Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1254

(09/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Gestión de identidades

Marco de garantía de autentificación de entidad

Recomendación UIT-T X.1254

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	**X.1250–X.1279**
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1254

Marco de garantía de autentificación de entidad

Resumen

En la Recomendación UIT-T X.1254 se definen tres niveles de garantía de autentificación de entidad (AAL) y los criterios y amenazas para cada uno de ellos.

Asimismo:

- se especifica un marco para la gestión de los niveles de garantía;
- se proporcionan directrices sobre las tecnologías de control que se deben utilizar para mitigar las amenazas a la autentificación, sobre la base de la evaluación de riesgos;
- se orienta sobre la correspondencia entre los tres AAL y otros planes de garantía de autentificación; y
- se facilita orientación para el intercambio de resultados de autentificación basados en los tres AAL.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1254	2012-09-07	17	11.1002/1000/11608
2.0	ITU-T X.1254	2020-09-03	17	11.1002/1000/14260

Palabras clave

AAL, autentificación, garantía, gestión de identidad, IdM, LOA, nivel de garantía, nivel de garantía de autentificación.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros textos 1
3.2 Términos definidos en esta Recomendación 3
4 Abreviaturas y acrónimos 3
5 Convenios 4
6 Flujo del proceso de autentificación digital 4
6.1 Aspectos generales 4
6.2 Garantía de identidad digital 5
6.3 Entes 6
6.4 Componentes del proceso de autentificación 7
7 Aplicación de la gestión de riesgos al marco de garantía de autentificación 8
7.1 Aspectos generales 8
7.2 Riesgo de autentificación 8
8 Categorías de amenazas, riesgos y controles 9
8.1 Niveles de garantía 10
8.2 Puesta en peligro del autentificador 11
8.3 Puesta en peligro de la transacción 14
8.4 Suplantación del verificador 15
8.5 Suplantación del abonado 16
8.6 Riesgos y controles de la puesta en peligro del servicio de autentificación 21
8.7 Riesgos y controles de privacidad 22
Apéndice I – Ejemplo de autentificación fuerte con [b-UIT-T X.1278] 25
I.1 Introducción 25
I.2 Categorías de amenazas 25
I.3 [b-UIT-T X.1278] permite la "autentificación fuerte con un alto nivel de garantía" 25
I.4 Autentificación por contraseñas obsoleta 26
I.5 Nueva autentificación con [b-UIT-T X.1278] 27
I.6 Interoperabilidad y certificación 28
Bibliografía 29

Introducción

Una identidad digital es la representación unívoca de una entidad implicada en una transacción en línea. La garantía, o fiabilidad, de que la identidad digital con la que se está interactuando es coherente con la identidad declarada es esencial para la confianza, la seguridad y el control de acceso en línea. Se identifican tres tipos de garantía para facilitar la confianza en una identidad digital: garantía de identidad, garantía de autentificación y garantía de federación.

En esta Recomendación se presenta un marco para la garantía de autentificación. A los efectos de esta Recomendación, la autentificación es el proceso mediante el cual se verifica una identidad declarada a fin de realizar una transacción en línea. En los servicios que pueden visitarse varias veces, una autentificación satisfactoria ofrece una garantía en función de los riesgos razonables de que el usuario que accede al servicio hoy es el mismo que accedió al servicio con anterioridad.

El marco establecido en esta Recomendación ofrece a los proveedores de servicios en línea (partes que confían (RP) y proveedores de servicios de credenciales (CSP) – un método sistemático para entender los riesgos que corren e identificar los controles que pueden reducirlos. Está diseñado para facilitar la selección metódica de controles y estrategias de reducción de riesgos en tres fases:

1) Identificación de funciones y servicios para definir las categorías de amenaza;
2) Aplicación de un proceso de gestión de riesgos adaptado para determinar la intensidad de los controles requeridos; e,
3) Identificación de las tecnologías – protocolos, tipos de credenciales, etc. – que se emplean para precisar los controles.

Modelo basado en amenazas

Esta Recomendación está diseñada para facilitar la selección metódica de controles y estrategias de reducción de riesgos. Antes de poder seleccionar los controles y estrategias de reducción adecuados es necesario identificar los tipos de riesgos y amenazas asociados a la(s) función(es) y servicios del proveedor de servicios en línea. Véase la Figura 0-1.

Figura 0-1 – Servicios, riesgos y controles

Este marco se organiza en torno a categorías de riesgos y amenazas, que dan a los proveedores en línea un vínculo funcional entre los procesos de evaluación de riesgos y los controles y actividades de reducción de riesgos.

Los proveedores de servicios de identidad pueden facilitar uno, algunos o todos los componentes funcionales de estas fases de identidad digital. Así, conviene evaluar los riesgos y abordar los controles y métodos de reducción de riesgos de manera similar, en función de sus componentes, en relación con el ciclo de vida de la transacción digital. En esta Recomendación se consideran los riesgos y controles de interés para las fases de autentificación y gestión de credenciales de ese ciclo de vida. En otros documentos (por ejemplo, [b-ISO/CEI TS 29003]) se consideran los riesgos y controles para las actividades de registro y demostración de la identidad, así como los controles orgánicos y de gestión. Se prevé que esos y otros documentos se armonicen para representar un conjunto coordinado de normas de gestión de identidad fundamentales (como se muestra en la Figura 0-2) que, al utilizarlas juntas, ofrezcan los procesos, riesgos y controles para todo el ciclo de vida de las transacciones de identidad digital.

En esta Recomendación se presenta también un catálogo de amenazas a la privacidad, consideraciones y controles específicos a su ámbito de aplicación (autentificación y gestión de credenciales). Esta Recomendación no contiene consideraciones sobre la privacidad en relación con la demostración de identidad o el registro.

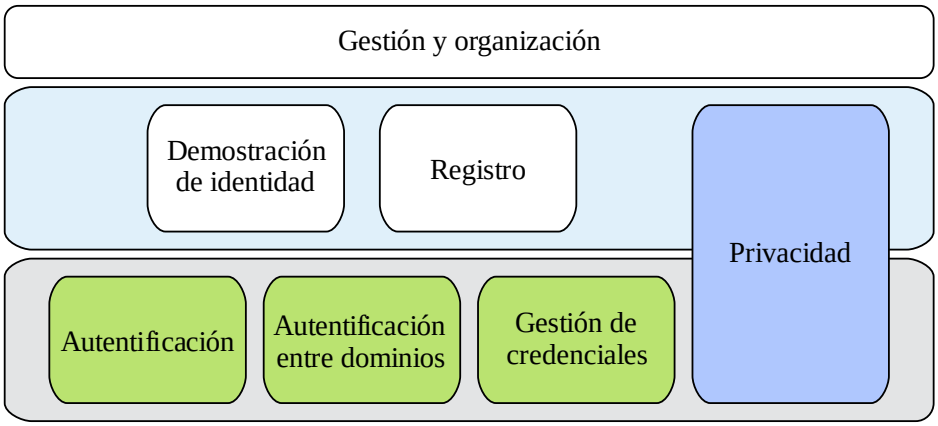


Figura 0-2 – Normas de gestión de la identidad armonizadas fundamentales

Relación con la anterior versión de esta Recomendación

En la primera edición de esta Recomendación [b-UIT-T X.1254 (2012)] se presentaba el ciclo de vida de las transacciones de identidad digital en tres fases: registro y demostración de la identidad, gestión de credenciales y autentificación de entidad. Desde 2012 la industria ha evolucionado y han surgido nuevos conceptos y métodos, como la autentificación sin contraseña y la autentificación avanzada. Así, la industria ha abandonado el concepto de nivel de garantía (LOA) como ordinal simple que determina requisitos específicos de la implementación. En su lugar, combinando adecuadamente la gestión de riesgos empresarial y de privacidad con la necesidad de la misión, los implementadores podrán seleccionar de manera independiente los niveles de garantía de identidad (IAL), niveles de garantía de autentificación (AAL) y niveles de garantía de federación (FAL). Esta Recomendación se centra en los AAL. Los IAL y FAL quedan fuera del alcance de esta Recomendación.

Recomendación UIT-T X.1254

Marco de garantía de autentificación de entidad

1 Alcance

En la presente Recomendación se describe un marco para gestionar la garantía de autentificación de entidad (EAA) en un determinado contexto. En particular:

– define tres niveles de garantía de autentificación de entidad (AAL);

– da directrices para entender esos AAL;

– especifica criterios y directrices para lograr cada uno de los niveles de EAA definidos;

– orienta sobre la comparación y correspondencia con otros planes de garantía de autentificación;

– facilita orientación para el intercambio de resultados de autentificación basados en los niveles de garantía especificados; y

– proporciona directrices sobre los controles que deberían emplearse para mitigar las amenazas a la autentificación sobre la base de una evaluación de los riesgos.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos definidos en otros textos:

3.1.1 aserto [b-UIT-T X.1252]: Afirmación formulada por una entidad sin presentar evidencias de su validez.

NOTA – Se entiende que el significado de los términos "declaración" y "aserto" son casi similares, pero que existen pequeñas diferencias. A los efectos de la presente Recomendación, se considera que un aserto es una afirmación más firme que una declaración.

3.1.2 autentificación [b-ISO/CEI 18014-2]: Acción de garantizar la identidad reclamada de una entidad.

3.1.3 factor autentificación [b-ISO/CEI 19790]: Fragmento de información y/o procedimiento utilizado para autentificar o verificar la identidad de una entidad.

NOTA – Los factores de autentificación se dividen en cuatro categorías:

– algo que la entidad tiene (por ejemplo, firma de dispositivo, pasaporte, dispositivo físico que contiene una credencial o clave privada);

– algo que la entidad sabe (por ejemplo, contraseña, PIN);

– algo intrínseco a la identidad (por ejemplo, características biométricas);

– algo que la entidad suele hacer (por ejemplo, patrón de conducta).

3.1.4 protocolo de autentificación [b-ISO/CEI 29115]: Secuencia definida de mensajes entre una entidad y un verificador que permite autentificar la identidad de la entidad

3.1.5 declaración [b-UIT-T X.1252]: Asegurar o dar por cierto algo, sin poder aportar pruebas de ello.

NOTA – Se entiende que el significado de los términos "declaración" y "aserto" son casi similares, pero que existen pequeñas diferencias. A los efectos de la presente Recomendación, se considera que un aserto es una afirmación más firme que una declaración.

