

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1254

(05/2013)

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

Seguridad en el ciberespacio – Gestión de identidades

Marco de garantía de autenticación de entidad

Recomendación UIT-T X.1254

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	
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	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
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/eurística	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

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

Recomendación UIT-T X.1254

Marco de garantía de autenticación de entidad

Resumen

En la presente Recomendación se definen cuatro niveles de garantía de autenticación de entidad (a saber, NdG1 – NdG4) y los criterios y amenazas para cada uno de esos cuatro niveles. Asimismo:

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

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1254	2012-09-07	17

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.

Se publicó un texto similar como ISO/CEI 29115. Difiere de este texto en cuatro puntos: 1) cláusula 3.1.6: la definición de credencial es distinta y esta Recomendación hace referencia a la definición que figura en la Recomendación UIT-T X.1252; 2) Cuadro 10-1: ISO/CEI 29115 incluye un ejemplo de suplantación que consiste en el uso de una identificación por parte de una entidad que no existe; 3) cláusula 10.2.2.1: ISO/CEI 29115 describe SSL como un ejemplo de canal protegido; 4) En esta Recomendación el Anexo A, *Características de una credencial*, es normativo.

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/>.

© UIT 2013

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

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	2
4 Abreviaturas y acrónimos	3
5 Convenios	4
6 Niveles de garantía	4
6.1 Nivel de garantía 1 (NdG1)	5
6.2 Nivel de garantía 2 (NdG2)	6
6.3 Nivel de garantía 3 (NdG3)	6
6.4 Nivel de garantía 4 (NdG4)	6
6.5 Selección del nivel de garantía adecuado.....	7
6.6 Correspondencia y compatibilidad de NdG	8
6.7 Intercambio de resultados de autenticación basado en los 4 NdG.....	9
7 Actores.....	9
7.1 Entidad.....	9
7.2 Proveedor de servicio de credenciales.....	10
7.3 Autoridad de registro	10
7.4 Parte que confía	10
7.5 Verificador.....	10
7.6 Tercero fiable.....	10
8 Fases del marco de garantía de autenticación de entidad.....	10
8.1 Fase de afiliación.....	11
8.2 Fase de gestión de credenciales	14
8.3 Fase de autenticación de la entidad.....	16
9 Consideraciones relativas a la gestión y organización	17
9.1 Establecimiento del servicio.....	17
9.2 Observancia jurídica y contractual	17
9.3 Disposiciones financieras	17
9.4 Gestión y auditoría de la seguridad de la información	17
9.5 Componentes externos del servicio	18
9.6 Infraestructura operativa.....	18
9.7 Evaluación de las capacidades operacionales.....	18

	Página
10 Amenazas y controles	18
10.1 Amenazas a la fase de afiliación y control de la misma.....	18
10.2 Amenazas a la fase de gestión de credenciales y control de la misma.....	21
10.3 Amenazas a la fase de autenticación y control de la misma	26
11 Criterios de garantía del servicio	31
Anexo A – Características de una credencial.....	32
Apéndice I – Privacidad y protección de la PII	34
Bibliografía	36

Introducción

Los requisitos de seguridad de muchas transacciones electrónicas entre sistemas TIC o internas dependen de un nivel de confianza tácito o específico en la identidad de las entidades implicadas. Estos requisitos pueden consistir en la protección de bienes y recursos contra el acceso no autorizado, para lo que puede recurrirse a un mecanismo de control de acceso, y/o la imputación de responsabilidades mediante el mantenimiento de registros de auditoría de eventos pertinentes, y para fines de contabilidad y tasación.

La Recomendación UIT-T X.1254 describe un marco para la garantía de autenticación de la entidad. Por garantía en la presente Recomendación se entiende la confianza depositada en todos los procesos, actividades de gestión y tecnologías empleadas para establecer y gestionar la identidad de una entidad que se emplea en transacciones con autenticación.

Características técnicas		Consideraciones relativas a la gestión y organización
Fase de afiliación	<ul style="list-style-type: none"> • Aplicación e iniciación • Demostración de la identidad y verificación de la información de identidad 	<ul style="list-style-type: none"> • Mantenimiento de registros • Inscripción
Fase de gestión de credenciales	<ul style="list-style-type: none"> • Creación de credenciales • Preprocesamiento de credenciales • Expedición de credenciales • Activación de credenciales • Almacenamiento de credenciales 	<ul style="list-style-type: none"> • Suspensión, revocación y/o destrucción de credenciales • Renovación y/o sustitución de credenciales • Mantenimiento de registros
Fase de autenticación de entidades	<ul style="list-style-type: none"> • Autenticación • Mantenimiento de registros 	<ul style="list-style-type: none"> • Establecimiento del servicio • Observancia jurídica y contractual • Disposiciones financieras • Gestión y auditoría de la seguridad de la información • Componentes externos del servicio • Infraestructura operativa • Evaluación de las capacidades operativas

X.1254(12)_F01

Figura 1 – Descripción general del marco de garantía de autenticación de entidad

En la presente Recomendación se indica cómo pueden emplearse las tecnologías de control, los procesos y las actividades de gestión, así como los criterios de garantía, para mitigar las amenazas de autenticación, recurriendo para ello a cuatro niveles de garantía (NdG) específicos. También describe cómo hacer corresponder otros planes de garantía de autenticación con los cuatro niveles específicos, y la forma de intercambiar los resultados de las transacciones de autenticación. Por último, en esta Recomendación se informa sobre la protección de información de identificación personal (PII) relacionada con el proceso de autenticación.

Esta Recomendación está destinada principalmente a los proveedores de servicios de credenciales (CSP) y otras entidades interesadas en sus servicios (por ejemplo, partes que confían, asesores y auditores de tales servicios). En este marco de garantía de autenticación de entidades (EAAF) se especifican los mínimos requisitos técnicos, de gestión y de procedimiento para los cuatro NdG con el fin de garantizar la equivalencia en las credenciales expedidas por diversos CSP. También se indican consideraciones adicionales en materia de gestión y organización que afectan a la garantía de la autenticación de entidad, aunque no se establecen criterios específicos para dichas consideraciones. Esta Recomendación también puede resultar útil a las partes que confían y otras entidades para comprender en qué consiste cada NdG. También puede adoptarse en un determinado marco de confianza para definir los requisitos técnicos de los NdG. El EAAF se ha concebido, entre otras cosas, para los casos basados en sesión o centrados en documentación en los que utilizan diversas tecnologías de autenticación. Se puede emplear tanto en situación de confianza directa como indirecta, ya sea en disposiciones o federaciones jurídico/bilaterales.

Recomendación UIT-T X.1254

Marco de garantía de autenticación de entidad¹

1 Alcance

En la presente Recomendación se describe un marco para gestionar la garantía de autenticación de entidad en un determinado contexto. En particular:

- especifica cuatro niveles de garantía de autenticación de entidad;
- especifica criterios y directrices para lograr cada uno de los cuatro niveles de garantía de autenticación de entidad;
- orienta sobre la correspondencia entre otros planes de garantía de autenticación y los cuatro NdG;
- facilita orientación para el intercambio de resultados de autenticación basados en los cuatro NdG; y
- proporciona directrices sobre los controles que deberían emplearse para mitigar las amenazas a la autenticación.

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

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

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

¹ Corea (República de) ha formulado una reserva y no aplicará esta Recomendación debido a su falta de conformidad con la reglamentación de su país en lo que concierne a los cuatro niveles de garantía de autenticación de entidad y sus criterios para lograr cada uno de esos cuatro niveles.

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.

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

3.1.6 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.

3.1.7 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.

3.1.8 identidad [b-ISO/CEI 24760]: 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.

3.1.9 autenticación multifactor [b-ISO/CEI 19790]: Autenticación en la que se emplea como mínimo dos factores de autenticación independientes.

3.1.10 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.

3.1.11 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.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 protocolo de autenticación: Secuencia definida de mensajes entre una entidad y un verificador que permite corroborar la identidad de la entidad.

3.2.2 fuente fidedigna: Depósito reconocido por ser una fuente de información precisa y actualizada.

3.2.3 proveedor de servicio de credenciales (CSP): Actor de confianza que expide y/o gestiona credenciales.

3.2.4 garantía de autenticación de entidad (EAA): Grado de confianza que se alcanza con el proceso de autenticación de que la entidad es lo que afirma ser o se espera que sea (esta definición está basada en la definición de "garantía de autenticación" contemplada en [b-UIT-T X.1252]).

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

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

3.2.6 verificación de la información de identidad: 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.

3.2.7 demostración de identidad: Proceso mediante el cual la Autoridad de Registro (RA) obtiene y verifica suficiente información para identificar una entidad con un nivel de garantía especificado o tácito.

3.2.8 ataque por intromisión (*man-in-the-middle*): Ataque en el que el atacante es capaz de leer, insertar y modificar mensajes entre las dos partes sin el conocimiento de éstas.

3.2.9 autenticación recíproca: Autenticación de las identidades en la que se garantiza a cada entidad la identidad de la otra.

3.2.10 usurpación de identidad (*phishing*): 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.

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

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

3.2.13 sal (*salt*): Valor no secreto, a menudo aleatorio, que se utiliza en el proceso de generación numérica.

NOTA – A veces también se denomina "*sand*" (arena).

3.2.14 secreto compartido: Secreto utilizado en la autenticación que sólo lo conocen la entidad y el verificador.

3.2.15 sello de tiempo: Parámetro de tiempo variable y fiable, que indica un instante en el tiempo respecto de una referencia común.

3.2.16 transacción: Evento singular entre una entidad y el proveedor de servicio que sirve para un fin comercial o programático.

3.2.17 marco de confianza: Conjunto de requisitos y mecanismos de aplicación para las partes que intercambian información de identidad.

3.2.18 tercero fiable (TTP): Autoridad o su agente, en la que confían otros actores en lo que respecta a actividades específicas (por ejemplo, actividades relacionadas con la seguridad).

NOTA – La entidad y/o el verificador confía en el tercero fiable a los efectos de la autenticación.

3.2.19 periodo de validez: Periodo durante el cual puede utilizarse la identidad o credencial para una o varias transacciones.

3.2.20 verificación: Proceso de verificación de información comparando la información facilitada con la información corroborada previamente.

3.2.21 verificador: Actor que corrobora información de identidad.

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

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas:

CA	Autoridad de certificación (<i>certification authority</i>)
CSP	Proveedor de servicio de credenciales (<i>credential service provider</i>)
EAA	Garantía de autenticación de entidad (<i>entity authentication assurance</i>)
EAAF	Marco de garantía de autenticación de entidad (<i>entity authentication assurance framework</i>)
IdM	Gestión de identidades (<i>identity management</i>)
IP	Protocolo Internet (<i>Internet protocol</i>)
MAC	Control de acceso a los medios (<i>media access control</i>)

NdG	Nivel/es de garantía (<i>level/levels of assurance</i>)
NPE	Entidad no humana (<i>non-person entity</i>)
PDA	Asistente digital personal (<i>personal digital assistant</i>)
PII	Información de identificación personal (<i>personally identifiable information</i>)
PIN	Número de identificación personal (<i>personal identification number</i>)
RA	Autoridad de registro (<i>registration authority</i>)
RP	Parte que confía (<i>relying party</i>)
SAML	Lenguaje de marcado de asertos de seguridad (<i>security assertion markup language</i>)
TCP/IP	Protocolo de control de transmisión/protocolo Internet (<i>transmission control protocol/Internet protocol</i>)
TIC	Tecnologías de la información y la comunicación (<i>information and communications technology</i>)
TLS	Seguridad en la capa de transporte (<i>transport layer security</i>)
TPM	Módulo de plataforma fiable (<i>trusted platform module</i>)
TTP	Parte fiable (<i>trusted third party</i>)
URL	Localizador uniforme de recursos (<i>uniform resource locator</i>)

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 y capacidad.

