SEGUROS

Datos biométricos

Centro de Protección Digital

Autenticación con datos biométricos

La biometría es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas.

La autenticación biométrica es el uso de características biológicas de una persona, **como la retina, el iris, patrones faciales, venas de las manos, la geometría de la palma de la mano, la huella dactilar, la voz, entre otros,** que sirven para verificar la identidad de esta.
La configuración de datos biométricos es otra de las opciones para configurar la seguridad de nuestros dispositivos y forma parte de la autenticación multifactorial o de doble factor. Se considera un remplazo frente al uso de las contraseñas y el problema que conlleva recordarlas.

Al configurar los datos biométricos, **estos datos quedan almacenados en las bases de datos privadas de cada compañía fabricante de dispositivos como Apple, Huawei, Samsung, etc.** Por políticas de privacidad, estás empresas no divulgarán la información confidencial que ellos recopilan.

Sin embargo, dependiendo del país donde se encuentre la empresa y su gobierno, este podría solicitarle datos de personas a estas empresas, como ya lo han realizado algunos gobiernos en ocasiones.

Puntos fuertes y puntos débiles de la autenticación biométrica

La autenticación a través de la biometría, permite autenticarnos frente a sistemas o aplicaciones con el **"algo que somos",** es decir, una parte de nuestro cuerpo.
Por ejemplo, biometría puede ser nuestros ojos, huella digital, voz, rasgos faciales, e incluso la firma manuscrita y la geometría de la mano.

Con el paso del tiempo, el hardware necesario para la biometría es cada vez más económico, sin embargo, sigue teniendo un costo elevado. **Una autenticación biométrica fiable debería cumplir algunas características:**

- **Universal:** cualquiera lo puede usar.

- **Diferenciador:** **certeza al 100%** de que somos quien decimos que somos, que no tenga falsos positivos ni falsos negativos.

- **Permanente:** que los rasgos que se miden no cambien con el paso del tiempo, por ejemplo, **la huella dactilar puede cambiar en algunas personas con el paso del tiempo, en el caso de que se trabaje en el sector de la construcción.**

- **Accesible:** los datos requeridos deben ser fáciles de recoger, que no haya que **«entrenar»** demasiado al software biométrico.

- **Errores biométricos:** **Tasa de fraude vs. tasa de insulto.** Este aspecto es fundamental para tener un buen sistema biométrico. La tasa de fraude son los falsos positivos, es decir, alguien que se hace pasar por nosotros se autentica en el sistema, y automáticamente **«pasa»** como legítimo. La tasa de insulto es lo contrario, nosotros intentamos autenticarnos en el sistema, y nos indica que no somos quienes decimos que somos.

Una de las composiciones más seguras, es entrar a un sistema a través de una combinación de **"algo que somos", "algo que sabemos" y "algo que tenemos".** El "algo que somos" significa utilizar biometría, el "algo que sabemos" son las contraseñas típicas que utilizamos en la mayoría de los servicios, y el "algo que tenemos" pueden ser tarjetas identificadoras, o nuestro Smartphone para autenticarnos con un código TOTP (código aleatorio que cambia en cierto tiempo, por ejemplo, la clave dinámica). Si utilizamos solamente uno de los métodos, el sistema no es del todo seguro, **siempre es recomendable como mínimo tener una combinación de dos (autenticación de dos factores).**[1]

Riesgos

Al igual que en otros factores de autenticación, existen algunos riesgos asociados a su uso:

1. **Robo de información:** En este caso el riesgo es aún mayor que con otros tipos de datos ya que podría ser utilizada indiscriminadamente, no solo para acceder a dispositivos sino para otros fines fraudulentos, sin posibilidad de controlar la situación o revertirla ya que no pueden cambiarse, como lo hacemos en el caso de las contraseñas. **Es decir, nuestra biometría es única y no puede reemplazarse.**

2. **Violación a la privacidad:** Compañías como Facebook, utilizan la **biometría facial para identificar automáticamente a las personas en las fotos.**

3. **Tracking y venta de datos:** Existen aplicaciones que piden acceder a toda nuestra información sin ser necesario para el funcionamiento esperado de la misma. Las compañías dueñas de dichas aplicaciones suelen realizar **venta y tracking con los datos a los que acceden.**

4. **Robo del dispositivo:** ya que se tendría acceso a la información, incluyendo los datos biométricos.

Buenas prácticas:

1. Proporcionar el menor número de datos biométricos, en la medida de lo posible.

2. Utilizar el servicio de **autenticación biométrica** como método secundario de protección que complemente otros métodos de seguridad.

3. Descargar aplicaciones únicamente en los centros de aplicaciones autorizados como **Google Play Store o AppStore.** Recuerda revisar los permisos que solicitan antes de descargarlas, cuando detectes abusos o que te solicitan permisos innecesarios, evita descargarlas.

4. Estar al tanto de la política o aviso de privacidad de las aplicaciones, con el objeto de informarse sobre los datos biométricos y el tratamiento de estos, para tomar decisiones más informadas al respecto.

5. Los ordenadores y dispositivos usados para el almacenamiento de los datos biométricos deberán mantener sus sistemas y aplicaciones actualizados.

¡Aprende más con el
Centro de Protección Digital SURA!

Conócenos aquí

[1] https://www.redeszone.net/tutoriales/seguridad/identificacion-biometrica-riesgos-seguridad/