3.1.6 contexto [b-UIT-T X.1252]: Entorno con condiciones de contorno definidas en las que existen e interactúan entidades.

3.1.7 credencial [b-UIT-T X.1252]: Conjunto de datos presentados como prueba de una identidad y/o derechos declarados o aseverados.

NOTA – Para más información sobre las características de una credencial, véase el Apéndice I.

3.1.8 entidad [b-UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

NOTA – A los efectos de la presente Recomendación, el término entidad se emplea también en el caso específico de cualquier cosa que declare una identidad.

3.1.9 identidad; identidad parcial [b-ISO/CEI 24760-1]: Conjunto de atributos relativos a una entidad.

NOTA – Una identidad puede tener uno o varios identificadores que permiten reconocer inequívocamente a la entidad en un determinado contexto.

3.1.10 verificación de la información de identidad [b-ISO/CEI 29115]: Proceso de verificación de la información y las credenciales que demuestran la identidad con respecto al expedidor, las fuentes de datos u otros recursos internos o externos respecto de la autenticidad, validez, corrección y vinculación con la entidad.

3.1.11 demostración de identidad [b-ISO/CEI 29115]: Proceso mediante el cual la autoridad de registro (AR) obtiene y verifica suficiente información para identificar una entidad con un nivel de garantía especificado o tácito.

3.1.12 ataque por intromisión (*man-in-the-middle*) [b-ISO/CEI 29115]: Ataque en el que el atacante es capaz de leer, insertar y modificar mensajes entre las dos partes sin el conocimiento de estas.

3.1.13 autentificación multifactor [b-ISO/CEI 19790]: Autentificación en la que se emplea como mínimo dos factores de autentificación independientes.

3.1.14 autentificación recíproca [b-ISO/CEI 29115]: Autentificación de las identidades en la que se garantiza a cada entidad la identidad de la otra.

3.1.15 no repudio [b-UIT-T X.1252]: Capacidad para dar protección contra la denegación por parte de una de las entidades que intervienen en una acción o han participado en la totalidad o parte de la acción.

3.1.16 usurpación de identidad (*phishing*) [b-ISO/CEI 29115]: Mensaje fraudulento que incita al usuario de correo electrónico a revelar datos personales o confidenciales que el originador del mensaje puede utilizar con fines ilícitos.

3.1.17 repudio [b-UIT-T X.1252]: Negación de haber participado en la totalidad o en parte de una acción por una de las entidades implicadas.

3.1.18 evaluación de riesgos [b-ISO/CEI 27000]: Proceso que comprende la identificación de riesgos, el análisis de riesgos y la valoración de riesgos.

3.1.19 secreto compartido [b-ISO/CEI 29115]: Secreto utilizado en la autentificación que sólo lo conocen la entidad y el verificador.

3.1.20 transacción [b-ISO/CEI 29115]: Evento singular entre una entidad y el proveedor de servicio que sirve para un fin comercial o programático.

3.1.21 verificación [b-ISO/CEI 29115]: Proceso de verificación de información comparando la información facilitada con la información corroborada previamente.

3.1.22 verificador [b-ISO/CEI 29115]: Actor que corrobora información de identidad.

NOTA – El verificador puede participar en numerosas etapas del marco de garantía de autentificación de entidades y llevar a cabo la verificación de la identidad y/o de la información de identidad.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 proveedor de servicio de credenciales (CSP): Actor de confianza que expide o gestiona credenciales.

NOTA – Esta definición se basa en la de [b-ISO/CEI 29115].

3.2.2 garantía de autentificación de entidad (EAA): Grado de confianza que se alcanza con el proceso de autentificación de que la entidad es lo que afirma ser o se espera que sea.

NOTA 1 – La confianza se basa en el grado de confianza en la relación que existe entre la entidad y la identidad presentada.

NOTA 2 – Esta definición se basa en la definición de "garantía de autentificación" de [b-UIT-T X.1252].

3.2.3 identificador: Uno o varios atributos que caracterizan inequívocamente una entidad en un determinado contexto.

NOTA – Esta definición se basa en la de [b-ISO/CEI 29115].

3.2.4 autoridad de registro (AR): Actor fiable que establece o verifica y avala la identidad de una entidad al proveedor de servicio de credenciales (CSP).

NOTA – Esta definición se basa en la de [b-ISO/CEI 29115].

3.2.5 parte que confía (RP): Actor que confía en el aserto o declaración de una identidad.

NOTA – Esta definición se basa en la de [b-ISO/CEI 29115].

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas:

AAL Nivel de garantía de autentificación (*authentication assurance level)*

AR Autoridad de registro

CSP Proveedor de servicio de credenciales (*credential service provider*)

EAA Garantía de autentificación de entidad (*entity authentication assurance*)

FAL Nivel de garantía de federación (*federation assurance level*)

FIDO Fast Identity On-line

HTML Lenguaje de marcaje hipertexto (*hypertext markup language*)

HTTP Protocolo de transferencia hipertexto (*hypertext transfer protocol*)

HTTPS Protocolo de transferencia hipertexto seguro (*hypertext transfer protocol secure)*

IAL Nivel de garantía de identidad (*identity assurance level)*

IdM Gestión de identidades (*identity management*)

IDP Proveedor de identidades (*identity provider*)

IIP Información de identificación personal

LoA Nivel de garantía (*level of assurance*)

MAC Control de acceso a los medios (*media access control*)

MItM Intermediario (*man-in-the-middle*)

MItB Intermediario en navegador (*man-in-the-browser)*

OAuth Autentificación abierta (*open authentication)*

OpenID Identidad abierta (*open identity)*

OTP Contraseña de uso único (*one time password)*

PIA Evaluación de la incidencia en la privacidad (*privacy impact assessment*)

PIN Número de identificación personal (*personal identification number*)

RP Parte que confía (*relying party*)

SAML Lenguaje de marcado de asertos de seguridad (*security assertion markup language*)

TLS Seguridad en la capa de transporte (*transport layer security*)

URL Localizador uniforme de recursos (*uniform resource locator*)

5 Convenios

La presente Recomendación se ajusta a las siguientes formas verbales de expresión de disposiciones:

a) "deberá" indica una obligación;

b) "debería" denota una recomendación;

c) "podría" significa que se da permiso;

d) "puede" indica posibilidad o capacidad.

6 Flujo del proceso de autentificación digital

6.1 Aspectos generales

La identidad digital es la representación unívoca de una entidad implicada en una transacción en línea. En su forma más simple, la autentificación digital conlleva la verificación, con un cierto grado de confianza, de la identidad declarada de una entidad a fin de concederle acceso a un servicio en línea. Una entidad registrada intenta autentificarse ante un servicio en línea demostrando la posesión del autentificador, también conocido como credencial, que se le concedió en el momento de registrarse. El servicio en línea, también conocido como parte que confía (RP, *relying party*) en la transacción, intenta verificar la validez del autentificador con el proveedor de identidades (IDP, *identity provider*) o el proveedor de servicios de credenciales (CSP, *credential service provider*) o el verificador. Se concede a la entidad acceso al servicio en línea una vez que el CSP/verificador ha comprobado su credencial.

En la Figura 6-1 se ilustra el flujo del proceso de autentificación digital siguiente:

1. una entidad accede a un servicio en línea de una RP;
2. la RP redirige a la entidad al CSP para su autentificación;
3. el CSP verifica que la entidad posee el/los autentificador(es) registrado(s);
4. el CSP envía un aserto de autentificación a la RP afirmando el estatus de autentificación de la entidad; y
5. se establece una sesión autentificada entre la entidad y la RP.

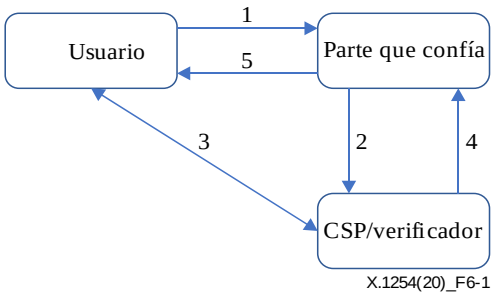


Figura 6-1 – Flujo del proceso de autentificación digital

Esta manera de ilustrar el proceso de autentificación digital permite entender los riesgos asociados con los distintos entes y funciones implicados en la autentificación digital.

Aunque una RP puede tener su propia solución de gestión de identidades (IdM, *identity management*) y actuar como su propio CSP, en esta Recomendación se presentan la RP y el CSP como entes distintos. Sin embargo, en ambos casos las funciones de los entes son las mismas.

Además, en la Figura 6-1 se combinan el CSP y el verificador. Aunque los CSP suelen ocuparse de la función de verificación, en ocasiones un CSP puede recurrir a un verificador independiente.

El proceso de autentificación digital descrito aquí supone que las entidades ya se han registrado en el CSP y han obtenido uno o más autentificadores registrados. Los procesos de registro e inscripción quedan fuera del alcance de esta Recomendación.

6.2 Garantía de identidad digital

Hay que entender cómo interactúan los servicios que intervienen en las fases y componentes funcionales del ciclo de vida de la identidad digital para soportar la confianza y fiabilidad general de una transacción en línea. Esa confianza suele expresarse en nivel de fiabilidad por grados o niveles de garantía. En esta Recomendación se dan los requisitos y orientaciones para la fase de garantía de autentificación de identidad digital y las funciones que componen el marco general de garantía de autentificación e identidad digital. En la Figura 6-2 se muestran los componentes, las descripciones de garantía y las actividades funcionales de un conjunto de documentos sobre IdM armonizados fundamentales para abordar la garantía y los controles en el marco global de identidad digital.

Componente garantía	Descripción	Actividades

IA *Garantía de identidad*	Robustez del proceso de demostración de identidad y vinculación del autentificador con la persona cuya identidad se ha demostrado	• Demostración de identidad
		  • Resolución
		  • Validación
		  • Verificación
		• Registro
		• Vinculación

AA *Garantía de autentificación*	Confianza en que un declarante dado es el abonado autentificado anteriormente	• Autentificación
		• Gestión de credenciales
		  • Expedición de credenciales
		  • Suspensión, revocación y/o destrucción de credenciales
		  • Renovación y/o sustitución de credenciales

FA *Garantía de federación*	Combinación de aspectos del modelo de federación, la intensidad de la protección del aserto y la presentación del aserto	• Gestión de claves • Decisiones de ejecución • Gestión de atributos

X.1254(20)_F6-2

Figura 6-2 – Niveles de garantía de identidad digital

Garantía de identidad: Se refiere a los procedimientos previstos para verificar la asociación de un sujeto con su identidad en el mundo real. La garantía de identidad se trata en [b-ISO/CEI TS 29003].