6 Niveles de garantía

En este marco de garantía de autenticación de entidad (EAAF) se definen cuatro niveles de garantía (NdG) para la autenticación de entidades. Cada NdG describe el grado de confianza en los procesos que conducen a la autenticación, incluido el proceso de autenticación propiamente dicho, lo que garantiza que la entidad que utiliza una determinada identidad es en realidad la entidad a la que se asignó dicha identidad. A los efectos de la presente Recomendación, el NdG es una función de los procesos, de las actividades de gestión y de los controles técnicos que aplica el proveedor de servicio de credenciales (CSP) en cada fase del EAAF basados en los criterios estipulados en la cláusula 10. Si bien la garantía de autenticación de entidad (EAA) se ve afectada por consideraciones de gestión y organización, en esta Recomendación no se especifican criterios normativos explícitos para dichas consideraciones. Una entidad puede ser una persona o una entidad no humana (NPE).

Por ejemplo, el NdG de una red puede ser una función de todos los componentes que la constituye, comprendidas NPE o dispositivos extremo (por ejemplo, teléfonos móviles, asistentes digitales personales (PDA), decodificadores, portátiles). En ciertos casos, los dispositivos extremo pueden hacerse pasar por entidades. Por consiguiente, la capacidad de distinguir con cierto nivel de confianza un dispositivo fiable de uno fraudulento es fundamental para la EAA.

El NdG1 es el nivel de garantía inferior, y el NdG4 el superior, especificados en la presente Recomendación. La determinación del NdG adecuado en una determinada situación depende de diversos factores. El NdG necesario se determina principalmente en función del riesgo: las consecuencias de un error de autenticación y/o utilización indebida de credenciales, el daño y repercusiones resultantes, la probabilidad de que suceda. Los NdG más altos deberán emplearse cuando los riesgos percibidos sean mayores.

El EAAF estipula los requisitos y ofrece una guía de aplicación para cada uno de estos cuatro NdG. En particular, describe los requisitos para la aplicación de los procesos en las siguientes fases:

- a) afiliación (por ejemplo, demostración de la identidad, verificación de la información de identidad, registro);
- b) gestión de credenciales (por ejemplo, expedición y activación de credenciales);
- c) autenticación.

También ofrece orientación sobre consideraciones de gestión y organización (por ejemplo, cumplimiento de la ley, gestión de la seguridad de la información) que afectan a la garantía de autenticación de entidad.

Los NdG se definen en el Cuadro 6-1.

Cuadro 6-1 – Niveles de garantía²

Nivel	Descripción
1 – Bajo	Poca o ninguna confianza en la identidad declarada o aseverada
2 – Medio	Cierta confianza en la identidad declarada o aseverada
3 – Alto	Mucha confianza en la identidad declarada o aseverada
4 – Muy alto	Muchísima confianza en la identidad declarada o aseverada

Este marco contiene requisitos para lograr el NdG deseado en cada fase del marco de garantías de autenticación de entidad. El NdG general alcanzado por una determinada materialización que utilice este marco será el nivel de la fase con menor NdG.

6.1 Nivel de garantía 1 (NdG1)

En el NdG1, el nivel de confianza en la identidad declarada o aseverada por una entidad es mínimo, pero existe cierta confianza en que la entidad es la misma en eventos de autenticación consecutivos. Este NdG se emplea cuando el riesgo que conlleva una autenticación errónea es mínimo. No hay ningún requisito específico para el mecanismo de autenticación utilizado; sólo que ofrece un nivel mínimo de garantía. Los requisitos de autenticación para este NdG pueden satisfacerse con muy diversas tecnologías disponibles, en particular las credenciales asociadas con mayores NdG. Este nivel no exige la utilización de métodos criptográficos de autenticación (por ejemplo, protocolo criptográfico basado en pregunta-respuesta).

El NdG1 puede aplicarse, por ejemplo, para una autenticación en la que la entidad presenta un nombre de usuario o contraseña registrado por sí misma en el sitio web de un proveedor de servicio para crear una página personalizada, o en transacciones por sitios web que exijan registrarse para acceder a cierto material y documentación, como el caso documentación sobre un producto o novedades.

² El NdG es una función de los procesos, de las actividades de gestión y de los controles técnicos que aplica el CSP en cada fase del EAAF basados en los criterios estipulados en la cláusula 10.

Por ejemplo, en el NdG1 una dirección de control de acceso a los medios (MAC) puede satisfacer un requisito de autenticación del dispositivo. Sin embargo, poco se confía en que otro dispositivo no pueda utilizar dicha dirección MAC.

6.2 Nivel de garantía 2 (NdG2)

En el NdG2, existe cierta confianza en la identidad declarada o aseverada por la entidad. Este NdG se utiliza en situaciones en las que el riesgo de una autenticación errónea es moderado. La autenticación mediante un solo factor es aceptable. La autenticación positiva dependerá de que la entidad demuestre, a través del protocolo de autenticación seguro, que tiene el control de la credencial. Deberán aplicarse controles para reducir la eficacia de las escuchas ilícitas y los ataques en línea para tratar de adivinar contraseñas. También deberán aplicarse controles para proteger los ataques para hacerse con credenciales almacenadas.

Por ejemplo, el sitio web de un proveedor de servicio puede permitir a los clientes que cambien la dirección que figura en su expediente. Esta transacción en la que el beneficiario cambia de dirección puede considerarse una transacción de autenticación con nivel NdG2, ya que podría conllevar un riesgo moderado de molestias. Dado que los avisos oficiales sobre la prima, la situación de la cuenta y el registro de cambios se envían a la dirección indicada en el expediente, la transacción conlleva también un riesgo moderado de revelación no autorizada de PII. Así, la aseguradora debería obtener cierta garantía mínima de autenticación antes de permitir esa transacción.

6.3 Nivel de garantía 3 (NdG3)

En el NdG3, existe gran confianza en la identidad declarada o aseverada por la entidad. Este NdG se utiliza cuando la autenticación errónea implica un riesgo considerable. En este NdG se recurrirá a una autenticación basada en múltiples factores. Toda información secreta que se intercambie en los protocolos de autenticación deberá estar encriptada en tránsito o en reposo (aunque NdG3 no necesita que se utilice un protocolo criptográfico basado en pregunta-respuesta). No hay requisitos en relación con la generación o almacenamiento de credenciales; se pueden almacenar o generar en computadores convencionales o en dispositivos especiales.

Por ejemplo, una transacción en la que una empresa envía por medios electrónicos cierta información confidencial a un organismo gubernamental podría requerir una autenticación de nivel NdG3. La divulgación indebida de esa información podría representar un riesgo importante en materia de pérdida económica. Otros ejemplos de transacciones de nivel NdG3 son el acceso en línea a cuentas que permite a una entidad efectuar ciertas transacciones financieras o a un contratista externo utilizar el sistema a distancia para acceder a información personal y confidencial del cliente.

6.4 Nivel de garantía 4 (NdG4)

En el NdG4, se tiene muchísima confianza en la identidad declarada o aseverada por la entidad. Este NdG se emplea cuando una autenticación errónea entraña un riesgo muy elevado. El NdG4 ofrece el mayor nivel de garantía de autenticación de entidad que se define en la presente Recomendación. El NdG4 es similar al NdG3, pero con el requisito adicional de demostrar en persona la identidad en el caso de entidades humanas y la utilización de dispositivos físicos a prueba de alteración para el almacenamiento de todas las claves criptográficas secretas o privadas. Asimismo, toda la PII y otros datos confidenciales que se incluyan en los protocolos de autenticación deberán estar encriptados en tránsito o en reposo.

Por ejemplo, en servicios que pueden correr un riesgo muy elevado de daño o deterioro debido a una autenticación errónea se puede exigir un nivel de protección NdG4. El responsable tiene que estar completamente seguro de que cierta información esencial ha sido facilitada por la entidad correcta, ya que puede ser considerado responsable penal si no verifica esa información. Por último,

la aprobación de una transacción que entraña un riesgo muy elevado de pérdida económica puede considerarse una transacción de nivel NdG4.

En el NdG4, puede recurrirse a certificados digitales (por ejemplo, UIT-T X.509, certificados de verificador de tarjeta (CV)) para autenticar entidades no humanas, tales como portátiles, teléfonos móviles, impresoras, máquinas de fax y otros dispositivos conectados a la red. Por ejemplo, el proceso de inscripción de teléfonos inteligentes podría requerir la implantación de certificados digitales en el mismo. Asimismo, para impedir el acceso no autorizado a la red de distribución eléctrica, se podrían emplear certificados digitales en la implantación de tecnologías de contadores inteligentes.

6.5 Selección del nivel de garantía adecuado

La selección del NdG adecuado debería basarse en una evaluación del riesgo de las transacciones o servicios para las que se autentifica a las entidades. Comparando los niveles de riesgo con los NdG, las partes que intervienen en una transacción de autenticación pueden determinar qué nivel NdG necesitan y, en consecuencia, contratar servicios y confiar en identidades debidamente garantizadas. En el Cuadro 6-2 se indican las posibles consecuencias y repercusiones de un error de autenticación a diversos NdG.

Cuadro 6-2 – Grado de repercusión en cada nivel de garantía

Posibles consecuencias en caso de error de autenticación	Grado de repercusión en caso de error de autenticación por NdG			
	1	2	3	4
Inconveniente, deterioro o menoscabo del prestigio o la reputación	Mín*	Mod	Con	Alto
Pérdidas económicas o responsabilidad jurídica	Mín	Mod	Con	Alto
Perjuicio a la organización, sus programas o al interés público	n.d.	Mín	Mod	Alto
Divulgación no autorizada de información confidencial	n.d.	Mod	Con	Alto
Seguridad humana	n.d.	n.d.	Mín Mod	Con Alto
Delitos civiles o penales	n.d.	Mín	Con	Alto
* Mín = Mínimo; Mod = Moderado; Con = Considerable; Alto = Alto				

La determinación de lo que constituye un riesgo mínimo, moderado, considerable o alto depende de los criterios definidos por la organización que utilice esta norma para cada una de las posibles consecuencias. Asimismo, puede haber numerosos tipos de repercusión (por ejemplo, daños a la organización, así como la divulgación no autorizada de información delicada). En numerosos tipos de repercusión, se aplicará el NdG más elevado correspondiente a las consecuencias.

Cada NdG se determinará por la intensidad y rigor de los controles y procesos en cada fase del EAAF que aplique el CSP a la prestación de su servicio. El EAAF establece la necesidad de disponer de criterios sobre la garantía de servicio operativa en cada NdG de los CSP. Si bien los criterios de garantía del servicio se presentan en la cláusula 11, los requisitos específicos quedan fuera del alcance de la presente Recomendación.

Al utilizar los resultados de la evaluación de riesgos para determinar el NdG aplicable, quizá se deban tomar en consideración otros factores de índole comercial, aparte de los relativos a la seguridad, entre los que cabe citar:

- a) el método de gestión del riesgo residual que adopte la organización;
- b) lo dispuesta que esté la organización a aceptar riesgos en relación con las repercusiones indicadas en el Cuadro 6-2;
- c) los objetivos comerciales del servicio (por ejemplo, un servicio con el objetivo comercial de impulsar su adopción podrían ofrecerse a un NdG menor utilizando credenciales de tipo contraseña, si la organización dispone de procedimientos para mitigar el fraude y está dispuesta a aceptar el riesgo de fraude).

La evaluación del riesgo de una transacción puede realizarse en el contexto de una evaluación general del riesgo de seguridad informática en la organización (por ejemplo, ISO/CEI 27001) y debería concentrarse en la necesidad específica de seguridad en las transacciones contempladas. Al evaluar el riesgo se tendrá en cuenta el riesgo relacionado con EAA. Los resultados de la evaluación del riesgo se compararán con los cuatro NdG y se seleccionará el NdG que mejor se ajuste a las necesidades.

Cuando se prevean transacciones de distintas clases, se podrá aplicar un NdG diferente a cada transacción o grupo de transacciones. Es decir, una misma organización puede aceptar diversos NdG, en función de la transacción específica de que se trate.

6.6 Correspondencia y compatibilidad de NdG

En cada dominio se pueden definir NdG diferentes. No tiene por qué haber una correspondencia biunívoca de dichos niveles con los cuatro NdG descritos en el presente marco. Por ejemplo, un dominio puede adoptar un modelo de cuatro niveles y otros uno de cinco niveles. Deberían definirse por separado y divulgarse ampliamente los diferentes criterios para cada modelo de autenticación.

