CN-PYTEC
centro criptológico nacional

CCN-TEC 013

Tecnologías Biométricas Seguras para el Control de Acceso

CCN
centro criptológico nacional

Diciembre 2024

Edita:

CCN-PYTEC

© Centro Criptológico Nacional, 2024

Fecha de Edición: diciembre de 2024

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.12.05 16:25:07 +01'00'

ÍNDICE

1. INTRODUCCIÓN

1. El **control de acceso** es un componente crucial en la seguridad, ya que determina quiénes pueden acceder a datos, aplicaciones, recursos o instalaciones, y bajo qué circunstancias. Los mecanismos de control de acceso protegen tanto los espacios físicos como los digitales. En resumen, permiten que las personas adecuadas entren y evitan que las personas equivocadas lo hagan.
2. Las **directivas de control de acceso** se basan en técnicas como autenticación y autorización. La autenticación verifica explícitamente que los usuarios son quienes dicen ser, mientras que la autorización otorga el nivel adecuado de acceso según el contexto, como el dispositivo, la ubicación y el rol.
3. En términos más simples, el control de acceso implica **verificar la identidad** de un usuario según sus credenciales y luego **autorizar** el nivel de acceso apropiado una vez que se ha autenticado. Es fundamental para garantizar la seguridad y la privacidad en sistemas y entornos diversos.
4. Una vez que se ha autenticado la identidad de un usuario, **las directivas de control de acceso** otorgan permisos específicos y permiten al usuario proceder como desea. Contraseñas, PIN, tokens de seguridad, o características biométricas, son credenciales que se utilizan comúnmente para identificar y autenticar a un usuario.
5. En lugar de gestionar los permisos manualmente, la mayoría de las organizaciones impulsadas por la seguridad recurren a soluciones de gestión de identidades y accesos **para implementar directivas de control de acceso**.
6. Los dos principales mecanismos para implementar el servicio de control de accesos son:
    - el basado en atributos y
    - el basado en la identidad.
7. El primero es el control de acceso que se basa en **atributos** relacionados con sujetos, objetos, objetivos, iniciadores, recursos, o con el entorno. Una regla de control de acceso permite o deniega el acceso en base a un conjunto de valores de los atributos. [NIST-SP800-53[1]]
8. En el control de acceso basado en la **identidad** del usuario, típicamente se emplea alguna característica del proceso que requiere el acceso actuando en nombre del usuario final. Los derechos de acceso se conceden en base a la identidad declarada. [NIST-SP800-53], en este sentido, **define el "control de acceso" como un mecanismo que en función de la identificación ya acreditada permite acceder a datos, recursos o instalaciones**.

[1] NIST-SP800-53 Rev 5 Security and privacy controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

2. TECNOLOGÍAS BIOMÉTRICAS

9. Según ISO 2382-37[2], **la biometría es "el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento"**.

10. La tecnología biométrica se refiere a aquellos procesos automáticos que tienen en cuenta aspectos físicos de las personas como la huella dactilar, el reconocimiento facial o el escáner de iris, o aspectos de comportamiento como el reconocimiento de voz o la firma manuscrita, entre otros. Su objetivo principal es verificar y autentificar los datos de una persona. Estas tecnologías utilizan características únicas e intransferibles de cada individuo para identificarlos y permitir su acceso a instalaciones, sistemas o aplicaciones.

11. Algunos de los datos biométricos más reconocidos incluyen: huellas dactilares, voz, iris, o rasgos faciales.

12. En general, los sistemas **biométricos para el control de acceso** son productos de composición modular con funcionalidades diferenciadas: módulo de captura de datos, módulo de procesamiento y módulo de comparación. Por ejemplo, en el caso del reconocimiento facial, el proceso es como sigue:

1. **Captura**	Un sensor, en este caso una cámara, procede a la captura de la imagen de una persona. La imagen puede mostrar a la persona de frente o con cierto ángulo respecto a la cámara.
2. **Procesamiento**	Una vez capturada, la imagen se analiza y se procesa en varias etapas para obtener el vector de características biométricas. En primer lugar, se realiza una segmentación para localizar dentro de la imagen la información útil, es decir, se obtiene el rostro de la persona. A continuación, se realiza la extracción de características. Tradicionalmente, se obtenían medidas de la geometría del rostro, considerando factores como la distancia entre los ojos, la profundidad de las cuencas oculares, la distancia desde la frente hasta el mentón y la forma de los pómulos, labios, orejas y mentón, etc. El objetivo era identificar puntos de referencia faciales clave -**características biométricas**- para distinguir de forma única un rostro. Finalmente, un proceso matemático (**algoritmo biométrico**) transformaba la información capturada (puntos de referencia faciales – datos biométricos) en un conjunto de datos digitales basado en los rasgos faciales. El resultado de la fórmula matemática era un código numérico denominado **"vector de características" biométrico**. En el caso de que sea la primera vez que se genera este vector (registro de la persona), este vector se denomina **"huella facial", "template" o "plantilla"** y se almacena como referencia biométrica de los individuos autorizados en listas de control. No obstante, en la actualidad se utilizan métodos de aprendizaje automático (Machine Learning) o incluso aprendizaje profundo (Deep Learning). En este caso la plantilla no es un conjunto de características, sino los parámetros generados por una red neuronal y se le denomina **"model" o "modelo" biométrico**.

