Recomendaciones de Seguridad para Autenticación Multi-Factor

1. INTRODUCCIÓN

El concepto de **identidad digital** se puede entender como la representación única de un sujeto, en un contexto digital determinado. Por ejemplo, un sujeto puede tener una identidad digital para el servicio de correo electrónico y otra para acceder a un sitio web.

Existen muchos conceptos y procesos relacionados con la identidad digital. En el presente documento se tratan los relacionados con la autenticación.

La **Autenticación** es el proceso de verificar la identidad de un sujeto (usuario, proceso, aplicación o dispositivo), a menudo como paso previo para permitir el acceso a los recursos de un servicio o un sistema de información de una organización.

El Solicitante será el sujeto (usuario, proceso, aplicación o dispositivo) que solicita el acceso a un recurso o información de la organización y que deberá superar el proceso de autenticación.

Un **factor de autenticación** es una evidencia que sirve para demostrar al solicitante su identidad y, por lo tanto, superar la autenticación. Los factores de autenticación se dividen en tres (3) categorías:

- ***Algo que se sabe*.** La evidencia es algo que solo el solicitante puede saber. Por ejemplo, una contraseña o PIN.
- ***Algo que se tiene*.** La evidencia es algo que solo el solicitante puede poseer. Por ejemplo, una contraseña de un solo uso (OTP) o una clave criptográfica privada.
- ***Algo que se es*.** La evidencia es algo que solo el solicitante puede ser. En general, se trata de alguna característica biométrica, ya que se trata de información inherente al usuario.

Un **Autenticador** es un elemento que el solicitante posee y controla y que utiliza para autenticarse. El autenticador permite presentar uno o varios factores de autenticación. Por ejemplo, un dispositivo OTP presenta el factor de autenticación *"algo que se tiene*" al generar el código OTP. Si, además, para encender el dispositivo es necesario presentar la huella dactilar, también presenta "*algo que se es*".

Un **verificador** es la entidad que verifica si el solicitante está en posesión y control de los autenticadores necesarios para superar el proceso de autenticación, usando para ello protocolos de autenticación.

La **autenticación multi-factor (MFA)** es un proceso de autenticación que requiere de más de un factor de autenticación para que la autenticación sea exitosa y el solicitante obtenga acceso a los recursos o información solicitados. Para lograr la autenticación, deben ser correctos todos los factores presentados, si uno es erróneo, se deniega el acceso al sistema o servicio solicitado.

El método de MFA más utilizado es la autenticación de **dos factores (2FA)**. Se trata de autenticar a un usuario utilizando una combinación de **dos (2)** factores pertenecientes a **distintas categorías**.

La ventaja principal de utilizar autenticación multi-factor es que el compromiso de alguno de los factores de autenticación no es suficiente para que un atacante acceda de forma no autorizada a los recursos de la organización, ya que deberá obtener los demás factores. Hoy en día, con el auge de los ataques de phishing, ingeniería social, fuerza bruta o simple robo, es fundamental una autenticación multi-factor que utilice factores de distintas categorías, ya que cada categoría tiene sus fortalezas y distintas superficies de ataque.

En líneas generales, la autenticación será más robusta cuantos más factores utilice, pero es necesario llegar a un compromiso entre la seguridad, usabilidad, eficiencia y costes.

2. DIFERENCIAS ENTRE MFA Y AUTENTICACIÓN EN VARIOS PASOS

La autenticación en varios pasos es una aproximación en niveles, para acceder a recursos o a información cada vez más sensible. Se irá accediendo de forma secuencial realizando una autenticación cada vez que se acceda a un nivel. Cada nivel de autenticación permite el acceso con mayores privilegios que los niveles anteriores, hasta obtener el nivel de privilegios deseado. En este caso, cada nivel de autenticación puede utilizar un solo factor o MFA.

Un ejemplo común de autenticación en varios pasos se da cuando un solicitante puede acceder a un recurso haciendo uso de una contraseña, pero el sistema requiere una autenticación adicional (por ejemplo, un código OTP) para realizar cambios de configuración o de credenciales.

La autenticación en varios pasos mejora la seguridad respecto al uso de un solo factor, ya que añade protección adicional para accesos a acciones privilegiadas o a información sensible. Sin embargo, si no se requieren acciones privilegiadas y existe un solo nivel de acceso, presentará la misma debilidad que el uso de un solo factor.

Recomendación 1:

En aquellos casos en los que se elija utilizar autenticación en varios pasos para acceder a determinadas acciones privilegiadas o a información sensible, **se recomienda utilizar autenticación multi-factor** en el proceso inicial de autenticación del solicitante.

3. TIPOS DE IMPLEMENTACIÓN DE LA AUTENTICACIÓN MULTI-FACTOR

A través de la autenticación multi-factor se puede proteger el acceso desde la red interna o desde el exterior, a cualquier tipo de recurso o información de la organización.

Recomendación 2:

Se recomienda utilizar autenticación MFA para permitir acceso externo (desde fuera de la red interna) de solicitantes, a recursos o información de la organización.

También se recomienda implementar autenticación MFA al acceso, interno o externo, a cuentas privilegiadas, que son aquellas que proporcionan al usuario un alto nivel de permisos para poder realizar acciones privilegiadas y administrativas sobre los sistemas, servicios y aplicaciones de la organización.

La autenticación multi-factor se puede implementar de tres (3) formas:

- **Autenticación adaptativa o basada en riesgo**. Se asigna un valor de riesgo a la autenticación del usuario en función de su contexto, por ejemplo: la ubicación, dirección IP, tipo de dispositivo, navegador utilizado, etc. Se define a partir de qué valor de riesgo se piden factores de autenticación adicionales al usuario.
- **Autenticación basada en dispositivo autorizado**. El recurso al que se quiere acceder, mantiene un seguimiento de los dispositivos autorizados para un solicitante. Cuando el solicitante inicia sesión desde un dispositivo que no ha sido previamente autorizado, se le solicitarán varios factores. En caso de que el dispositivo sí esté autorizado y haya sido utilizado previamente, suele permitir habilitar la opción de "recordar mi dispositivo" para utilizar un único factor desde dicho dispositivo.
- **Autenticación MFA permanente por solicitante.** El recurso al que se quiere acceder requiere el uso de MFA cada vez que un solicitante solicite acceso.

Recomendación 3:

Se recomienda utilizar la autenticación multi-factor permanente por solicitante, de forma que los solicitantes deban **presentar siempre, todos los factores de autenticación**.

4. AUTENTICADORES

Un **autenticador** es algo que el solicitante posee y controla y que utiliza para autenticar su identidad, ya que permite presentar las evidencias o los factores de autenticación necesarios. Los autenticadores se pueden dividir en dos grupos:

- **Autenticadores de un solo factor**. Se trata de autenticadores que proporcionan un solo factor de autenticación y que, por lo tanto, deben ser combinados con otros autenticadores para lograr MFA. Por ejemplo, una contraseña, un dispositivo OTP simple, un certificado.
- **Autenticadores de varios factores**. Se trata de autenticadores que proporcionan varios factores, por lo que pueden ser utilizados por si solos como MFA. Por ejemplo, un dispositivo OTP de doble factor, que solo muestra los códigos tras validar la huella dactilar. O una clave privada que requiere de una contraseña para poder ser utilizada.

Recomendación 4:

Se recomienda utilizar **autenticadores físicamente separados** para aumentar la seguridad. De esta forma, el compromiso de un autenticador no afecta a los demás autenticadores.

Por ejemplo, el uso de credenciales usuario/contraseña junto a un dispositivo OTP, o el uso de biometría junto a notificaciones *push* en un dispositivo móvil.

A continuación, se incluye un esquema sobre los autenticadores que se describirán en el presente apartado.

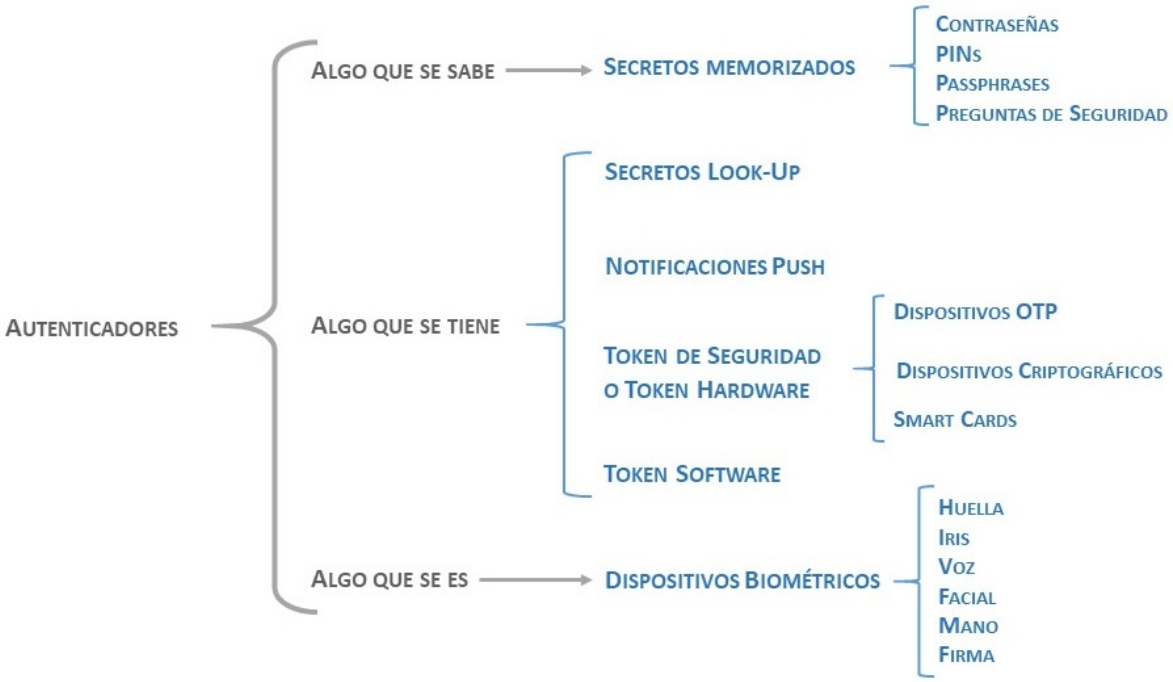


Ilustración 1. Esquema autenticadores

4.1. ALGO QUE SE SABE: SECRETOS MEMORIZADOS

El factor *'algo que se sabe'* está constituido por secretos memorizados por el solicitante y acordados previamente con el verificador, normalmente determinados por el solicitante. En esta categoría se encuentran las contraseñas, frases de contraseña (*passphrase*), las preguntas de seguridad y los PIN.