Para lograr la compatibilidad entre los diferentes modelos de NdG, se deberá explicar la correspondencia de cada dominio con los NdG definidos en la presente Recomendación, mediante:

- a) la elaboración de una metodología bien definida sobre garantía de autenticación de entidad, que comprenda también categorías de NdG; y
- b) la amplia difusión de esta metodología para que las organizaciones que deseen concertar acuerdos de tipo federación entiendan claramente los procesos y la terminología de las demás.

La metodología de NdG tendrá en cuenta y definirá claramente los NdG en cuanto a una evaluación del riesgo que especifique y cuantifique:

- a) las posibles amenazas;
- b) la repercusión (es decir, mínima, moderada) en caso de que las amenazas se hagan realidad;
- c) la identificación de amenazas que pueden controlarse en cada NdG;
- d) las tecnologías y procesos de seguridad recomendados para efectuar el control de cada NdG, tales como la especificación de una credencial para un dispositivo físico (por ejemplo, una tarjeta inteligente) o la especificación de requisitos para la generación y almacenamiento de credenciales;
- e) los criterios para determinar la equivalencia de diferentes combinaciones de factores de autenticación, teniendo en cuenta las pruebas de identidad y las correspondientes credenciales.

Una forma de resolver el problema de hacer corresponder/conciliar los diferentes modelos NdG sería recurrir al modelo de cuatro niveles definido en este documento y hacerlos corresponder con otros modelos de n niveles. Este método permitiría identificar federaciones que emplean modelos

distintos de garantía de autenticación para hacerlos corresponder con el modelo de cuatro niveles. Se deberá estipular cómo gestionar los NdG sin correspondencia, ya sea hacer sencillamente caso omiso de los mismos o hacerlos corresponder con el siguiente nivel inferior (puesto que no hay fundamentos para suponer un NdG mayor, a no ser que se haya determinado específicamente de antemano).

6.7 Intercambio de resultados de autenticación basado en los 4 NdG

Los actores que participan en una transacción de autenticación (por ejemplo, CSP, RP) quizá tengan que intercambiar información para completar dicha transacción o actividad.

Las posibles acciones son, entre otras, las siguientes:

- a) permitir a una parte que confía manifestar sus expectativas en cuanto al NdG con el que debería autenticarse la entidad;
- b) permitir a una entidad o CSP indicar el NdG real en sus respuestas;
- c) permitir a una entidad o CSP a anunciar el NdG con el que ha sido certificada su capacidad para cumplir los requisitos asociados con dicho NdG.

Los actores que participan en una transacción de autenticación deberán convenir el protocolo, la semántica, el formato y la estructura de la información que van a intercambiar. La RP tal vez necesite especificar si acepta otra respuesta de autenticación aparte de la exactamente solicitada.

Si bien los certificados digitales son una forma establecida de transmitir información sobre la garantía de las correspondientes credenciales, cada vez se recurre más a metadatos para comunicar qué garantías exigen las partes que intercambian información. Las "clases de contexto", como la "clase contexto de autenticación del SAML (lenguaje de marcado de asertos de seguridad)" en la forma de un localizador uniforme de recursos (URL), es un mecanismo bien conocido que emplean las partes para expresar dichas clases relativas a la garantía de autenticación en las solicitudes y asertos de autenticación. Por ejemplo, un aserto característico de un proveedor de identidad puede contener información del tipo: "Este usuario es Juan Pérez; su dirección de correo electrónico es `juan.perez@ejemplo.com`, y se ha autenticado en este sistema mediante una contraseña".

En el resto de este marco se describe la estructura con la que se establecen procesos y requisitos para los servicios y las amenazas y repercusiones que conlleva la autenticación de entidades. Para terminar, se explica la necesidad de criterios de evaluación de los servicios para garantizar que se asigne el NdG adecuado con el fin de obtener servicios de acreditación adecuados.

7 Actores

Los actores que participan en el EAAF son entidades, CSP, RA, RP, verificadores y TTP. Estos actores pueden pertenecer a una misma organización o a varias. Las relaciones entre las distintas organizaciones y las capacidades que ofrecen pueden ser muy diversas, en particular componentes, sistemas y servicios compartidos o interactivos.

7.1 Entidad

La identidad de una entidad puede autenticarse. La capacidad para autenticar una entidad depende de varios factores. En el contexto de este marco, para poder autenticar una entidad ésta tiene que haberse registrado, disponer las credenciales adecuadas expedidas por un CSP y además tiene que haberse especificado un protocolo de autenticación. Durante la autenticación, la entidad puede atestiguar su propia identidad. También puede haber una parte independiente que represente a la entidad a los efectos de autenticación.

7.2 Proveedor de servicio de credenciales

El proveedor de servicio de credenciales (CSP) expide y/o gestiona credenciales o el hardware, software y los datos correspondientes que pueden emplearse para producirlas. Como ejemplos de credenciales que pueden expedir y gestionar los CSP cabe citar las contraseñas y los datos biométricos. Las tarjetas inteligentes que contienen claves privadas son un ejemplo de hardware y datos correspondientes (que se utilizan para producir credenciales) que pueden expedir y gestionar los CSP. Los CSP también pueden expedir y gestionar datos para autenticar credenciales. Si como credenciales se utilizan contraseñas, estos datos pueden ser los valores de las funciones unidireccionales de las contraseñas. Si las credenciales se basan en información firmada por medios digitales, los CSP pueden producir certificados de clave pública que pueden emplear los verificadores. Las credenciales que expide y admite el CSP, así como las salvaguardias que aplica, son factores esenciales a la hora de determinar qué NdG se alcanzará en una determinada transacción de autenticación (véase también la cláusula 10.3).

A cada entidad se le expedirá una o varias credenciales, o medios para producirlas, que permitan su ulterior autenticación. Las credenciales, o los medios para producirlas, sólo se expiden después de terminar satisfactoriamente el proceso de afiliación, al final del cual la entidad queda registrada.

7.3 Autoridad de registro

La autoridad de registro (RA) establece y/o verifica y avala la identidad de una entidad a un CSP. El CSP deberá confiar en la RA para ejecutar los procesos relacionados con la fase de afiliación y el registro de entidades que permitan luego a los CSP realizar la asignación de credenciales.

Cada RA realizará algún tipo de comprobación y verificación de la identidad con arreglo a un procedimiento especificado. Para diferenciar una entidad de las demás, a cada entidad se le suele asignar uno o varios identificadores que permiten reconocerla más adelante en el contexto del caso.

7.4 Parte que confía

La RP es un actor que confía en la declaración o aserto de entidad. La parte que confía puede exigir la autenticación de la identidad para diversos fines, tales como gestión de cuentas, control de acceso, decisiones de autorización, etc. La parte que confía puede realizar ella misma las operaciones necesarias para autenticar la entidad, o puede encargar dichas operaciones a un tercero.

7.5 Verificador

El verificador es un actor que corrobora la información de identidad. Puede participar en numerosas etapas del EAA y llevar a cabo la verificación de la identidad y/o de la información de identidad.

7.6 Tercero fiable

Un TTP es una autoridad o agente, en el que confían otros actores en lo que respecta a ciertas actividades (por ejemplo, las relacionadas con la seguridad). En este marco, las entidades y/o el verificador confían en el TTP a los efectos de autenticación. Como ejemplos de TTP con fines de autenticación de entidades pueden citarse a los organismos de certificación (CA) y a los organismos que estampan sellos de tiempo.

8 Fases del marco de garantía de autenticación de entidad

En esta cláusula se describen las fases y procesos de EAA. Si bien algunos modelos de EAA pueden tener una estructura diferente, para declarar la conformidad con el presente modelo es necesario que las capacidades funcionales cumplan íntegramente los requisitos estipulados en el presente marco, que es neutral respecto de la tecnología.

Las organizaciones que adopten este marco deberán establecer políticas, procedimientos y capacidades que comprendan los procesos necesarios y cumplan el conjunto de requisitos establecidos en este marco. Éstos variarán según la función que desempeñe la organización en concreto y, por ejemplo, los NdG a los que la organización ofrece credenciales. Así, la organización tendrá que cumplir:

- a) los requisitos para determinadas acciones en nombre de la organización o sus representantes con respecto a un determinado NdG;
- b) los requisitos para la evaluación externa o por terceros de la capacidad operativa de la organización en el EAAF; y
- c) las políticas, acciones y capacidades necesarias para obtener confianza en los procesos, servicios y capacidades que ofrecen las organizaciones que adoptan el marco.

8.1 Fase de afiliación

La fase de afiliación consta de cuatro procesos: solicitud e iniciación; demostración de la identidad; verificación de la identidad; y registro/mantenimiento de registros. Estos procesos puede realizarlos en su totalidad una sola organización o pueden consistir en diversas relaciones y capacidades que ofrecen varias organizaciones, en particular componentes, sistemas y servicios compartidos o interactivos.

Los procesos necesarios varían según el rigor que exija el NdG aplicable. En el caso de una entidad afiliada a nivel NdG1, estos procesos son mínimos (basta, por ejemplo, con pulsar un botón "nuevo usuario" en una página web para crear un nombre de usuario y contraseña). En otros casos, los procesos de afiliación pueden ser exhaustivos. Por ejemplo, la afiliación a nivel NdG4 exige una reunión en persona entre la entidad y el RA, así como una demostración cabal de la identidad.

8.1.1 Aplicación e iniciación

La fase de afiliación se inicia de varias formas. Por ejemplo, a petición de entidades que desean obtener por su cuenta una determinada credencial (cuando, por ejemplo, un nuevo usuario de un sitio web quiere obtener un nombre de usuario y contraseña). También es posible que el proceso de afiliación lo inicie un tercero en nombre de la entidad o bien el propio CSP (por ejemplo, una tarjeta de identificación expedida por el Estado, una tarjeta de identificación de empleado). Por ejemplo, a niveles NdG más altos, puede que sólo se acepten aplicaciones cuya entidad haya sido refrendada por un tercero.

En cualquier caso, el proceso de iniciación de la fase de afiliación para personas implicará que se rellene un formulario de solicitud. De esta manera se recopilará información suficiente para garantizar que la entidad pueda identificarse de manera unívoca dentro de un contexto (por ejemplo, registrando el nombre completo, la fecha y el lugar de nacimiento). En el caso de NPE, por ejemplo un dispositivo móvil, la afiliación puede requerir la inicialización mediante la instalación de credenciales en el dispositivo, que le permitan identificarse de manera unívoca y recibir parámetros de configuración adaptados al mismo a través de un perfil de configuración encriptado.

Los CSP deberán establecer las condiciones de la afiliación y en las que pueden utilizarse los servicios asociados a la misma. Las condiciones de los servicios asociados pueden establecerse con arreglo a un marco de confianza. Si se estima oportuno, la entidad o quien actúe en su nombre habrá de aceptar cláusulas de exención de responsabilidad antes de proseguir los procesos de afiliación.

8.1.2 Demostración de la identidad y verificación de la información de identidad

La demostración de la identidad consiste en obtener y verificar información suficiente para identificar una entidad con un nivel de garantía especificado o tácito. La verificación de la información de identidad es el proceso de corroboración de la información de identidad y las credenciales con expedidores, fuentes de datos u otros recursos internos o externos, con respecto a la autenticidad, validez, exactitud y vinculación a la entidad. Dependiendo del contexto, para

cumplir las exigencias de demostración de la identidad las fuentes fidedignas expiden o aprueban diversa información de identidad (por ejemplo, tarjeta de identidad del país, permiso de conducir, información biométrica, certificados basados en máquinas, certificado de nacimiento). La información de identidad real que se ha de presentar para cumplir los requisitos de demostración de la identidad varía según el NdG.

La demostración de la identidad puede comprender la verificación física de los documentos de identidad presentados para detectar posible fraude, alteración o falsificación. También se puede comprobar si la identidad se ha utilizado en otros contextos (es decir, si ha sido verificado por otros RA). Los requisitos de demostración de identidad podrán ser más rigurosos a niveles más altos de NdG. Además, la demostración de la identidad será más estricta en el caso de entidades que aseveren o declaren una identidad a distancia (por ejemplo, por un canal en línea) que cuando se realiza localmente (por ejemplo, en persona en el RA).

