CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 807

Criptología de empleo en el Esquema Nacional de Seguridad

Mayo 2022

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.20 17:24:40 +02'00'

P.º de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-225-X

Fecha de Edición: mayo de 2022
ISDEFE ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 6
1.1 ORGANISMOS DE ESTANDARIZACIÓN 7
2. OBJETIVO 8
3. MECANISMOS CRIPTOGRÁFICOS AUTORIZADOS 9
3.1 CIFRADO SIMÉTRICO 9
3.2 PRIMITIVAS ASIMÉTRICAS 10
3.2.1. PROBLEMA DE LA FACTORIZACIÓN DE NÚMEROS ENTEROS (RSA) 11
3.2.2. PROBLEMA DEL LOGARITMO DISCRETO MULTIPLICATIVO (FF-DLOG) 11
3.2.3. PROBLEMA DEL LOGARITMO DISCRETO ADITIVO (EC-DLOG) 11
3.3 FUNCIONES RESUMEN 12
3.4 CIFRADO DE CLAVE PÚBLICA 13
3.5 ACUERDO DE CLAVES 14
3.6 FIRMA ELECTRÓNICA 15
3.7 CÓDIGO DE AUTENTICACIÓN DE MENSAJES (MAC) 16
3.8 CIFRADO CON AUTENTICACIÓN (AE / AEAD) 17
3.9 FUNCIONES DE DERIVACIÓN DE CLAVES (KDF) 18
3.10 PROTECCIÓN DE CLAVES (KEY WRAPPING) 19
4. PROTOCOLOS CRIPTOGRÁFICOS 21
4.1 TLS 21
4.2 SSH 23
4.2.1. INTERCAMBIO DE CLAVES – KEY EXCHANGE 24
4.2.2. CIFRADO – ENCRYPTION ALGORITHM 25
4.2.3. AUTENTICACIÓN – PUBLIC KEY AUTHENTICATION 26
4.2.4. INTEGRIDAD Y AUTENTICIDAD DE ORIGEN – MAC ALGORITHM 26
4.3 IPSEC 27
4.3.1. ACUERDO DE CLAVE (DIFFIE-HELLMAN GROUPS TRANSFORMS) 29
4.3.2. CIFRADO (ENCRYPTION ALGORITHMS TRANSFORMS) 30
4.3.3. INTEGRIDAD Y AUTENTICACIÓN DE ORIGEN (INTEGRITY ALGORITHMS TRANSFORMS) 31
4.3.4. FUNCIONES PRF (PSEUDORANDOM FUNCTIONS TRANSFORMS) 32
4.3.5. MECANISMO DE AUTENTICACIÓN 33
5. MEDIDAS DE SEGURIDAD 35
5.1 DIMENSIONES DE SEGURIDAD CONSIDERADAS 35
5.2 NIVELES DE AMENAZA 35
5.3 IDENTIFICACIÓN. [OP.ACC.1] 36
5.4 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS) [OP.ACC.5] 37
5.4.1. REQUISITOS GENERALES PARA EL ESTABLECIMIENTO DE CONTRASEÑAS (CONCERTADAS O ALEATORIAS) 40
5.4.2. PROTOCOLOS DE AUTENTICACIÓN 42
5.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS INTERNOS) [OP.ACC.6] 42
5.5.1. PROTOCOLOS DE AUTENTICACIÓN 45
5.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS [OP.EXP.10] 46

5.7 PROTECCIÓN DE LA CONFIDENCIALIDAD. [MP.COM.2] 46
5.8 PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD [MP.COM.3] 48
5.9 CRIPTOGRAFÍA [MP.SI.2] Y PROTECCIÓN DE EQUIPOS PORTÁTILES [MP.EQ.3] 49
5.10 FIRMA ELECTRÓNICA [MP.INFO.3] 50
5.11 SELLOS DE TIEMPO [MP.INFO.4] 52
5.12 EJEMPLO DE APLICACIÓN: TLS 53
6. REFERENCIAS 55

1. INTRODUCCIÓN

1. El Esquema Nacional de Seguridad (en adelante, ENS) tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación. En él se determinan los principios básicos y requisitos mínimos exigidos para garantizar adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

2. El anexo II de dicho texto detalla las medidas de seguridad, estructuradas en tres grupos: el **marco organizativo** [org], constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el **marco operacional** [op], formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las **medidas de protección** [mp], que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

3. Entre dichas medidas, existen algunas que se basan en la utilización de algoritmos y mecanismos criptográficos para ofrecer el nivel de seguridad requerido. No obstante, la mera utilización de criptografía no es suficiente si (1) los algoritmos o mecanismo criptográficos no son lo suficientemente robustos o (2) la implementación concreta de dicho algoritmo/mecanismo no es correcta.

4. En lo referente a este segundo punto, la evaluación y certificación de un producto o servicio de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo en su Artículo 1 y en su Artículo 2.1, el cual establece que el Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN, en adelante) es la autoridad de certificación de la seguridad de las tecnologías de la información y la comunicación y autoridad de certificación criptológica.

5. Así mismo, el Real Decreto que regula el ENS, indica que el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del CCN, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas, determinará los requisitos de certificación requeridos, así como el criterio a seguir en los casos en los que no existan productos o servicios certificados.

6. En base a estas competencias, el CCN publica la guía **CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)**. Este catálogo tiene como finalidad ofrecer a los organismos de la Administración un conjunto de productos o servicios STIC de referencia cuyas funcionalidades de seguridad relacionadas con el objeto de su adquisición han sido certificadas y cumplen con los requisitos de seguridad mínimos establecidos por el CCN.

1.1 ORGANISMOS DE ESTANDARIZACIÓN

7. Existen diferentes organismos internacionales que se encargan de establecer como «*estándares*» determinados sistemas, productos y equipos, entre los que también se encuentran algoritmos y protocolos criptográficos. Estos organismos son los que determinan la calidad y fiabilidad de los diferentes sistemas y productos para su uso comercial. La mayor parte de los organismos son entidades independientes (aunque otras pertenezcan a organismos gubernamentales).

8. Los organismos de estandarización internacionales más importantes son los siguientes:

   a) ANSI (*American National Standards Institute*): el Instituto Nacional Americano de Estándares (http://www.ansi.org/) es una organización norteamericana que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas. Es miembro de ISO y de IEC. Se encarga de la coordinación entre los estándares norteamericanos e internacionales.

   b) IEC (*International Electrotechnical Commission*): la Comisión Electrotécnica Internacional (http://www.iec.ch/) es un organismo de estandarización en los campos eléctrico, electrónico y de otras tecnologías relacionadas con ellos. Muchas normas se desarrollan conjuntamente con ISO, por lo que muchas de ellas se conocen como normas ISO/IEC.

   c) IEEE (*Institute of Electrical and Electronics Engineers*): el Instituto de Ingenieros Eléctricos y Electrónicos (http://www.ieee.org/index.html) es una asociación mundial de carácter técnico-profesional dedicada a la estandarización de tecnologías derivadas de la electricidad: ingeniería computacional, tecnología biomédica y aeroespacial, energía eléctrica, telecomunicaciones, etc.

   d) ISO (*International Organization for Standardization*): la Organización Internacional para la Estandarización (http://www.iso.org/iso/home.html) es el organismo encargado de desarrollar normas internacionales de fabricación, comercio y comunicación en todas las ramas de la industria (salvo las relativas a la industria eléctrica y electrónica), especialmente en los temas relacionados con las normas de los productos y la seguridad.

   e) NIST (*National Institute of Standards and Technology*): es una agencia del Departamento de Comercio de los Estados Unidos (http://www.nist.gov/index.html). Promociona la innovación y la competencia industrial en Estados Unidos mediante avances en las normas aplicadas y en la propia tecnología. Sus principales áreas de actuación son biotecnología, nanotecnología y tecnologías de la información.

   f) SECG (*Standards for Efficient Cryptography Group*): el Grupo de Estándares para la Criptografía Eficiente (http://www.secg.org/) es un consorcio internacional cuyo principal objetivo es promover el uso de la criptografía basada en curvas elípticas. Entre sus miembros destacan Certicom, Entrust, Fujitsu y Visa.

2. OBJETIVO

9. El objeto de la presente guía es la presentación de los **mecanismos criptográficos que han sido autorizados para su uso en el ENS**, así como la fortaleza requerida y las garantías de evaluación y certificación que deben presentar, atendiendo al nivel de seguridad exigido, para cada una de las medidas que así lo requieran.

10. Para ello, en las Secciones 3 y 4 del presente documento se recoge un listado de los mecanismos criptográficos autorizados y sus correspondientes estándares junto con algunos protocolos comúnmente utilizados, mientras que en la Sección 5 se presenta una relación de los mecanismos que deben utilizarse para cada una de las medidas recogidas en el Anexo II del ENS junto con la fortaleza requerida, atendiendo al nivel de seguridad exigido para cada una de las dimensiones consideradas o la categoría del sistema.

3. MECANISMOS CRIPTOGRÁFICOS AUTORIZADOS

11. En este apartado se recoge la relación de mecanismos criptográficos que se consideran autorizados por el CCN para su uso dentro del ENS, siempre que se realice una implementación correcta de estos, siguiendo las indicaciones especificadas para cada caso.