Las contraseñas y frases de contraseña, son combinaciones de letras, números y caracteres especiales de diferente longitud. Los PIN son combinaciones de números de diferente longitud. Las preguntas de seguridad son palabras o frases cortas, con la respuesta a la correspondiente pregunta.

Recomendación 5:

Se recomienda **utilizar como secreto memorizado las contraseñas**, utilizando una política de contraseñas adecuada. Añaden una mayor seguridad gracias a la combinación de los conjuntos de caracteres utilizados para crearlas, que junto a la longitud, dificulta los ataques de fuerza bruta o adivinación.

Se recomienda **no utilizar las preguntas de seguridad** (ni como factor de autenticación, ni como método de recuperación) ya que es la opción menos segura debido a que, mediante ingeniería social, se pueden obtener las respuestas a las preguntas configuradas.

Los secretos memorizados son el factor más extendido y utilizado actualmente. Los solicitantes están acostumbrados al uso de este tipo de factores, pero también presentan varias debilidades muy conocidas, como los ataques de phishing o de adivinación de contraseñas (ver Apartado 6. Ataques, amenazas y mecanismos de protección).

Para el uso seguro de secretos memorizados, se recomiendan una serie de requisitos que deben cumplir, por un lado, los solicitantes durante la generación de los secretos y, por otro lado, el sistema de verificación:

Componente	Recomendación
Secreto memorizado	Utilizar una longitud mínima. Se recomienda, al menos, 12 caracteres, formados por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
	Utilizar la concatenación de varias palabras para crear secretos largos.
	No contener datos del solicitante o de su contexto que sean fácilmente adivinables (como nombres o fechas).
	Ser diferentes a cualquier secreto utilizado anteriormente por el solicitante.
	Ser sustituidos si existe sospecha de que han sido comprometidos.
	Ser fáciles de recordar, buscando un compromiso entre la robustez y la facilidad de recordarse.
	No apuntarlos en papel o bajo otro procedimiento no seguro.
	No utilizar el mismo secreto para distintos servicios web o en el acceso a distintos dispositivos.
	Definir el tiempo de vigencia y expiración.
Sistema de verificación	Impedir el uso de secretos menores de 12 caracteres. Impedir el uso de secretos que no estén formados por caracteres de cada uno de los siguientes grupos: letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
	Ayudar al solicitante en la creación del secreto, mediante el uso de medidores de seguridad de la contraseña, recomendando modificarlo en caso de no alcanzar una seguridad alta.
	No ofrecer al solicitante mecanismos para recordar su secreto memorizado, como pistas o preguntas. Deshabilitar las funcionalidades de “recordar mi contraseña”.
	Comprobar el secreto con una “lista negra” de secretos inaceptables por ser ampliamente utilizados, ser fácilmente deducibles o por haber sido comprometidos. Por ejemplo, palabras de diccionarios, uso de caracteres repetitivos (“*aaa*”) o palabras relacionadas con el contexto. En estos casos, el sistema de verificación deberá rechazar el secreto e instar al solicitante a generar uno nuevo.
	Limitar el número máximo de intentos fallidos de autenticación, y establecer un mecanismo de bloqueo tras alcanzar el máximo, de forma que se impidan los ataques por fuerza bruta.

Componente	Recomendación
	Permitir al solicitante la función de "pegar" (*paste*), lo que facilitará el uso de gestores de contraseñas. Es recomendable que esta aparezca siempre ofuscada, dando la oportunidad de visualizar los caracteres únicamente si se considera un entorno confiable.
	Usar un canal protegido en el proceso de verificación.
	Los secretos de los solicitantes nunca deberán almacenarse en claro. Deberán usarse procedimientos seguros, de forma que los haga resistentes a ataques *offline*. Un procedimiento habitual es almacenar el *hash* del secreto utilizando un valor "*salt*" aleatorio y de, al menos, 32 bits. Dicho valor se concatena junto al secreto memorizado, antes de generar el hash. Las contraseñas y los valores "*salt*" se almacenarán, además, en bases de datos separadas.
	Ejecutar un programa de adivinación de contraseñas (*password-cracker*) dentro de las 24 horas tras el establecimiento de la contraseña, revocando las contraseñas que no superen dicha prueba.
	Analizar todas las contraseñas con un programa de adivinación de contraseñas al menos cada 30 días, revocando las contraseñas que no superen dicha prueba.
	Revocar las contraseñas de más de un año de antigüedad.

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador y el solicitante. El solicitante introduce manualmente el secreto memorizado en el verificador y este lo verifica, permitiendo o denegando el acceso.

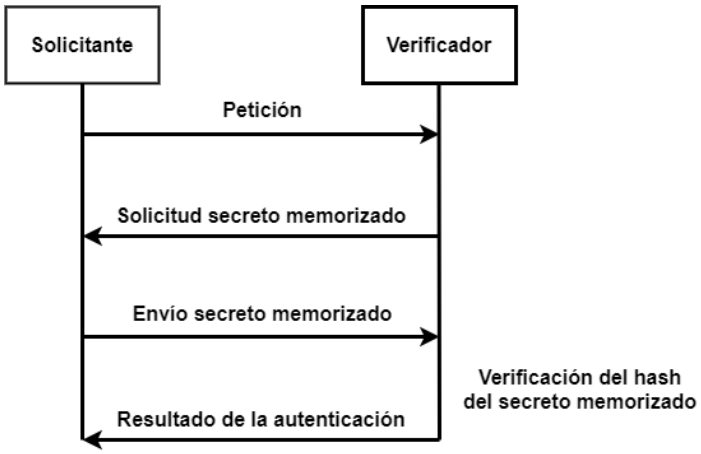


Ilustración 2. Diagrama de uso de secretos memorizados.

4.2. ALGO QUE SE TIENE

4.2.1 SECRETOS LOOK-UP

Son un conjunto de **secretos o códigos de un solo uso** acordados y compartidos previamente entre el solicitante y el verificador, y almacenados física o electrónicamente. Por ejemplo, solicitante y

verificador comparten un fichero con un conjunto de códigos generados aleatoriamente y ordenados. El verificador pide al solicitante el código de una posición concreta y comprueba que es correcto.

Para el uso seguro de secretos *Look-up*, se recomiendan una serie de requisitos que se deben cumplir en el proceso de generación, distribución, uso y almacenamiento de los secretos:

Ámbito	Recomendación
Generación	Tener al menos 20 bits de entropía[1].
Distribución	Utilizar canales seguros autenticados para la distribución de los códigos. Pueden ser entregados físicamente.
Uso	Cada secreto solo debe ser utilizado una vez.
Almacenamiento	**Los secretos de los solicitantes nunca deberán almacenarse en claro**. Deberán usarse procedimientos seguros, de forma que los haga resistentes a ataques *offline*. Por ejemplo, el uso del *hash* con un valor '*salt*' indicado en el apartado anterior para los secretos memorizados.

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador y un solicitante. El verificador indica la posición del código de un solo uso, tras lo cual el solicitante busca dicho código y lo introduce manualmente. Finalmente se verifica el código, permitiendo o denegando el acceso.

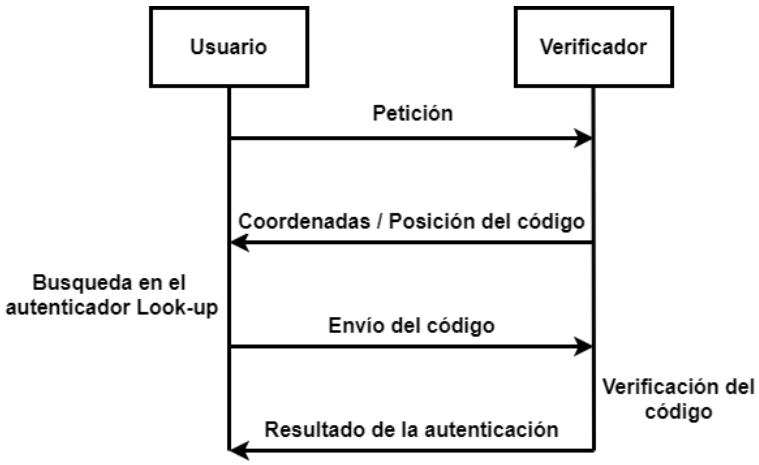


Ilustración 3. Diagrama de uso de secretos *Look-up*.

4.2.2 NOTIFICACIONES *PUSH*

Son **aplicaciones software** que, una vez vinculadas con la identidad de un solicitante, envían una notificación *push* al dispositivo configurado, que debe ser aceptada por el solicitante para permitir la autenticación.