El rigor de los requisitos de demostración de identidad se basa en los objetivos que deberían satisfacerse en cada NdG. En el NdG1, el único objetivo es asegurarse de que la identidad es única en el contexto de que se trate. Dos entidades diferentes no deberían tener la misma identidad. En el NdG2, hay dos objetivos. En primer lugar, la identidad deberá ser única en el contexto. En segundo lugar, la entidad a quien pertenece la identidad deberá existir objetivamente, es decir, la identidad no es ficticia ni se ha inventado deliberadamente para fines fraudulentos³. Por ejemplo, para demostrar la identidad de una persona a nivel NdG2 quizá se compruebe las fechas de nacimiento y defunción registradas para garantizar su procedencia (aunque con ello no se demuestra que la entidad que posee el certificado de nacimiento corresponda a la entidad para la que éste se expidió). Análogamente, la demostración de identidad a nivel NdG2 en el caso de NPE puede consistir en verificar con el fabricante el número de serie.

En el NdG3 se cumplen los requisitos del NdG1 y NdG2, y además se verifica la información de identidad con una o varias fuentes fidedignas, por ejemplo en una base de datos externa. La verificación de la información comprueba que la identidad está activa y guarda relación con la entidad. Ahora bien, no existen garantías de que la información sobre la entidad está en posesión del propietario real o legítimo de la misma. En el caso de personas, en el NdG4 se exige un requisito adicional respecto del NdG3 y se solicita a las entidades que se presenten en persona con el fin de evitar la suplantación de identidad.

Los procesos de demostración de identidad a niveles NdG más altos incluirán los procesos de los NdG inferiores. Por ejemplo, al demostrar la identidad a nivel NdG3 se supone que se han pasado los controles de demostración de identidad a niveles NdG1 y NdG2.

³ No se excluye la utilización de pseudónimos.

Cuadro 8-1 – Aplicación de los objetivos de demostración de identidad a los NdG

NdG	Descripción	Objetivo	Controles	Método de procesamiento⁴
NdG1 – Bajo	Poca o ninguna confianza en la identidad declarada o aseverada	Identidad única en un contexto	Autodeclarada o autoaseverada	Local o a distancia
NdG2 – Medio	Cierta confianza en la identidad declarada o aseverada	Identidad única en un contexto y la correspondiente entidad existe objetivamente	La identidad se demuestra mediante la información de identidad procedente de una fuente fidedigna	Local o a distancia
NdG3 – Alto	Mucha confianza en la identidad declarada o aseverada	Identidad única en un contexto, la correspondiente entidad existe objetivamente, la identidad se verifica y se utiliza en otros contextos	La identidad se demuestra mediante la información de identidad procedente de una fuente fidedigna + verificación de la información de identidad	Local o a distancia
NdG4 – Muy alto	Muchísima confianza en la identidad declarada o aseverada	Identidad única en un contexto, la correspondiente entidad existe objetivamente, la identidad se verifica y se utiliza en otros contextos	La identidad se demuestra mediante la información de identidad procedente de una fuente fidedigna + verificación de la identidad + control de identidad en persona ⁵	Local únicamente

Los controles de NdG necesarios para proteger contra amenazas a la fase de afiliación se determinarán a partir de los controles enumerados en la cláusula 10.1.2.

Toda aplicación del EAAF se basa en (un subconjunto de) los recursos y la información de identidad disponibles para las posibles entidades y/o la RA.

La fiabilidad y precisión de estas credenciales, información de identidad y recursos determinan el nivel real de garantía que se ofrece en la fase de afiliación. Por consiguiente, cuando se aplique el EAAF se deberá examinar detenidamente la garantía que ofrece la infraestructura (de gestión) de identidad utilizada por las diversas fuentes y expedidores a la hora de decidir las credenciales, la información de identidad y/o los recursos en los que basarse para demostrar y verificar la identidad. Toda aplicación del EAAF implicará la publicación de un documento (por ejemplo, la política de demostración de identidad descrita en la cláusula 10.1.2.1) en el que se efectúe una descripción general de la información de identidad, fuentes y/o expedidores que son fiables para la fase de afiliación.

⁴ La demostración de identidad a distancia se realiza por una red y, por ende, no se puede ver físicamente a la entidad, mientras que la demostración local de la identidad exige ver físicamente a la entidad.

⁵ El control de la identidad en persona se aplica sólo a entidades humanas.

8.1.3 Registro/Mantenimiento de registros

Proceso con el que concluye la afiliación de la entidad. Se trata del proceso de registro de la fase de afiliación, en la que se crea un registro a tal efecto. Dicho registro incluirá la información y documentación recabada (que podría retenerse), información sobre el proceso de verificación de la información de identidad, los resultados de estas etapas y otros datos pertinentes. Luego se toma y registra una decisión de aceptar, denegar o suspender la afiliación hasta que se examine con mayor detenimiento o se cumplan otros criterios.

8.1.4 Inscripción

La inscripción es el proceso mediante el cual una entidad solicita utilizar un servicio o recurso. Aunque en general se suele considerar que el proceso de inscripción forma parte de la fase de afiliación, también puede llevarse a cabo ulteriormente. A diferencia de otros procesos en la afiliación, que probablemente sólo se haya de realizar una vez, es posible que la entidad tenga que realizar la inscripción cada vez que solicite acceder por primera vez a un servicio o recurso.

8.2 Fase de gestión de credenciales

La fase de gestión de credenciales comprende todos los procesos relativos a la gestión del ciclo de vida de una credencial, o los medios para generar credenciales, que permiten al usuario participar en una actividad o contexto. La fase de gestión de credenciales puede comprender todos o algunos de los siguientes procesos: creación de credenciales, expedición de credenciales o de los medios para su producción, activación de credenciales o de los medios para su producción, almacenamiento de credenciales, revocación y/o destrucción de credenciales o de los medios para su producción, renovación y/o sustitución de credenciales o de los medios para su producción, y registro. Algunos de estos procesos dependen de si la credencial está incorporada en un dispositivo físico.

8.2.1 Creación de credenciales

La creación de credenciales comprende todos los procesos necesarios para crear por vez primera una credencial, o los medios para producirla. Estos procesos pueden constar de preprocesamiento, inicialización y vinculación.

8.2.1.1 Preprocesamiento de credenciales

Algunas credenciales, o los medios para producirlas, requieren preprocesamiento antes de su expedición, como una personalización cuando la credencial se adapta a la identidad de la entidad. La personalización puede adoptar varias formas diferentes en función de la credencial. Por ejemplo, la personalización de una tarjeta inteligente que contiene credenciales puede implicar la impresión (en la superficie de la misma) o la escritura (en el chip de la tarjeta) del nombre de la entidad a quien se expedirá la tarjeta. También hay credenciales que no requieren personalización, tales como las contraseñas.

8.2.1.2 Inicialización de credenciales

La inicialización de la credencial comprende todas las medidas necesarias para garantizar que los medios para su producción podrán hacer uso de todas las funcionalidades previstas. Por ejemplo, es posible que el chip de una tarjeta inteligente tenga que calcular los pares de claves criptográficas necesarias para poder generar firmas digitales. Análogamente, podría expedirse una tarjeta inteligente en estado "bloqueado" que requiera un PIN para su activación.

8.2.1.3 Vinculación de credenciales

La vinculación es el proceso de crear una relación entre la credencial, o los medios para su producción, y la entidad a la que se le asigna. La forma de llevar a cabo la vinculación y la confianza en la misma varía según el NdG. Por ejemplo, cuando se vincula en línea el identificador, que consiste en un pseudónimo permanente de la entidad, con el registro de cliente de la entidad,

durante el proceso de vinculación puede transmitirse por un canal seguro un "código de activación" para la primera vez en una cookie encriptada de sesión única. Otra posibilidad sería que el código de activación se solicitara al final del proceso, una vez que la vinculación de la entidad con el identificador permanente se haya completado, con el fin de vincular dicho identificador con el registro del cliente.

8.2.2 Expedición de credenciales

La expedición de credenciales es el proceso de proporcionar o, en su defecto, asociar una entidad a una determinada credencial, o con los medios para producirla. La complejidad de este proceso depende del NdG exigido. En NdG superiores será necesaria la entrega segura de un dispositivo físico (por ejemplo, una tarjeta inteligente) que contiene la credencial y puede implicar la entrega en mano del dispositivo. En el caso de NdG inferiores, la expedición podría consistir sencillamente en enviar una contraseña o PIN a la dirección de correos o electrónica de la entidad.

En el caso de NPE, tales como dispositivos, la expedición a NdG superiores suele comenzar cuando el fabricante del dispositivo hace un pedido al por mayor de certificados digitales y le indica al CSP una lista de números unívocos de identificación de dispositivo para cada uno de los certificados digitales. El CSP suministra en su respuesta al fabricante los certificados y las claves privadas en formato encriptado. Durante la fabricación, el fabricante puede integrar el certificado digital en cada dispositivo, lo que crea un identificador de dispositivo único.

8.2.3 Activación de credenciales

La activación de credenciales es el proceso mediante el cual una credencial, o los mecanismos para producirla, se deja lista para su utilización. La activación puede implicar diversas medidas, dependiendo de la credencial. Por ejemplo, una credencial, o mecanismo para producirla, puede haberse "bloqueado" después de su inicialización hasta el momento de su expedición a la entidad con objeto de evitar que entretanto se utilice indebidamente. En tales casos, la activación puede implicar el "desbloqueo" de la credencial (por ejemplo, mediante una contraseña). Las credenciales, o los medios para producirlas, también pueden reactivarse después de un periodo de suspensión durante el cual dejen de ser válidas temporalmente.

8.2.4 Almacenamiento de credenciales

El almacenamiento de credenciales es el proceso mediante el cual las credenciales, o los medios para su producción, se guardan a buen recaudo de modo que están protegidas contra su divulgación, utilización, modificación o destrucción no autorizada. El almacenamiento de credenciales implica a la entidad relacionada con la credencial y las medidas necesarias para impedir su utilización no autorizada.

El almacenamiento de credenciales no incluye necesariamente la protección de la información empleada para verificar que la credencial es legítima, si dicha información no forma parte de la credencial. A NdG superiores se exige la protección de información, como tablas de contraseñas generadas para la autenticación.

8.2.5 Suspensión, revocación y/o destrucción de credenciales

La revocación es el proceso mediante el cual se termina permanentemente la validez de la credencial. La suspensión es un proceso relacionado en virtud del cual la validez de la credencial se suspende temporalmente. La revocación puede resultar conveniente en diferentes situaciones. Se producirá una revocación en los siguientes supuestos:

- a) la credencial, o los medios para su producción, se ha perdido, robado o ha quedado comprometida de algún modo;
- b) la credencial ha expirado;
- c) ya no existen fundamentos para la credencial (por ejemplo, el empleado deja a su empleador);

- d) la credencial se ha utilizado para fines no autorizados; o
- e) se ha expedido otra credencial que sustituyera la anterior.

El plazo entre la notificación de un evento que exige una revocación y la finalización del proceso de revocación es prerrogativa de la política de la organización. A NdG superiores, el plazo admisible suele ser más breve. Algunas credenciales, como las de tarjetas inteligentes, pueden destruirse físicamente una vez revocadas. Ahora bien, la información asociada con la credencial no siempre puede destruirse.

8.2.6 Renovación y/o sustitución de credenciales

La renovación consiste en ampliar el periodo de validez de una credencial existente. La sustitución consiste en expedir a una entidad una nueva credencial, o los mecanismos para su producción, que sustituye a una anterior que ha sido revocada. Un ejemplo de sustitución de credencial es cuando un CSP envía una contraseña temporal a la dirección de correo electrónico de la entidad que le permite a ésta crear una nueva contraseña utilizando la contraseña temporal. Otro ejemplo es el código que desbloquea un PIN, que debería tratarse como si fuera un PIN. El rigor del proceso de renovación y sustitución de credenciales varía según el NdG.

8.2.7 Registros

Deberían mantenerse registros adecuados durante toda la vida útil de la credencial. En dichos registros debería figurar, como mínimo, la siguiente información:

- a) el hecho de que se ha creado una credencial;
- b) el identificador de la credencial (en su caso);
- c) la entidad a quien se ha expedido la credencial (en su caso);
- d) la situación de la credencial (en su caso).