Garantía de autentificación: La autentificación determina que un sujeto que intenta acceder a un servicio digital controla las tecnologías utilizadas para la autentificación. Esta garantía consiste en los procedimientos empleados para verificar que una identidad declarada es idéntica a la que participó en el proceso de registro y que el sistema ya ha autentificado.

Garantía de federación: se refiere a los procedimientos empleados para comunicar, proteger y validar los asertos de identidad que se formulan en distintos dominios de seguridad. La federación de identidad es la compartición de la información sobre identidad en línea y autentificación entre dos o más partes.

Quedan fuera del alcance de la revisión de esta Recomendación los componentes y actividades de garantía de identidad que soportan la garantía de federación.

6.3 Entes

6.3.1 Aspectos generales

En tanto que modelo centrado en los riesgos, el proceso de autentificación digital ayuda a identificar las categorías de amenazas asociadas con tres entes primarios: CSP, RP y entidades.

6.3.2 Proveedores de servicios en línea

Los proveedores de servicios en línea son organizaciones que ofrecen servicios, aplicaciones e información en línea que necesitan un acceso restringido, como los servicios bancarios, los servicios de atención sanitaria y los comerciantes. En función de la implementación del servicio, los proveedores de servicios en línea pueden asumir uno o varios de los siguientes papeles:

- CSP;
- proveedor de servicios de identidad;
- verificador;
- RP.

6.3.3 Proveedor de servicios de credenciales

El CSP es responsable de verificar una credencial (es decir, un identificador) presentada por la entidad. El proceso y grado de rigor con que se efectúa esta verificación están determinados por el nivel de riesgo asociado a la transacción en línea y al entorno en que se utilizará la identidad. La función de CSP puede ejercerla el sistema de IdM propio del proveedor de servicios en línea o un servicio de identidades tercero. Además, el CSP suele encargarse de la gestión de las credenciales.

6.3.4 Proveedor de servicios de identidad

El proveedor de servicios de identidad (IDP) es responsable de demostrar la identidad declarada de una entidad y garantizar que esa identidad declarada está asociada a la credencial utilizada por la entidad. El proceso y grado de rigor con que se efectúa esta verificación están determinados por el nivel de riesgo asociado a la transacción en línea y al entorno en que se utilizará la identidad. El IDP puede encargarse también de las entidades de registro e inscripción en programas y servicios específicos. Los riesgos y controles de que se ocupan estas funciones del componente IDP quedan fuera del alcance de esta Recomendación.

Además, el IDP puede asumir el papel de CSP. Dado que esta Recomendación se centra en la autentificación y la gestión de credenciales, siempre que se utilice el término CSP, se considerará que también representa a un IDP que asume ese papel en una transacción.

6.3.5 Verificador

El verificador se encarga de confirmar la identidad de la entidad verificando que ésta posee y controla un autentificador utilizando un protocolo de autentificación. Para ello el verificador también podrá tener que validar las credenciales que vinculan el autentificador al identificador de la entidad y verificar su estatus. Los CSP o IDP que prestan servicios de credenciales suelen asumir el papel de verificador.

6.3.6 Parte que confía (RP)

La parte que confía (RP) acepta (confía) y utiliza los asertos de estatus de autentificación de la entidad formulados por sus propios servicios de IdM o por CSP externos. La RP debe poder confiar en la información de identidad que recibe de esos servicios para poder tomar decisiones en función de los riesgos y permitir o no a entidades específicas acceder a sus servicios y productos en línea.

6.3.7 Entidades

A los efectos de esta Recomendación las entidades son los usuarios de los servicios ofrecidos por los proveedores de servicios en línea.

Las entidades son responsables de proteger sus identidades y credenciales digitales contra el fraude y la utilización indebida y de utilizar sus credenciales de la manera en que se supone que se han de utilizar.

6.4 Componentes del proceso de autentificación

En esta Recomendación se ofrece a los proveedores de servicio una metodología para identificar las amenazas y riesgos asociados con su servicio, en función del papel que asumen, como se describen en la cláusula 6.3, y de las tecnologías empleadas.

Para facilitar la evaluación de los riesgos y amenazas asociados específicamente a un servicio en línea, es importante identificar qué funciones y tecnologías están implicadas en el proceso de autentificación.

Entre los componentes del proceso se cuentan los siguientes:

- autentificadores, por ejemplo, secretos memorizados (como las contraseñas), dispositivos de contraseña de un solo uso (OTP, *one-time password*), tarjetas inteligentes, certificados digitales y biometría (por ejemplo, huellas digitales);
- software cliente y servidor;
- protocolos de comunicación y autentificación, por ejemplo, lenguaje de marcaje hipertexto (HTML, *hypertext markup language*), lenguaje de marcaje de asertos de seguridad (SAML, *security assertion markup language*), seguridad de la capa de transporte (TLS, *transport layer security*), autentificación abierta (OAuth, *open authentication*) e identidad abierta (OpenID, *open identity*).

Las transacciones de autentificación son el objeto de ataques que las ponen en peligro y apuntan a las vulnerabilidades de uno o más de los componentes enumerados en el párrafo anterior. La mayoría de las tecnologías de autentificación, incluidos el hardware, el software y los protocolos de comunicación, tienen amenazas y vulnerabilidades específicas asociadas. Dentro de sus actividades de evaluación de riesgos, los proveedores de servicios en línea deben considerar las vulnerabilidades asociadas a cada componente. En la cláusula 8 se describen las categorías específicas de amenazas, los riesgos y los controles.

6.4.1 Autentificadores

Un autentificador es algo que una entidad posee y controla, y que se utiliza para autentificar la identidad de esa entidad. Una entidad puede tener asociados más de un autentificador. Entre los **factores** de la autentificación se cuentan *algo que se conoce*, como una contraseña; *algo que se posee*,

como una tarjeta inteligente, y *algo que se es*, como un dato biométrico. La fuerza de una transacción de autentificación aumenta cuando se utilizan uno o más factores distintos.

Un proveedor de servicios en línea deberá considerar el perfil de riesgo de sus servicios al seleccionar los autentificadores aceptables para autentificar los servicios. Además, una RP considerará los requisitos de garantía de su servicio antes de aceptar los servicios de un CSP.

Como tipos de autentificadores pueden citarse los siguientes:

- secretos memorizados;
- secretos buscados;
- dispositivos fuera de banda;
- dispositivos OTP monofactoriales;
- dispositivos OTP multifactoriales;
- software criptográfico monofactorial;
- dispositivos criptográficos monofactoriales;
- software criptográfico multifactorial;
- dispositivos criptográficos multifactoriales.

6.4.2 Autentificador

Se trata de un objeto o estructura de datos con autoridad para vincular una identidad – a través de uno o varios identificadores – y (facultativamente) atributos adicionales, a al menos un autentificador que el abonado posee y controla. Aunque normalmente se supone que la entidad mantiene el autentificador, en esta Recomendación también se utiliza el término para hacer referencia a los registros electrónicos mantenidos por el CSP que establecen la vinculación entre el/los autentificador(es) del abonado y su identidad. La forma más común de autentificador es un nombre de usuario y el registro de usuario asociado, vinculado a una contraseña u otro tipo de autentificador.

7 Aplicación de la gestión de riesgos al marco de garantía de autentificación

7.1 Aspectos generales

Un sistema de IdM efectivo depende de la comprensión de los niveles de riesgo asociados a los tipos de servicios en línea que ofrece la organización. Para entender esos riesgos los proveedores de servicios en línea considerarán el/los papel(es) específicos que asumen dentro del marco, la naturaleza de sus usuarios y los tipos de datos y transacciones procesados por sus aplicaciones.

La aplicación de una metodología de gestión de riesgos estructurada tendrá el siguiente resultado: identificación de riesgos y amenazas; toma de decisiones sobre cómo se han de tratar, e información necesaria para seleccionar y aplicar controles. En cuanto a la IdM, hay directrices específicas que ayudan a las organizaciones a entender la equivalencia entre los niveles de riesgo y los niveles de garantía, es decir, los grados de confianza relativa en la integridad de las identidades en línea.

Los proveedores de servicios en línea utilizarán una metodología de gestión de riesgos y prepararán un plan para la gestión de sus riesgos relacionados con la autentificación digital.

La evaluación de riesgos asociados a la identidad digital deberá tener en cuenta, como mínimo, el tipo y nivel de las consecuencias derivadas de cada uno de los riesgos identificados. También se tomará en consideración la probabilidad de ocurrencia de cada riesgo.

7.2 Riesgo de autentificación

Al considerar un riesgo de autentificación la cuestión fundamental reside en determinar "qué está en juego" en caso de que falle la autentificación, es decir, qué consecuencias puede tener conceder acceso a una entidad que no es el propietario legítimo de la credencial y la cuenta asociada.

A la hora de evaluar los riesgos asociados a un fallo de autentificación los proveedores de servicios en línea deberán considerar lo siguiente:

- Datos – Identificar los tipos de datos que se procesan y protegen dentro de los límites del sistema es fundamental para determinar "qué está en juego". Entre los tipos de datos se incluyen los financieros, privados, públicamente disponibles, muy sensibles y la información de identificación personal (IIP).
- Usuarios – Identificar y entender quiénes son los usuarios de un sistema o empresa es fundamental para identificar y clasificar los riesgos específicos. Los usuarios pueden clasificarse, entre otros, en internos, externos y privilegiados. Las organizaciones deben asimismo considerar si sus usuarios están vinculados por algún acuerdo contractual, legal o de otro tipo.
- Motivaciones de ataque – Una vez definidos sus usuarios y tipos de datos, la organización estará en mejor postura para entender las motivaciones de un ataque. Por ejemplo, si el sistema procesa y protege información de cuentas bancarias, el motivo de los atacantes puede ser el acceso fraudulento al sistema a fin de obtener beneficios financieros.

Los proveedores de servicios en línea escogerán los controles y demás opciones de mitigación de amenazas en función de los riesgos evaluados.