12. Los mecanismos criptográficos autorizados indicados en los siguientes apartados se han clasificado en dos (2) **categorías** (CAT) de acuerdo con su fortaleza estimada a corto y largo plazo:

    a) **Recomendados (R)**: mecanismos que ofrecen un nivel adecuado de seguridad a largo plazo. Se considera que representan el estado del arte actual en seguridad criptográfica y que, a día de hoy, no presentan ningún riesgo de seguridad significativo. Se pueden utilizar de forma segura a largo plazo, incluso teniendo en cuenta el aumento en potencia de computación esperado en un futuro próximo. Cualquier riesgo residual, solo podrá proceder del desarrollo de ataques muy innovadores.

    b) **Heredado o *Legacy* (L):** mecanismos con una implementación muy extendida a día de hoy, pero que ofrecen un nivel de seguridad aceptable solo a corto plazo. Únicamente deben utilizarse en escenarios en los que la amenaza sea baja/media y el nivel de seguridad requerido por el sistema bajo/medio (como veremos en el apartado 5) y deben ser reemplazados tan pronto como sea posible, ya que se consideran obsoletos respecto al estado del arte actual en seguridad criptográfica, y su garantía de seguridad es limitada respecto a la que ofrecen los mecanismos recomendados. Como consecuencia de ello, para estos mecanismos se define el periodo de validez hasta **2025** (31 de diciembre), salvo indicación expresa de otro periodo.

3.1 CIFRADO SIMÉTRICO

13. En este apartado se recogen los **esquemas de cifrado simétrico**, que permiten proporcionar confidencialidad al mensaje y a los datos. Para ello, el procedimiento de cifrado transforma un texto plano en un texto cifrado utilizando una clave secreta, mientras que el procedimiento de descifrado permite obtener el texto plano a partir del texto cifrado y de la clave.

14. Los esquemas de cifrado simétrico autorizados que se recogen en este apartado están compuestos por un *cifrador de bloque,* también llamado *primitiva*, que actúa según un *modo de operación.* Casi todos ellos se basan en el cifrador **AES** (*Advanced Encryption Standard*).

15. En la **Tabla 3-1** se indican los esquemas de cifrado simétrico autorizados. Como se puede observar, todos ellos son mecanismos recomendados pero obligatoriamente deberán emplearse con alguno de los mecanismos de *autenticación* que se recogen en el apartado 3.7. De manera excepcional en cifrado de disco duro se acepta el uso AES-XTS.

Cifrador / Especificaciones		Modo de Operación / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
AES	ISO/IEC 18033-3 FIPS 197	CBC	NIST SP800-38A ISO/IEC 10116	128 192 256	128 192 256	R[1]
AES	ISO/IEC 18033-3 FIPS 197	CTR	NIST SP800-38A ISO/IEC 10116	128 192 256	128 192 256	R[1]
AES	ISO/IEC 18033-3 FIPS 197	CFB	NIST SP800-38A ISO/IEC 10116	128 192 256	128 192 256	R[1]
AES	ISO/IEC 18033-3 FIPS 197	OFB	NIST SP800-38A ISO/IEC 10116	128 192 256	128 192 256	R[1]
AES	ISO/IEC 18033-3 FIPS 197	XTS	NIST SP800-38E IEEE 1619	128 192 256	128 192 256	R[2]

Tabla 3-1. Esquemas de cifrado simétrico autorizados

3.2 PRIMITIVAS ASIMÉTRICAS

16. La criptografía asimétrica (a veces también llamada de clave pública) tiene como propiedad distintiva que cada usuario emplea dos claves, una para el proceso de cifrado y otra diferente para el de descifrado. La primera de las claves es la clave pública que cada usuario da a conocer para que sea utilizada como clave para cifrar los mensajes que se le envíen; mientras que la otra es la clave privada (o secreta), que solo conoce dicho usuario y le permite descifrar los mensajes cifrados que recibe. Ambas claves están relacionadas mediante un problema matemático dado que llevan a cabo procesos inversos (una cifra y la otra descifra).

17. Las primitivas asimétricas que están aceptadas y los problemas matemáticos correspondientes se presentan a continuación.

[1] Siempre junto con un mecanismo de autenticación del apartado 3.7-
[2] Aceptado sin mecanismo de autenticación para cifrado de disco

3.2.1. PROBLEMA DE LA FACTORIZACIÓN DE NÚMEROS ENTEROS (RSA)

18. En la tabla siguiente se muestran los tamaños de las claves acordadas para la primitiva basada en el problema de la factorización de números enteros (RSA) y otras características.

Primitiva	Tamaño de los parámetros (bits)	CAT
RSA	$n \geq 3000, \log_2(e) > 16$	R
	$n \geq 2048, \log_2(e) > 16$	L

Tabla 3-2. Tamaño de las primitivas RSA acordadas

3.2.2. PROBLEMA DEL LOGARITMO DISCRETO MULTIPLICATIVO (FF-DLOG)

19. En la tabla siguiente se muestran los tamaños de las claves acordadas para la primitiva basada en el problema del logaritmo discreto multiplicativo sobre un cuerpo finito.

Primitiva	Grupo	CAT
MODP [RFC 3526]	3072 bits	R
	4096 bits	R
	6144 bits	R
	8192 bits	R
	2048 bits	L

Tabla 3-3. Tamaño de las primitivas acordadas del logaritmo discreto multiplicativo sobre un cuerpo finito

3.2.3. PROBLEMA DEL LOGARITMO DISCRETO ADITIVO (EC-DLOG)

20. En la tabla siguiente se muestran las familias de las curvas elípticas acordadas.

Familia	Curva	CAT
Brainpool [RFC5639]	*BrainpoolP256r1*	R
	BrainpoolP384r1	R
	BrainpoolP5121r1	R
NIST [FIPS186-4, Appendix D.1.2]	*NIST P-256 o secp256r1*[1]	R
	NIST P-384 o secp384r1 [1]	R
	NIST P-521 o secp521r1 [1]	R
Bernstein	*Curve25519*	R
	Curve448	R

[1] En TLS (RFC 4492) o IPsec w/ IKE v2 (RFC 5903)

Tabla 3-4. Curvas elípticas acordadas

21. Es preciso verificar que los puntos considerados están en la curva, es decir, verifican su ecuación.

22. También es preciso verificar que los puntos considerados están en el subgrupo considerado de la curva. Nótese que el uso de subgrupos de la curva tiene lugar cuando el orden de la misma no es un número primo. Sin embargo, si el orden del subgrupo es un número primo, esto es, q = r, y es tal que r^2 no divide al cardinal de la curva, las comprobaciones se reducen a verificar que los puntos considerados tienen orden precisamente r.

3.3 FUNCIONES RESUMEN

23. En este apartado se recogen las **funciones resumen o funciones hash,** que son funciones que, sin utilizar ninguna clave criptográfica, procesan una entrada consistente en un mensaje de longitud arbitraria, y producen una salida de longitud predeterminada (dependiendo de la función). A esta salida se le llama *valor hash*. Las funciones resumen se utilizan en muchos servicios, como la generación y verificación de firmas, la derivación de claves, la generación de valores aleatorios o en la computación de los códigos MAC. También pueden usarse por sí solas, para proporcionar servicios de integridad al mensaje.

24. Las funciones resumen o funciones hash autorizadas, son las funciones **SHA-2** y **SHA-3**, siendo de uso recomendado aquellas que proporcionan una fortaleza de seguridad de 128 bits o más, y de uso Legacy las que proporcionan una fortaleza entre 112 y 128 bits. En la **Tabla 3-5** se indican estas funciones y sus correspondientes especificaciones.

25. No se autoriza el uso de la función SHA-1, salvo en construcciones HMAC (ver apartado 3.7).

Función Resumen	Especificaciones	MBL *Message Block Length*	HVL *Hash Value Length*	Nivel de Seguridad (bits)	CAT
SHA2-224	*ISO 10118-3 FIPS 180-4*	512	224	112	L
SHA2-512/224	*ISO 10118-3 FIPS 180-4*	1024	224	112	L
SHA2-256	*ISO 10118-3 FIPS 180-4*	512	256	128	R
SHA2-512/256	*ISO 10118-3 FIPS 180-4*	1024	256	128	R
SHA2-384	*ISO 10118-3 FIPS 180-4*	1024	384	192	R

Función Resumen	Especificaciones	MBL *Message Block Length*	HVL *Hash Value Length*	Nivel de Seguridad (bits)	CAT
SHA2-512	*ISO 10118-3 FIPS 180-4*	1024	512	256	R
SHA3-256	*FIPS 202*	1088	256	128	R
SHA3-384	*FIPS 202*	832	384	192	R
SHA3-512	*FIPS 202*	576	512	256	R
BLAKE2s/BLAKE2b	*RFC7693*	512/1024	>=256	>128	R[1]

Tabla 3-5. Funciones resumen autorizadas

3.4 CIFRADO DE CLAVE PÚBLICA

26. En este apartado se recogen los **esquemas de cifrado de clave pública o cifrado asimétrico**. Estos esquemas no están recomendados para el cifrado de datos en grandes cantidades, para lo que es más eficiente el cifrado simétrico.

27. El uso más extendido y para el que se recomienda el cifrado asimétrico, es para proteger el envío de las claves simétricas, que se utilizarán para el cifrado de los datos. Este uso es lo que hace que los esquemas de cifrado asimétrico indicados en este apartado, sean considerados en muchos estándares como esquemas de **Transporte de Clave (*Key Transport*)**.

28. Los esquemas de cifrado asimétrico clásico utilizan mecanismos de *padding* para incrementar la longitud del mensaje a cifrar (es decir, de las claves simétricas, que tienen una longitud limitada).

29. Dentro de los esquemas de cifrado asimétrico clásico, los dos (2) esquemas autorizados se basan en primitiva RSA, y se especifican en la RFC 8017 (una re-publicación del estándar PKCS #1 de *RSA Laboratories*). El esquema **RSAES-OAEP** es el autorizado para uso recomendado, y el esquema RSAES-PKCS1-v1_5 está autorizado únicamente para uso *Legacy*.

30. En la **Tabla 3-6** se indican los esquemas de cifrado asimétrico autorizados y la longitud de clave necesaria para proporcionar un nivel de seguridad de 112 y 128 bits.