Se mantendrán registros en todo proceso (aplicable) que interviene en la fase de gestión de credenciales. Cuando las credenciales se expiden a personas, el mantenimiento de registros implicará probablemente el procesamiento de la PII. Véase el Apéndice I.

8.3 Fase de autenticación de la entidad

En la fase de autenticación de la entidad, ésta utiliza su credencial para dar fe de su identidad al RP. El proceso de autenticación consiste exclusivamente en la creación (o no) de confianza en la identidad declarada o aseverada, y no tiene consecuencias ni guarda relación con las acciones que pudiera realizar luego la parte que confía sobre la base de dicha declaración o aseveración.

8.3.1 Autenticación

La autenticación comprende la utilización de un protocolo para demostrar la posesión y/o control de una credencial a los efectos de crear confianza en una identidad. Los requisitos del protocolo de autenticación varían en función del NdG aplicable. Por ejemplo, en el caso de un NdG inferior, la autenticación podría consistir en utilizar una contraseña. A niveles de NdG superiores, la autenticación podría implicar un protocolo criptográfico basado en pregunta-respuesta. A NdG superiores se exige la autenticación basada en múltiples factores. No todos los factores de autenticación proporcionan la misma robustez, por lo que se utilizan múltiples factores para aumentar el nivel de garantía. Véase la cláusula 10.

8.3.2 Mantenimiento de registros

La supervisión y el registro de eventos en la fase de autenticación pueden resultar necesarios para diversos fines, tales como la configuración del servicio, el cumplimiento, la rendición de cuentas y/o las prescripciones legales.

Cuando se trata de personas, la información contenida en estos registros puede incluir datos sensibles. Estos registros se deberán gestionar de manera que se tenga en cuenta la protección de PII y su reducción al mínimo imprescindible. Véase también el Apéndice I.

9 Consideraciones relativas a la gestión y organización

La EAA no es el resultado de factores técnicos exclusivamente, sino también de reglamentos, acuerdos contractuales y de consideraciones relativas a la gestión y organización del servicio. Sin una gestión y utilización competentes, una solución rigurosa desde el punto de vista técnico puede ofrecer una seguridad muy por debajo de sus auténticas posibilidades en la prestación de EAA.

La presente cláusula es informativa y describe algunas consideraciones de gestión y organización que afectan a la EAA. No se indican criterios específicas para cada NdG. Los criterios específicos y la evaluación de la conformidad para las consideraciones de gestión y organización quedan fuera del alcance de la presente Recomendación, aunque deberían proporcionarse dentro de un marco de confianza.

9.1 Establecimiento del servicio

El establecimiento del servicio abarca tanto la situación jurídica del proveedor de servicio como la situación de la prestación del servicio funcional. Por ejemplo, saber que el proveedor de servicios de gestión de identidad y autenticación es una entidad jurídica registrada ofrece confianza en que el CSP es una empresa genuina en la jurisdicción en la que desempeña sus actividades. Este aspecto adquiere aún más importancia cuando los componentes del servicio están integrados por diferentes personas jurídicas (por ejemplo, la inscripción es una función aparte).

Aunque los requisitos esenciales son los mismos para todos los NdG, cuanto más alto sea el NdG mayor dependencia tendrá en que la prestación del servicio sea íntegra y fiable. Por ejemplo, a nivel NdG3 y superiores, se deberían obtener mayores garantías sobre la prestación del servicio en lo que respecta a conocer sus relaciones con otras empresas y comprender el nivel de independencia con que la empresa puede desempeñar sus operaciones.

9.2 Observancia jurídica y contractual

Todos los actores del EAAF deberían comprender y cumplir los requisitos jurídicos que les incumben en relación con la explotación y suministro del servicio. Las repercusiones son, entre otras, los tipos de información que podría recabarse, cómo se demuestra la identidad, y qué información debería conservarse. La gestión de PII reviste especial preocupación jurídica (véase el Apéndice I). También se deberían tomar en consideración todas las jurisdicciones en la que actúan los actores. A NdG2 y niveles superiores, se deberían especificar requisitos contractuales y una política concreta.

9.3 Disposiciones financieras

Cuando la disponibilidad de los servicios a largo plazo es un aspecto a considerar tanto para la entidad como para las partes que confían, debería mostrarse estabilidad financiera suficiente para garantizar la prestación continua del servicio y garantizar el grado de exposición a responsabilidades que conlleva. Para un nivel de confianza y servicios NdG1, es poco probable que se tomen en consideración estas disposiciones, mientras que los servicios que exijan transacciones más importantes a NdG2 y niveles superiores deberían tomar en consideración estas necesidades.

9.4 Gestión y auditoría de la seguridad de la información

A NdG2 y niveles superiores, los actores del EAAF deberían de tener documentadas las prácticas de gestión de seguridad de la información, las políticas, los métodos de gestión de riesgos y otros controles reconocidos, para ofrecer garantías de que se aplican prácticas eficaces. A NdG3 y niveles

superiores, debería emplearse un sistema oficial de gestión de seguridad de la información (por ejemplo, la serie ISO/CEI 27000).

En función de los acuerdos relativos al cumplimiento jurídico, contractual y técnico, los actores deberían asegurarse de que las partes cumplen sus compromisos y podrían ofrecer una vía para rectificar en caso de que no las cumplan. A NdG2 y niveles superiores, esta garantía debería estar avalada por auditorías de seguridad, internas y externas, y el registro seguro de eventos importantes, incluidas esas auditorías. Las auditorías pueden utilizarse para verificar que las prácticas de las partes están en consonancia con lo acordado. En caso de litigio podrían recurrirse a servicios de resolución de controversias.

9.5 Componentes externos del servicio

Cuando una organización depende de terceros para algunas partes de su servicio, la forma en que dirige y supervisa las acciones de esas partes contribuye a la garantía general de la prestación del servicio. La naturaleza y extensión de los acuerdos debería ser proporcional al NdG exigido y al sistema de gestión de seguridad de la información aplicado. A NdG1, dicha garantía debería tener un efecto mínimo, pero a partir de NdG2, estas medidas contribuyen a la garantía general que se ofrece.

9.6 Infraestructura operativa

Para crear redes de confianza a gran escala, podrían recurrirse a un marco de confianza. En un marco de confianza, los actores dan soporte al flujo de información entre ellos. Dependiendo de los acuerdos, puede recurrirse a actores adicionales para garantizar que todos ellos cumplen sus compromisos y ofrecer una vía de rectificación en caso de que no los cumplan.

9.7 Evaluación de las capacidades operacionales

Los encargados de elaborar políticas establecen los requisitos técnicos y contractuales de los marcos de confianza. Entre esos requisitos técnicos pueden figurar, por ejemplo, los niveles de versión del producto, la configuración del sistema, ajustes y protocolos, mientras que los requisitos contractuales pueden estar orientados a unas prácticas de información leales. Al estipular estos requisitos, los encargados de elaborar políticas deben incluir los criterios a tenor de los cuales se pueden evaluar las posibles entidades del marco de confianza. En vez de concebir criterios ellos mismos, puede ser conveniente que éstos recurran a los criterios normalizados que ya han sido elaborados por expertos, como esta Recomendación. Cuanto más las esferas decisorias utilicen criterios normalizados a través de los diferentes marcos de confianza, más fácil le resultará a las entidades comprender y aplicar esos criterios de una manera coherente. Además, los conjuntos de criterios designados pueden servir de símbolo para indicar los diversos grados o tipos de rigor en los requisitos o capacidades a varios NdG.

10 Amenazas y controles

En esta cláusula se describen las amenazas a cada fase del EAAF y se facilitan los controles requeridos para cada NdG.

10.1 Amenazas a la fase de afiliación y control de la misma

10.1.1 Amenazas a la fase de afiliación

En el Cuadro 10-1 se identifican y describen las amenazas a la fase de afiliación.

Cuadro 10-1 – Amenazas a la fase de afiliación

Amenaza	Ejemplos
Suplantación de identidad	Cuando una entidad aprovecha ilegalmente la información de identidad de otra entidad y cuando un dispositivo se registra en una red utilizando una dirección de control de acceso a los medios (MAC) falsa.

10.1.2 Controles de NdG necesarios para proteger contra amenazas a la fase de afiliación

En el Cuadro 10-2 se identifican los controles necesarios para la fase de afiliación de conformidad con el NdG.

Cuadro 10-2 – Controles de la fase de afiliación para cada NdG

Amenazas	Controles	Controles necesarios			
		NdG1	NdG2	NdG3	NdG4
Suplantación de identidad	Demostración de identidad: observancia de la política	#1	#1	#1	#1
	Demostración de identidad: en persona	/	/	/	#2
	Demostración de identidad: información fidedigna	#3	#4	#5	#6

NOTA – En este cuadro, los identificadores #1-#6 corresponden a los controles específicos necesarios para proporcionar protección a cada NdG. En la cláusula 10.1.2.1 se describe cada uno de esos controles. Los recuadros del cuadro marcados con una línea diagonal indican que el control respectivo no es aplicable en ese NdG.

10.1.2.1 Controles contra amenazas a la fase de afiliación

Los siguientes controles contra amenazas a la fase de afiliación corresponden a los #1 a #6 indicados en el Cuadro 10-2.

Demostración de identidad: observancia de la política

#1. Publicación de la política de demostración de identidad y realización de todas las pruebas de identidad, de conformidad con la política publicada de demostración de identidad.

Demostración de identidad: en persona

#2. Para los seres humanos se utilizará la demostración de identidad en persona.

Demostración de identidad: información fidedigna

#3. La información de identidad puede ser autodeclarada o autoaseverada.

#4. Se aplican los siguientes controles:

- Todos los controles de #3.
Además:
- La entidad proporcionará información de identidad procedente por lo menos de una fuente fidedigna acorde con la política.
 - a) Para seres humanos:
 - i) En persona:
 - asegurar que la entidad está en posesión de un documento de identificación procedente por lo menos de una fuente fidedigna acorde con la política, con una fotografía del titular que corresponda a la imagen de la entidad; y
 - asegurar que el documento de identificación presentado es auténtico, y que ha sido correctamente expedido y es válido en ese momento.

ii) No en persona:

- la entidad proporcionará evidencias de que está en posesión de información de identidad personal acorde con la política (ejemplos de información de identidad aceptable podrían ser un permiso de conducir o un pasaporte);
- la existencia y validez de la evidencia proporcionada será confirmada de conformidad con los requisitos de la política.

b) Para las NPE:

- registrar información procedente de una fuente fidedigna de información de identidad tal como nombre común, descripción, número de serie, dirección MAC, propietario, ubicación, fabricante, etc.

#5. Se aplican los siguientes controles:

- Todos los controles de #4.

Además:

a) Para seres humanos:

i) En persona:

- verificar la exactitud de la información de contacto indicada en el documento de identificación, utilizándolo para ponerse en contacto con la entidad;
- verificar por lo menos un documento de identificación (por ejemplo, certificado de nacimiento, matrimonio o inmigración) en los registros de la correspondiente fuente fidedigna;
- corroborar la información personal en las fuentes de información fidedigna aplicables y (siempre que sea posible) en fuentes de otros contextos, lo suficiente como para asegurar una identidad única; y
- verificar la información proporcionada previamente por la entidad o que probablemente sólo ésta conozca.

ii) No en persona:

- garantizar la verificación por un tercero fiable del aserto/declaración de la entidad en el sentido de que posee una credencial NdG3 (o superior) procedente de una fuente fidedigna; y/o
- verificar la información proporcionada previamente por la entidad o que sea probable que solamente ésta conozca.

b) Para las NPE:

- en el NdG3 se utilizará un hardware fiable (por ejemplo, TPM);
- en el caso de las NPE que ya están en uso, la NPE se afiliará físicamente con un dispositivo RA utilizando una credencial NdG3 expedida por un ser humano. Cuando se utiliza un hardware fiable, éste debería estar activado;
- las NPE aún no adquiridas se solicitarán utilizando autenticación humana NdG3 o firma digital para confirmar que la entidad que presenta la solicitud está autorizada para ello. La RA del fabricante registrará la NPE, habilitará todos los hardware fiables y controlará la expedición y suplantación de identidad de la NPE. El hardware fiable se inicializará al conectarlo a la red;
- en el caso de las NPE que no sean computadoras, la vinculación entre el dispositivo, el propietario, la red o el operador de la comunicación y la RA se protegerá criptográficamente de manera similar a un hardware fiable; y

- cuando se utilice software, el código se firmará digitalmente con una credencial NdG3 expedida por un ser humano antes de la expedición, y llevará la contrafirma de la AR como prueba de aceptación antes de entrar en servicio.