[1] Recomendación del *NIST SP 800-63b Digital Identity Guidelines – Authentication and Lifecycle Management [REF5].*

Generalmente las aplicaciones se instalan en dispositivos móviles, y la notificación muestra información sobre la localización, hora y dirección IP desde la que se realiza el intento de autenticación. El solicitante logra una autenticación satisfactoria probando la posesión y control del dispositivo al aceptar la notificación recibida, tras comprobar la información.

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador, el solicitante y el autenticador. El verificador envía la notificación al autenticador y el solicitante la confirma para que, finalmente, el verificador permita o deniegue el acceso.

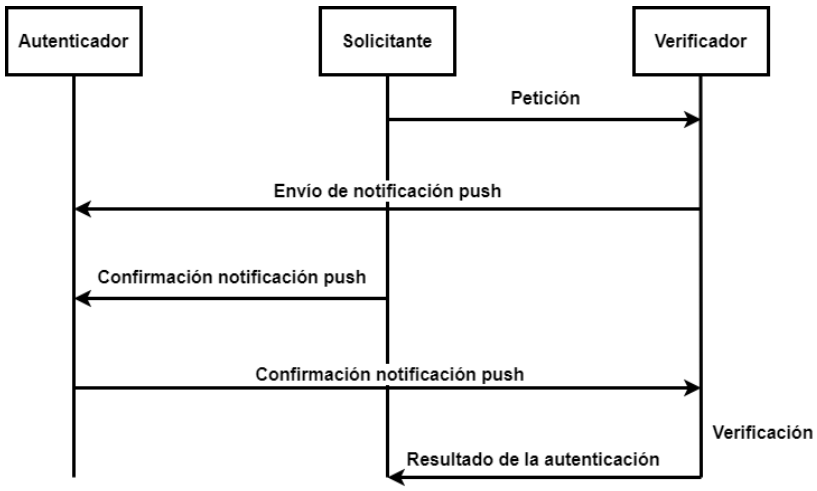


Ilustración 4. Diagrama de uso de notificaciones *push*.

4.2.3 TOKEN DE SEGURIDAD O TOKEN *HARDWARE*

Los *token* de seguridad son **dispositivos *hardware*** que generan, reciben o contienen almacenada la evidencia o factor que el solicitante debe presentar al verificador para la autenticación. Esta evidencia puede ser una contraseña, datos biométricos del solicitante, claves criptográficas, etc.

Hay tres (3) tipos de *token* de seguridad:

- ***Token* desconectados**. El dispositivo no requiere conexión ni física ni lógica con el verificador. El solicitante tendrá que introducir manualmente en el verificador (normalmente a través de un teclado), el código generado y mostrado en el dispositivo. Los *token* más utilizados dentro de esta categoría son los **dispositivos OTP**.
- ***Token* conectados**. El dispositivo requiere una conexión con el verificador. Mediante esta conexión, el *token* transmite la evidencia para autenticación al verificador. Esta conexión puede ser física, normalmente a través de puertos USB o lectores de *smart cards*, o puede ser lógica, con *bluetooth*, RFID o NFC. Este último tipo de conexión se denomina *contactless* y es muy utilizada para autenticación en puertas de entrada sin llaves. Los *token* más utilizados dentro de esta categoría son las ***smart cards*** y los **dispositivos criptográficos**.
- ***Token* out-of-band.** Normalmente, se trata de móviles que se comunican con el verificador utilizando un canal fuera de banda (*out-of-band*), como puede ser un SMS o una llamada de voz, a través del cual el verificador envía la evidencia que el usuario debe presentar al verificador por otro canal para la autenticación.

4.2.4 DISPOSITIVOS OTP

Son **dispositivos *hardware* de generación de códigos de un solo uso** (*One Time Password - OTP*).

Cuando el solicitante requiere autenticación, el verificador le pide el código OTP. El solicitante debe obtener este código de su dispositivo OTP e introducirlo en el verificador, que lo comparará con el que él ha generado, para lograr autenticarse con éxito.

Generalmente, el dispositivo OTP contiene un secreto que persiste durante todo su ciclo de vida, y que es necesario para la generación de los códigos OTP. Este secreto debe ser conocido por el verificador, y esto se logra con el proceso de vinculación. El intercambio del secreto entre el dispositivo OTP y el verificador, debe realizarse a través de un canal cifrado con autenticación.

Además del secreto, para la generación de los códigos OTP se utilizan otros valores que dependen del algoritmo de generación que se utilice. Los más extendidos son los basados en un contador (HOTP), y los basados en una variable temporal (TOTP):

- **HOTP (*HMAC-Based One Time Passwords*).** Es un algoritmo de generación de códigos OTP que utiliza la función HMAC-SHA1, a partir de un contador incremental y del secreto compartido, ambos conocidos previamente por el dispositivo y el verificador OTP. Dado que la salida del valor HMAC-SHA1 es de 160 bits, utiliza un truncado para obtener valores manejables por el usuario (de 6 a 10 caracteres decimales). Este algoritmo se especifica en la RFC 4226.
- **TOTP (*Time-Based One Time Passwords*).** Es una extensión del algoritmo HOTP que sustituye el contador incremental por un contador basado en tiempo. Utiliza dos parámetros fijos: la duración de una etapa temporal (por ejemplo, 30 segundos) y un tiempo inicial (T0) a partir del cual contar las etapas temporales. El contador que se va a utilizar en el momento de generar un código OTP, será el número de etapas temporales trascurridas entre el T0 inicial y el tiempo actual. De esta forma, los códigos generados solo son válidos durante un tiempo de vida limitado. Este algoritmo, además, puede usar funciones SHA-256 y SHA-512. Se especifica en la RFC 6238.

Los dispositivos OTP pueden ser de un factor o multi-factor. La diferencia consiste en si el dispositivo OTP requiere de algún factor de autenticación previo, para que el solicitante pueda acceder al código OTP. En este caso, se tratará de un dispositivo OTP multi-factor, donde el dispositivo es *algo que se tiene*, y el factor para acceder a él deberá ser *algo que se sabe* (por ejemplo, una contraseña), o *algo que se es* (por ejemplo, una huella digital).

El secreto compartido debe ser inaccesible y debe ser protegido frente a la modificación, tanto en los dispositivos OTP, como en los sistemas de verificación.

Recomendación 6:

Se recomienda el uso de **códigos OTP basados en tiempo (*time-based*)**, ya que los códigos generados tienen una duración temporal (cuanto menor sea ese período de validez, mayor será la fortaleza del algoritmo, por lo que se recomienda configurar períodos cortos). Además, el algoritmo TOTP usa la función SHA-256, que es más segura que SHA-1.

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador, un solicitante y un autenticador. El verificador solicita el código, el solicitante lo obtiene del autenticador y lo introduce manualmente en el verificador, el cual permite o deniega el acceso.

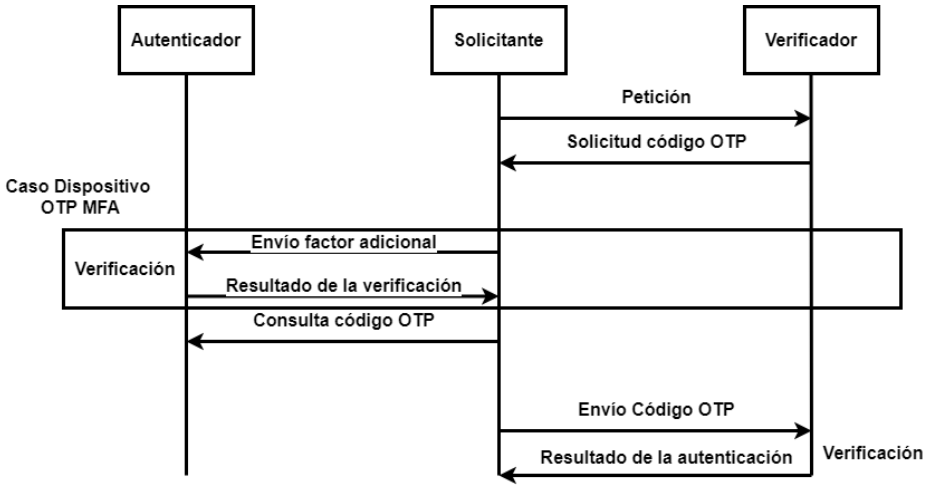


Ilustración 5. Diagrama de uso de dispositivos OTP.

4.2.5 DISPOSITIVOS CRIPTOGRÁFICOS

Son **dispositivos *hardware* que contienen una o varias claves secretas** (simétricas o asimétricas) que utilizan para realizar una operación criptográfica para la autenticación (normalmente una firma).

Estas claves secretas serán exclusivas del dispositivo. El verificador debe tener las correspondientes claves simétricas o asimétricas, para poder verificar la operación criptográfica realizada por el dispositivo.

El dispositivo y el verificador se comunican a través de un interfaz (por ejemplo, un puerto USB del equipo, al que el dispositivo criptográfico está conectado).

La operativa consiste en que el verificador genera un valor aleatorio (*nonce*) y se lo envía al dispositivo criptográfico, a través del interfaz. Este realiza la operación criptográfica, por ejemplo, firma el valor con su clave privada. El verificador recibe la salida del dispositivo y verifica la firma realizada con la clave pública asociada.

Uno de los dispositivos criptográficos cuyo uso se encuentra más extendido son las **tarjetas inteligentes** (*smartcards***)**. Se trata de tarjetas con un circuito integrado para almacenar y procesar información. La tarjeta inteligente almacena las claves secretas de forma segura y, tras conectarse con la interfaz del verificador, realiza y envía la operación criptográfica. Se dividen en dos (2) tipos, según su conexión con la interfaz de comunicación:

- Tarjetas inteligentes sin contacto. El dispositivo consta de una antena integrada para realizar la conexión remota con el lector y comunicarse con la interfaz.
- Tarjetas inteligentes de contacto. Requieren ser insertadas en un lector de tarjetas para comunicarse con la interfaz y realizar las operaciones.

Los dispositivos criptográficos también pueden ser de uno o varios factores:

- Dispositivos criptográficos de un factor. El dispositivo criptográfico no requiere ser activado y realiza la operación criptográfica cuando el verificador se lo solicita.
- Dispositivos criptográficos multi-factor. El dispositivo criptográfico requiere activación mediante un segundo factor de autenticación, para realizar la operación criptográfica. Por ejemplo, a través de una contraseña o algún factor biométrico.

Para el uso seguro de dispositivos criptográficos, se recomienda:

Componente	Recomendación
Dispositivo criptográfico	El dispositivo almacenará las claves secretas de forma segura, y no permitirá su extracción.
Sistema de Verificación	El sistema de verificación almacenará las claves secretas en una ubicación segura, especialmente protegidas contra el acceso no autorizado y la revelación.
Sistema de Verificación	El valor (*nonce*) enviado por el sistema de verificación debe tener, al menos, 64 bits de longitud y ser único para cada intento de autenticación.
Dispositivo criptográfico	El dispositivo debe ser activado por el usuario. Por ejemplo, pulsado un botón. Esto evita que el dispositivo pueda estar operando sin conocimiento del usuario cuando haya sido comprometido.

Recomendación 8:
Para sistemas bajo el alcance del ENS, deberán utilizarse algoritmos autorizados en la guía CCN-STIC-807. Estos son:

- Algoritmos simétricos: AES.
- Algoritmos de firma: RSA y ECC con funciones SHA-2 o SHA-3.

Deberán utilizarse claves que proporcionen una seguridad **equivalente a 112 bits o superior**. Y para aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS) de categoría Alta**, deberán utilizarse claves con una **seguridad equivalente a 128 bits**. Esto supone:

- Claves RSA 3072 bits o superiores.
- Claves ECC 256 bits o superiores.

Dispositivos o *Token* U2F

FIDO Alliance es una asociación abierta de la industria, que desarrolla y promueve estándares de autenticación segura. Uno de los estándares que desarrolla es **U2F/CTAP1**, que fue iniciado originalmente por Google. Este estándar promueve el uso de un dispositivo criptográfico (*FIDO security key*) como segundo factor, para la autenticación en aplicaciones y servicios de internet *U2F-enabled* (por ejemplo, Gmail, Dropbox, Facebook o Salesforce).

El dispositivo utiliza criptografía de clave pública de curvas elípticas (ECC). Genera un par de claves pública/privada para cada servicio online con el que queramos autenticarnos, durante el proceso de registro. Cuando se accede al servicio online, este solicita usuario y contraseña. Tras la

autenticación correcta con este primer factor, solicita la inserción del dispositivo criptográfico, que deberá activarse pulsando un botón. Los dispositivos U2F pueden realizar la conexión con el verificador mediante puertos USB, NFC o Bluetooth.

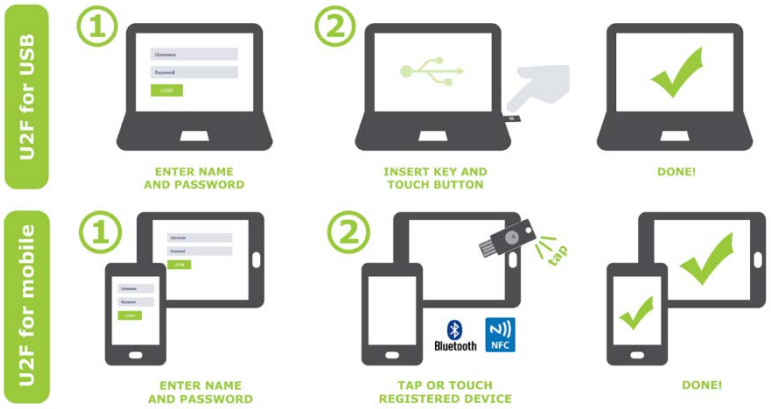


Ilustración 6. Funcionamiento de FIDO U2F/CTAP1[2].

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador, un solicitante y un autenticador. El solicitante conecta el autenticador al verificador y lo utiliza para firmar un mensaje con la clave privada. Se envía el mensaje al verificador, que utiliza la clave pública para comprobar dicha firma y permitir o denegar el acceso.

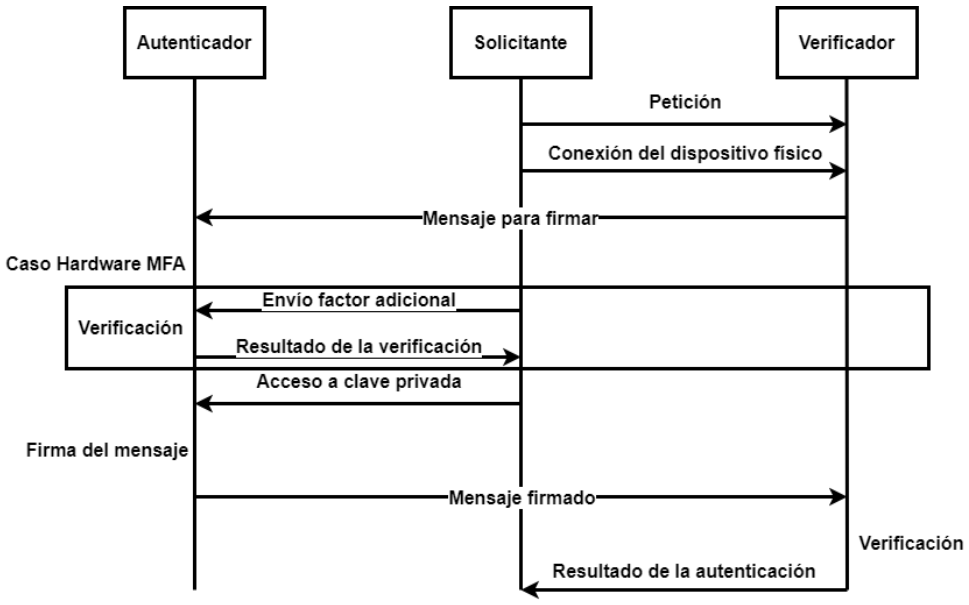


Ilustración 7. Diagrama de empleo de *hardware* criptográfico.

4.2.6 TOKEN *SOFTWARE*

Es un ***software* que genera o almacena evidencias o factores**, en dispositivos electrónicos de propósito general como equipos de sobremesa, portátiles, móviles o tabletas. Las evidencias pueden ser una contraseña, datos biométricos del solicitante, claves criptográficas, etc., y permiten la autenticación de un solicitante al ser presentadas al verificador.

[2] Esta figura, así como información sobre el estándar, se puede encontrar en la URL: https://www.yubico.com/authentication-standards/fido-u2f/#toggle-id-8

Funcionan de forma similar a los *token* de seguridad o *hardware*. Pueden generar códigos OTP o realizar operaciones criptográficas con claves secretas (*software* criptográfico).

Del mismo modo, pueden ser de un factor, o multi-factor. En este último caso, el *software* requiere un segundo factor para su activación. Normalmente se trata de una contraseña o de algún factor biométrico.

Los token *software*, a diferencia de los token *hardware*, tienen un riesgo mayor de recibir ataques software e infecciones de malware, debido a que están más expuestos a amenazas basadas en la duplicación del material criptográfico o de los secretos que contienen.

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador, un solicitante y un autenticador. El solicitante realiza una petición al verificador. En caso de tratarse de *software* de generación de códigos OTP, el solicitante consultará el código con el autenticador y lo introducirá manualmente en el verificador. En caso de tratarse de software criptográfico, el solicitante utilizará el autenticador para realizar la operación criptográfica y enviarla al verificador.

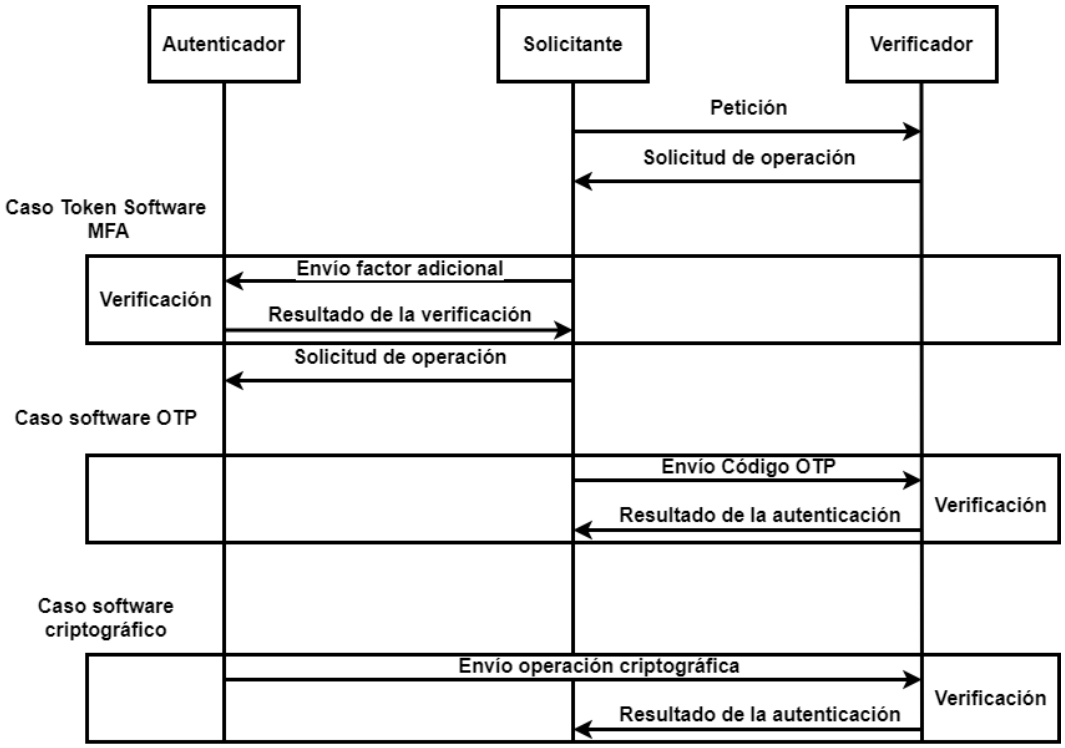


Ilustración 8. Diagrama de empleo de token *software*.

4.3. ALGO QUE SE ES: BIOMÉTRICOS

Esta categoría está formada por todos los factores biométricos, los cuales permiten el reconocimiento automático de características físicas o de comportamiento, de un solicitante.

Los sistemas biométricos utilizan dos (2) procesos:

- **Registro biométrico (*enrollment*).** Durante este proceso los solicitantes son dados de alta en el sistema. El sistema realiza una captura de los datos biométricos del solicitante, extrae los datos con los que trabaja y se asocian con la identidad del solicitante. Se almacenan como una

plantilla biométrica en una base de datos. Es recomendable autenticar al dispositivo o sensor biométrico antes de realizar la captura.

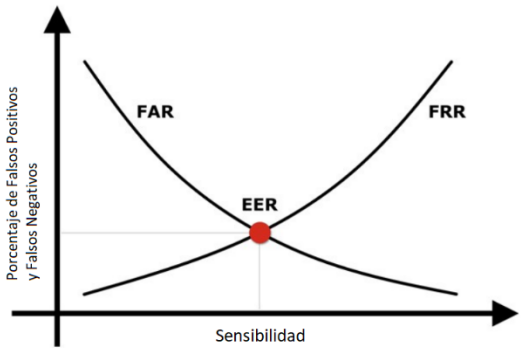
- **Verificación biométrica.** Durante este proceso el sistema valida la identidad de un solicitante. El solicitante introduce su identidad y presenta sus rasgos biométricos. El sistema realiza una captura y recupera de la base de datos la plantilla asociada a la identidad del solicitante. Compara la captura con la plantilla y genera un valor de similitud entre ambos datos. En base al grado de similitud, el solicitante es aceptado o rechazado. Es fundamental que el canal de comunicaciones entre el dispositivo biométrico y el verificador, sea un canal autenticado protegido.

La comprobación biométrica es probabilística, mientras que otros factores son deterministas. Esto significa que, al realizar la comprobación entre la plantilla y la captura actual, se verifica cómo de similares son los rasgos. Se establece un umbral, a partir del cual, si es superado, se determina que los dos rasgos corresponden al mismo solicitante. En caso contrario, se determina que corresponden a solicitantes diferentes. Este umbral representa la sensibilidad del dispositivo.

Entre los principales parámetros de un sistema biométrico se encuentran:

- **FAR (*False Acceptance Rate*)**. Tasa de falsos positivos. Un falso positivo es cuando se permite acceso a solicitantes que no están autorizados. La tasa de falsos positivos es el porcentaje de verificaciones autorizadas que, en realidad, no debían haberlo sido. Este parámetro debe ajustarse para evitar el fraude.
- **FRR (*False Rejection Rate*)**. Tasa de falsos negativos. Un falso negativo es cuando se deniega el acceso a un solicitante legítimo. La tasa de falsos negativos es el porcentaje de verificaciones no autorizadas que deberían haberlo sido. Este parámetro debe ajustarse para que no parezca que el sistema funciona erróneamente.
- **ERR (*Equal Error Rate*)**. Punto en el que las tasas FAR y FRR son iguales.

Los parámetros FAR y FRR dependen de cómo se ajuste la sensibilidad del dispositivo (el umbral). Cuando mayor sea el umbral, más sensible será el dispositivo y más falsos negativos se producirán. Cuando menor sea el umbral, menos sensible será el dispositivo y más falsos positivos se producirán. Es recomendable que el dispositivo biométrico tenga un FAR muy bajo pero es necesario evaluar también, cual es la tasa FRR para dicho FAR.



Recomendación 9:

Deberá **minimizarse el número de falsos positivos.** Se recomienda un FAR del 0.01% para sistemas de que exigen un nivel de seguridad medio y del 0.001% o inferior, para sistemas de un nivel de seguridad alto, conforme a lo definido en ISO / IEC 30107-1.

Para esos FAR, se recomienda que el FRR sea del 0.2% o inferior.

Uno de los principales ataques a los sistemas biométricos consiste en la presentación de datos biométricos artificiales o alterados al dispositivo biométrico, con objeto de interferir en su operación. Estos ataques se conocen como "ataque de presentación". Para prevenir este tipo de ataques, los dispositivos biométricos, especialmente cuando no son supervisados, deben disponer de un subsistema de detección de ataque de presentación o PAD (*Presentation Attack Detection*).

Recomendación 10:

Se recomienda que el dispositivo biométrico implemente un **sistema de detección de ataques de presentación** (PAD), detectando, al menos, un 90% de los mismos, de acuerdo a lo definido en la ISO/ IEC 30107-3.

Se recomienda implementar un **umbral de intentos fallidos de autenticación** con el consiguiente sistema de bloqueo, para impedir los ataques de fuerza bruta.

Existen diversos rasgos biométricos empleados en la actualidad. Cada uno presenta ciertas ventajas y desventajas. A continuación, se indican los más extendidos.

- **Huella dactilar.** Se ha demostrado que el rendimiento de los sistemas basados en huella dactilar es muy alto. Además, es un rasgo altamente distintivo de cada individuo. El coste de los sensores de huella dactilar es bajo y son fácilmente integrables en numerosos aparatos electrónicos. La principal desventaja de este rasgo biométrico es que requieren de una gran capacidad computacional y que las huellas de una pequeña fracción de la población no pueden ser utilizadas debido a un excesivo deterioro de las mismas.
- **Iris.** Se ha demostrado que el iris es altamente distintivo para cada individuo y, además, es permanente e inalterable. La captura requiere participación por parte del usuario ya que debe situarse a una distancia y posición determinada del sensor. Suele ser extremadamente preciso y rápido, pero es una tecnología costosa.
- **Voz.** Es un rasgo biométrico muy aceptado y fácil de obtener. Las principales desventajas son que no es muy distintivo y es fácil de imitar. Además, se trata de un rasgo muy variable.
- **Rostro.** Es un rasgo biométrico también muy aceptado. La adquisición se realiza mediante una fotografía, por lo que es uno de los rasgos menos invasivos con el usuario. La principal desventaja es la posibilidad de utilizar máscaras, no detectables en sistemas no supervisados. Debe adaptarse a los cambios de aspecto con la edad, iluminación, expresiones y posición respecto a la cámara.
- **Geometría de la mano.** Se trata de un rasgo poco distintivo. Es necesario que el usuario sitúe la palma de la mano sobre un escáner. Su principal ventaja es que requiere muy poco almacenamiento y procesamiento, por lo que es una opción a tener en cuenta en sistemas con un ancho de banda o almacenamiento limitados.

- **Firma.** Es un rasgo muy aceptado. La principal desventaja es que la firma tiene un alto grado de variabilidad. Su identificación es compleja.

A continuación, se muestra una tabla con una comparativa entre las principales tecnologías biométricas y sus principales características[3]:

- **Universalidad**. Cómo de extendido está el uso de la tecnología.
- **Distintividad**. Cuánto varía la información biométrica de un individuo a otro.
- **Estabilidad**. Cuánto varía la información biométrica de un mismo individuo con el paso del tiempo. Un valor de estabilidad alto indica que la información varía poco con el tiempo.
- **Evaluabilidad**. Capacidad de medir cuantitativamente la característica biométrica.
- **Aceptabilidad**. Cómo de aceptado está su uso por los usuarios.
- **Vulnerabilidad**. Cómo de extensa es la superficie de ataque de la tecnología.

Rasgo biométrico	Universalidad	Distintividad	Estabilidad	Evaluabilidad	Aceptabilidad	Vulnerabilidad
Huella dactilar	Alta	Muy alta	Muy alta	Media	Baja	Media
Iris	Muy alta	Muy alta	Muy alta	Media	Baja	Alta
Voz	Alta	Media	Baja	Alta	Alta	Media
Rostro	Muy alta	Media	Baja	Media	Alta	Baja
Geometría de la mano	Alta	Media	Media	Alta	Media	Baja
Firma	Media	Media	Baja	Alta	Muy alta	Baja

Recomendación 11:
Se recomienda el **uso de sistemas biométricos basados en huella dactilar o en iris**.

Estos rasgos biométricos son los que permanecen más estables a lo largo de la vida del individuo, y son altamente distintivos de cada uno. Tienen también un alto grado de universalidad y rendimiento.

[3] Según la *'CCN-STIC-490 Dispositivos biométricos de huella dactilar'* [REF2]

A continuación, se muestra un diagrama con un ejemplo de las acciones entre el verificador, un solicitante y el autenticador. Pueden encontrarse dos (2) situaciones: que la verificación del escaneo biométrico se lleve a cabo en el autenticador o que se lleve a cabo en el verificador.

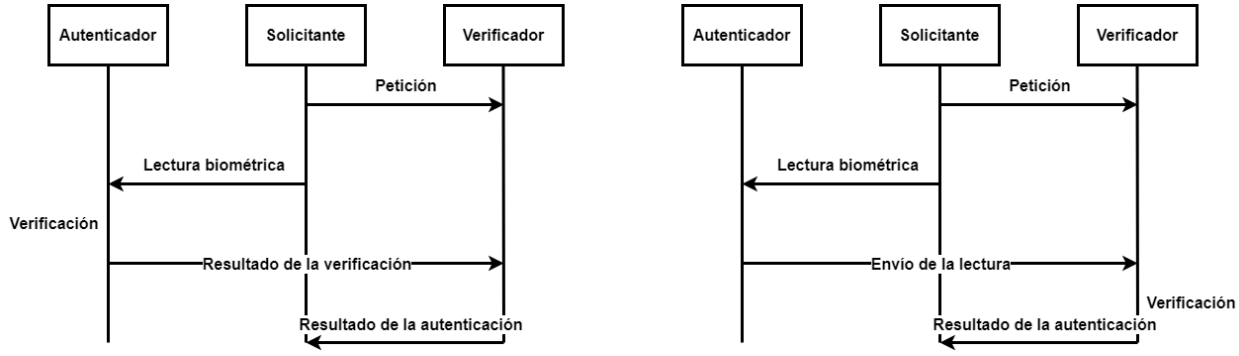


Ilustración 9. Diagrama de empleo de sistemas biométricos.

Cuando la verificación se lleva a cabo en el mismo dispositivo utilizado para el escaneo (autenticador), las plantillas biométricas se almacenan en este dispositivo. En este caso, los datos biométricos no se centralizan ni se muestran al exterior. Sin embargo, se pierde control sobre dichos datos y existe el riesgo de pérdida o compromiso de los dispositivos, lo que provocaría la pérdida o divulgación de los datos.

Cuando el verificador es un dispositivo aparte, las plantillas biométricas están almacenadas en él de forma centralizada. El autenticador realiza el escaneo y lo envía al verificador para su comprobación. En este caso se tiene mayor control sobre los datos y se facilita la gestión.

Recomendación 12:

Se recomienda que el **sistema de verificación sea un sistema centralizado** en la organización, de forma que las plantillas se almacenen en una base de datos centralizada, con protección frente a accesos y modificaciones no autorizadas. Las comunicaciones entre el dispositivo biométrico y el verificador deberán realizarse a través de canales seguros autenticados.

4.4. AUTENTICADORES PARA EL ENS

Recomendación 13:

La medida [op.acc.5] determina los autenticadores admitidos para aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**. Son los siguientes, según el nivel que tenga el sistema respecto a las dimensiones de Integridad [I], Confidencialidad [C], Autenticidad [A] y Trazabilidad [T]:

- **Nivel BAJO**: se admite el uso de un único factor de autenticación, que podrá pertenecer a cualquiera de las 3 categorías: *algo que se sabe, algo que se tiene o algo que se es*.
- **Nivel MEDIO**: se deben usar, al menos, **dos (2) factores** de autenticación. En caso de utilizar *algo que se sabe*, el secreto debe tener la longitud y complejidad recomendadas en el apartado 4.1.
- **Nivel ALTO**: se deben usar, al menos, **dos (2) factores** de autenticación:
  - En caso de utilizar *algo que se sabe*, el secreto debe tener una longitud mínima de 12 caracteres y seguir las reglas de composición indicadas en el apartado 4.1.
  - En caso de utilizar *algo que se tiene* o *algo que se es*, se deben usar dispositivos criptográficos recogidos en el apartado de **Productos Cualificados** dentro del Catálogo de Productos y Servicios STIC (CPSTIC). Deberá tenerse en cuenta la categoría del ENS para la cual está cualificado el producto, y su Procedimiento de Empleo Seguro (PES).

4.5. SOLUCIONES MFA

En el mercado, existen soluciones tecnológicas que permiten a las organizaciones centralizar la gestión de la verificación de identidades y autenticación multi-factor. Estas soluciones proporcionan a la organización autenticadores integrados de varios factores, fáciles de usar para los usuarios. De esta forma y, según las necesidades de cada aplicación o servicio, la organización puede usar los factores de autenticación más apropiados.

Este tipo de soluciones, suelen estar compuestas por:

- Un gestor centralizado.
- Aplicaciones para dispositivos móviles o PCs, que son las que actúan como autenticadores, permitiendo lecturas biométricas (normalmente de huellas o iris), generando códigos OTP, recibiendo notificaciones *push*, etc.

A continuación, se incluye un diagrama del funcionamiento general de este tipo de soluciones.

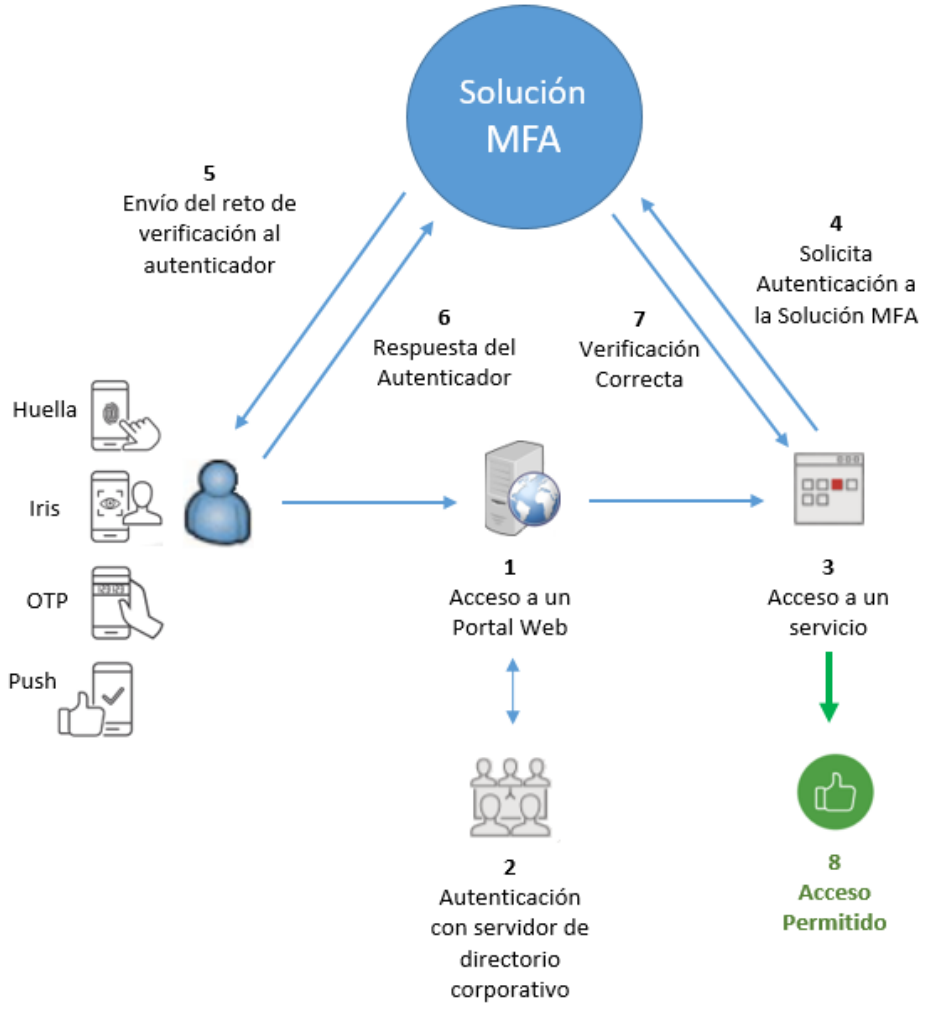


Ilustración 10. Diagrama soluciones multi-factor.

Las características principales de estas soluciones son las siguientes:

- Ayudan a centralizar el proceso de autenticación de solicitantes, simplificando la implementación y gestión de la autenticación multi-factor en los distintos entornos que se pueden encontrar dentro de la organización: cuentas locales, cuentas en la nube, aplicaciones móviles, etc.
- Presentan una alta adaptabilidad a los distintos solicitantes, entornos y casos de uso de la organización gracias a que permiten definir distintos factores para cada situación.
- Simplifican y mejoran la integración entre los factores de autenticación utilizados.
- Generalmente permiten habilitar la autenticación adaptativa basada en riesgo, analizando los atributos contextuales del solicitante y su entorno (por ejemplo, hora de conexión, dirección IP o localización). En ocasiones, pueden tomar datos del entorno de la organización, como los datos a los que se trata de acceder, para ajustar la autenticación.

- Gestionan la creación de políticas de seguridad para incrementar la seguridad de los factores o del proceso de autenticación, como las políticas de contraseñas o políticas de autenticación para obligar el uso de ciertos factores en determinadas situaciones.
- Facilitan las acciones de auditoría y monitorización del proceso de autenticación y de las sesiones gracias a la centralización del proceso.

5. CICLO DE VIDA DE LOS AUTENTICADORES

Existen varios eventos que pueden ocurrir a lo largo del ciclo de vida de un autenticador.

El primer evento es la **vinculación o *enrollment***, que es la fase del ciclo de vida en la cual se asocian los autenticadores con el solicitante. La asociación de la identidad del solicitante con el autenticador que este posee y controla, da lugar a las credenciales.

El término **credenciales** se refiere a un objeto o estructura de datos que asocia la identidad del solicitante, representada por un identificador (y opcionalmente algunos atributos más), al autenticador que el solicitante posee y controla. Por ejemplo, unas credenciales habituales son el conjunto identificador de usuario / contraseña (lo que se conoce comúnmente como *login/password*). Estas credenciales unen el autenticador que posee el solicitante (la contraseña) con su identidad (su identificador de usuario).

Para obtener las credenciales, el solicitante debe identificarse y registrarse durante el proceso de vinculación o *enrollment*.

Recomendación 14:

Para obtener las credenciales en aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**, según la medida [op.acc.5], el registro del solicitante deberá llevarse a cabo de las siguientes formas:

- Presencial: mediante la presentación física del solicitante y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática: mediante un certificado electrónico cualificado.
- De forma telemática: usando un certificado electrónico cualificado en un dispositivo cualificado de creación de firma (por ejemplo, DNI electrónico).

En el caso de sistemas con nivel ALTO en las dimensiones [I], [C], [A] o [T], solo son válidas las opciones a) y c).

Recomendación 15:

En aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**, según la medida [op.acc.5], deben seguirse las siguientes recomendaciones sobre las credenciales:

- Se activarán solo cuando se encuentren bajo control del solicitante.
- Deberán ser custodiadas exclusivamente y de forma segura, por el solicitante.
- El solicitante reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
- Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
- Las credenciales se retirarán y serán deshabilitadas cuando el solicitante termina su relación con el sistema o cuando hay indicios de que ha podido producir un incidente de seguridad.
- En el caso de sistemas con nivel ALTO en las dimensiones [I], [C], [A] o [T], las credenciales deberán suspenderse tras un tras un periodo definido de no utilización.

Otro de los eventos importantes que pueden ocurrir es el compromiso de los autenticadores. Cuando un autenticador ha sido perdido, robado, duplicado o dañado, se dice que ha sido **comprometido**. Generalmente la pérdida se trata igual que el robo, asumiendo que el autenticador perdido ha podido ser robado por un individuo con malas intenciones. Los autenticadores dañados también se consideran comprometidos, ya que podrían permitir la extracción del secreto que contienen. La excepción son los secretos memorizados que son olvidados, ya que en estos casos puede asegurarse que no han sido comprometidos. En caso de darse alguna de estas situaciones, la notificación y revocación del autenticador y de las correspondientes credenciales, debe realizarse lo más rápido posible.

Para permitir que los solicitantes puedan notificar el compromiso del autenticador y acceder al recurso o a la información en estas circunstancias, es necesario implementar un mecanismo alternativo de autenticación que demuestre la identidad del solicitante. Algunos de estos mecanismos son los siguientes:

- Uso de un autenticador adicional, como autenticador de *backup* o alternativo.
- Generación de códigos de recuperación de un solo uso, bien en el proceso inicial de generación de las credenciales, bien cuando el solicitante lo pida. Este código de recuperación debe entregarse al solicitante utilizando un método que verifique que es el solicitante legítimo. Haciendo uso, por ejemplo, de algún atributo asociado a su identidad, como su dirección de correo electrónico o su número de teléfono, o de forma presencial.

Recomendación 16:

Se recomienda el uso de **códigos de recuperación de un solo uso** como mecanismo de recuperación ante casos de compromiso del autenticador.

Estos códigos deben tener suficiente longitud y complejidad para prevenir ataques de adivinación. El verificador debe implementar los controles preventivos contra ataques de fuerza bruta (por ejemplo, con el umbral de intentos fallidos de autenticación).

El último evento del ciclo de vida de un autenticador es la **revocación**, que se produce cuando el autenticador deja de estar asociado a la identidad del solicitante. A partir de ese momento no podrá realizarse ninguna autenticación con ese autenticador y las credenciales dejan de ser válidas.

La revocación sucede por petición del solicitante, generalmente en casos de pérdida o robo del autenticador, o cuando la identidad del solicitante deja de existir debido a que finaliza la relación entre el usuario y la organización.

Tras la revocación, se requerirá a los usuarios la devolución de aquellos autenticadores físicos que puedan contener información sensible.

Recomendación 17:

Se recomienda crear un **proceso de revocación de credenciales** que defina el borrado seguro de las mismas. Se deben eliminar todos los datos sensibles que se hayan almacenado en las credenciales, como claves criptográficas o valores *hash* de contraseñas.

6. ATAQUES, AMENAZAS Y MECANISMOS DE PROTECCIÓN

Cada una de las tres categorías de los factores de autenticación presenta distintas superficies de ataque y vulnerabilidades:

- *Algo que se sabe*. Puede ser revelado a un atacante.
- *Algo que se tiene*. Puede ser robado, duplicado o corrompido.
- *Algo que se es*. Puede ser replicado o suplantado.

Como se ha indicado en la *Recomendación 4*, **es una buena práctica el uso de autenticadores físicamente separados**. Esto hace que el compromiso de un autenticador no afecte a los demás. De esta forma, un atacante no podrá autenticarse con éxito cuando solo haya, por ejemplo, robado un token de seguridad, ya que le hará falta el segundo factor que podrá ser, por ejemplo, una contraseña de usuario.

En la tabla que se muestra a continuación, se describen las amenazas a los factores y dispositivos de autenticación, así como posibles mitigaciones o medidas de protección contra dichas amenazas.

Amenaza	Descripción	Tipo de Autenticador afectado	Medidas de protección o mitigación
Descubrimiento	Adivinación de Secretos (contraseñas, PINs, preguntas de seguridad, etc.) mediante el análisis del contexto del solicitante.	Secretos memorizados	▪ Definición de una política de contraseñas segura. ▪ No utilizar preguntas de seguridad como factor de autenticación.
Ingeniería social	Obtención secretos estableciendo cierto nivel de confianza con el solicitante para que este los revele.	Secretos memorizados	▪ Cursos de formación y concienciación en la seguridad para los solicitantes.
Ataques de presentación	Presentación de instrumentos durante el proceso de registro o verificación biométrica, con objeto de suplantar o enmascarar una identidad.	Dispositivos biométricos	▪ Uso de sistemas de detección de ataques de presentación (sistemas PAD).
Robo	Robo de un dispositivo físico por un atacante. El robo de un dispositivo puede derivar en diferentes ataques, como el análisis del dispositivo (o el acceso al mismo) para la obtención de las claves secretas.	Token de seguridad o token *hardware*	▪ Uso de dispositivos MFA. Si el dispositivo requiere de otro factor de autenticación como un PIN o huella para su uso, un dispositivo robado será inútil para el atacante. Especialmente si el dispositivo lleva implementado un mecanismo de protección con un número máximo de intentos fallidos de autenticación. ▪ Correas electrónicas, sensores o alarmas. ▪ Notificación inmediata del robo. ▪ Definir el procedimiento de revocación de autenticadores. ▪ Uso de mecanismos de seguridad físicos para proteger los autenticadores. Pueden aportar evidencias y detección y respuesta frente al robo.

Amenaza	Descripción	Tipo de Autenticador afectado	Medidas de protección o mitigación
Extracción o Duplicación	Obtención del material criptográfico, secretos o códigos que contiene el autenticador, a través de introducción de código malicioso u otras técnicas.	Token de seguridad o token *hardware* Token *Software*	▪ Implementar en los token hardware, mecanismos resistentes a la manipulación (*tamper-resistant*). ▪ Uso de sistemas de detección de malware. ▪ Uso de mecanismos de seguridad físicos para proteger los autenticadores. Pueden aportar evidencias y detección y respuesta frente a la duplicación.
Ataques a la criptografía	Obtención de claves o códigos mediante diversas técnicas, debido al uso de algoritmos o longitudes de clave poco seguras.	Token de seguridad o token *hardware* Token *Software*	▪ Uso de algoritmos criptográficos seguros, siguiendo las recomendaciones de longitud de clave indicadas en el presente documento
Compromiso de dispositivos	Introducción de código malicioso en los dispositivos para la obtención o manipulación de claves o códigos.	Token *Software*	▪ Uso de software *anti-malware* en los dispositivos. ▪ Uso de controles de seguridad en los sistemas y redes que intervienen en el proceso de autenticación. Esto ayuda a prevenir que un atacante pueda instalar software malicioso en los sistemas.

Amenaza	Descripción	Tipo de Autenticador afectado	Medidas de protección o mitigación
Descifrado offline y fuerza bruta	Obtención de códigos o contraseñas utilizando métodos analíticos fuera del mecanismo de autenticación o mediante sucesivos intentos de autenticación sobre el verificador.	Secretos memorizados Token de seguridad o token hardware Token Software	▪ Uso de claves con un alto nivel de entropía. ▪ Almacenar los hashes de los secretos compartidos haciendo uso de *salt*. ▪ Uso de claves privadas que se bloqueen tras un número de intentos fallidos de activación. ▪ Petición de un CAPTCHA al solicitante antes de poder realizar un intento de autenticación. ▪ Uso de un tiempo de espera incremental tras cada intento de inicio de sesión fallido. ▪ Uso de listas blancas de IPs.

También es necesario tener en cuenta las diferentes amenazas a las que está expuesto el proceso de autenticación. Se indican también posibles mitigaciones o medidas de protección.

Amenaza	Descripción	Medidas de protección o mitigación
Phishing	Obtención de las credenciales de un solicitante mediante el engaño, generalmente haciendo uso de un verificador falso.	▪ Uso de protocolos de autenticación que establecen un canal seguro y autenticado entre el solicitante y el verificador. ▪ Validar la autenticidad del verificador mediante métodos criptográficos
Eavesdropping	Obtención de información mediante la escucha pasiva del canal de autenticación. Esta información puede ser utilizada posteriormente en ataques activos para la suplantación del solicitante.	▪ El proceso de autenticación es resistente a este tipo de ataques si el coste de obtener el secreto a partir de los mensajes transmitidos es excesivamente elevado. ▪ Uso de protocolos de seguridad criptográficos, como TLSv1.2 o superior. ▪ Evitar el uso de redes remotas no seguras.

Amenaza	Descripción	Medidas de protección o mitigación
Repetición (Replay attacks)	Uso de mensajes capturados previamente para lograr una autenticación como un solicitante frente al verificador.	▪ Uso de protocolos que usan valores *nonce*, contadores o *challenges* para probar que la transacción es nueva. El verificador puede detectar si un mensaje del protocolo es antiguo y por tanto no válido.
Robo de sesión	Obtención de los mensajes de una sesión. El atacante simula ante el solicitante que es el verificador y ante el verificador que es el solicitante.	▪ Cifrar el tráfico entre el solicitante y el verificador, por ejemplo, con TLSv1.2 o superior. Especialmente la clave de sesión. Previene la obtención de la clave, que podría usarse posteriormente para robar la sesión. ▪ Regenerar las claves de sesión con cada inicio de sesión, impidiendo así la reutilización de claves antiguas.
Man-in-the-Middle	Obtención y alteración de los mensajes de una sesión. El atacante se sitúa en el medio de la comunicación entre el solicitante y el verificador.	▪ Realizar autenticación mutua entre el solicitante y el verificador, de tal forma que se pueda detectar la participación de un "tercero" en las comunicaciones. ▪ Empleo de protocolos de comunicación que ofrezcan autenticación mutua, como en TLSv1.2 o superiores. ▪ Empleo de certificados X.509v3 para la autenticación.

7. RESUMEN

A continuación, se incluye una tabla con las recomendaciones realizadas a lo largo de este documento. **Se ha indicado con un asterisco (*) las que son de obligado cumplimiento para aquellos sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS).**

Nº	Ámbito		Resumen de la Recomendación
1	General		En aquellos casos en los que se elija utilizar autenticación en varios pasos para acceder a determinadas acciones privilegiadas o a información sensible, **se recomienda utilizar autenticación multi-factor** en el proceso inicial de autenticación del solicitante.
2	General		**Utilizar autenticación MFA para permitir acceso externo** (desde fuera de la red interna) de solicitantes, a recursos o información de la organización. **Implementar autenticación MFA** al acceso, interno o externo, **a cuentas privilegiadas**, que son aquellas que proporcionan al usuario un alto nivel de permisos para poder realizar acciones privilegiadas y administrativas sobre los sistemas, servicios y aplicaciones de la organización.
3	General		Utilizar la autenticación multi-factor permanente por solicitante, de forma que los solicitantes deban **presentar siempre, todos los factores de autenticación**.
4	Autenticadores		Utilizar **autenticadores físicamente separados** para aumentar la seguridad. De esta forma, el compromiso de un autenticador no afecta a los demás autenticadores.
5	Autenticadores	Secretos memorizados	**Utilizar como secreto memorizado las contraseñas**. Utilizando una política de contraseñas adecuada, añaden una mayor seguridad gracias a la combinación de los conjuntos de caracteres utilizados para crearlas, que junto a la longitud, dificulta los ataques de fuerza bruta o adivinación. **No utilizar las preguntas de seguridad** (ni como factor de autenticación, ni como método de recuperación) debido a que, mediante ingeniería social, se pueden obtener las respuestas a las preguntas configuradas, siendo esta la opción menos segura.
6		Dispositivos OTP	Utilizar **códigos OTP basados en tiempo (*time-based*)**, ya que los códigos generados tienen una duración temporal (cuanto menor sea ese período de validez, mayor será la fortaleza del algoritmo, por lo que se recomienda configurar períodos cortos). Además, el algoritmo TOTP usa la función SHA-256, la cual es más segura que SHA-1.

Nº	Ámbito		Resumen de la Recomendación
8 (*)	Autenticadores	Dispositivos criptográficos	Usar algoritmos aprobados en la guía CCN-STIC-807. Estos son: • Algoritmos simétricos: AES. • Algoritmos de Firma: RSA y ECC con funciones SHA-2 o SHA-3. Usar de longitudes de clave que proporcionen una seguridad **equivalente a 112 bits o superior**. Para aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS) categoría ALTA**, deberán utilizarse claves con una **seguridad equivalente a 128 bits**. Esto supone: • Claves RSA 3072 bits o superiores. • Claves ECC 256 bits o superiores. • Claves AES 128 bits o superiores.
9		Biometría	**Minimizar el número de falsos positivos.** Se recomienda un FAR del 0.01% para sistemas de un nivel de seguridad medio y del 0.001% o inferior, para sistemas de un nivel de seguridad alto, conforme a lo definido en ISO / IEC 30107-1. Para esos FAR, se recomienda que el FRR sea del 0.2% o inferior.
10		Biometría	Se recomienda que el dispositivo biométrico implemente un **sistema de detección de ataques de presentación** (PAD), detectando, al menos, un 90% de los mismos, conforme a lo definido en ISO / IEC 30107-3. Implementar un **umbral de intentos fallidos de autenticación** con el consiguiente sistema de bloqueo, para impedir los ataques de fuerza bruta.
11		Biometría	**Usar sistemas biométricos basados en huella dactilar o en iris**. Estos rasgos biométricos son los que permanecen más estables a lo largo de la vida del individuo, y son altamente distintivos de cada uno. Tienen también un alto grado de universalidad y rendimiento.
12		Biometría	Se recomienda que el **sistema de verificación sea un sistema centralizado** en la organización, de forma que las plantillas se almacenen en una base de datos centralizada, con protección frente a accesos y modificaciones no autorizadas. Las comunicaciones entre el dispositivo biométrico y el verificador deberán realizarse a través de canales seguros autenticados.

Nº	Ámbito		Resumen de la Recomendación
13 (*)	Autenticadores	ENS	La medida [op.acc.5] determina los autenticadores admitidos para aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**. Son los siguientes, según el nivel que tenga el sistema respecto a las dimensiones [I], [C], [A] y [T]: ▪ **Nivel BAJO**: se admite el uso de un único factor de autenticación, que podrá pertenecer a cualquiera de las 3 categorías: *algo que se sabe, algo que se tiene o algo que se es*. ▪ **Nivel MEDIO**: se deben usar, al menos, **dos (2)** factores de autenticación. En caso de utilizar *algo que se sabe*, el secreto debe tener la longitud y complejidad recomendadas en el apartado 4.1. ▪ **Nivel ALTO**: se deben usar, al menos, **dos (2)** factores de autenticación: o En caso de utilizar *algo que se sabe*, el secreto debe tener una longitud mínima de 12 caracteres y seguir las reglas de composición indicadas en el apartado 4.1. o En caso de utilizar *algo que se tiene*, se deben usar dispositivos criptográficos recogidos en el apartado de **Productos Cualificados** dentro del Catálogo de Productos y Servicios STIC (CPSTIC). Deberá tenerse en cuenta la categoría del ENS para la cual está cualificado el producto, y su guía de configuración aprobada.
14 (*)	Credenciales		Para obtener las credenciales en aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**, según la medida [op.acc.5], el registro del solicitante deberá llevarse a cabo de las siguientes formas: ▪ Presencial: mediante la presentación física del solicitante y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello. ▪ De forma telemática: mediante un certificado electrónico cualificado. ▪ De forma telemática: usando certificado electrónico cualificado en un dispositivo cualificado de creación de firma (por ejemplo, DNI electrónico). En el caso de sistemas con nivel ALTO en las dimensiones [I], [C], [A] o [T], solo son válidas las opciones a) y c).

Nº	Ámbito	Resumen de la Recomendación
15 (*)	Credenciales	En aquellos **sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS)**, según la medida [op.acc.5], deben seguirse las siguientes recomendaciones sobre las credenciales: ▪ Se activarán solo cuando se encuentren bajo control del solicitante. ▪ Deberán ser custodiadas exclusivamente y de forma segura, por el solicitante. ▪ El solicitante reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida. ▪ Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede. ▪ Las credenciales se retirarán y serán deshabilitadas cuando el solicitante termina su relación con el sistema. ▪ Cuando el nivel de las dimensiones del sistema [I], [C], [A] o [T] sea **ALTO**, las credenciales deberán suspenderse tras un tras un periodo definido de no utilización.
16	Credenciales	Usar **códigos de recuperación de un solo uso** como mecanismo de recuperación ante casos de compromiso del autenticador. Estos códigos deben tener suficiente longitud y complejidad para prevenir ataques de adivinación. El verificador debe implementar los controles preventivos contra ataques de fuerza bruta (por ejemplo, con el umbral de intentos fallidos de autenticación).
17	Credenciales	Crear un **proceso de revocación de credenciales** que defina el borrado seguro de las mismas. Se deben eliminar todos los datos sensibles que se hayan almacenado en las credenciales, como claves criptográficas o valores hash de contraseñas.

8. ABREVIATURAS

2FA	*Two Factor Authentication*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
ENS	Esquema Nacional de Seguridad
FIDO	*Fast ID Online*
FMR	*False Match Rate*
MFA	*Multi Factor Authentication*
OTP	*One Time Password*
PIN	*Personal Identification Number*
SMS	*Short Message Service*
STIC	Seguridad de lasTecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*

9. REFERENCIAS

REF1 CCN-STIC-821 Normas de Seguridad en el ENS. Apéndice V: Normas de creación de contraseñas NP40

REF2 CCN-STIC-490 Dispositivos biométricos de huella dactilar

REF3 CCN-STIC-491 Dispositivos biométricos de iris

REF4 *NIST SP 800-63-3 Digital Identity Guidelines*

REF5 *NIST SP 800-63B Digital Identity Guidelines – Authentication and Lifecycle Management*

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**Enlace web**
Youtube	**youtube.com/channel/UCuSR7guHgx5kgoj6kafOF1Q**

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.

Praeventio sit vincere