[1] Se autoriza su uso únicamente en el contexto de ciertos protocolos modernos como por ejemplo Wireguard o Noise

Tipo de Criptografía	Esquema de cifrado / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
RSA	RSAES-OAEP	PKCS#1v2.2 (RFC 8017), PKCS#1v2.1 (RFC 3447)	112 ≥128	2048 ≥3072	L R
RSA	RSAES-PKCS1-v1_5	PKCS#1v2.2 (RFC 8017), PKCS#1v2.1 (RFC 3447)	112 ≥128	2048 ≥3072	L

Tabla 3-6. Esquemas de cifrado de clave pública autorizados.

3.5 ACUERDO DE CLAVES

31. En este apartado se recogen los **esquemas de acuerdo de claves** (***Key Agreement***), mediante los cuales el material de claves secreto a obtener por los participantes de la comunicación se deriva de la información contribuida por todos ellos.

32. Los esquemas de acuerdo de claves más extendidos se basan en primitivas *Diffie-Hellman (DH)*, fundamentadas en el problema del logaritmo discreto (DLOG). Se consideran autorizados para uso recomendado el esquema **DH** correspondiente a criptografía de campos finitos (FFC) y el esquema **ECDH** correspondiente a criptografía de curva elíptica (ECC).

33. Otro mecanismo que cumple la función de un protocolo de intercambio de claves es la encapsulación de claves o KEM *(Key Encapsulation Mechanism*).

34. Los mecanismos KEM autorizados para uso recomendado son: **DLIES-KEM** (basados en criptografía de Campos Finitos, FFC) y **ECIES-KEM** (basados en criptografía de Curva Elíptica, ECC).

35. En la **Tabla 3-7** se indican los esquemas de acuerdo de clave autorizados y la longitud de clave necesaria para proporcionar un nivel de seguridad de 112 y 128 bits.

Tipo de Criptografía	Esquema de Acuerdo de claves / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
FF-DLOG	DH	NIST SP 800-56A ISO/IEC 11770-3 ANSI X9.42 IEEE 1363	112 ≥128	2048 ≥3072	L R
	DLIES-KEM	ISO/IEC 18033-2	112 ≥128	2048 ≥3072	L R
EC-DLOG	ECDH	NIST SP 800-56A ISO/IEC 11770-3 ANSI X9.63 IEEE 1363 SEC1	112 ≥128	224 ≥ 256	L R

Tipo de Criptografía	Esquema de Acuerdo de claves / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
	ECIES-KEM	ISO/IEC 18033-2	112 ≥128	224 ≥ 256	L R

Tabla 3-7. Esquemas de acuerdo de claves (*Key Agreement*) autorizados

3.6 FIRMA ELECTRÓNICA

36. En este apartado se recogen los **esquemas de firma electrónica**, empleados para dotar al mensaje de los servicios de integridad, autenticación de origen y no repudio. Para ello, proporcionan una función de generación de firma y una función de verificación de firma.

37. Los esquemas de firma electrónica autorizados para uso recomendado basados en primitiva RSA, son: **RSA-PSS** (RFC3447 y ISO 9796-2)

38. Respecto a los esquemas de firma basados en Logaritmo Discreto (DLOG), se aceptan para uso recomendado ***DSA***, **KCDSA** y ***Schnorr*** así como sus variantes de curva elíptica ***ECDSA***, ***ECKCDSA*** *y* ***EC Schnorr*** junto con ***ECGDSA*** definidos en la ISO/IEC 14888-3.

39. Adicionalmente, se considera autorizado para uso recomendado el esquema de firma basado en funciones hash: **XMSS** (*eXtended Merkle Signature Scheme*), implementado según se define en la RFC 8391.

40. En la **Tabla 3-8** se indican los esquemas de firma autorizados y la longitud de clave necesaria para proporcionar un nivel de seguridad de 112 y 128 bits.

Tipo de Criptografía	Esquema de Firma / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
RSA	*RSASSA-PSS*	*PKCS#1v2.2 (RFC 8017)* *PKCS#1v2.1 (RFC 3347)* *FIPS 186-4 (Apdo 5.5)*	112 ≥128	2048 ≥3072	L R
RSA	*RSASSA-PKCS1-v1_5*	*PKCS#1v2.2 (RFC 8017)* *PKCS#1v2.1 (RFC 3347)* *FIPS 186-4 (Apdo 5.5)*	112 ≥128	2048 ≥3072	L
FF-DLOG	*DSA*	*FIPS 186-4 (Apdo 4)* *ISO 14888-3* *ANSI X9.30*	112 ≥128	2048 ≥3072	L R
FF-DLOG	*KCDSA (Korean DSA)*	*ISO 14888-3*	112 ≥128	2048 ≥3072	L R

Tipo de Criptografía	Esquema de Firma / Especificaciones		Fortaleza (bits)	Longitud de clave (bits)	CAT
FF-DLOG	*Schnorr*	*ISO 14888-3 (Ad1)*	112 ≥128	2048 ≥3072	L R
EC-DLOG	*ECDSA*	*FIPS 186-4 (Apdo 6)* *ISO 14888-3* *ANSI X9.62* *SEC.1*	112 ≥128	224 ≥ 256	L R
EC-DLOG	*ECKCDSA*	*ISO 14888-3*	112 ≥128	224 ≥ 256	L R
EC-DLOG	*ECGDSA*	*ISO 14888-3*	112 ≥128	224 ≥ 256	L R
EC-DLOG	*EC Schnorr*	*ISO 14888-3 (Ad1)*	112 ≥128	224 ≥ 256	L R
Funciones Hash SHA2	*XMSS* *eXtended Merkle Signature Scheme*	*RFC 8391* *NIST SP 800-208*			R

Tabla 3-8. Esquemas de Firma electrónica autorizados.

3.7 CÓDIGO DE AUTENTICACIÓN DE MENSAJES (MAC)

41. En este apartado se recogen las **construcciones MAC (*Message Authentication Code*)**, que se utilizan para proporcionar servicios de integridad y autenticidad de origen, basados en mecanismos de clave simétrica.

42. Los esquemas MAC se clasifican en tres tipos: basados en cifradores de bloque, basados en funciones resumen y basados en cifrador más función resumen. La fortaleza de seguridad ofrecida por un esquema MAC depende de la primitiva criptográfica que se utilice (el cifrador de bloque o la función hash) y de la longitud de la clave criptográfica.

43. En la categoría de esquemas MAC basados en cifradores de bloque se autoriza para uso recomendado **CBC-MAC**[1]. Deberá estar basado en el cifrador simétrico autorizado AES.

44. En la categoría de esquemas MAC basados en funciones resumen (también llamados *Keyed-Hash Functions*), se autorizan para uso recomendado los esquemas **HMAC** basados en las funciones resumen **SHA-2** y **SHA-3**. HMAC-SHA-1 se autoriza únicamente para uso Legacy.

45. En la categoría de esquemas MAC basados en función resumen y cifrador de bloque (también llamados *Universal Hash Functions*), se autoriza para uso recomendado el esquema GMAC especificado en NIST SP 800-38D.

[1] Solo se autoriza en contextos donde sean idénticos los tamaños de todas las entradas para las cuales se computa CBC-MAC con la misma clave.

46. En la **Tabla 3-9** se indican los esquemas MAC autorizados y la longitud de clave necesaria para proporcionar un nivel de seguridad de 112 y 128 bits

Tipo de esquema MAC	Esquema MAC / Especificaciones		Cifrador / Función resumen	Fortaleza (bits)	Longitud de clave (bits)	CAT
Basado en cifrador de bloque	CBC-MAC	*ISO 9797-1 (MAC Algorithm 1)*	AES	128 192 256	128 192 256	R[1]
	CMAC	*ISO 9797-1 (MAC Algorithm 5) SP800-38B*	AES	128 192 256	128 192 256	R
Basado en función resumen	HMAC	*ISO/IEC 9797-2 RFC 2104 FIPS 198-1*	SHA-1	112 ≥128	≥100	L
			SHA-2	112 ≥128	≥100 ≥125	L R
			SHA-3	112 ≥128	≥100 ≥125	L R
Basado en Cifrador y Función Hash	GMAC	*NIST SP800-38D*	AES GHASH	128 192 256	128 192 256	R[1]

Tabla 3-9. Esquemas MAC autorizado

3.8 CIFRADO CON AUTENTICACIÓN (AE / AEAD)

47. En este apartado se recogen los **esquemas de cifrado con autenticación**, también conocidos por sus siglas **AE (*Authenticated Encryption*),** que proporcionan servicios de confidencialidad, integridad y autenticación de origen a los mensajes. Para ello utilizan un cifrador simétrico (de bloque o de flujo) y un mecanismo MAC (*Message Authentication Code*). Se autoriza el uso de una composición genérica (*Encrypt-then-mac*) siempre que los mecanismos de cifrado y los esquemas MAC estén recomendados en esta guía (Tabla 3-1 y Tabla 3-9). Cuando se use este esquema se debe tener especial atención en verificar que el IV esté también autenticado.

48. Los esquemas presentados en este apartado ofrecen una característica adicional, consistente en la capacidad de aplicar el cifrado solo a una parte del mensaje, dejando el resto de datos (por ejemplo, una cabecera) sin cifrar, y aplicándoles únicamente la autenticación. Los esquemas AE con esta característica se denominan AEAD (*Authentication Encryption with Associated Data*).

49. Los esquemas AE/AEAD autorizados para uso recomendado son **EAX**, **GCM y CCM** basados en el cifrador de bloque AES.

[1] Se debe evitar la repetición de IV con la misma clave, la longitud del IV debe de ser de 96 bits y para su construcción debe utilizarse el método determinista definidos en la sección 8.2.1 de SP8000-38D. La longitud del MAC debe ser 128.