#6. Se aplican los siguientes controles:

- Todos los controles de #5.

Además:

a) Para seres humanos:

- la entidad proporcionará información de identidad procedente por lo menos de otra fuente fidedigna acorde con la política.

b) Para las NPE:

- los dispositivos adicionales conectados a una computadora, un teléfono móvil, o un procesador similar se registrarán en el momento de la expedición y se vincularán criptográficamente al dispositivo de anclaje (por ejemplo, un dispositivo habilitado por un hardware fiable, un lector biométrico, una tarjeta inteligente, un geo-autentificador GPS);
- la RA se encargará de gestionar cualquier cambio en los acuerdos vinculantes entre los dispositivos. Siempre que sea posible, la capacidad de gestión de red alertará a la RA o a la administración de la red respecto de cualquier cambio en las relaciones entre los dispositivos y comunicará las medidas correctivas adoptadas;
- se debe disponer de capacidades para impedir funcionar a cualesquiera relaciones de dispositivos alterados; y
- el código del software NdG4 estará firmado digitalmente con una credencial NdG4 expedida por un ser humano y llevará la contrafirma de la RA como prueba de aceptación antes de ser puesto en uso.

10.2 Amenazas a la fase de gestión de credenciales y control de la misma

10.2.1 Amenazas a la gestión de credenciales

En el Cuadro 10-3 se indican las amenazas a la fase de gestión de credenciales.

Cuadro 10-3 – Amenazas a la gestión de credenciales

Amenaza	Ejemplos
Creación de credencial: alteración	Un atacante altera la información que circula del proceso de afiliación al proceso de creación de credenciales.
Creación de credencial: creación no autorizada	Un atacante hace que un CSP cree una credencial basada en una entidad ficticia.
Expedición de credencial: divulgación	Un atacante copia una credencial creada por el CSP para una entidad cuando ésta se transfiere del CSP a la entidad durante el establecimiento de credencial.
Activación de credencial: posesión no autorizada	Un atacante obtiene una credencial que no le pertenece y haciéndose pasar por la verdadera entidad hace que el CSP active la credencial.
Activación de credencial: falta de disponibilidad	1) La entidad asociada con la credencial, o los medios para generarla, no se encuentra en la ubicación habitual y es incapaz de autenticar adecuadamente su identidad ante el CSP. 2) Se retarda la entrega de una credencial, o de los medios para generarla, y no es posible activar la credencial dentro del periodo prescrito.

Cuadro 10-3 – Amenazas a la gestión de credenciales

Amenaza	Ejemplos
Almacenamiento de credencial: divulgación	Se revelan las credenciales almacenadas en el fichero de un sistema. Por ejemplo, un atacante accede a un registro almacenado de nombres de usuario y contraseñas.
Almacenamiento de credencial: alteración	El fichero que hace corresponder los nombres de usuario con las credenciales puede verse comprometido, de modo que se modifican las correspondencias y se sustituyen las credenciales existentes por credenciales a las cuales tiene acceso el atacante.
Almacenamiento de credencial: duplicación	Un atacante utiliza la información almacenada para crear una credencial duplicada (por ejemplo, duplicando una tarjeta inteligente que puede generar la credencial) que puede ser utilizada por una entidad no autorizada.
Almacenamiento de credencial: divulgación por la entidad	La entidad mantiene un registro escrito de nombre de usuario y contraseña en un lugar al que otros pueden tener acceso.
Revocación de credencial: revocación tardía	La información de revocación no se difunde a su debido tiempo y da lugar a una amenaza de entidades con credenciales revocadas que todavía pueden autenticar antes de que el verificador de la credencial ponga al día la información de revocación más reciente.
Revocación de credencial: utilización tras desmantelamiento	Las cuentas de usuario no se borran cuando los empleados abandonan la empresa, lo que da lugar a una posible utilización indebida de cuentas antiguas por personas no autorizadas. – Una credencial almacenada en un dispositivo de hardware es utilizada después de que sus claves criptográficas han sido revocadas.
Renovación de credencial: divulgación	Un atacante copia la credencial renovada por el CSP para una entidad mientras es transportada.
Renovación de credencial: alteración	Un atacante modifica una nueva credencial creada por una entidad cuando ésta se presenta al CSP para sustituir una credencial caducada.
Renovación de credencial: renovación no autorizada	Un atacante logra sacar provecho de un protocolo de renovación de credencial débil con el fin de ampliar el periodo de validez de la credencial para una entidad actual. Un atacante logra engañar al CSP para que éste expida una nueva credencial para una entidad actual, y la nueva credencial vincula la identidad de la entidad actual con una credencial proporcionada por el atacante. En el caso de las entidades NPE, un ejemplo de esto es el re-etiquetado (re-expedición) de un componente del sistema (por ejemplo, RAM) como nuevo después de que éste ya ha sido utilizado.
Mantenimiento de registros de credencial: repudio	Una entidad asevera o declara que una credencial auténtica es fraudulenta o contiene información incorrecta con miras a negar falsamente que ha utilizado esa credencial.

10.2.2 Controles de NdG necesarios para proteger contra amenazas a la fase de gestión de credenciales

En el Cuadro 10-4 se indican los controles necesarios contra las amenazas a la gestión de credenciales de conformidad con el NdG.

Cuadro 10-4 – Controles de gestión de credenciales para cada NdG

Amenazas	Controles	Controles necesarios			
		NdG1	NdG2	NdG3	NdG4
Creación de credencial: alteración	Creación de credencial adecuada	#1	#1	#2	#2
	Únicamente hardware	/	/	/	#3
	Estado bloqueado	/	/	/	#4
Creación de credencial: creación no autorizada	Inventario rastreado	#5	#5	#5	#5
Expedición de credencial: divulgación	Expedición de credencial adecuada	#6	#7	#7	#8
Activación de credencial: posesión no autorizada Activación de credencial: falta de disponibilidad	Activada por la entidad	#9	#9	#10	#11
Almacenamiento de credencial: divulgación Almacenamiento de credencial: alteración Almacenamiento de credencial: duplicación Almacenamiento de credencial: divulgación por la entidad	Almacenamiento seguro de credencial	#12	#13	#14	#15
Revocación de credencial: revocación tardía Revocación de credencial: uso tras desmantelamiento	Revocación y destrucción seguras de credencial	#16	#16	#16	#16
Renovación de credencial: divulgación Renovación de credencial: alteración Renovación de credencial: renovación no autorizada	Renovación segura de credencial	#17	#17	#18	#19
Mantenimiento de registro de credencial: repudio	Retención de registro	#20	#20	#21	#21
NOTA – En este cuadro, los identificadores #1-#21 corresponden a los controles específicos necesarios para proporcionar protección a cada NdG. En la cláusula 10.2.2.1 se describe detalladamente cada uno de esos controles. Los recuadros del cuadro marcados con una línea diagonal indican que el control respectivo no es aplicable en ese NdG.					

10.2.2.1 Controles contra amenazas a la fase de gestión de credenciales

Los siguientes controles contra las amenazas a la fase de gestión de credenciales corresponden a los números #1-#21 indicados en el Cuadro 10-4.

Creación de credencial adecuada

#1. Se aplican los siguientes controles:

- Para la creación de credenciales se utilizarán procesos formalizados y documentados.
- Antes de finalizar la vinculación de una credencial a una entidad, el CSP debe tener la suficiente garantía de que la credencial está y sigue estando vinculada a la entidad correcta.

#2. Se aplican los siguientes controles:

- Todos los controles desde #1.
Además:
- La vinculación de credenciales proporcionará protección contra la falsificación utilizando:
 - a) firmas digitales; o
 - b) los mecanismos descritos en StateLocked para las credenciales incorporadas en un dispositivo de hardware.

Sólo hardware

#3. Las credenciales estarán contenidas en un módulo de seguridad de hardware⁶.

Estado bloqueado

#4. Las credenciales incluidas en un dispositivo de hardware se pondrán en estado de bloqueo al final del proceso de creación.

Inventario rastreado

#5. Si una credencial, o los medios para producirla, está incluida en un dispositivo de hardware, este dispositivo deberá mantenerse físicamente en un lugar seguro y deberá realizarse un seguimiento del inventario. Por ejemplo, las tarjetas inteligentes no personalizadas deben almacenarse en un sitio seguro y deben registrarse sus números de serie para protegerlas contra el robo e intentos posteriores de crear credenciales no autorizadas.

Expedición adecuada de credenciales

#6. Para la emisión de credenciales deberán utilizarse procesos formalizados y documentados.

#7. Se aplican los siguientes controles:

- Todos los controles desde #6.
Además:
- El proceso de emisión deberá incluir un mecanismo para garantizar que se concede una credencial a la entidad correcta o a un representante autorizado de la misma. Si la credencial no se entrega en persona, se empleará un mecanismo para verificar que existe la dirección de entrega y que está legítimamente asociada a la entidad.

#8. Se aplican los siguientes controles:

- Todos los controles desde #7.
Además:
- Si una credencial no se entrega en persona deberá entregarse utilizando un canal seguro y la entidad o un representante autorizado de la misma deberá firmar un acuse de recibo de la credencial.

Activada por la entidad

#9. Deberá establecerse un procedimiento para garantizar que una credencial, o los medios para generarla, se activa únicamente si está bajo el control de la entidad correspondiente. No hay requisitos específicos para este procedimiento.

#10. Deberá establecerse un procedimiento para garantizar que una credencial, o los medios para generarla, se activa únicamente si está bajo el control de la entidad correspondiente. Este procedimiento deberá demostrar que la entidad está vinculada a la activación de la credencial (por ejemplo, protocolo basado en pregunta-respuesta).

⁶ El contorno de un módulo de seguridad de hardware se define en la norma ISO/CEI 19790:2012.

#11. Deberá establecerse un procedimiento para garantizar que una credencial, o los medios para generarla, sólo se activa si está bajo el control de la entidad correspondiente. Este procedimiento deberá:

- a) demostrar que la entidad está vinculada a la activación de la credencial (por ejemplo, protocolo basado en pregunta-respuesta), y
- b) permitir únicamente la activación en un periodo de tiempo determinado por un plan.

Almacenamiento seguro de la credencial

#12. Se aplican los siguientes controles:

- las credenciales basadas en secretos compartidos deberán protegerse mediante controles de acceso que limiten el acceso únicamente a los administradores y aplicaciones que requieran el acceso; y
- la política de protección para las credenciales almacenadas deberá describirse en la documentación asociada a la utilización de estas credenciales, puesta a disposición de las entidades.

#13. Se aplican los siguientes controles:

- Todos los controles desde #12.
Además:
- Estos ficheros secretos compartidos no deberán contener claves o secretos de texto en clave; puede emplearse un método alternativo para proteger el secreto compartido.

#14. Se aplican los siguientes controles:

- Todos los controles desde #13.
Además:
- Los secretos compartidos deben protegerse mediante controles de acceso que limiten el acceso únicamente a los administradores y las aplicaciones que requieran dicho acceso. Estos secretos compartidos deberán encriptarse. La clave de inscripción para los secretos compartidos deberá ser a su vez encriptada y almacenada en un módulo (hardware o software). La clave de encriptación para el secreto compartido sólo deberá desencriptarse cuando sea inmediatamente necesaria para una operación de autenticación.
- Las entidades o los representantes de las mismas deberán reconocer que comprenden estos requisitos y comprometerse a proteger las credenciales de conformidad con los mismos.

#15. Se aplican los siguientes controles:

- Todos los controles desde #14.
Además:
- Las entidades o los representantes autorizados de las mismas deberán firmar un documento asegurando que comprenden los requisitos de almacenamiento de las credenciales y comprometiéndose a protegerlas.

Destrucción y revocación seguras de credenciales

#16. Los CSP deberán revocar o destruir (si es posible) las credenciales (incluidas las que se basan en secretos compartidos) en un plazo de tiempo específico para cada NdG como define la política de organización.