8 Categorías de amenazas, riesgos y controles

En esta cláusula se presenta un catálogo de amenazas y controles, organizados en categorías. Los proveedores de servicios de identidad deben identificar las categorías de amenazas específicas de les atañen en función de sus servicios y funciones en el marco de la autentificación. Los controles se agrupan en las siguientes categorías de amenazas:

- puesta en peligro del autentificador;
- puesta en peligro de la transacción;
- suplantación del CSP;
- suplantación de la entidad;
- puesta en peligro del servicio de autentificación.

La RP y el CSP comparten la responsabilidad de protección contra todas las amenazas a la autentificación. Las funciones y responsabilidades en el marco de una transacción de autentificación deberán estar claramente establecidas y acordadas entre todas las partes.

En la Cuadro 8-1 se presentan las categorías de amenazas de autentificación y los entes a los que se suele asignar la responsabilidad de mitigar esas amenazas.

Cuadro 8-1 – Entes y categorías de amenazas

Componente garantía	Descripción
RP	• Suplantación del verificador • Puesta en peligro de la transacción • Privacidad • Federación
CSP	• Suplantación del verificador • Puesta en peligro de la transacción • Suplantación del abonado • Puesta en peligro del autentificador • Puesta en peligro del servicio de autentificación • Privacidad • Federación

8.1 Niveles de garantía

En esta Recomendación, la autentificación es un proceso mediante el cual se verifica una identidad declarada a fin de realizar una transacción en línea. Un mayor rigor en el proceso aplicado para verificar las identidades declaradas aumenta la confianza en que la identidad autentificada representa al sujeto a que corresponde esa identidad. La garantía de autentificación es una medida de esa confianza y hay sistemas, o esquemas, que definen una serie de niveles relativos de confianza, denominados AAL.

En esta Recomendación se describe un modelo de garantía de autentificación basado en el concepto de identificación y mitigación de amenazas y riesgos para las transacciones de autentificación. En muchos casos, las organizaciones, órganos nacionales y comunidades de interés pueden optar por establecer un esquema AAL que agrupe los riesgos, amenazas y controles en función del entorno en que se aplican, lo que reporta numerosos beneficios tangibles, entre ellos la definición de los requisitos para participar en las transacciones a los niveles común mente definidos y la capacidad de crear lotes de productos normalizados para responder a las necesidades de la comunidad.

Esta Recomendación elimina el concepto de nivel de garantía (LOA, *level of assurance*) como un único ordinal que define los requisitos específicos de la implementación. En su lugar, combinando la adecuada gestión de riesgos privados y empresariales con la necesidad de la misión, los implementadores seleccionan los IAL, AAL y nivel de garantía de federación (FAL, *federation assurance level*) por separado. Si bien muchos sistemas utilizan los mismos niveles numéricos para los IAL, AAL y FAL, no se trata de un requisito y los implementadores no deberán suponer que serán idénticos en todos los sistemas.

A continuación, se indican los componentes de la garantía de identidad que se detallan en estas directrices:

- IAL es el proceso de demostración de identidad.
- AAL es el proceso de autentificación.
- FAL es la fuerza de un aserto en un entorno federado, utilizado para comunicar la información de autentificación y atributos (si procede) a una RP.

La división en estas categorías ofrece a los implementadores flexibilidad a la hora de identificar soluciones y aumenta la capacidad de integrar técnicas que aumentan la privacidad como elementos esenciales de los sistemas de identidad sea cual sea el nivel de garantía. Por ejemplo, este modelo soporta la posibilidad de utilizar interacciones pseudónimas incluso cuando se emplean autentificadores multifactoriales fuertes.

En el entorno actual la solución de identidad de una organización no tiene porqué ser monolítica y que un solo sistema o vendedor se ocupe de todas las funcionalidades. Los servicios de identidad pueden estar formados por múltiples componentes, lo que permite a las organizaciones y agencias utilizar soluciones de identidad modulables y normalizadas en función de las necesidades de la misión.

Los tres AAL definen los subconjuntos de opciones que los implementadores pueden seleccionar en función de su perfil de riesgo y del daño que podría causar un atacante de controlar un autentificador y acceder al sistema. Los AAL son los siguientes:

AAL1: AAL1 da una cierta garantía de que la entidad controla un autentificador vinculado a la cuenta de la entidad. AAL1 exige la autentificación monofactorial o multifactorial con una amplia gama de tecnologías de autentificación disponibles. Para que la autentificación se lleve a cabo con éxito el declarante debe demostrar la posesión y el control del autentificador siguiendo un protocolo de autentificación seguro.

AAL2: AAL2 da una alta confianza en que la entidad controla uno o varios autentificadores vinculados a la cuenta de la entidad. Tiene que demostrar la posesión y el control de dos factores de

autentificación distintos siguiendo uno o varios protocolos de autentificación seguros. AAL2 y los niveles superiores exigen la utilización de técnicas criptográficas globalmente aceptadas.

AAL3: AAL3 da un muy alto grado de confianza en que la entidad controla uno o varios autentificadores vinculados a la cuenta de la entidad. La autentificación a nivel AAL3 se basa en la demostración de la posesión de una clave siguiendo un protocolo criptográfico. Para la autentificación a nivel AAL3 se utilizará un autentificador criptográfico de hardware y un autentificador que resista a la suplantación del verificador; ambos requisitos pueden cumplirse con el mismo dispositivo. Para autentificarse a nivel AAL3 los declarantes deberán demostrar la posesión y control de dos factores de autentificación diferentes siguiendo uno o varios protocolos de autentificación seguros. Se exige la utilización de técnicas criptográficas globalmente aceptadas.

En esta revisión de la Recomendación no se propone un único conjunto de niveles de garantía normalizado y normativo. La definición de una única estructura de garantía normalizada para todas las comunidades menoscaba la capacidad de comunidades concretas para gestionar los riesgos en adecuación a su entorno. Sin embargo, se reconoce que esos distintos esquemas de garantía existen y que con frecuencia los proveedores de servicios de identidad deben poder demostrar que alcanzan uno o más AAL.

Dado que los esquemas AAL representan niveles crecientes de confianza en la verificación de una identidad declarada, con niveles crecientes de rigor en el proceso de autentificación correspondientes, en las descripciones de los controles de esta Recomendación se emplean términos relativos en lugar de AAL discretos. Para los controles que pueden modificarse para aumentar el nivel de confianza, las condiciones que ofrecen la menor confianza se señalan con "AAL más bajo"; una mayor confianza se señala con "AAL más alto", y las condiciones que ofrecen la mayor confianza se señalan con "AAL superior". El Cuadro 8-2 da una idea de cómo este convenio puede equipararse con algunos de los esquemas de garantía de autentificación más comunes. (Téngase en cuenta que la disposición del Cuadro 8-2 en modo alguno pretende establecer una equivalencia directa entre los diversos esquemas).

Cuadro 8-2 – Niveles de garantía de autentificación

AAL	Esquema de 4 AAL	Esquema de 3 AAL	Esquema de 3 niveles
Superior	AAL 4	AAL 3	Alto
Más alto	AAL 3	AAL 2	Notable
	AAL 2		
Más bajo	AAL 1	AAL 1	Bajo

En el resto de esta cláusula se presenta un superconjunto de controles normativos, agrupados en función de las amenazas que mitigan. Los proveedores de servicios de identidad identificarán las amenazas específicas a que se enfrentan de acuerdo con sus funciones y servicios, como se describe en esta Recomendación. Una vez determinadas esas amenazas, y para poder evaluar la conformidad con esta Recomendación, los proveedores de servicios de identidad documentarán las amenazas y las correspondientes descripciones de control, así como los resultados deseados, como se indica a continuación.

8.2 Puesta en peligro del autentificador

8.2.1 Riesgos de puesta en peligro del autentificador

La puesta en peligro del autentificador es cualquier ataque que duplique o altere la información de credencial, o que provoque su divulgación no autorizada, que puede utilizarse para efectuar la autentificación y obtener acceso no autorizado a un sistema de información. La puesta en peligro del

autentificador suele ocurrir en cualquier punto del ciclo de vida de la IdM. No obstante, las amenazas y controles que entran dentro del alcance de esta Recomendación sólo se refieren a la autentificación.

Las credenciales pueden ponerse en peligro mediante una serie de vectores de ataque, incluidos la peska, el robo, la duplicación de credenciales, el ataque por repetición y los ataques de fuerza bruta en línea o fuera de línea. La protección contra el riesgo de que se pongan en peligro las credenciales no se limita a los controles de esta categoría de amenaza. Cabe señalar que un fallo de control en cualquiera de las demás categorías de amenazas puede poner en peligro las credenciales. Por ejemplo, si un proveedor de servicios de autentificación sufre una intrusión en sus datos, la información obtenida puede utilizarse para acceder sin autorización al sistema de información.

8.2.2 Controles de puesta en peligro del autentificador

En el Cuadro 8-3 se enumeran los controles de puesta en peligro del autentificador.

Cuadro 8-3 – Controles de puesta en peligro del autentificador

Control N.°	Descripción del control	Resultado deseado
AC-1	Para alcanzar el AAL superior se ha de utilizar para la autentificación un autentificador criptográfico de hardware y un autentificador resistente a la suplantación del verificador. El mismo dispositivo puede cumplir ambos requisitos.	Se utilizan los autentificadores adecuados para lograr el AAL deseado.
AC-2	Para alcanzar el ALL superior los declarantes deben demostrar la posesión y el control de dos factores de autentificación diferentes siguiendo uno o varios protocolos de autentificación seguros.	Se siguen los protocolos de autentificación adecuados para lograr el AAL deseado.
AC-3	Se han de validar los autentificadores multifactoriales al nivel AAL superior en la medida exigida por un programa de verificación de módulo criptográfico	Se valida la criptografía del autentificador en la medida necesaria para lograr el AAL deseado.
AC-4	Se ha de validar que los autentificadores adquiridos por los IDP cumplen los requisitos del programa de verificación de módulo criptográfico aprobado.	Se utiliza criptografía aprobada.
AC-5	El verificador debe aplicar controles para proteger contra ataques por adivinación en línea, si ello es aplicable al tipo de autentificador.	El verificador aplica controles para proteger los autentificadores contra ataques por adivinación en línea.
AC-6	A menos que se especifique lo contrario en la descripción de un autentificador dado, el verificador debe limitar los intentos de autentificación fallidos consecutivos a no más de 100 para una sola cuenta.	El verificador aplica controles para proteger los autentificadores contra ataques por adivinación en línea.
AC-7	Los autentificadores criptográficos deben utilizar criptografía aprobada.	Se utiliza criptografía aprobada.

