto, el peligro de sustraer los datos biométricos de los usuarios representa una de las mayores desventajas de la biometría, ya que se piensa que pueden ser utilizados para realizar actos de delincuencia no sólo virtuales, sino también físicos.

La seguridad biométrica plantea un nuevo método en la rama de la seguridad informática que día a día está logrando probar ser la mejor opción para la protección de datos, tanto por ser sencillo de utilizar (no se pierde, no se olvida) como por basarse en los rasgos únicos de una persona como llave de acceso.

Por ahora, los expertos en seguridad informática plantean que la estrategia más óptima para la protección de datos no es elegir entre utilizar una contraseña rebuscada y complicada, un sistema biométrico o cualquier otro método de autenticación, sino la combinación de los mismos.

En PRAXIS contamos con ciertas aplicaciones en el mercado que cuentan con biometría para poder agilizar sus trámites una de estas es **contrato electrónico** (Creado principalmente con formularios, escaneo de documentación, reconocimiento óptico de caracteres (OCR) y biometría (huella electrónica, firma autógrafa, voz y reconocimiento facial) – características que ampliaremos a continuación- el documento electrónico puede contar con cualquier funcionalidad que lleve a automatizar los procesos de trabajo internos de la compañía, mejorando la experiencia de los usuarios y revolucionando la forma de trabajo.

Utilizando factores de identificación como las *huellas dactilares*, un mensaje de voz o la *firma digital*, al momento de iniciar sesión, acceder a un documento, solicitar permisos o autorizar procesos, la biometría es una de las herramientas hoy en día más eficientes para realizar procesos de identificación y *autenticación* empresarial.

Según cálculos de *Juniper Research "(empresa que ofrece inteligencia de mercados), el 80% de los móviles tendrán hardware biométrico en 2023, contando con reconocimiento facial y escaneado de iris."*

¿Estarías dispuesto a poner en manos de la seguridad biométrica la información de tus cuentas bancarias y/o personales?