Renovación segura de credenciales

#17. Se aplican los siguientes controles:

- el CSP deberá establecer políticas adecuadas para la renovación y sustitución de las credenciales;
- la prueba de posesión de la credencial actual en vigor deberá demostrarla la entidad antes de que el CSP permita su renovación y/o sustitución;
- las claves deberán cumplir los mínimos requisitos políticos del CSP en cuanto a potencia y reutilización de los mismos;
- una vez expirada la credencial en vigor, no se permitirá la renovación;
- todas las interacciones se llevarán a cabo en un canal protegido.

#18. Se aplican los siguientes controles:

- Todos los controles desde #17.
Además:
- Llevarán a cabo una demostración de identidad NdG2 de conformidad con la cláusula 10.1.2.1 (Demostración de identidad: observancia de la política; Demostración de identidad: información fidedigna).

#19. Se aplican los siguientes controles:

- Todos los controles desde #17.
Además:
- Llevarán a cabo una demostración de identidad NdG3 de conformidad con la cláusula 10.1.2.1 (Demostración de identidad: observancia de la política; Demostración de identidad: información fidedigna).

Mantenimiento de registros

#20. El CSP mantendrá un registro de la inscripción, historia y estado de cada credencial (incluida la revocación). La duración de retención deberá especificarse en la política del CSP.

#21. Se aplican los siguientes controles:

- Todos los controles desde #20.
- Deberán establecerse procedimientos formalizados y documentados para la cadena de custodia de cada registro.

10.3 Amenazas a la fase de autenticación y control de la misma

10.3.1 Amenazas a la fase de autenticación

Las amenazas a la fase de autenticación comprenden las asociadas con la utilización de credenciales durante la autenticación y las amenazas generales a la autenticación. Las amenazas generales a la autenticación son, entre otras: software malicioso (por ejemplo, virus, Troyanos, registradores de teclas); ingeniería social (por ejemplo "espíar por la espalda", robo de dispositivos de hardware); errores de usuario (por ejemplo, claves fáciles de detectar, fallos en la protección de la información de autenticación); falso repudio; interceptación no autorizada y/o modificación de los datos de autenticación durante la transmisión; denegación de servicio y debilidad del procedimiento. Con la excepción del uso de la autenticación multifactor, los controles para las amenazas generales a la autenticación caen fuera del ámbito de esta norma. Esta cláusula se centra en las amenazas asociadas al empleo de credenciales para la autenticación, describe dichas amenazas y hace una lista de los controles para cada tipo de amenaza.

Salvo en el caso del requisito de utilizar autenticación multifactor para NdG 3 y 4, no conviene diseñar controles específicos en términos de NdG para la fase de autenticación. Algunos controles pueden que no sean apropiados para todos los contextos. Por ejemplo, los controles para la autenticación de usuarios que acceden a suscripción de una revista únicamente en línea probablemente son distintos a los controles para los médicos que deben acceder a los informes de sus pacientes. Por tanto, se recomienda que, para evitar riesgos y consecuencias más severas, el CSP considere el tema de la seguridad detenidamente, es decir, que establezca controles por capas adecuados al entorno operativo, a la aplicación y al NdG. Corresponde al ingeniero de sistemas, basándose en un análisis de riesgos, tomar decisiones en cuanto a cómo, cuándo y qué combinaciones deben utilizarse en estos controles.

Existen muchas amenazas a las credenciales utilizadas en la autenticación. El Cuadro 10-5 presenta algunas categorías amplias de amenazas a la utilización de credenciales y proporciona ejemplos específicos que ilustran las amenazas.

Cuadro 10-5 – Resumen de amenazas a la utilización de credenciales en la fase de autenticación

Amenaza	Ejemplos
Amenazas generales	Las amenazas generales a la autenticación incluyen muchas categorías de amenazas, comunes a cualquier tipo de TIC. Algunos ejemplos incluyen registradores de teclas, ingeniería social y errores de usuario. Salvo en lo referente a la autenticación multifactor, los controles contra estas amenazas caen fuera del ámbito de esta Recomendación. Conviene recordar que la autenticación multifactor no supone una protección contra todas las posibles amenazas generales.
Adivinar en línea	Un atacante lleva a cabo intentos repetidos de entrar en el sistema tratando de adivinar los posibles valores de la credencial.
Adivinar fuera de línea	Los secretos asociados con la generación de credenciales se exponen utilizando métodos analíticos fuera de la transacción de autenticación. El desciframiento de una clave se basa a menudo en métodos de fuerza bruta, tales como la utilización de ataques de diccionario en los que el atacante utiliza un programa para iterar a través de todas las palabras de un diccionario (o múltiples diccionarios en distintos idiomas), calcula el valor del troceo para cada palabra y verifica el valor de troceo resultante comparándolo con la base de datos. La utilización de cuadros arco iris es otro método para descifrar claves. Se trata de cuadros precalculados de pares texto claro/valores de troceo. Son más rápidos que los ataques con fuerza bruta porque utilizan funciones de reducción para disminuir el espacio de búsqueda. Una vez generados u obtenidos, estos cuadros pueden ser utilizados repetidamente por un atacante.
Duplicación de la credencial	La credencial de la entidad, o los medios para generarla, han sido ilegítimamente copiados. Un ejemplo sería la copia no autorizada de una clave privada.
Peska (<i>phishing</i>)	Se convence a una entidad para que interactúe con un verificador falso y se le engaña para que revele su clave o sus datos personales sensibles, que luego pueden utilizarse para suplantar a la entidad. Un ejemplo es cuando una entidad recibe un correo electrónico que le redirige a una dirección web fraudulenta y pide al usuario que se registre utilizando su nombre de usuario o su contraseña.
Escucha subrepticia	Un atacante escucha pasivamente la transacción de autenticación para obtener información que puede utilizarse posteriormente en un ataque activo posterior a los efectos de suplantar a la entidad.
Ataque por repetición	Un atacante puede reproducir mensajes previamente captados (entre una entidad legítima y una RP) para autenticarse como dicha entidad ante la RP.

Cuadro 10-5 – Resumen de amenazas a la utilización de credenciales en la fase de autenticación

Amenaza	Ejemplos
Piratería de sesión	Un atacante puede insertarse entre una entidad y un verificador tras un intercambio de autenticación correcto entre estas últimas dos partes. El atacante puede hacerse pasar por una entidad ante la parte que confía o viceversa para controlar el intercambio de datos en la sesión. Un ejemplo es un atacante que puede introducirse en una sesión de autenticación por escucha subrepticia o prediciendo el valor de los "cookies" de autenticación para marcar las peticiones de HTTP enviadas por la entidad.
Ataque por intromisión	El atacante se ubica entre la entidad y la parte que confía de manera que puede interceptar y alterar el contenido de los mensajes del protocolo de autenticación. El atacante normalmente suplanta la identidad de la parte que confía ante la entidad y simultáneamente suplanta la identidad de la entidad ante el verificador. Llevando a cabo un intercambio activo con ambas partes simultáneamente el atacante puede utilizar los mensajes de autenticación enviados por una parte legítima para autenticarse adecuadamente ante la otra parte.
Robo de credencial	Un dispositivo que genera o contiene credenciales es robado por un atacante.
Falsificación y suplantación	La falsificación y la suplantación se refieren a situaciones en las que un atacante suplanta la identidad de otra entidad para poder llevar a cabo una acción que de otra forma no podría realizar (por ejemplo, obtener acceso a una cuenta inaccesible de cualquier otra forma). Esto puede realizarse haciendo uso de las credenciales de una entidad o haciéndose pasar por una entidad (por ejemplo, falsificando una credencial). Algunos ejemplos son un atacante que finge ser una entidad y se apropia de una o más características biométricas creando una huella falsa que se ajusta al patrón de la entidad; un atacante falsifica una dirección MAC haciendo que su dispositivo difunda una dirección MAC que pertenece a otro dispositivo que tiene un permiso en una red particular; o un atacante se hace pasar por un editor de software legítimo responsable de la descarga de aplicaciones software en línea y/o de las actualizaciones.

10.3.2 Controles NdG requeridos para protegerse contra las amenazas a la utilización de credenciales

El Cuadro 10-6 identifica los controles necesarios para contrarrestar las amenazas a la utilización de credenciales de acuerdo con el NdG.

Cuadro 10-6 – Resumen de los controles para las amenazas a la utilización de credenciales de acuerdo con el NdG

Amenazas	Controles	Controles Requeridos				
		NdG*	NdG1	NdG2	NdG3	NdG4
General**	Autenticación multifactor	/	/	/	#1	#1
Adivinar en línea	Contraseña robusta Bloqueo de credenciales Utilización de cuenta por defecto Auditoría y análisis	#2 #3 #4 #5	/	/	/	/
Adivinación fuera de línea	Contraseña "troceada" con "sal"	#6	/	/	/	/

Cuadro 10-6 – Resumen de los controles para las amenazas a la utilización de credenciales de acuerdo con el NdG

Amenazas	Controles	Controles Requeridos				
		NdG*	NdG1	NdG2	NdG3	NdG4
Aplicación de credencial	Antifalsificación	#7				
Peska (<i>phishing</i>)	Detección en mensajes Adopción de prácticas anti-peska Autenticación recíproca	#8 #9 #10				
Escucha subrepticia	No transmitir contraseñas Autenticación encriptada Diferentes parámetros de autenticación	#11 #12 #13				
Ataque por reproducción	Diferentes parámetros de autenticación Sello de tiempo Seguridad física	#13 #14 #15				
Piratería de sesión	Sesión encriptada Resolver vulnerabilidades del protocolo Protocolo mutuo criptográfico	#16 #17 #18				
Ataque por intromisión	Autenticación recíproca Sesión encriptada	#10 #16				
Robo de credencial	Activación de credencial	#19				
Falsificación y suplantación de identidad	Firma digital codificada Detección de actividad	#20 #21				
NdG* – Estos controles se aplicarán cuando se estime necesario al evaluar el riesgo. General** – La autenticación multifactor no puede ofrecer resistencia a todas estas amenazas.						

NOTA – En el cuadro *supra*, los identificadores #1-#21 corresponden a los controles específicos necesarios para la protección de cada NdG. Cada uno de esos controles se describe en detalle en la cláusula 10.3.2.1.

10.3.2.1 Controles contra amenazas a la utilización de credenciales en la fase de autenticación

Los siguientes controles contra amenazas a la utilización de credenciales durante la fase de autenticación corresponden a los números #1-#21 indicados en el Cuadro 10-6.

Autenticación multifactor

#1. Se utilizarán dos o más credenciales con factores de autenticación diferentes (por ejemplo, un elemento que se ha combinado a otro elemento conocido).

Contraseña robusta

#2. Será obligatoria la utilización de contraseñas robustas (por ejemplo, cadenas complejas sin significado que contengan una combinación de mayúsculas, minúsculas, números y caracteres especiales).

Bloqueo de credenciales

#3. Se utilizará un mecanismo de anulación o bloqueo tras un cierto número de intentos infructuosos de introducir una contraseña.

Utilización cuenta por defecto

#4. No se utilizarán nombres de cuentas ni contraseñas por defecto (por ejemplo, datos del fabricante).

Auditoría y análisis

#5. Se mantendrá un registro de verificación de los accesos fallidos para analizar modelos de intentos de obtención directa de contraseñas en línea.

Contraseña "troceada" con "sal"

#6. Se utilizarán contraseñas con funciones *hash* (troceo) y valores *salt* (sal) para frenar ataques de fuerza bruta (*brute-force attack*) o ataques a la tabla arcoíris (*rainbow table*).

Medidas contra la falsificación

#7. Se aplicarán medidas contra la falsificación (por ejemplo, hologramas, microimpresiones) en dispositivos que funcionan con credenciales.

Detección de ataques de *peska* en mensajes

#8. Se efectuarán controles concebidos concretamente para detectar ataques de *peska* (por ejemplo, filtros bayesianos, listas negras IP, filtros URL, esquemas heurísticos y huellas dactilares).

Adoptación de prácticas contra la *peska*

#8. Se utilizarán prácticas como la desactivación de imágenes e hiperenlaces provenientes de fuentes no fiables y el suministro de indicaciones visuales en clientes de correo electrónico, para la protección de entidades contra ataques de *peska*.

Autenticación recíproca

#9. Se utilizará la autenticación recíproca.