[2] ISO/IEC 2382-37:2022 Information technology – vocabulary – part 37: Biometrics.

3. **Comparación**	El **vector de características biométrico obtenido es comparado** con la plantilla biométrica de las personas autorizadas que se encuentran almacenados. Esta comparación no es una comparación absoluta, sino que se calcula un porcentaje de coincidencia (también llamado similitud o semejanza) o diferencia (scoring).

Tabla 1. Ejemplo del proceso de los sistemas biométricos para el control de acceso por reconocimiento facial

13. Mediante estas técnicas, en algunas modalidades, se llegan a conseguir un alto rendimiento a la hora de verificar a las personas con **tasas de falsos positivos** por debajo de 0.000001 y **tasas de falsos negativos** inferiores a 0.005. Esto significa que sólo un 0.0001% de las veces el sistema biométrico confunde a dos personas diferentes indicando que son la misma persona. Al mismo tiempo, se mantiene un nivel de conveniencia muy adecuado, donde sólo el 0,5% de las personas legítimas son rechazadas de forma incorrecta.

3. SEGURIDAD DE LAS TECNOLOGÍAS BIOMÉTRICAS

14. Hoy en día, los productos o sistemas biométricos para control de acceso son productos complejos en los que la **fiabilidad, privacidad y seguridad** son factores clave para su selección y adquisición.

15. Esta necesidad es especialmente relevante cuando se utilizan técnicas biométricas ya que el **template o plantilla biométrica es un código generado a partir de características fuertemente ligadas a medidas del cuerpo humano** o de su comportamiento y estas medidas son de carácter permanente.

16. Existe, un amplio marco técnico de normas que pueden ser utilizadas para evaluar y garantizar los requisitos de **fiabilidad, privacidad y seguridad** que la tecnología biométrica demanda. Por ejemplo las normas **ISO 24745**[3] e **ISO 30136**[4] establecen las principales recomendaciones técnicas para que los sistemas **biométricos puedan garantizar la privacidad, confidencialidad, integridad, revocabilidad y renovación** de los datos biométricos y su evaluación.

17. En concreto, la norma **ISO 24745** estandariza protecciones adicionales de seguridad a las plantillas biométricas creando las denominadas **"Renewables Biometric References (RBR)"** o "**plantillas biométricas RBRs**" que tienen las características siguientes:

    - **Multiplicidad**. Sobre cada rostro de una persona pueden obtenerse una cantidad casi infinita de plantillas "RBRs" distintas.
    - **Irreversibilidad**. Es imposible obtener a partir de una plantilla RBR los rasgos biométricos de una persona.
    - **No interoperabilidad**. Para cada caso de uso se crea una plantilla "RBR" específica partiendo de los mismos rasgos, pero utilizando factores de ordenación distintos.
    - **Revocabilidad**. En caso de compromiso de un sistema, las plantillas RBR pueden ser revocadas y sustituidas por otras.
    - **No permanencia**. La expresión numérica concreta de una plantilla "RBRs" se puede modificar mediante cambios en el sistema.

18. En la actualidad **se están redactando normas por parte del CEN (Comité Europeo Normalización) y por parte del ETSI (Instituto Europeo de Normas de Telecomunicaciones), sobre seguridad de la información biométrica, que siguen los mismos fundamentos tecnológicos que la Norma ISO 24745:2022** y que contemplan el cambio tecnológico operado en la biometría.

19. No obstante, hay que destacar que la utilización de estas protecciones puede suponer una degradación del rendimiento de los sistemas biométricos en sus tasas de fiabilidad, por lo que habrá que asegurar que la utilización de estas protecciones no supone una disminución de las tasas que alcanza la tecnología.

[3] ISO/IEC 24745:2022(EN) Information security, cybersecurity and privacy protection — Biometric information protection.

[4] ISO/IEC 30136:2018(EN) Information technology — Performance testing of biometric template protection schemes.

4. PLANTILLA BIOMÉTRICA RBR Y PROTECCIÓN DE DATOS

20. Los sistemas de control de acceso basados en la obtención de una plantilla biométrica RBR a partir de una determinada característica biométrica de la persona, cumplen con los exigido en materia de protección de datos por el Reglamento General de Protección de Datos[5] y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales[6], gracias a las siguientes características:

- **Irreversible.** La plantilla biométrica RBR resultante no puede invertirse para obtener los datos brutos originales utilizados (por ejemplo, la imagen facial del individuo) para su generación. La plantilla se asemeja al resultado de una función hash y como tal, es irreversible.
- **Anónimo**. La plantilla biométrica RBR no contiene ningún tipo de característica biométrica concreta (no representa la distancia entre ojos, el color de piel, el sexo, etc.), sino únicamente datos derivados de las mismas.
- **Privado**. No es posible conocer de qué persona se trata simplemente teniendo acceso a la plantilla biométrica RBR.
- **No interoperable**. No es posible emplear la plantilla biométrica RBR generada para un propósito distinto al establecido cuando se generó. Cada plantilla biométrica RBR se genera de forma única y asociada al caso de uso o aplicativo específico.
- **Uso controlado**: como consecuencia de lo anterior, las plantillas biométricas RBR son datos con una usabilidad limitada, y sólo pueden ser utilizadas eficazmente por el individuo al que pertenecen. Incluso en caso de posible robo, el impacto sobre el usuario es mínimo. La plantilla por sí sola no da acceso a ningún sistema.
- **Renovación:** Las características biométricas de una persona son inmutables, pero las plantillas biométricas RBR obtenidas a partir de dichas características no lo son. La obtención de la plantilla depende del algoritmo biométrico utilizado y de los mecanismos utilizados en su protección, que siempre puede parametrizarse, modificarse y/o renovarse. Dos algoritmos distintos producirán dos plantillas biométricas distintas a partir de los mismos datos biométricos.
- **Cifrado en origen:** Los sistemas biométricos que incluyen la generación de plantillas RBR, además de obtener la plantilla biométrica, suele incorporar mecanismos de cifrado, añadiendo una capa adicional de protección. La plantilla biométrica cifrada sólo puede ser descifrada por los propios mecanismos que la generaron.

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[6] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

5. PLANTILLA BIOMETRICA RBR Y REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

21. El nuevo Reglamento Europeo de Inteligencia Artificial (RIA)[7] distingue claramente, dentro de los sistemas biométricos, entre los de:
    - Reconocimiento biométrico, en el que se puede diferenciar:
        - Identificación biométrica.
        - Verificación biométrica.
    - Categorización biométrica (perfilado).
    - Reconocimiento o inferencia de emociones.
22. Los sistemas de inferencia de emociones y de categorización (salud, raza, orientación sexual, etc.) a partir de rasgos biométricos están prohibidos o considerados de alto riesgo en el nuevo RIA.
23. Sin embargo, **los sistemas de identificación biométrica no remotos en los que existe participación activa del usuario, así como los sistemas de verificación biométrica no están prohibidos y están calificados de riesgo bajo o nulo**.
24. El nuevo RIA considera que el uso de las tecnologías biométricas con la finalidad exclusiva de identificar a personas naturales, contando con su participación activa y en proximidad, mediante la comparación de sus datos biométricos con los contenidos en una base de datos de referencia – lista de control-, no representa un riesgo alto para los derechos fundamentales y la seguridad de los ciudadanos.
25. Y esto es así porque las plantillas biométricas RBR no permiten inferir ninguna de las características anteriormente mencionadas (raza, salud, etc.), al no poder invertirse para obtener los datos brutos originales.

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

6. BIOMETRÍA Y ESQUEMA NACIONAL DE SEGURIDAD

26. El Esquema Nacional de Seguridad (ENS)[8] , incluye entre las medidas de seguridad, varias relacionadas con el uso de la biometría para identificación y control de accesos.

27. En el ENS la biometría se considera como un factor de autenticación. Hay 3 tipos de factores de autenticación:

    (1) algo que se sabe, una contraseña o secreto;

    (2) algo que se tiene, un token o autenticador; y

    (3) algo que se es, una característica biométrica.

    Por ello, se contempla como **uno de los componentes que forma parte del sistema de identificación y autenticación de usuarios**, que es parte de la medida [op.pl.2 Arquitectura de Seguridad]. También aparece como refuerzo en las medidas [op.acc.5 Mecanismo de autenticación (usuarios externos)] y [op.acc.6 Mecanismo de autenticación (usuarios de la organización)]

28. Los métodos biométricos dificultan la usurpación y la réplica de contraseñas. Por otra parte, la utilización del **factor de inherencia** que es consustancial a la biometría, aporta una garantía de identidad real que no se pueden obtener de los factores de posesión o conocimiento, los cuales pueden ser cedidos o sustraídos por otras personas.

29. Los sistemas biométricos son el único mecanismo automático que permite acreditar la identidad real. Los sistemas basados en contraseñas (“algo que sabes”) o basados en la tenencia de un dispositivo (“algo que tienes”) no permiten acreditar que la persona que lleva a cabo el proceso de autenticación es realmente quien dice ser. Se trata de sistemas **basados en la presunción** de que la persona que conoce una contraseña o tiene un dispositivo es quien dice ser. Sin embargo, **el factor de inherencia** (“algo que eres”) está recogido como un factor que, combinado con los anteriores, aporta una capa más de seguridad y puede ser empleado en entornos con mayores exigencias.

30. Es evidente que desde el punto de vista de seguridad no es irrelevante que se produzca la suplantación de la identidad de una persona por otra que utilice sus “tarjetas, certificados, claves, tokens” bien por cesión o por sustracción a su verdadero titular. De hecho, en el ámbito presencial y digital se asiste en los últimos años a múltiples ejemplos de procesos de acreditación en los que **se ha producido una suplantación de la identidad**, y que no hubiera sido posible en caso **de combinar factores de posesión o conocimiento con factores de inherencia**.

[8] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/buscar/pdf/2022/BOE-A-2022-7191-consolidado.pdf

7. CASO DE USO ESPECIAL: CONTROL DE ACCESO A ESPACIOS FÍSICOS

31. La acreditación de identidad para el acceso a instalaciones o espacios físicos se puede llevar a cabo de forma manual o automática.

32. La acreditación de identidad de forma manual, con un nivel de equivalencia similar al biométrico, consiste en la revisión manual por parte de una persona de la autenticidad del documento de identidad del portador, así como de la correspondencia del documento con la persona que lo porta. Cualquier otra alternativa manual que no incluya lo anterior no supone una alternativa "equivalente".

33. En el caso de llevar a cabo el proceso de forma automática, como ya se indicó anteriormente, **el uso de tecnologías biométricas aporta garantías de inherencia**, a diferencia de otros medios basados en contraseñas o el uso de dispositivos físicos, cuyo uso sólo puede dar lugar a una identidad presunta (dado que pueden ser cedidas o robadas).

8. CONCLUSIONES

34. **La plantilla biométrica RBR** obtenida a partir de los rasgos (datos) biométricos es específica de una persona, pero **no es en absoluto única ni tampoco permanente**. Además, es **privada, irreversible, no interoperable, revocable y múltiple**.

35. Los mecanismos de control de acceso basados en la autenticación mediante comparación de una plantilla biométrica RBR dificultan la falsificación en comparación con otros métodos de autenticación, proporcionando una capa adicional de seguridad. **El factor de inherencia propio de la biometría** ofrece garantías de que la identidad es real, presentando ventajas significativas en comparación con factores de posesión o conocimiento que podrían ser cedidos o sustraídos por terceros.

36. El **reglamento europeo de Inteligencia Artificial**, que clasifica las aplicaciones de los sistemas de reconocimiento biométrico según el riesgo que puedan representar, califica las soluciones de **uso de la biometría** para el acceso con la intervención voluntaria del usuario y habitualmente en proximidad, **como de bajo o nulo riesgo** para los derechos fundamentales de las personas.

37. El Centro Criptológico Nacional recomienda para el nivel alto de seguridad 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.

9. REFERENCIAS

[1] NIST-SP800-53 Rev 5 Security and privacy controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

[2] ISO/IEC 2382-37:2022 Information technology – vocabulary – part 37: Biometrics.

[3] ISO/IEC 24745:2022(EN) Information security, cybersecurity and privacy protection — Biometric information protection.

[4] ISO/IEC 30136:2018(EN) Information technology — Performance testing of biometric template protection schemes.

[5] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[6] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

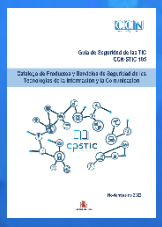
[8] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/buscar/pdf/2022/BOE-A-2022-7191-consolidado.pdf

CCN-PyTec
centro criptológico nacional

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

CPSTIC
CATÁLOGO DE PRODUCTOS Y SERVICIOS STIC

CATÁLOGO DE PRODUCTOS Y SERVICIOS DE SEGURIDAD TIC



PDF

ONLINE

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC

www.ccn.cni.es **https://oc.ccn.cni.es** **www.ccn-cert.cni.es**