Cuadro 8-3 – Controles de puesta en peligro del autentificador

Control N.°	Descripción del control	Resultado deseado
AC-8	Si para la autentificación se utiliza más de un autentificador, al menos uno de ellos debe ser resistente a los ataques por repetición.	Se protegen los autentificadores contra los ataques por repetición.
AC-9	Todos los autentificadores de dispositivos criptográficos deben ser resistentes a los ataques por repetición.	Se emplean controles para proteger los autentificadores contra los ataques por repetición.
AC-10	La evaluación de riesgos efectuada por el CSP debe determinar los ataques de canal paralelo pertinentes.	El CSP efectúa las evaluaciones de riesgos adecuadas.
AC-11	La comunicación entre el declarante y el verificador (utilizando el canal primario en el caso de un autentificador fuera de banda) debe realizarse por un canal protegido autentificado.	Se protege la comunicación entre el declarante y el verificador.
AC-12	Los dispositivos criptográficos monofactoriales utilizados con el nivel AAL superior deben validarse en la medida que lo exige un programa de verificación de módulo criptográfico aprobado.	Se valida la criptografía del autentificador en la medida necesaria para lograr el AAL deseado.
AC-13	Cuando se utiliza un dispositivo como un teléfono inteligente en el proceso de autentificación, el desbloqueo de ese dispositivo (generalmente mediante un número de identificación personal (PIN) o un factor biométrico) no debe considerarse un factor de autentificación.	Se utilizan los autentificadores adecuados para lograr el nivel AAL deseado.
AC-14	El sistema biométrico no debe permitir más de 10 intentos de autentificación fallidos. Una vez alcanzado el límite, el autentificador debe: • imponer un tiempo de espera mínimo de 30 s antes de proceder al siguiente intento, que aumente exponencialmente con cada intento sucesivo (por ejemplo, 1 min antes del siguiente intento fallido, 2 min antes del segundo intento fallido), o • Desactivar la autentificación biométrica del usuario y ofrecer otro factor (por ejemplo, un factor biométrico diferente o un PIN/contraseña, si no es un factor ya requerido), si se dispone de tal método alternativo.	El sistema biométrico aplica controles para proteger los autentificadores contra ataques por adivinación.

8.3 Puesta en peligro de la transacción

8.3.1 Riesgos de puesta en peligro de la transacción

La puesta en peligro de la transacción es un ataque que menoscaba la confidencialidad de los datos en tránsito, o su disponibilidad, mientras se intercambian entre dos partes. Los ataques más comunes que pueden poner en peligro una transacción son los ataques por intermediario (MItM, *man-in-the-middle*) y por intermediario de navegador (MItB, *man-in-the-browser*), la escucha clandestina y el pirateo de sesión.

8.3.2 Controles de puesta en peligro de la transacción

En el Cuadro 8-4 se enumeran los controles de puesta en peligro de la transacción.

Cuadro 8-4 – Controles de puesta en peligro de la transacción

Control N.°	Descripción de control	Resultado deseado
TC-1	Cuando el verificador y el CSP son entidades distintas, las comunicaciones entre el verificador y el CSP deben realizarse por un canal seguro mutuamente autentificado (como una conexión TLS autentificada por el cliente) utilizando criptografía aprobada.	Se protegen las comunicaciones entre el verificador y el CSP.
TC-2	El software del abonado y el servicio a que se accede deben compartir un secreto de sesión.	Se utilizan y protegen los secretos de sesión.
TC-3	El contenido de localizadores uniformes de recursos (URL, *uniform resource locators*) o HTTP POST [b-IETF RFC 7231] debe incluir un identificador de sesión que la RP ha de verificar para garantizar que las acciones ajenas a la sesión no afectan a la sesión protegida.	La RP verifica los identificadores de sesión.
TC-4	El software del abonado debe presentar directamente el secreto o demostrar que posee el secreto utilizando un mecanismo criptográfico.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.
TC-5	Los secretos utilizados para la vinculación de sesión no deben estar disponibles para las comunicaciones no seguras entre el anfitrión y el punto extremo del abonado. Tras la autentificación las sesiones autentificadas no deben retroceder a un transporte no seguro, por ejemplo, de protocolo de transferencia hipertexto seguro (HTTPS) a protocolo de transferencia hipertexto (HTTP).	Se protege la transmisión de secretos de sesión.
TC-6	El anfitrión de la sesión debe generar secretos para la vinculación de sesión durante la interacción, por lo general inmediatamente después de autentificar al usuario.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.
TC-7	Los secretos utilizados para la vinculación de sesión deben estar generados por un generador de bits aleatorios aprobado y contener al menos 64 bits de entropía.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.

Cuadro 8-4 – Controles de puesta en peligro de la transacción

Control N.°	Descripción de control	Resultado deseado
TC-8	Cuando el usuario se desconecta el sujeto de la sesión debe borrar o invalidar los secretos utilizados para la vinculación de sesión.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.
TC-9	Los secretos utilizados para la vinculación de sesión deben enviarse y recibirse desde y hacia los dispositivos utilizando un canal protegido autentificado.	Se protege la transmisión de secretos de sesión.
TC-10	Los secretos utilizados para la vinculación de sesión deben expirar y el CSP no debe aceptarlos tras un plazo definido.	Se protege la transmisión de secretos de sesión.
TC-11	El secreto utilizado para la vinculación de sesión debe ser generado por el anfitrión de la sesión como respuesta directa a un evento de autentificación.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.
TC-12	Las cookies de navegador deberán estar etiquetadas para que sólo sean accesibles en sesiones HTTPS.	Se protege la transmisión de secretos de sesión.
TC-13	Las cookies de navegador serán accesibles al mínimo de nombres de anfitrión y trayectos posible.	Se protege la transmisión de secretos de sesión.
TC-14	La continuidad de las sesiones autentificadas deberá basarse en la posesión de un secreto de sesión expedido por el verificador en el momento de la autentificación y, optativamente, renovado durante la sesión.	Los secretos de sesión se generan aleatoriamente, se utilizan adecuadamente y se destruyen adecuadamente tras su utilización.
TC-15	Si la comparación se efectúa de manera centralizada, todas las transmisiones de datos biométricos se efectuarán por el canal protegido autentificado.	Se protege la transmisión de información biométrica.
TC-16	Se ha de establecer un canal protegido autentificado ente el sensor (por un punto extremo con un sensor resistente a la sustitución de sensores) y el verificador.	Se protegen las comunicaciones entre el verificador y los puntos extremos.

8.4 Suplantación del verificador

8.4.1 Riesgos de suplantación del verificador

La suplantación del verificador es un ataque en el que la entidad interactúa con un verificador falso que la induce a revelar información de credenciales. La información obtenida por el atacante supone un riesgo importante de suplantación de abonado o de puesta en peligro de las credenciales. Uno de los ataques más comunes asociados con la suplantación del verificador es la peska. Un atacante engaña a una entidad para que transmita información de credenciales de abonado a un cliente, un servidor o un servicio no fiable y utiliza la información de credenciales obtenida para acceder sin autorización al sistema de información.

8.4.2 Controles de suplantación del verificador

En el Cuadro 8-5 se enumeran los controles de suplantación del verificador.

Cuadro 8-5 – Controles de suplantación del verificador

Control N.°	Descripción del control	Resultado deseado
VI-1	Se ha de validar que los verificadores cumplen los requisitos de un programa de verificación de módulo criptográfico aprobado.	Se utiliza criptografía aprobada.
VI-2	Un protocolo de autentificación resistente a la suplantación del verificador debe establecer un canal protegido autentificado con el verificador.	Se protege la salida del autentificador.
VI-3	Un canal protegido autentificado debe vincular fuerte e irreversiblemente el identificador de canal negociado al establecer el canal protegido autentificado con la salida del autentificador.	Se protege la salida del autentificador.
VI-4	El verificador debe validar la firma u otra información utilizada para demostrar la resistencia a la suplantación del verificador.	Los verificadores realizan efectivamente la validación.
VI-5	Se deben utilizar algoritmos criptográficos aprobados para establecer la resistencia a la suplantación del verificador allá donde sea necesario.	Se utiliza criptografía aprobada.
VI-6	Las claves utilizadas para establecer la resistencia a la suplantación del verificador deben ofrecer al menos la intensidad de seguridad mínima especificada en una norma criptográfica aplicable.	No se suplantan los verificadores.
VI-7	Para poder considerarse resistentes a la puesta en peligro del verificador, las claves públicas almacenadas por el verificador deben asociarse a la utilización de algoritmos criptográficos aprobados y deben ofrecer al menos la intensidad de seguridad mínima especificada en una norma criptográfica aplicable.	Los verificadores no están en peligro.
VI-8	Los secretos resistentes a la puesta en peligro del verificador deben utilizar algoritmos de aleatorización y los secretos subyacentes deben tener al menos la intensidad de seguridad mínima especificada en una norma criptográfica aplicable.	Los verificadores no están en peligro.
VI-9	Los autentificadores que conllevan la introducción manual de una salida de autentificador, como los autentificadores OTP y fuera de banda, no se considerarán resistentes a la suplantación del verificador, pues la introducción manual no vincula la salida del autentificador a la sesión concreta que se autentifica.	No se utilizan autentificadores que exigen la introducción manual para la protección contra la suplantación del verificador.

8.5 Suplantación del abonado

8.5.1 Riesgos de suplantación del abonado

La suplantación del abonado es un ataque que implica la falsificación de una identidad legítima para pervertir el proceso de autentificación y obtener acceso no autorizado a una red o sistema de información. Los ataques de suplantación del abonado comunes son la falsificación de identidad y el pirateo de sesión. Un ejemplo de ataque por usurpación de identidad sería cuando un atacante que usurpa la identidad de la RP falsifica una dirección de control de acceso a medios (MAC, *media access control*) que pertenece a un dispositivo autentificado que obtiene acceso no autorizado a la red. Otro ejemplo es la simulación, que ocurre cuando un atacante suplanta a un usuario legítimo

ofreciendo pruebas falsificadas o robadas y puede seguir con éxito el protocolo de reinicialización de credenciales.

8.5.2 Controles de suplantación del abonado

En el Cuadro 8-6 se enumeran los controles de suplantación del abonado.

Cuadro 8-6 – Controles de suplantación del abonado

Control N.°	Descripción del control	Resultado deseado
SI-1	El resultado de un proceso de autentificación es un identificador que debe utilizarse cada vez que un abonado se autentifica ante esa RP.	Los autentificadores están vinculados al abonado apropiado.
SI-2	Para satisfacer los requisitos de un AAL dado, el declarante debe autentificarse como mínimo con un nivel de intensidad dado para que se le reconozca como abonado.	El abonado se autentifica utilizando los autentificadores apropiados con el nivel de intensidad adecuado para lograr el AAL deseado.
SI-3	Todos los procesos de autentificación y reautentificación deben demostrar la voluntad de autentificación de al menos un autentificador.	Se demuestra la voluntad del autentificador.
SI-4	Los CSP deben facilitar al abonado instrucciones sobre cómo proteger adecuadamente los autentificadores contra el robo o la pérdida.	El abonado puede recuperar los autentificadores sin sortear el AAL deseado.
SI-5	La autentificación al nivel AAL más bajo se llevará a cabo cuando se utilice uno de los tipos de autentificadores siguientes: • secretos memorizados; • secretos buscados; • dispositivos fuera de banda; • dispositivos OTP monofactoriales; • dispositivos OTP multifactoriales; • software criptográfico monofactorial; • dispositivo criptográfico monofactorial; • software criptográfico multifactorial; • dispositivo criptográfico multifactorial.	El abonado se autentifica utilizando los autentificadores apropiados con el nivel de intensidad adecuado para lograr el AAL deseado.
SI-6	La autentificación al nivel AAL más alto se llevará a cabo cuando se utilice un autentificador multifactorial o una combinación de dos autentificadores monofactoriales. Cuando se utilice un autentificador multifactorial se podrá utilizar cualquiera de los siguientes: • dispositivo OTP multifactorial; • software criptográfico multifactorial; • dispositivo criptográfico multifactorial;	El abonado se autentifica utilizando los autentificadores apropiados con el nivel de intensidad adecuado para lograr el AAL deseado.

Cuadro 8-6 – Controles de suplantación del abonado

Control N.°	Descripción del control	Resultado deseado
SI-7	Cuando se utiliza una combinación de dos autentificadores monofactoriales, se ha de incluir un autentificador de secreto memorizado y un autentificador por posesión (es decir, "algo que tienes") de la lista siguiente: • secreto buscado; • dispositivo fuera de banda; • dispositivo OTP monofactorial; • software criptográfico monofactorial; • dispositivo criptográfico monofactorial;	El abonado se autentifica utilizando los autentificadores apropiados con el nivel de intensidad adecuado para lograr el AAL deseado.
SI-8	La autentificación al nivel AAL superior se llevará a cabo utilizando una combinación de autentificadores, entre las que se pueden citar las siguientes: • dispositivo criptográfico multifactorial; • dispositivo criptográfico monofactorial y secreto memorizado; • dispositivo OTP multifactorial (software o hardware) y dispositivo criptográfico monofactorial; • dispositivo OTP multifactorial (sólo hardware) y software criptográfico monofactorial; • dispositivo OTP monofactorial (sólo hardware) y software criptográfico multifactorial; • dispositivo OTP monofactorial (sólo hardware) y software criptográfico monofactorial y secreto memorizado.	El abonado se autentifica utilizando los autentificadores apropiados con el nivel de intensidad adecuado para lograr el AAL deseado.
SI-9	El CSP debe facilitar un mecanismo para revocar o suspender el autentificador inmediatamente después de que el abonado notifique su sospecha de pérdida o robo del autentificador.	Los autentificadores inválidos no pueden utilizarse para autentificar satisfactoriamente a una entidad.
SI-10	Para facilitar la comunicación segura de la pérdida, el robo o el daño de un autentificador, el CSP facilitará al abonado un método de autentificación ante el CSP utilizando un autentificador de reserva o alternativo. Este autentificador de reserva debe ser un secreto memorizado o un autentificador físico.	El abonado puede recuperar los autentificadores sin sortear el AAL deseado.
SI-11	La suspensión debe ser reversible si el abonado se autentifica satisfactoriamente ante el CSP utilizando un autentificador válido (es decir, no suspendido) y solicita la reactivación de un autentificador suspendido.	El abonado puede recuperar los autentificadores sin sortear el AAL deseado.
SI-12	Cuando un autentificador expire, si expira, quedará inutilizable para la autentificación.	Los autentificadores inválidos no pueden utilizarse para autentificar satisfactoriamente a una entidad.

Cuadro 8-6 – Controles de suplantación del abonado

Control N.°	Descripción del control	Resultado deseado
SI-13	El CSP debe exigir a los abonados que abandonen o destruyan todo autentificador físico que contenga certificados atributo firmados por el CSP tan pronto como sea posible después de que el autentificador se invalide por expiración revocación, terminación, renovación o cualquier otro medio definido por el CSP.	Los autentificadores inválidos no pueden utilizarse para autentificar satisfactoriamente a una entidad.
SI-14	Los CSP deben revocar rápidamente la vinculación de los autentificadores cuando una identidad en línea deje de existir, cuando así lo solicite el abonado o cuando el CSP determine que el abonado ya no cumple los requisitos de admisibilidad.	Los autentificadores inválidos no pueden utilizarse para autentificar satisfactoriamente a una entidad.
SI-15	La biometría sólo debe utilizarse como parte de una autentificación multifactorial con un autentificador físico (algo que tienes).	La biometría se utiliza adecuadamente como autentificador.
SI-16	En el nivel AAL más alto, el CSP debe vincular al menos uno, y debe vincular al menos dos, identificadores físicos (algo que tienes) a una identidad en línea de abonado, además de un secreto memorizado o uno o más factores biométricos.	Los autentificadores están vinculados al abonado apropiado
SI-17	En el nivel AAL más alto, si el registro y la vinculación no pueden completarse en un único encuentro físico o transacción electrónica, se utilizarán los siguientes métodos para garantizar que la misma parte hace de solicitante a lo largo de los procesos: Para las transacciones a distancia: 1) El solicitante debe identificarse en cada nueva transacción presentando un secreto temporal, creado durante una transacción anterior o enviado al número de teléfono, la dirección de correo-e o la dirección postal registrados del solicitante. 2) Los secretos autentificadores a largo plazo sólo se expedirán al solicitante en el marco de una sesión protegida. Para las transacciones presenciales: 1) El solicitante debe identificarse en persona utilizando un secreto, como se indica para las transacciones a distancia 1) anteriores, o mediante un factor biométrico registrado durante un encuentro anterior. 2) Los secretos temporales no deben reutilizarse. 3) Si el CSP expide secretos autentificadores a largo plazo durante una transacción física, éstos deben cargarse en un dispositivo físico que se entrega al solicitante en persona o utilizando un medio que confirme la dirección registrada.	Los autentificadores están vinculados al abonado apropiado.
SI-18	Al vincular un autentificador adicional a la cuenta de un abonado, el CSP debe pedir primero al abonado que se autentifique como mínimo al nivel AAL que se utilizará con el nuevo autentificador.	Los autentificadores están vinculados al abonado apropiado.

Cuadro 8-6 – Controles de suplantación del abonado

Control N.°	Descripción del control	Resultado deseado
SI-19	En el nivel AAL más alto, si un abonado pierde todos los autentificadores de un factor necesario para completar la autentificación multifactorial, el abonado deberá repetir el proceso de demostración de identidad.	El abonado puede recuperar los autentificadores sin sortear el AAL deseado.
SI-20	Al sustituir un factor de autentificación perdido para el nivel AAL más alto, el CSP debe exigir al declarante que se autentifique con un autentificador de cualquiera de los factores restantes para confirmar la vinculación con la identidad existente.	El abonado puede recuperar los autentificadores sin sortear el AAL deseado.
SI-21	Se ha de proceder a la reautentificación periódica de las sesiones para confirmar la presencia continua del abonado en una sesión autentificada.	El abonado se ha de reautentificar periódicamente con el/los autentificador(es) adecuados de la intensidad necesaria para lograr el AAL deseado.
SI-22	Se ha de proceder a la reautentificación periódica de las sesiones del abonado. a) En el nivel AAL más bajo, la reautentificación del abonado debe repetirse al menos una vez cada 30 días en el caso de una sesión prolongada, independientemente de la actividad del usuario. b) En el nivel AAL más bajo, la sesión debe terminarse (es decir, por desconexión) cuando se alcance este límite temporal. c) En el nivel AAL más alto, la reautentificación del abonado debe repetirse al menos una vez cada 12 h en el caso de una sesión prolongada, independientemente de la actividad del usuario. d) En el nivel AAL más alto, la reautentificación del abonado debe repetirse tras cualquier periodo de inactividad igual o superior a 30 m. e) En el nivel AAL más alto, la sesión debe terminarse (es decir, por desconexión) cuando se alcance cualquiera de esos límites temporales. f) En el nivel AAL superior, la autentificación del abonado debe repetirse al menos una vez cada 12 h durante una sesión prolongada, independientemente de la actividad del usuario. g) En el nivel AAL superior, la reautentificación del abonado debe repetirse tras cualquier periodo de inactividad igual o superior a 15 m. h) En el nivel AAL superior, la sesión debe terminarse (es decir, por desconexión) cuando se alcance cualquiera de los límites (f o g). i) En el nivel AAL superior, la reautentificación periódica de las sesiones de abonado deberá realizarse utilizando todos los factores de autentificación originales.	El abonado se ha de reautentificar periódicamente con el/los autentificador(es) adecuados de la intensidad necesaria para lograr el AAL deseado.

Cuadro 8-6 – Controles de suplantación del abonado

Control N.°	Descripción del control	Resultado deseado
SI-23	Una sesión no debe ampliarse por la simple presentación del secreto de sesión.	El abonado se ha de reautentificar periódicamente con el/los autentificador(es) adecuados de la intensidad necesaria para lograr el AAL deseado.
SI-24	Una vez terminada una sesión, por expiración del temporizador u otros medios, el usuario deberá volver a seguir el proceso de autentificación para establecer una nueva sesión.	El abonado se ha de reautentificar periódicamente con el/los autentificador(es) adecuados de la intensidad necesaria para lograr el AAL deseado.
SI-25	Los secretos de sesión deben ser no persistentes, es decir, que no se conservarán tras el reinicio de la aplicación en cuestión o la reinicialización del dispositivo anfitrión.	El abonado se ha de reautentificar periódicamente con el/los autentificador(es) adecuados de la intensidad necesaria para lograr el AAL deseado.

8.6 Riesgos y controles de la puesta en peligro del servicio de autentificación

8.6.1 Riesgos de puesta en peligro del servicio de autentificación

La puesta en peligro del servicio de autentificación es un ataque a la entidad que facilita el servicio de identidad y hace que sea inválido, inexacto, esté indisponible o no pueda funcionar como corresponde. Toda vulnerabilidad explotada del entorno de control del sistema de información de la entidad puede poner en peligro el servicio de autentificación. Se trata, por ejemplo, del caso en que un atacante puede explotar una vulnerabilidad de software no corregida y obtener acceso privilegiado no autorizado al sistema de información del servicio de autentificación.

8.6.2 Controles de puesta en peligro del servicio de autentificación

En el Cuadro 8-7 se enumeran los controles de puesta en peligro del servicio de autentificación

Cuadro 8-7 – Controles de puesta en peligro del servicio de autentificación

Control N.°	Descripción del control	Resultado deseado
ASC-1	El CSP debe emplear controles de seguridad adecuadamente adaptados al nivel de seguridad, como se especifica en [b-ISO/CEI 27002] o una norma equivalente.	Se protege la integridad del servicio de autentificación contra su puesta en peligro.
ASC-2	El CSP debe garantizar la satisfacción de los controles de garantía mínimos dentro del contexto de riesgo del sistema global.	Se protege la integridad del servicio de autentificación contra su puesta en peligro.
ASC-3	Si se realiza una comparación centralizada, se implementará la revocación biométrica, denominada protección de la plantilla biométrica en [b-ISO/CEI 24745].	El servicio de autentificación protege la información biométrica.

Cuadro 8-7 – Controles de puesta en peligro del servicio de autentificación

Control N.°	Descripción del control	Resultado deseado
ASC-4	El autentificador debe establecer la intención de autentificación, aunque los dispositivos criptográficos multifactoriales pueden establecer la intención mediante la reintroducción de los otros factores de autentificación en el punto extremo en que se utiliza el autentificador.	Sólo el autentificador establece la intención de autentificación.
ASC-5	A lo largo del ciclo de vida de la identidad digital el CSP debe mantener un registro de todos los autentificadores que están o han estado asociados a cada identidad.	Se registra y conserva la información del autentificador.
ASC-6	El CSP o el verificador también conservarán la información necesaria para acelerar los intentos de autentificación, cuando sea necesario.	Se registra y conserva la información del autentificador.
ASC-7	El registro creado por el CSP contendrá la fecha y hora en que el autentificador se vinculó a la cuenta.	Se registra y conserva la información del autentificador.
ASC-8	Los autentificadores deben vincularse a las cuentas: • por expedición por el CSP como parte del registro; o • por asociación a un autentificador facilitado por el abonado que sea aceptable para el CSP.	Los autentificadores se vinculan adecuadamente a las cuentas de los abonados.
ASC-9	Cuando un nuevo autentificador se vincula a una cuenta de abonado, el CSP debe garantizar que se siguen el protocolo de vinculación y el protocolo de configuración de la(s) clave(s) asociada(s) con un nivel de seguridad acorde al AAL en el que se utiliza el autentificador.	Los autentificadores se vinculan adecuadamente a las cuentas de los abonados.
ASC-10	La vinculación de autentificadores multifactoriales debe exigir la autentificación multifactorial o la asociación con la sesión en que se ha completado la demostración de identidad.	Los autentificadores se vinculan adecuadamente a las cuentas de los abonados.

8.7 Riesgos y controles de privacidad

8.7.1 Riesgos de privacidad

La autentificación digital soporta la protección de la privacidad reduciendo los riesgos de acceso no autorizado a la información de las personas. Al mismo tiempo, dado que la demostración de identidad, la autentificación, la autorización y la federación implican el procesamiento de información personal, esas funciones también pueden plantear riesgos de privacidad. Por consiguiente, en estas directrices se incluyen requisitos y consideraciones de privacidad para reducir los posibles riesgos asociados a la privacidad.

El CSP procederá a una evaluación de los riesgos de privacidad para la retención de registros. La evaluación de los riesgos de privacidad puede considerar lo siguiente:

1) La probabilidad de que la retención de registros suponga un problema para el abonado, por ejemplo, invasividad o acceso no autorizado a la información.

2) Las consecuencias que podría tener ese problema.

El CSP debe poder justificar razonablemente toda respuesta opuesta a los riesgos de privacidad identificados, incluidas la aceptación del riesgo, la mitigación del riesgo y la compartición del riesgo.

La utilización del consentimiento del abonado es una forma de compartir el riesgo, por lo que sólo conviene utilizarlo cuando se puede esperar razonablemente que el usuario tiene la capacidad de evaluar y aceptar el riesgo compartido.

8.7.2 Controles de privacidad

En el Cuadro 8-8 se enumeran los controles de privacidad.

Cuadro 8-8 – Controles de privacidad

Control Nº	Descripción del control	Resultado deseado
P-1	UN IDP debe seleccionar como mínimo un nivel AAL adecuado cuando se facilita en línea IIP autoaseverada u otro tipo de información personal.	El CSP aplica políticas y controles de privacidad a la autentificación.
P-2	El CSP debe respetar sus propias políticas de retención de registros de conformidad con la legislación, la reglamentación y las políticas aplicables. Si el CSP opta por conservar registros sin que ello se le exija obligatoriamente, el CSP deberá realizar un proceso de gestión de riesgos, incluidas la evaluación de los riesgos de privacidad y seguridad, para determinar cuánto tiempo se han de conservar los registros y debe informar al abonado acerca de la política de retención.	El CSP autentifica a los abonados de conformidad con la legislación, la reglamentación y las políticas aplicables.
P-3	Se ha de velar por que la utilización de IIP se limita al objetivo original por el que se recabó.	El CSP obtiene la mínima IIP necesaria para lograr el AAL deseado.
P-4	Si la utilización de IIP no tiene por objetivo la autentificación o el cumplimiento con leyes o procedimientos legales, el CSP debe notificarlo al abonado y obtener su consentimiento.	El CSP autentifica a los abonados de conformidad con la legislación, la reglamentación y las políticas aplicables.
P-5	El IDP debe realizar o publicar una evaluación de la incidencia en la privacidad (PIA, *privacy impact assessment*) para que la obtención de IIP y demás información personal sea conforme a las leyes y reglamentos aplicables.	El CSP realiza PIA.
P-6	El CSP no debe utilizar o divulgar información sobre los abonados para fines distintos de la autentificación, la mitigación del fraude o el cumplimiento de la ley o procesos legales, a menos que el CSP lo notifique claramente al abonado y obtenga su consentimiento para usos adicionales.	El CSP autentifica a los abonados de conformidad con la legislación, la reglamentación y las políticas aplicables.
P-7	El CSP debe emplear controles de privacidad adecuadamente adaptados especificados en [ISO/CEI 27002] o normas equivalentes.	El CSP aplica políticas y controles de privacidad a la autentificación.

Cuadro 8-8 – Controles de privacidad

Control Nº	Descripción del control	Resultado deseado
P-8	El CSP no debe exigir que el consentimiento sea una condición del servicio.	El CSP autentifica a los abonados de conformidad con la legislación, la reglamentación y las políticas aplicables.
P-9	Si bien el CSP puede vincular un autentificador AAL más bajo a una identidad AAL más alto, si el abonado se autentifica en el nivel AAL más bajo, el CSP no debe exponer la información personal, ni siquiera la autoaseverada, al abonado.	El CSP obtiene la mínima IIP o información necesaria para lograr el AAL deseado.
P-10	La aceptación por el abonado de los usos adicionales no debe ser una condición para la prestación de servicios de autentificación.	El CSP autentifica a los abonados de conformidad con la legislación, la reglamentación y las políticas aplicables.

Apéndice I

Ejemplo de autentificación fuerte con [b-UIT-T X.1278]

(Este apéndice no forma parte integrante de esta Recomendación.)

I.1 Introducción

En el *Marco de autentificación universal* [b-UIT-T X.1277] y el *Protocolo cliente a autentificador/ Marco Universal de 2 factores* [b-UIT-T X.1278] se presentan métodos de autentificación y garantía de autentificación que ofrecen una autentificación fuerte basada en Recomendaciones abiertas e interoperables. En este Apéndice se presenta un ejemplo de autentificación fuerte con [b-UIT-T X.1278].

I.2 Categorías de amenazas

En la Figura I.1 se agrupan las amenazas en dos categorías:

1) Ataques adaptables – que se ataquen 1 000 o 1 000 000 de objetivos no influye en el coste del ataque.
    a) Ataques a distancia a servidores y robo de contraseñas. Este ataque es muy serio porque los usuarios no pueden protegerse contra él; tienen que hacerlo las RP. Sin embargo, los usuarios pueden empeorar la situación si comparten contraseñas con múltiples RP, pues la menos segura de ella puede ser pirateada y afectar a todas las demás.
    b) Ataques a distancia a múltiples dispositivos de usuario. Por ejemplo, intentar **robar datos** del dispositivo para suplantar al usuario.
    c) Los ataques a distancia a dispositivos de usuario también pueden causar la **utilización indebida** de los dispositivos de usuario para suplantar a los usuarios.
    d) Ataques a distancia a dispositivos de usuario para utilizar indebidamente una sesión fuertemente autentificada. Esto se conoce como ataque MITB.

Conviene señalar que las tarjetas inteligentes no protegen por sí solas contra la utilización indebida de credenciales, pues la tarjeta inteligente no puede saber si el PIN ha sido introducido por el usuario o inyectado por un malware que lo haya obtenido ilícitamente del usuario con anterioridad.

2) Ataques físicos, para los que se requiere acceso físico al dispositivo. Los ataques físicos no son adaptables, pues el robo (activo) de teléfonos inteligentes tiene un elevado costo por objetivo.
    a) Ataques físicos a dispositivos de usuario para **robar datos** para la suplantación.
    b) Ataques físicos a dispositivos de usuario para **utilizarlos indebidamente** para la suplantación.