No transmisión de contraseñas

#11. Se utilizarán mecanismos que no transmitan contraseñas por la red (por ejemplo, protocolo Kerberos).

Autenticación encriptada

#12. Si es necesario intercambiar información de autenticación por una red, los datos anteriores al tránsito serán encriptados.

Parámetro de autenticación diferente

#13. Se utilizará un parámetro de autenticación diferente para cada transacción de autenticación (por ejemplo, contraseña de un solo uso, credencial de sesión).

Sello de tiempo

#14. Cada mensaje tendrá un sello de tiempo no falsificable.

Seguridad física

#15. Se utilizarán mecanismos físicos de seguridad (es decir, comprobar, detectar y reaccionar en caso de alteración).

Sesión encriptada

#16. Se utilizarán sesiones encriptadas.

Resolver vulnerabilidades del protocolo

#17. Se efectuarán correcciones de plataforma para adaptarse a las vulnerabilidades del protocolo (por ejemplo, TCP/IP).

Protocolo mutuo criptográfico

#18. Se utilizará un protocolo mutuo de toma de contacto basado en la criptografía (por ejemplo, TSL).

Activación de credenciales

#19. Se exigirá la activación para poder utilizar la credencial (por ejemplo, introducir un PIN o información biométrica en el dispositivo lógico que contiene la credencial).

Firma digital codificada

#20. Se verificarán las firmas digitales mediante una fuente fiable para contrarrestar la descarga de software que ha sido modificada por partes no autorizadas.

Detección de vida

#21. Se aplicarán técnicas de detección de vida para identificar la utilización de características biométricas artificiales (por ejemplo, huellas dactilares falsificadas).

11 Criterios de garantía del servicio

Los operadores de marcos de confianza que desean ajustarse a este marco establecerán criterios específicos para cumplir los requisitos de cada NdG que procuran respaldar y evaluarán a los CSP que reclaman su conformidad con el marco con arreglo a esos criterios. De la misma manera, los CSP determinarán el NdG que cumplen sus servicios con respecto a este marco mediante la evaluación de sus mecanismos técnicos y procesos comerciales globales en relación con los criterios específicos establecidos.

Anexo A

Características de una credencial

(Este anexo forma parte integral de la presente Recomendación.)

- a) Una credencial es un conjunto de datos.
Una credencial no incluye ningún tipo de contenedor o dispositivo físico que contenga los datos, ni tampoco un generador de los datos que componen la credencial. Por lo tanto, un generador de código de acceso nunca forma parte de una credencial, y no es una tarjeta inteligente que puede firmar datos, ni un software que genera firmas digitales ni tampoco un papel en el que puedan hacerse anotaciones.
- b) Una credencial debe contener datos que demuestren una identidad y/o sus derechos.
A título de ejemplo:
- 1) algo que se conoce (por ejemplo, una contraseña estática);
 - 2) una característica biométrica o su representación; o
 - 3) datos generados por algo que se posee (por ejemplo, códigos de acceso de un solo uso producidos por un generador de código, datos con firmas digitales efectuadas por hardware o software utilizando una clave privada que, supuestamente, debe estar en posesión de una entidad).
- c) Una credencial puede ir acompañada de otros datos que pueden ser de utilidad en los procesos de autenticación e identificación, pero que no forman parte de la credencial propiamente dicha.
Entre esos datos pueden mencionarse el nombre de una entidad y un certificado de clave pública. Ninguno de ellos constituye necesariamente una prueba de identidad o sus derechos, pero son útiles en los protocolos de autenticación. Asociar el nombre de la entidad a una credencial confirma la identidad. Asociar un certificado de clave pública a una credencial facilita información que contribuye a verificar las pruebas, y también podrían facilitar información sobre la identidad o derechos de una entidad.
- d) Una credencial también puede ser una credencial derivada.
En este caso, puede tratarse de una recopilación de información derivada de una serie de credenciales, creadas y enviadas generalmente por una entidad de autenticación a un verificador de credenciales. Por ejemplo, en algunos tipos de autenticación anónima, la entidad transforma la credencial expedida por el CSP en una credencial derivada utilizada en la autenticación.
- e) No todos los datos que componen una credencial deben ser secretos.
- f) Una credencial puede ser utilizada para la autenticación, identificación o autorización de la entidad, o para una combinación de los tres procesos.
- g) Una credencial debe ser verificada antes de aceptarse como auténtica y fiable para la finalidad a la que está destinada (por ejemplo, autenticación, identificación, autorización).
- h) Una credencial debe superar diversas etapas de verificación, como por ejemplo:
- 1) comprobar la autenticidad de la credencial para asegurarse de que procede del supuesto expedidor;
 - 2) confirmar la validez y fiabilidad de la credencial (por ejemplo, determinar si existe un vínculo directo con una raíz fiable del expedidor de la credencial);
 - 3) confirmar la precisión de los cálculos matemáticos/criptografía.

- i) Una credencial puede ser auténtica pero no válida en todos los contextos (por ejemplo, la credencial de una tarjeta inteligente, como las tarjetas telefónicas de previo pago, puede ser auténtica pero sólo válida para las llamadas efectuadas desde las instalaciones del expedidor).

Apéndice I

Privacidad y protección de la PII

(Este apéndice no forma parte integral de la presente Recomendación.)

La conveniencia de aplicar un método de autenticación en especial a una determinada utilización dependerá no sólo de la evaluación de la eficacia de la autenticación sino también de los riesgos que comporta para las organizaciones implicadas y de su tolerancia a los mismos. La utilización indebida de la protección de la PII (información de identificación personal) de las entidades, o la falta de una protección adecuada de esa información, entraña riesgos importantes para las organizaciones, desde daños a su reputación hasta responsabilidades jurídicas. Por este motivo, la utilización de la PII para fines de autenticación y su protección debe ser examinada y estimada con sumo cuidado. En este Apéndice se facilitan, a título orientativo, algunas consideraciones en materia de privacidad que convendría que las organizaciones tuvieran en cuenta al tomar una decisión con respecto a la utilización y aplicación de un determinado método de autenticación.

Cuando las entidades son individuos, la mayoría de los métodos de autenticación supondrá el tratamiento de la PII durante una o más de las siguientes etapas:

- a) el proceso de afiliación, cuando se recopila, demuestra y verifica la identidad y otras informaciones relativas a las entidades;
- b) la creación, emisión y gestión de las credenciales de las entidades;
- c) la utilización de credenciales por la entidad y su verificación por las partes confiantes y los verificadores.

Es posible lograr una autenticación y privacidad sólidas. Hay numerosos métodos de autenticación sólidos en materia criptográfica que tienen una incidencia negativa limitada en la privacidad (por ejemplo, credenciales anónimas, firmas de grupo). Asimismo conviene no olvidar que el aumento del nivel de garantía (por ejemplo, NdG4 en comparación con NdG2) puede, aunque no necesariamente, afectar en forma negativa la privacidad de un individuo. Ello dependerá en gran medida del método de autenticación elegido y de la manera de aplicarlo. Al tomar estas decisiones, cada organización debe considerar detenidamente la necesidad de proteger la PPI de las entidades, además de proteger sus recursos y procurar que las entidades rindan cuentas en caso de actividades no autorizadas.

La mayoría de los métodos de autenticación supone la utilización de identificadores que distingan inequívocamente una entidad de otras posibles entidades en el contexto de una autenticación. La utilización de identificadores inequívocos también suele ser necesaria para muchos otros propósitos como, por ejemplo, la gestión de cuentas y el mantenimiento de registros de verificación adecuados. Las principales inquietudes sobre la privacidad en relación con el uso de identificadores inequívocos no guarda relación con la utilización de un identificador inequívoco como tal, sino más bien con la reutilización del mismo identificador en numerosos entornos diferentes. Por ejemplo, un número de cuenta asignado con un sólo propósito se considera por lo general menos sensible que una referencia administrativa gubernamental utilizada para diversos fines (por ejemplo, impuestos, atención de la salud, jubilación). En ciertas jurisdicciones, podría haber también una legislación que restrinja la utilización de ciertos identificadores.

Teniendo en cuenta las consideraciones anteriores, las organizaciones deberían implantar medidas eficaces para proteger la información de identificación personal de las entidades en las fases y los procesos descritos en este EAAF. En particular, convendría que el método de autenticación elegido fuera concebido y aplicado de tal manera que redujese al mínimo el tratamiento de la PII. Por otra parte, la utilización de identificadores inequívocos que también se utilizan en otros contextos o

dominios debería limitarse a los casos en que es necesario utilizarlos y a las leyes de la jurisdicción correspondiente que los autoricen.

Pueden hallarse otras consideraciones orientativas de la ISO/CEI para la protección de la PII en dos fuentes:

- a) [b-ISO/CEI 29100] describe los requisitos básicos en materia de privacidad con respecto a tres factores principales: 1) disposiciones legales y reglamentarias para la protección de la privacidad de un individuo y la protección de su PII; 2) disposiciones para actividades particulares y casos de utilización; y 3) preferencias en materia de privacidad de la PII de la entidad. [b-ISO/CEI 29100] describe además los siguientes principios básicos de privacidad: consentimiento y selección, especificación de objetivos, limitaciones de la recopilación, utilización, limitaciones en la retención y divulgación de la información, minimización de los datos, precisión y calidad, transparencia y notificación, acceso y participación individual, rendición de cuentas, controles de seguridad y observancia. Además de realizar una evaluación de los riesgos para analizar las amenazas, las organizaciones deberían efectuar una evaluación de la incidencia de su método de autenticación en la privacidad para determinar qué componentes de sus sistemas necesitarán una atención concreta en términos de medidas de protección de la privacidad.
- b) [b-ISO/CEI 29101] describe un marco de arquitectura para sistemas TIC encargados del tratamiento de la PII. Dicho marco se expresa en relación con varios criterios arquitecturales. Se define un conjunto de componentes para la implantación de sistemas TIC que efectúan el tratamiento de la PII. Ese marco sirve para construir arquitecturas de sistemas que se ajustan a los principios de privacidad indicados en [b-ISO/CEI 29100].

Para una orientación más completa sobre los requisitos, los principios y el diseño de sistemas con respecto a la protección de la PII, se remite al lector a las normas indicadas *supra*.

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 Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autenticación y autorización para las NGN, versión 1*.
- [b-UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en las redes de la próxima generación*.
- [b-UIT-T Y.2721] Recomendación UIT-T Y.2721 (2010), *Requisitos de gestión de identidad en las NGN y ejemplos de utilización*.
- [b-UIT-T Y.2722] Recomendación UIT-T Y.2722 (2010), *Mecanismos de gestión de identidad en las NGN*.
- [b-ISO/IEC 9798] ISO/IEC 9798:2010, *Information technology – Security techniques – Entity authentication*.
- [b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.
- [b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- [b-ISO/IEC 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.
- [b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- [b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements*.
- [b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.
- [b-ISO/IEC 29101] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*.
- [b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*.
- [b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- [b-NIST SP800-36] NIST Special Pub 800-36 (2003), *Guide to Selecting Information Technology Security Products*.
<<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>>
- [b-NIST SP800-63] NIST Special Pub 800-63 (2006), *Electronic Authentication Guideline Version 1.0.2*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>
- [b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure*.
<http://www.gatekeeper.gov.au/>

- [b-DuD] Van Alsenoy B., and De Cock, D. (2008), '*Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card*', *Datenschutz und Datensicherheit*, Vol. 32, No. 3, pp. 178-183.
- [b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0*, 2009.
<<http://www.dia.govt.nz/EOI/pdf/EOIv2.0.pdf>>
- [b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0*.
- [b-IAF] *Kantara Initiative Identity Assurance Framework v2.0*.
<http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework>
- [b-MOV] Menezes, A., van Oorschot, P., and Vanstone, S. (1997), '*Handbook of Applied Cryptography*', pp. 3-4.
<<http://www.cacr.math.uwaterloo.ca/hac/>>
- [b-NeAF] *The National e-Authentication Framework*.
<<http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>>
- [b-OECD] OECD (2007), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*.
<<http://www.oecd.org/dataoecd/32/45/38921342.pdf>>
- [b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies*.
<<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>
- [b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian Framework*.
<http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_qv00240e.html>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación