ECIJA

NOTA INFORMATIVA

Tecnologías biométricas seguras para el control de acceso

El Centro Criptológico Nacional (CCN) ha publicado recientemente una Píldora tecnológica relativa a "Tecnologías biométricas seguras para el Control de Acceso", en la que analiza las posibilidades de uso de esta tecnología, cuyo uso recomienda, destacando el alto grado de seguridad y confianza alcanzado por algunas de las técnicas de bioidentifcación.

Lo que necesitas saber:

- El CCN destaca el alto grado de seguridad, fiabilidad y confianza alcanzada por algunas técnicas de bioidentificación, **concretamente los sistemas de control de acceso basados en la obtención de una plantilla biométrica RBR cuyas características consiguen dar cumplimiento a la normativa vigente en protección de datos.**

- Aunque el CCN evita la confrontación de criterios con la AEPD, **este documento pone en tela de juicio, sobre la base de fundamentos técnicos robustos, muchos de los riesgos identificados por la AEPD en relación con el uso de la biometría.**

- No obstante, y a pesar de que el CCN emite **argumentos técnicos que permiten refutar algunas de las afirmaciones y criterios que han servido hasta la fecha para vetar el uso de la biometría en los sistemas de control de acceso**, este documento carece de un carácter normativo que permita generar seguridad jurídica en las entidades que pretendan implantarlo.

La tecnología biométrica, es entendida como aquellos procesos automáticos que tienen en cuenta las características biológicas y/o de comportamiento para verificar y autenticar los datos de una persona, con el fin de identificarla y permitir, por ejemplo, el acceso a instalaciones, sistemas o aplicaciones.

El Centro Criptológico Nacional (CCN) a través de su departamento de Productos y Tenologías de Seguridad TIC ha publicado, en el mes de diciembre de 2024, una "Píldora Tecnológica" denominada "**Tecnologías biométricas seguras para el control de acceso**" en la que analiza el grado de madurez alcanzado por la identificación por medios biométricos, y el grado de seguridad y confianza que permite esta tecnología en la actualidad.

Resalta que, a través del uso de la biometría, se ha llegado a conseguir un alto grado de eficacia, pero su uso ha de garantizar un alto nivel de fiabilidad, privacidad y seguridad.

En este contexto, se refiere específicamente al uso de las denominadas "Renewables Biometric References" (RBRs) o "plantillas biométricas RBRs" como medio para el reconocimiento de personas, que son objeto de estandarización en la ISO/IEC 24745:2022, y cuyo uso garantizaría la privacidad, confidencialidad, integridad, revocabilidad y renovación de los datos biométricos y su evaluación.

En concreto, **el CNN considera que el uso de estos sistemas de control de acceso basados en la obtención de una plantilla biométrica RBR sería conforme con la normativa de protección de datos**, gracias a que reúnen las siguientes características:

- **Irreversibles:** las RBRs se asemejan a las funciones hash, en el sentido de que no pueden invertirse el proceso de su creación para la obtención de los datos brutos originales que dieron lugar a las mismas.
- **Anónimas:** No contienen características biométricas concretas del individuo, si no datos derivados de las mismas.
- **Privadas:** No es posible conocer la identidad de la persona, aunque se tuviera acceso a la plantilla biométrica RBR.
- **No interoperables:** Cada plantilla biométrica RBR se genera de forma única y asociada al caso de uso o aplicativo específico.
- **Uso controlado:** Su uso limitado, por lo que solamente podrán ser utilizadas de manera eficaz por el individuo al que pertenezcan.
- **Renovables:** La obtención de la plantilla depende del algoritmo biométrico utilizado, los cuales podrán parametrizarse, modificarse o renovarse.
- **Cifrado en origen:** incorporan mecanismos de cifrado, lo cual supone una capa adicional de protección.

EL CNN enfatiza, igualmente, que para el **Reglamento Europeo de Inteligencia Artificial (RIA)** un sistema de reconocimiento biométrico no remoto en el que existe participación del usuario representa un **riesgo bajo o nulo** respecto a los derechos fundamentales y la seguridad de los ciudadanos.

Adicionalmente, el CCN recomienda, para las entidades sujetas a la aplicación del nivel alto de seguridad de ENS, el uso de sistemas de control de acceso basados en el uso de plantillas biométricas RBR (u otras que puedan surgir en un futuro que presenten protecciones equivalentes), evaluados y certificados conforme a las normas y estándares nacionales e internacionales sobre la materia.
No obstante, ha de tenerse en cuenta que esta recomendación se recoge en una Píldora Tecnológica, **que no tiene carácter normativo**, lo que no sirve para generar seguridad jurídica en relación con el uso de esta tecnología, cuya licitud ha sido puesta en duda reiteradamente por parte de la Agencia Española de Protección de Datos (AEPD).

A este respecto, ha de considerarse que, aunque el CCN evita confrontar con estos criterios de la AEPD, **este documento pone en tela de juicio, sobre la base de fundamentos técnicos robustos, muchos de los riesgos identificados por la AEPD en relación con el uso de la biometría.**

En particular, es relevante que el CCN considera, que para obtener un nivel de seguridad equivalente al ofrecido por un sistema de control de acceso biométrico sería necesario implantar un proceso de revisión manual de la autenticidad del documento de identidad del portador, así como de la correspondencia del documento con la persona que lo porta, lo que supone una clara divergencia con las manifestaciones de la AEPD en las que interpreta que ese grado de seguridad podría alcanzarse con el uso de tarjetas individuales de acceso.

Por tanto, esta publicación aporta **argumentos técnicos respaldados por una institución con la autoridad y relevancia suficientes como para permitir refutar algunas de las afirmaciones y criterios que han servido hasta la fecha para vetar el uso de la biometría en los sistemas de control de acceso**, pero carece de un carácter normativo que permita generar seguridad jurídica en las entidades que pretendan implantarlo.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60