I.3 [b-UIT-T X.1278] permite la "autentificación fuerte con un alto nivel de garantía"

Por autentificación fuerte con un alto nivel de garantía se entiende:

1) La utilización de dos o más factores
2) Que al menos uno de los factores utilice la criptografía de clave pública
3) Que no sea susceptible a ataques de peska, MITM o de otro tipo dirigidos a las credenciales

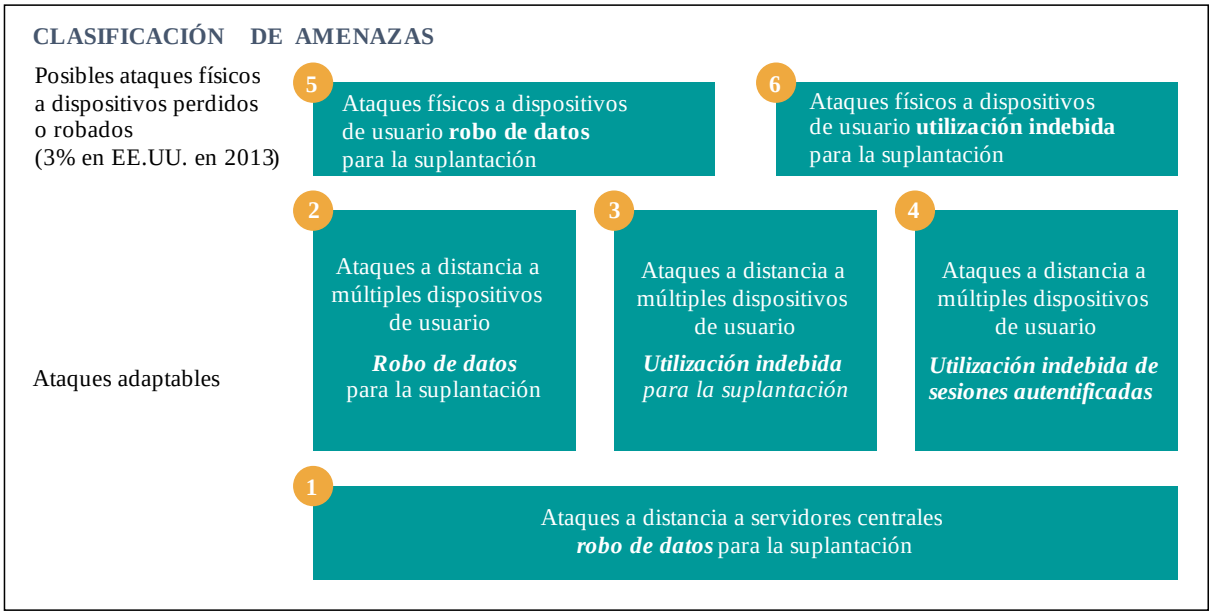
Las principales características distintivas del método fast identity on-line (FIDO) son las siguientes:

- No hay secretos compartidos – se utiliza lo que tienes (por ejemplo, dispositivos de hardware) y lo que eres (por ejemplo, huellas digitales);
- Se utiliza la criptografía de clave pública en lugar de secretos compartidos simétricos;

- El autentificador verifica al usuario y la RP autentifica al autentificador; y
- Es una autentificación multifactorial resistente a la peska.

Estos métodos respetan los siguientes principios de seguridad y privacidad:

- No hay vinculación posible entre servicios o cuentas.
- No intervienen terceros en el protocolo.
- De utilizarse, la información biométrica nunca sale del dispositivo.
- Las claves criptográficas permanecen en el dispositivo.
- No hay secretos compartidos en el lado servidor; y
- Se basan en la criptografía de clave pública.



X.1254(20)_FI.1

Figura I.1 – Clasificación de amenazas

I.4 Autentificación por contraseñas obsoleta

Los procesos de autentificación por contraseña típicos conllevan varios riesgos, como se muestra en la Figura I.2.

1) Las contraseñas pueden robarse del servidor (fuga de datos).
2) Las contraseñas pueden introducirse en aplicaciones o sitios web no fiables (peska); y
3) Tener que recordar demasiadas contraseñas induce a su reutilización (lo que facilita la adivinación de contraseñas en varios sitios).
4) No es cómodo escribir contraseñas en teléfonos (los usuarios eligen contraseñas más fáciles de adivinar).

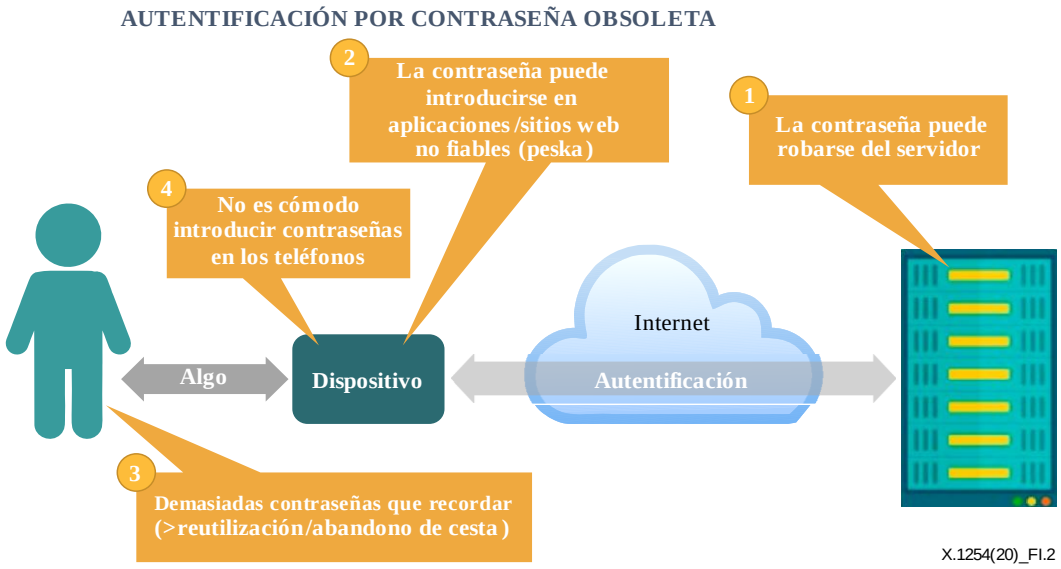


Figura I.2 – Autentificación por contraseña obsoleta

I.5 Nueva autentificación con [b-UIT-T X.1278]

FIDO separa la autentificación de la identidad. En la Figura I.3 se muestran las ventajas de este método.

1) No se almacenan secretos en el servidor (protección contra las fugas de datos).
2) La peska no pone en peligro los autentificadores.
3) No hay contraseñas que recordar ni fricciones añadidas al proceso de autentificación.
4) Comodidad de uso para el usuario.

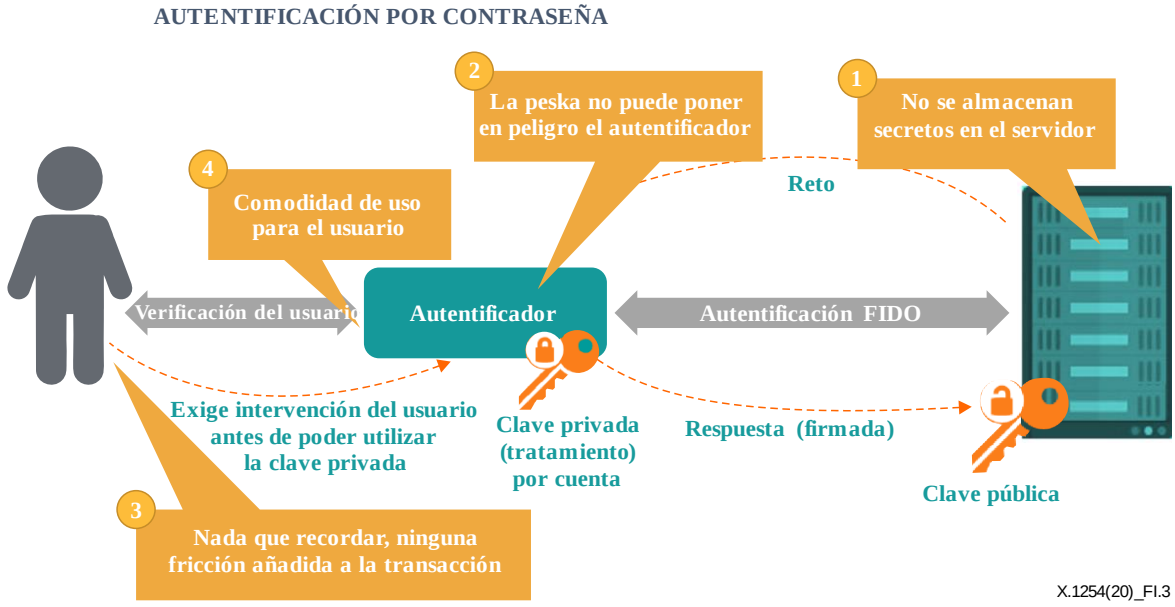


Figura I.3 – Nueva autentificación con [b-UIT-T X.1278]

I.6 Interoperabilidad y certificación

Además de crear nuevos métodos de autentificación, la fuerza de la autentificación aumenta gracias a las pruebas de interoperabilidad y certificación.

- Aumento de la aceptabilidad de la autentificación fuerte por los usuarios o los consumidores.
- Menor riesgo robo de identidad, y sus consecuencias, gracias al amplio despliegue de la autentificación fuerte.
- Experiencia del usuario cómoda y mejorada gracias a una amplia gama de dispositivos y servicios de autentificación.
- La reducción de costes aumenta la adopción de la autentificación fuerte.

Bibliografía

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autentificación de entidad*.

[b-UIT-T X.1277] Recomendación ITU-T X.1277 (2018), *Marco de autentificación universal*.

[b-UIT-T X.1278] Recomendación ITU-T X.1278 (2018), *Protocolo cliente a autentificador/Marco Universal de 2 factores*.

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/CEI 19790] ISO/CEI 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/CEI 24745] ISO/CEI 24745:2011, *Information technology – Security techniques – Biometric information protection*.

[b-ISO/CEI 24760-1] ISO/CEI 24760-1:2019, *IT security and privacy – A framework for identity management – Part 1: Terminology and concepts.*

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/CEI 27002] ISO/CEI 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

[b-ISO/CEI 29003] ISO/CEI TS 29003:2018, *Information technology – Security techniques – Identity proofing*.

[b-ISO/IEC 29115] ISO/CEI 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework.*

[b-IETF RFC 7231] IETF, RFC 7231 (2014), *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021