50. Se autoriza también para uso recomendado el esquema **ChaCha20+Poly1305**, que se basa en el cifrador de flujo ChaCha20 y en la función hash universal Poly1305.

51. En la **Tabla 3-10** se indican los esquemas AE/AEAD autorizados y la longitud de clave.

Esquema AE / Especificaciones		Cifrador / Función Hash	Fortaleza (bits)	Longitud de clave (bits)	CAT
ChaCha20+Poly1305	RFC 8439 RFC 7905	ChaCha20 Poly1305	256[1]	256	R
EAX	ISO/IEC 19772	AES	128 192 256	128 192 256	R
GCM	ISO/IEC 19772 NIST SP800-38D	AES	128 192 256	128 192 256	R
CCM	ISO/IEC 19772 NIST SP800-38C	AES	128 192 256	128 192 256	R

Tabla 3-10. Esquemas AE/AEAD autorizados

3.9 FUNCIONES DE DERIVACIÓN DE CLAVES (KDF)

52. En este apartado se recogen las **Funciones de derivación de claves (KDF, *Key Derivation Functions*)**. Estas funciones se utilizan para obtener las claves criptográficas a partir de un secreto compartido, el cual habrá sido generado por los mecanismos de acuerdo/transporte de claves, o a partir de una fuente de entropía.

53. En la **Tabla 3-11** se listan una serie de KDFs muy extendidas, y autorizadas para uso recomendado. Existen además otros modelos autorizados para implementar funciones de derivación de claves como los que incluyen los protocolos IKEv2, TLS 1.2 y TLS 1.3 que tienen su propia implementación de KDFs, tal y como se especifica en las correspondientes RFCs (RFC 7296 y 5246 respectivamente).

54. Lo que se considerará requisito para que una KDF sea autorizada para uso recomendado, es que los mecanismos criptográficos que utilice (generalmente esquemas MAC o funciones resumen) se encuentren entre los autorizados en la presente guía.

[1] ChaCha20 especificado en la RFC 8439 es una variante de ChaCha que utiliza 20 rondas y una clave de 256 bits. Existen variantes con claves de 128 bits y de 8 a 12 rondas, pero no son las autorizadas.

KDF / Especificaciones		Mecanismo en el que se basan	CAT
NIST 800-56A-KDF	NIST SP 800-56A	Función Resumen (Hash)[1]	R
NIST 800-56B-KDF	NIST SP 800-56B	Función Resumen (Hash) [1]	R
NIST 800-56C-KDF	NIST SP 800-56C	Esquema MAC[2]	R
NIST 800-108	NIST SP 800-108	HMAC / CMAC	R
X9.63-KDF	ANSI X9.63	Función Resumen (*Hash*) [1]	R
PBKDF2	RFC 8018 (PKCS#5 v2.1) NIST SP 800-132	HMAC[2]	R
SCRYPT	RFC7914	HMAC[2]	R

Tabla 3-11. Funciones de derivación de claves (KDF) autorizadas

3.10 PROTECCIÓN DE CLAVES (KEY WRAPPING)

55. En este apartado se recogen los **mecanismos de protección de claves (*Key Wrapping*),** que permiten almacenar y transmitir claves criptográficas de forma segura, garantizando su confidencialidad, integridad y autenticación de origen.

56. Estos mecanismos utilizan cifradores de bloque para "envolver" la clave que protegen. Una consideración muy importante a tener en cuenta es que el nivel de seguridad de la clave a proteger, está determinado por el nivel de seguridad del mecanismo de protección que se utilice. Por ejemplo, si se utiliza un mecanismo de protección basado en AES-128 para proteger una clave de AES-256, el nivel de seguridad de esta quedará reducido a 128 bits.

57. En la **Tabla 3-12** se listan los mecanismos de protección de claves o *Key Wrapping* autorizados. No obstante, también podrán utilizarse para la protección de claves cualquiera de los mecanismos criptográficos autorizados en los apartados anteriores como, por ejemplo, los esquemas de cifrado con autenticación (AE) (ver apartado 3.8) o una combinación de esquemas de cifrado (ver apartado 3.1) con mecanismos MAC (ver apartado 3.7).

[1] Las KDF basadas en funciones resumen, deben utilizar funciones autorizadas según se indica en la **Tabla 3-5**.

[2] Las KDF basadas en MAC deben utilizar esquemas MAC autorizados según se indica en la **Tabla 3-9**.

Mecanismo de Protección de claves / Especificaciones		Cifrador	Fortaleza (bits)	Longitud de clave (bits)	CAT
SIV	RFC 5297	AES	128 192 256	128 192 256	R
AES-KeyWrap (KW)	NIST SP 800-38F RFC 3394 ISO/IEC 19772	AES	128 192 256	128 192 256	R
AES-KeyWrap with Padding (KWP)	NIST SP 800-38F RFC 5649	AES	128 192 256	128 192 256	R

Tabla 3-12. Mecanismos de *Key Wrapping* autorizados

4. PROTOCOLOS CRIPTOGRÁFICOS

4.1 TLS

58. **TLS (*Transport Layer Security Protocol*)** es un protocolo de seguridad criptográfico que permite proteger las comunicaciones.

59. TLS tiene un uso muy extendido. El más conocido es la protección del tráfico HTTP entre un cliente web sin autenticar (*web browser*) y un *web site* autenticado, aunque en la actualidad el protocolo ya se utiliza en muchas otras aplicaciones debido, en parte, a la disponibilidad y facilidad de uso de una variedad de librerías que lo implementan.

60. El protocolo TLS se divide en dos (2) fases: la fase de negociación o *Handshake*, en la que se negocian los parámetros de la conexión, se realiza la autenticación y se generan las claves criptográficas, y la fase de cifrado o *Record Protocol*, en la que se lleva a cabo en envío y recepción de los mensajes, usando las claves y algoritmos negociados.

61. Existen varias versiones de TLS, algunas de las cuales ya se han demostrado inseguras. Deberán utilizarse versiones de TLS 1.2 y 1.3 y **no se autoriza el uso de versiones TLS inferiores.**

62. Respecto a los mecanismos criptográficos que utiliza TLS, estos se establecen en la fase de negociación o *Handshake*, y se identifican mediante lo que se denomina la suite criptográfica o *cipher suite*. De forma general, una *cipher suite* de TLS 1.2 se representa así:

    - TLS_KeyExchange_Auth_WITH_Cipher_KeyLength_Mode_HashFunction

    En el sitio web de IANA[1] para TLS, se encuentra una lista completa de todas las cipher suites de TLS.

63. No se autorizan las *cipher suites* que:

    a) No utilicen mecanismos criptográficos para: Acuerdo de clave (*Key Agreement o Key Transport*), Autenticación, Cifrado, Integridad y Autenticidad de origen. Es decir, aquellas cipher suites que indiquen "*NULL*" o "*anon*" en alguno de sus campos.

       Por ejemplo: *TLS_RSA_WITH_NULL_SHA o TLS_DH_anon_WITH_AES_128_CBC_SHA*

    b) Que utilicen mecanismos criptográficos que no se encuentren entre los autorizados en la presente guía (ver apdo. 3).

       Por ejemplo: *TLS_RSA_WITH_RC4_128_MD5 o TLS_RSA_WITH_IDEA_CBC_SHA*

[1] http://www.iana.org/assignments/tls-parameters/tls-parameters.xml

64. No se recomiendan las *cipher suites* que:

a) Utilicen claves precompartidas (PSK) como método de autenticación, ya que lo recomendado es la autenticación con certificados X.509v3. Es decir, *cipher suites* del tipo:

TLS_ ❋_PSK_WITH_ ❋

TLS_PSK_WITH_ ❋

b) El motivo de no recomendarlas es doble:

- Cualquier parte que sepa la PSK podría autenticarse y conectarse a la VPN.
- Suelen ser vulnerables a ataques de diccionario.

c) Únicamente deberían utilizarse cuando sea posible asegurar que:

- Han sido generadas con un generador aleatorio, es decir, que no hayan sido derivadas de contraseñas con poca entropía.
- Son renovadas en cada sesión establecida.

65. Se autorizan las siguientes *cipher suites de TLS 1.2:*

Cipher suites TLS 1.2	CAT
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	R
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 [1] TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 [1] TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 [1] TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 [1]	L
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CCM TLS_DHE_RSA_WITH_AES_128_CCM TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 [1] TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 [1]	L

[1] El uso de suites de cifrado cuyo mecanismo de cifrado este basado en CBC se recomienda usar la extensión *encrypt_then_mac*

Cipher suites TLS 1.2	CAT
TLS_RSA_WITH_AES_256_GCM_SHA384 [1] TLS_RSA_WITH_AES_128_GCM_SHA256 [2] TLS_RSA_WITH_AES_256_CCM [2] TLS_RSA_WITH_AES_128_CCM [2] TLS_RSA_WITH_AES_256_CBC_SHA256 [1 2] TLS_RSA_WITH_AES_128_CBC_SHA256 **¡Error! Marcador no definido.** [1 2]	L

Tabla 4-1. Cipher suites TLS 1.2 autorizadas

66. Respecto a TLS 1.3, se introducen varios cambios relacionados con la criptografía. Las *cipher suites* pasan a usar únicamente mecanismos AEAD, y se elimina el uso de la función SHA-1. En cuanto al método de Acuerdo de Clave (*Key Agreement*), este ya no aparece en la cipher suite y se negocia en el *Handshake* utilizando nuevas extensiones (*Supported Groups*). Los métodos de acuerdo de clave disponibles son: clave precompartida (PSK), DHE o ECDHE, y PSK con DHE.

67. Las cinco (5) *cipher suites* actuales para TLS 1.3 están autorizadas para uso recomendado. No se autoriza el uso de claves precompartidas como mecanismo de acuerdo de clave, sino que los mecanismos autorizados para uso recomendado serán DHE o ECDHE (consultar 3.2 y 3.5).

Cipher suites TLS 1.3	CAT
TLS_AES_128_GCM_SHA256	R
TLS_AES_256_GCM_SHA384	R
TLS_CHACHA20_POLY1305_SHA256	R
TLS_AES_128_CCM_SHA256	R
TLS_AES_128_CCM_8_SHA256	R

Tabla 4-2. *Cipher suites* TLS 1.3 autorizadas

4.2 SSH

68. **SSH (*Secure Shell*)** es un protocolo de seguridad criptográfico diseñado originalmente, para sustituir a los protocolos de conexión remota *shell* inseguros como, por ejemplo, Telnet.

69. En la actualidad SSH se incluye de forma nativa, y se utiliza como principal mecanismo de administración remota de muchos sistemas operativos y dispositivos, incluyendo *Linux, Unix, routers, firewalls*, dispositivos de red, etc. También puede ser usado por otras aplicaciones (por ejemplo, FTP).

[1] No proporciona *Forward Secrecy*

70. SSH sigue una arquitectura típica cliente/servidor. Una aplicación cliente SSH en el Host A inicia una conexión SSH con una aplicación servidor SSH en el Host B. Ambos hosts negocian los mecanismos criptográficos, establecen una clave criptográfica para la sesión, realizan la autenticación para el Host servidor (B) y finalmente el cliente (A) envía las credenciales de autenticación (por ejemplo, usuario y contraseña) al servidor (B). Si la autenticación es válida, se inicia la sesión SSH entre los dos (2) hosts.

71. La única versión de SSH autorizada es SSHv2. Versiones anteriores han demostrado tener vulnerabilidades conocidas de carácter grave, por lo que no están autorizadas.

Versión SSH	Estándar	CAT
SSHv2	*RFC 4251* *RFC 4252* *RFC 4253* *RFC 4254*	R

Tabla 4-3. Versiones SSH autorizada

72. Todos los mecanismos criptográficos existentes para SSH, se listan en el *web site* de IANA[1] para SSH: mecanismos de Acuerdo de clave (*Key Exchange Method*), autenticación (*Public Key Algorithm*), cifrado (*Encryption Algorithm*) y autenticidad e integridad de mensajes (*MAC Algorithm*). A continuación, se indica cuáles son los mecanismos autorizados.

4.2.1. INTERCAMBIO DE CLAVES – KEY EXCHANGE

El mecanismo de acuerdo de clave (*Key Exchange*) en SSH, se basa en *Diffie-Hellman*.

La RFC 4253 indica que deben soportarse los mecanismos *diffie-hellman-group1-sha1 (Oackley Group 2*, 1024 bits) y *diffie-hellman-group14-sha1* (*Oackley Group 14*, 2048 bits). Sin embargo, el servidor SSH puede proponer nuevos grupos que el cliente deberá aceptar, tal y como se indica en la RFC 4419.

Solo se autorizan los métodos de *Key Exchange* que utilicen mecanismos de acuerdo de clave de los autorizados en el apartado 3.5, y que proporcionen una fortaleza de seguridad de, al menos, 112 bits.

SSH- Key Exchange Method	Grupos DH / Curvas Elípticas	Estándar	Fortaleza (bits)	CAT
diffie-hellman-group14-sha1	*2048-bit MODP group14 (RFC3526)*	RFC 4253	112	L
diffie-hellman-group14-sha256	*2048-bit MODP group14 (RFC3526)*	RFC 8268	112	L
diffie-hellman-group15-sha512	*3072-bit MODP group15 (RFC3526)*	RFC 8268	128	R

[1] https://www.iana.org/assignments/ssh-parameters/ssh-parameters.xml

SSH- Key Exchange Method	Grupos DH / Curvas Elípticas	Estándar	Fortaleza (bits)	CAT
diffie-hellman-group16-sha512	*4096-bit MODP group16 (RFC3526)*	RFC 8268	>128	R
diffie-hellman-group17-sha512	*6144-bit MODP group17 (RFC3526)*	RFC 8268	>128	R
diffie-hellman-group18-sha512	*8192-bit MODP group18 (RFC3526)*	RFC 8268	>128	R
ecdh-sha2-nistp256	*nistp256 (NIST) o secp256r1 (SEC2)*	RFC 5656	128	R
ecdh-sha2-nistp384	*nistp384 (NIST) o secp384r1 (SEC2)*	RFC 5656	>128	R
ecdh-sha2-nistp521	*nistp521 (NIST) o secp521r1 (SEC2)*	RFC 5656	>128	R

Tabla 4-4. Métodos SSH- Key Exchange autorizados

4.2.2. CIFRADO – ENCRYPTION ALGORITHM

Una vez que se han obtenido las claves mediante el método de *Key Exchange*, todos los mensajes se envían cifrados utilizando el protocolo BPP (*Binary-Packet Protocol*, RFC 4253). Este especifica el uso de un esquema de cifrado basado en una construcción *Encode-then-Encrypt-and-MAC* usando un cifrador de bloque en modo CBC o el cifrador de flujo RC4. En la RFC 4344 se definen nuevos mecanismos de cifrado que utilizan un cifrador de bloque en modo CTR, y en la RFC 5647 se define el uso de esquemas AEAD en SSH.

Solo se autorizan aquellos mecanismos de cifrado que utilicen un esquema de cifrado de los autorizados en el apartado 3.1, o un esquema AEAD de los autorizados en el apartado 3.8.

SSH – *Encryption Algorithm*	Composición	Estándar	Fortaleza (*bits*)	CAT
aes128-cbc	*AES in CBC mode - 128 bit key*	RFC4253	128	L [1]
aes192-cbc	*AES in CBC mode - 192 bit key*	RFC4253	192	L [1]
aes256-cbc	*AES in CBC mode - 256 bit key*	RFC4253	256	L [1]
aes128-ctr	*AES in CTR mode - 128 bit key*	RFC4344	128	R[1]
aes192-ctr	*AES in CTR mode - 192 bit key*	RFC4344	192	R[1]
aes256-ctr	*AES in CTR mode - 256 bit key*	RFC4344	256	R[1]
AEAD_AES_128_GCM	*AES GCM -128 bit key*	RFC5647	128	R
AEAD_AES_256_GCM	*AES GCM- 256 bit key*	RFC5647	256	R

[1] Si se escoge un modo de cifrado no autenticado (i.e. aes-ctr, aes-cbc) será obligatorio utilizar alguna de las opciones recomendadas para proteger la integridad y autenticidad de los mensajes (i.e. HMAC-SHA2)

Tabla 4-5. Mecanismos *SSH- Encryption* autorizados.

4.2.3. AUTENTICACIÓN – PUBLIC KEY AUTHENTICATION

La autenticación de servidor SSH se lleva a cabo mediante criptografía de clave pública, usando claves públicas o certificados (*public-key authentication*). La autenticación de cliente puede llevarse a cabo mediante varios métodos, pero el recomendado es, igualmente, la criptografía de clave pública, al menos como uno de los factores.

La RFC 4253 define los algoritmos de clave pública inicialmente soportados por SSH. Otras RFCs han ido sumando más algoritmos y construcciones.

Solo se autorizan los mecanismos de autenticación de clave pública que utilicen esquemas de firma de los autorizados en el apartado 3.6.

SSH - Public Key Algorithm	Composición	Estándar	Fortaleza	CAT
rsa-sha2-256	RSASSA-PKCS1-v1_5 (RFC 8017) & SHA-256 (FIPS 180-4)	RFC8332	112 (RSA key 2048) 128 (RSA key 3072)	L
rsa-sha2-512	RSASSA-PKCS1-v1_5 (RFC 8017) & SHA-512 (FIPS 180-4)	RFC8332	112 (RSA key 2048) 128 (RSA key 3072)	L
ecdsa-sha2-nistp256	ECDSA (SEC1) nistp256 & SHA-256 (FIPS 180-3)	RFC5656	128	R
ecdsa-sha2-nistp384	ECDSA (SEC1) nistp384 & SHA-384 (FIPS 180-3)	RFC5656	>128	R
ecdsa-sha2-nistp521	ECDSA (SEC1) nistp521 & SHA-512 (FIPS 180-3)	RFC5656	>128	R
x509v3-rsa2048-sha256	RSASSA-PKCS1-v1_5 (RFC3347) & SHA-256 (FIPS 180-3)	RFC6187	112 (RSA key 2048)	L
x509v3-ecdsa-sha2-nistp256	ECDSA (FIPS 184-3) nistp256 & SHA-256 (FIPS 180-3)	RFC6187	128	R
509v3-ecdsa-sha2-nistp384	ECDSA (FIPS 184-3) nistp384 & SHA-384 (FIPS 180-3)	RFC6187	>128	R
x509v3-ecdsa-sha2-nistp521	ECDSA (FIPS 184-3) nistp521 & SHA-512 (FIPS 180-3)	RFC6187	>128	R

Tabla 4-6. Mecanismos de autenticación *SSH-Public Key* autorizados

4.2.4. INTEGRIDAD Y AUTENTICIDAD DE ORIGEN – MAC ALGORITHM

La RFC 4253 especifica esquemas HMAC con las funciones SHA-1 o MD5 para las construcciones MAC. Según se indica en el apartado 3.7, la construcción HMAC-SHA1

se autoriza solo para uso *Legacy*, y construcciones con MD5 no están autorizadas. La RFC 6668 detalla el uso de construcciones HMAC-SHA-2.

Solo se autorizan los mecanismos MAC que utilicen esquemas MAC de los autorizados en el apartado 3.7 o un esquema AEAD de los autorizados en el apartado 3.8.

MAC Algorithm	Composición	Estándar	Fortaleza (bits)	CAT
hmac-sha1	*HMAC con SHA-1 - 160 bit key*	RFC4253	>128	L
hmac-sha1-96	*HMAC con SHA-1 - 160 bit key*	RFC4253	>128	L
hmac-sha2-256	*HMAC con SHA-256 - 256 bit key*	RFC6668	>128	R
hmac-sha2-512	*HMAC con SHA-512 - 512 bit key*	RFC6668	>128	R
AEAD_AES_128_GCM	*AES GCM -128 bit key*	RFC5647	>128	R
AEAD_AES_256_GCM	*AES GCM- 256 bit key*	RFC5647	>128	R

Tabla 4-7. Mecanismos SSH- MAC autorizados

4.3 IPSEC

73. **IPsec** es un estándar abierto que proporciona seguridad a nivel de capa de red IP en la pila del protocolo TCP/IP. Esto difiere de los protocolos TLS y SSH mencionados en otros apartados, ya que proporcionan seguridad en capas superiores, como las capas de aplicación.

74. El principal uso de IPsec es para crear VPNs (*Virtual Private Networks*) que establecen canales de comunicación seguros a través de redes IP inseguras, como Internet.

75. IPsec se puede desplegar en dos modos: túnel y transporte.

    a) En modo túnel se protege criptográficamente el paquete IP al completo (más los campos de seguridad insertados), es decir, se trata al paquete como el *payload* de un nuevo paquete IP exterior, con su propia cabecera. Se puede decir que el paquete IP original se encapsula dentro del paquete IP exterior.

    b) En modo transporte la cabecera del paquete IP original se conserva y se le añaden algunos campos de seguridad. Es el *payload* junto con algún campo de la cabecera, el que se somete al procesamiento criptográfico. El modo transporte proporciona protección en su mayor parte al *payload*.

El modo túnel, por lo tanto, ofrece una mayor seguridad que el modo transporte. Por ello, siempre que sea posible se trabajará en esta configuración. La elección del modo transporte solamente debe justificarse en el caso de que el tamaño del paquete sea problemático debido a restricciones impuestas por la red.

76. IPsec tiene dos componentes principales:

a) **El acuerdo de claves que se lleva a cabo con el protocolo IKE (*Internet Key Exchange*)**. Es el protocolo empleado por IPsec para establecer una Asociación de Seguridad (SA) de un modo automático. Esto incluye la negociación de los parámetros de la conexión, establecimiento del secreto compartido y derivación del material de claves criptográficas. Se encarga de llevar a cabo, también, la autenticación mutua de los extremos de la comunicación (*peers*).

La versión actual autorizada para uso recomendado es IKEv2, especificada en la RFC 7296[1]. La versión anterior IKEv1, se autoriza únicamente para uso Legacy y solo en los modos: *Main* y *Quick mode*. No en el modo *Agressive Mode*[2].

b) **La protección de los datos que se puede realizar con los protocolos AH (Authentication Header) o ESP (*Encapsulating Security Payload*)**. Son los protocolos que proporcionan protección de autenticidad, integridad y/o confidencialidad a los datos. El protocolo AH garantiza la integridad y autenticidad, pero no la confidencialidad. ESP garantiza la confidencialidad y opcionalmente la integridad y la autenticidad.

Existen ataques conocidos cuando se implementa IPsec en cualquier configuración *MAC-then-Encrypt* (como, por ejemplo, si se usa AH en modo transporte antes de un ESP sólo cifrado en modo túnel). Por otro lado, no se conocen ataques a IPsec si se usa ESP sólo cifrado seguido de AH o ESP con autenticidad e integridad sin que le siga otro AH. Por lo tanto, **se recomienda el uso de ESP siempre con las opciones de protección de integridad y autenticidad, además de confidencialidad.**

Protocolo	Estándar	Modos recomendados	CAT
IPsec	RFCs 4301 a 4309 RFC 8221	Modo túnel	R
ESP	RFC 4303	Confidencialidad & Integridad y Autenticidad	R

[1] La RFC 7296 es la revisión de las anteriores RFC 5996 y RFC 4306. RFC 7296 define la base del protocolo IKEv2, pero existen muchas otras RFCs en las que se especifican extensiones de IKE.

[2] IKEv1 utiliza principalmente dos métodos de *Key Exchange* durante la Fase 1 de negociación: *Main mode* y *Agressive Mode.* Ambos se diferencian en el número de rondas de la negociación y en la información intercambiada en cada una de ellas. *Main mode* usa más rondas y es, por ello, más lento y complejo de implementar. *Agressive mode* es más rápido, pero parte de la información intercambiada en las rondas no va cifrada, por lo que es más inseguro. *Quick mode* es similar al *Agressive mode* excepto que toda la información va protegida en una asociación de seguridad IKE SA.

Protocolo	Estándar	Modos recomendados	CAT
IKEv1	RFCs 2407, 2408, 2409 RFC 4109	*Main Mode y Quick Mode*	L
IKEv2	RFC 7296 RFC 8247	Todos	R

Tabla 4-8. Versiones IPsec autorizadas.

77. Durante el primer intercambio que se produce en el protocolo IKE (IKE_SA_INIT), se negocian los parámetros criptográficos de la conexión (esquemas de cifrado, acuerdo de clave, integridad, etc.). A estos parámetros se les llama "*Transforms*". El listado de todos los parámetros o *Transforms*, se encuentra en el *web site* de IANA[1].

Los tipos de parámetros criptográficos o *Transforms*, son:

- *Diffie-Hellman Group Transforms*: Grupos (EC)DH que se utilizarán para el acuerdo de clave (*Key Exchange*).
- *Pseudorandom Function Transforms*: funciones pseudoaleatorias (PRF) que se utilizarán para la generación de los valores aleatorios, y para la derivación del material de claves.
- *Encryption Algorithm Transforms*: esquemas de cifrado clásicos o esquemas AEAD que se usarán para la protección de confidencialidad.
- *Integrity Algorithm Transforms*: esquemas MAC que se usarán para la protección de integridad.

4.3.1. ACUERDO DE CLAVE (DIFFIE-HELLMAN GROUPS TRANSFORMS)

El mecanismo de acuerdo de clave (*Key Exchange*) utilizado en el protocolo IKEv2, se basa en *Diffie-Hellman*. Durante el primer intercambio IKE_SA_INIT se envían también los parámetros *Diffie-Hellman* necesarios de forma que, una vez que se completa el intercambio, los dos extremos (*peers*) han finalizado el acuerdo de clave y han generado el secreto compartido.

Se han definido varios grupos *Diffie-Hellman*, tanto MODP (*Modular Exponential*) como de Curva Elíptica (ECC), para su uso en IKEv2. Estos grupos se definen, tanto en el documento base de la especificación de IKEv2 (RFC 7296), como en otras RFC que definen extensiones para IKEv2.

De entre todos los grupos (EC)DH o *Diffie-Hellman Group Transforms* definidos, se autorizan los que se indican en la siguiente tabla.

[1] https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml

Grupo (EC)DH		Estándar IKEv2	Fortaleza (bits)	CAT
14	2048-bit MODP Group	RFC 3526	112	L
15	3072-bit MODP Group	RFC 3526	128	R
16	4096-bit MODP Group	RFC 3526	>128	R
17	6144-bit MODP Group	RFC 3526	>128	R
18	8192-bit MODP Group	RFC 3526	>128	R
19	256-bit random ECP group	RFC 5903	128	R
20	384-bit random ECP group	RFC 5903	>128	R
21	521-bit random ECP group	RFC 5903	>128	R
28	brainpoolP256r1	RFC 6954	128	R
29	brainpoolP384r1	RFC 6954	>128	R
30	brainpoolP512r1	RFC 6954	>128	R
31	x25519	RFC 8031	128	R
32	x448	RFC 8031	>128	R

Tabla 4-9. Grupos (EC)DH autorizados para IKEv2.

4.3.2. CIFRADO (ENCRYPTION ALGORITHMS TRANSFORMS)

Las propuestas para los esquemas de cifrado IKEv2 y ESP, pueden incluir tanto esquemas de cifrado clásico como esquemas AEAD.

Siguiendo las recomendaciones realizadas en los apartados 3.1 y 3.8, de los esquemas de cifrado o esquemas de cifrado con autenticación definidos, se autorizan los que se indican en la siguiente tabla.

Esquema de Cifrado /AEAD	Estándar IKEv2	Estándar ESP	Fortaleza (bits)	Longitud de clave (bits)	CAT
ENCR_AES_CBC	RFC 7296	RFC 3602	128 192 256	128 192 256	R[1]
ENCR_AES_CTR	RFC 5930	RFC 3686	128 192 256	128 192 256	R
ENCR_AES_CCM_12 (1)	RFC 5282 RFC 8247	RFC 4309	128 192 256	128 192 256	R
ENCR_AES_CCM_16 (1)	RFC 5282 RFC 8247	RFC 4309	128 192 256	128 192 256	R
ENCR_AES_GCM_12 (1)(2)	RFC 5282 RFC 8247	RFC 4106 RFC 8750	128 192 256	128 192 256	R
ENCR_AES_GCM_16 (1)(2)	RFC 5282 RFC 8247	RFC 4106 RFC 8750	128 192 256	128 192 256	R
ENCR_CHACHA20_POLY1305 (2)	RFC 7634	RFC 7634 RFC 8750	256	256	R

Tabla 4-10. Esquemas de cifrado / AEAD autorizados para IKEv2 y ESP.

(1) 12/16 se refiere al valor en bytes del ICV[2](*Integrity Check Value*). De los tres (3) posibles valores (8, 12 y 16 bytes) definidos en las RFC, el valor recomendado es de 16 bytes aunque también es aceptable el de 12 bytes.

(2) Se incluyen las variantes con vector de inicialización implícito (IIV)[3] definidas en la RFC 8750 solo para ESP (AES_GCM_16_*IIV* y CHACHA20_POLY1305_*IIV)*.

4.3.3. INTEGRIDAD Y AUTENTICACIÓN DE ORIGEN (INTEGRITY ALGORITHMS TRANSFORMS)

Los protocolos ESP e IKEv2 utilizan mecanismos MAC para la verificación de integridad y autenticación de origen, es decir, para garantizar que los paquetes son auténticos y no han sido modificados en tránsito.

En los casos en los que dentro de la propuesta para los *Encryption Algorithm Transforms* se incluya un esquema AEAD, no se utilizará ningún mecanismo para

[1] Siempre junto con un mecanismo de autenticación del apartado 3.7-

[2] El ICV (*Integrity Check Value*) es el *Authentication Tag*, o valor generado por el esquema AEAD para la verificación de integridad y autenticidad de origen.

[3] Los esquemas AEAD definidos para ESP (AES_CCM, AES_GCM, CHACHA20_POLY1305), requieren de un vector de inicialización (IV) o valor *nonce*. Para generarlo se utiliza otro vector de inicialización que trae cada paquete ESP. Esta generación del *nonce* o IV, se llama IV explícito. En algunas implementaciones, en lugar de transportar en cada paquete los bytes extra que suponen los datos del IV, puede ser preferible generar el IV de forma local en cada dispositivo (*peer*). Esta generación local del IV se llama IV implícito (IIV).

protección de integridad y autenticación de origen. Este se utilizará solo cuando se incluya un esquema de cifrado clásico en la propuesta.

Los mecanismos MAC autorizados para uso recomendado son los basados en esquemas AES-CMAC, AES-GMAC y HMAC-SHA2.

Respecto a los esquemas HMAC-SHA2, cuando se utilizan en IPsec como mecanismos de integridad y autenticidad, la longitud de la clave será fija en función del tamaño del valor hash de salida, y se realiza un truncado de la salida[1]:

- HMAC-SHA-256-128: usa una clave de 256 bits y un truncado de la salida a 128 bits.
- HMAC-SHA-384-192: se usa una clave de 384 bits y un truncado de la salida a 192 bits.
- HMAC-SHA-512-256: se usa una clave de 512 bits y un truncado de la salida a 256 bits.

Respecto al esquema HMAC-SHA-1_96[2], utiliza una longitud de clave fija de 160 bits y un truncado de la salida a 96 bits. Tal y como se indica en el apartado 3.7, los mecanismos basados en HMAC-SHA1 solo se autorizan para uso Legacy.

Esquema MAC	Estándar IKEv2/ESP	Longitud de clave (bits)	Fortaleza (bits)	CAT
AUTH_HMAC_SHA1_96	RFC 2404 RFC 7296	160	≥128	L
AUTH_HMAC_SHA2_256_128	RFC 4868	256	≥128	R
AUTH_HMAC_SHA2_384_192	RFC 4868	384	≥128	R
AUTH_HMAC_SHA2_512_256	RFC 4868	512	≥128	R
AUTH_AES_CMAC_96[3]	RFC 4494	128	128	R
AUTH_AES_GMAC	RFC 4543	128 192 256	128 192 256	R

Tabla 4-11. Esquemas MAC autorizados para IKEv2 y ESP.

4.3.4. FUNCIONES PRF (PSEUDORANDOM FUNCTIONS TRANSFORMS)

Las claves para el cifrado y la autenticación de mensajes (MAC) serán derivadas del secreto compartido obtenido con el intercambio *Diffie-Hellman*, utilizando la Función PRF negociada.

[1] Especificado en la RFC 4868, que define cómo se usan los esquemas HMAC-SHA2 en IPsec.
[2] Especificado en la RFC 2402, que define HMAC-SHA-1 para ESP.
[3] El mecanismo AES-CMAC-96 es una variante de AES128-CMAC con la salida truncada a los 96 bits más significativos (MSB), definida para uso como mecanismo de integridad solo para ESP (RFC 4494).

Las funciones PRF utilizadas en IKEv2 son similares a los mecanismos MAC indicados anteriormente, salvo que se elimina la restricción de claves de tamaño fijo y se elimina el truncado, debido a la criticidad del tamaño de la salida de la función.

Las funciones PRF autorizadas para uso recomendado serán, por lo tanto, las basadas en esquemas AES-CMAC y HMAC-SHA2.

Función PRF	Estándar IKEv2	Longitud de clave (bits)	Fortaleza (bits)	CAT
PRF_HMAC_SHA1	RFC 2104	≥100	112	L
PRF_HMAC_SHA2_256	RFC 4868	≥100 ≥125	112 ≥128	L R
PRF _HMAC_SHA2_384	RFC 4868	≥100 ≥125	112 ≥128	L R
PRF _HMAC_SHA2_512	RFC 4868	≥100 ≥125	112 ≥128	L R
PRF_AES128_CMAC	RFC 4615	128	128	R

Tabla 4-12. Funciones PRF autorizadas para IKEv2.

4.3.5. MECANISMO DE AUTENTICACIÓN

La autenticación de los extremos de la conexión (*peers*) se lleva a cabo a través de los intercambios IKE_AUTH, tras finalizar la negociación de los parámetros y el establecimiento y derivación del material criptográfico.

El principal mecanismo de autenticación utilizado en IKEv2 es la firma electrónica con claves pública/privada (*public-key-signature-based authentication*). Se recomienda el uso de certificados X.509 para vincular las claves con las identidades de los *peers*. Los certificados, tanto de los *peers* como de las CAs (*Certification Authorities*) intermedias, serán intercambiados en los mensajes IKE_AUTH.

Los esquemas de firma autorizados para uso con IKEv2 se basan en ECDSA y RSA y se indican en la siguiente tabla.

Esquema de Firma	Estándar IKEv2	Longitud de clave (bits)	Fortaleza (bits)	CAT
RSA Digital Signature (RSASSA-PKCS1-v1_5)	RFC 7296	2048 ≥3072	112 ≥128	L
RSA Digital Signature (RSASSA-PSS)	RFC 4055	2048 ≥3072	112 ≥128	L R
ECDSA with SHA-256 on the P-256 curve	RFC 4754	256	128	R
ECDSA with SHA-384 on the P-384 curve	RFC 4754	384	192	R
ECDSA with SHA-512 on the P-521 curve	RFC 4754	512	256	R
ECDSA-256 with BrainpoolP256r1	RFC 7427	256	128	R
ECDSA-384 with BrainpoolP384r1	RFC 7427	384	192	R

Esquema de Firma	Estándar IKEv2	Longitud de clave (bits)	Fortaleza (bits)	CAT
ECDSA-512 with BrainpoolP512r1	RFC 7427	512	256	R
ECGDSA-256 with BrainpoolP256r1	RFC 7427	256	128	R
ECGDSA-384 with BrainpoolP384r1	RFC 7427	384	192	R
ECGDSA-512 with BrainpoolP512r1	RFC 7427	512	256	R

Tabla 4-13. Esquemas de Firma autorizados para IKEv2.

Otra opción de autenticación son las claves precompartidas (PSK), cuyo uso no está recomendado, tal y como se ha indicado en apartados anteriores[1]. También existe la opción de no autenticación, la cual no debe utilizarse en ningún caso.

Finalmente, indicar que IKEv2 soporta también la autenticación con los métodos EAP (*Extensible Authentication Protocol*) definidos en la RFC 3748. No se recomienda este tipo de autenticación, ya que la mayor parte de estos métodos son asimétricos y no conllevan la autenticación mutua, sino que se utilizan para la autenticación del cliente frente al servidor. En caso de usar este tipo de autenticación, deberá combinarse con la autenticación de firma electrónica con claves pública/privada, del servidor frente al cliente, y deberán tenerse en cuenta las recomendaciones de seguridad para su implementación indicadas en las especificaciones de IKEv2 (RFC 7296)[2].

[1] En caso de utilizar PSKs, un aspecto crítico es asegurar que tengan suficiente entropía. La PSK deberá contener tanta aleatoriedad como la clave más fuerte que se está negociando. Derivar la PSK de una contraseña de usuario o cualquier otra práctica con baja entropía, no es seguro. Estas fuentes son vulnerables a ataques de diccionario, ingeniería social, etc.

[2] En la RFC 7296 se recomienda, entre otras cosas, utilizar solo métodos EAP que generen una clave compartida (*shared key*) que se use para proteger el *payload* de los intercambios IKE_AUTH, proporcionando protección frente a los ataques de suplantación del servidor y ataques *man-in-the-middle.*

5. MEDIDAS DE SEGURIDAD

78. A continuación, se listan cada una de las medidas de seguridad especificadas en el ENS que hacen uso de mecanismos criptográficos. Estos mecanismos deberán encontrarse entre los autorizados en la presente guía (ver apartado 3) y, en función del nivel de seguridad requerido para las dimensiones de seguridad a las que afecte la medida y el nivel de amenaza considerado para cada escenario de uso, se determinará la fortaleza criptológica mínima necesaria.

79. En el apartado 5.12 se recoge un ejemplo de aplicación de estas medidas al protocolo TLS.

5.1 DIMENSIONES DE SEGURIDAD CONSIDERADAS

80. En función de la medida de seguridad, se tendrán en cuenta las siguientes dimensiones de seguridad que serán identificadas por sus correspondientes iniciales en mayúsculas:

    a) Disponibilidad [D]

    b) Autenticidad [A]

    c) Integridad [I]

    d) Confidencialidad [C]

    e) Trazabilidad [T]

Salvo que se indique lo contrario, el nivel de seguridad exigido para cada medida, vendrá determinado por el mayor nivel de seguridad requerido para cada una de las dimensiones a las que sea aplicable la medida

5.2 NIVELES DE AMENAZA

81. Las amenazas a las que deberá hacer frente una medida de seguridad, tanto accidentales como deliberadas, están ligadas al entorno operativo del sistema de información en el que se despliegan, puesto que este hecho limita el perfil de los individuos que pueden acceder a explotar las vulnerabilidades de dicho sistema.

82. En concreto, las amenazas pueden proceder de los siguientes tipos de individuos:

    a) **Individuos no autenticados ni autorizados** a acceder a los activos sensibles que protege el sistema (individuos ajenos al sistema).

    b) **Individuos autenticados no autorizados** a acceder a los activos sensibles que protege el sistema (usuarios del sistema sin privilegios suficientes).

    c) **Individuos autenticados y autorizados** a acceder a los activos sensibles que protege el sistema (usuarios autorizados y autenticados).

83. Los niveles de amenaza se pueden clasificar en los siguientes, atendiendo al origen de las amenazas:

    a) **Nivel de amenaza ALTO**: cuando un activo está expuesto a ataques originados por individuos no autorizados y no autenticados.

    b) **Nivel de amenaza MEDIO**: cuando un activo está expuesto a ataques originados por individuos no autorizados, pero sí autenticados.

    c) **Nivel de amenaza BAJO**: cuando un activo está expuesto a ataques originados por individuos autenticados y autorizados.

84. En general, la fortaleza requerida para una determinada medida de seguridad vendrá determinada por el nivel de amenaza que deba mitigar.

5.3 IDENTIFICACIÓN. [OP.ACC.1]

85. Como se señala en [op.acc.1.5] del Anexo II del ENS, en los supuestos de comunicaciones electrónicas las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, concretamente mediante los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, en adelante **Reglamento eIDAS** y, cuando resulte de aplicación, por lo dispuesto en la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre, y por el Real decreto 203/2021, de 30 de marzo, por el que se aprueba el reglamento de actuación y funcionamiento del sector público por medios electrónicos.

86. Se establecerán distintos niveles de seguridad para esta medida, dependiendo del máximo nivel de seguridad exigido por el sistema para cualquiera de las dimensiones de Trazabilidad [T] y Autenticidad [A]. La siguiente tabla muestra una correspondencia entre los niveles de seguridad establecidos por el Reglamento eIDAS en su artículo 8 y los niveles de requeridos por el ENS:

		Nivel de seguridad eIDAS
Nivel máximo requerido ENS en [T] o [A]	**BAJO**	BAJO, SUSTANCIAL O ALTO
	MEDIO	SUSTANCIAL O ALTO
	ALTO	ALTO

Tabla 5-1. [op.acc.1] Correspondencia niveles ENS – Niveles requeridos eIDAS

5.4 MECANISMOS DE AUTENTICACIÓN (USUARIOS EXTERNOS) [OP.ACC.5]

87. Para garantizar la seguridad de los sistemas se recurre a la identidad digital de quienes requieren acceder a los mismos. Cada persona debe tener una identidad y esto permite que los sistemas puedan identificarla, distinguiéndola de las demás. En este escenario, diferenciaremos entre: **identificación**, que es el proceso mediante el cual el usuario del sistema aporta las credenciales o evidencias que lo identifican; **autenticación**, que consiste en la verificación por parte del sistema de las credenciales aportadas por el usuario, comprobando que realmente es quién dice ser; **autorización**, consistiendo en los privilegios que se le otorgan al usuario, o acciones que se le permiten realizar, a partir de la autenticación con las credenciales que lo identifican.

88. En general, los mecanismos de autenticación se basan en el uso de tres (3) posibles propiedades o características de la parte que ha de ser autenticada (factores de autenticación):

    a) "**algo que sabe**": contraseñas o claves concertadas.

    b) "**algo que se tiene**": componentes lógicos (tales como certificados software) o certificados en dispositivo físico.

    c) "**algo que se es**": elementos biométricos (un rasgo o propiedad biométrica, fisonomía facial, la huella digital, el patrón de iris, etc.).

89. Para la autenticación de usuarios externos al sistema bajo el alcance del ENS se considerarán los siguientes métodos de autenticación:

    a) **Contraseña (1 factor: "algo que se sabe")**: Orientado a sistemas de categoría BÁSICA, consiste en una cadena de caracteres alfanuméricos empleada como mecanismo de autenticación. Para estas contraseñas se define una robustez, periodicidad mínima y un número de intentos fallidos de autenticación, a partir de los cuales el sistema debe:

        1. Bloquearse y requerir una intervención específica para reactivar la cuenta. Esta opción es la recomendada.

           o

        2. Incluir un retardo entre intentos de autenticación, de cara a evitar ataques de autenticación por fuerza bruta. Se recomienda que dicho retardo sea incremental.

    b) **Contraseñas + OTP (2 factores: "algo que se sabe" + "algo que se tiene")**: Además de emplear una contraseña, este mecanismo requerirá una contraseña adicional de un solo uso (OTP, en inglés) como complemento, generada o remitida a un dispositivo sobre el que el usuario tiene, con un alto nivel de confianza, un control exclusivo

    c) **Certificados cualificados (de acuerdo a lo establecido en el Reglamento eIDAS), cuyo uso esté protegido por un segundo factor, del tipo PIN ("algo**

que se tiene" + "algo que se sabe") o biométrico ("algo que se tiene" + "algo que se es"). Además, las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

d) **Certificados cualificados en dispositivo físico que permita la creación de firma cualificada. El uso del certificado estará también protegido por un segundo factor del tipo PIN ("algo que se tiene" + algo que se sabe") o biométrico ("algo que se tiene" + "algo que se es")**. Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

90. Como norma general, el ENS establece que antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos externos estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

91. Se considerarán distintos niveles de seguridad para los mecanismos de autenticación de usuarios externos, dependiendo del máximo nivel de seguridad exigido por el sistema para cualquiera de las dimensiones de Confidencialidad [C], Integridad [I], Trazabilidad [T] o Autenticidad [A]. La siguiente tabla muestra los métodos de autenticación recomendados para cada uno de los niveles, así como los requisitos de robustez para cada uno de ellos:

	Métodos de autenticación permitidos	Requisitos
Nivel BAJO (1 o 2 factores)	**Contraseñas**	Longitud mínima: 8 caracteres con un mínimo de tres tipos diferentes, de entre los descritos en la sección 5.4.1. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5 Prohibición de reutilizar 5 contraseñas anteriores.
	Contraseñas + OTP	Longitud mínima: 8 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5

		Prohibición de reutilizar 5 contraseñas anteriores.
	Certificados	Utilización de certificados X509v3. Fortaleza mínima de mecanismos criptográficos: 112. Se permite la utilización de algoritmos *Legacy*. Máximo número de intentos fallidos de autenticación: 10
	Certificados en dispositivo físico	Utilización de certificados X509v3 Fortaleza mínima de mecanismos: criptográficos: 112. Se permite la utilización de algoritmos *Legacy.* Máximo número de intentos fallidos de autenticación: 10
Nivel MEDIO (2 factores)	**Contraseñas + OTP**	Longitud mínima de contraseña 12 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5 Prohibición de reutilizar 10 contraseñas anteriores.
	Certificados + pin o biométrico. **Opción recomendada para nivel MEDIO.**	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: criptográficos: 128. Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: entre 10 y 5
	Certificados en dispositivo físico + pin o biométrico.	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: criptográficos: 128.

	Opción Recomendada para nivel MEDIO.	Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: entre 10 y 5
Nivel ALTO (2 factores)	**Contraseñas + OTP**	Longitud mínima de contraseña 12 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 3 Prohibición de reutilizar 10 contraseñas anteriores.
	Certificados	Utilización de certificados X509v3 Fortaleza mínima de mecanismos: 128. Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: 5
	Certificados en dispositivo físico + pin o biométrico. **Opción recomendada para nivel ALTO.**	Utilización de certificados X509v3 Fortaleza mínima de mecanismos: 128. Se permite la utilización de algoritmos recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: 5

Tabla 5-2. [op.acc.5] Requisitos de autenticación para usuarios externos.

5.4.1. REQUISITOS GENERALES PARA EL ESTABLECIMIENTO DE CONTRASEÑAS (CONCERTADAS O ALEATORIAS)

92. A la hora de seleccionar contraseñas, deberán seguirse las siguientes directrices y opciones de configuración:

a) En caso de que sea necesario guardar una copia de la contraseña, se hará en un contenedor seguro.

b) Deberán generarse contraseñas de un solo uso cuando estas sean establecidas por el administrador de contraseñas para un tercero, de tal forma que se exija su modificación en accesos posteriores.

c) De acuerdo al nivel de seguridad exigido y respetando los valores límite establecidos anteriormente, la política de gestión de contraseñas determinará:

- La ventana de reutilización de contraseñas (número de contraseñas anteriores que no debe repetirse).
- La periodicidad con la que deben cambiarse. Estableciendo un período mínimo y uno máximo. El hecho de establecer un período mínimo es para evitar que realicen todos los cambios de contraseña permitidos de manera consecutiva con objeto de mantener la misma contraseña.
- El número mínimo de tipos de caracteres alfanuméricos que deben contener de entre los siguientes: Números, mayúsculas, minúsculas, signos de puntuación y caracteres especiales (del tipo: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")").

93. En el caso en que las contraseñas se establezcan manualmente, se establecerá una lista negra de contraseñas que no deben utilizarse dado que, con ayuda de ingeniería social, combinados con ataques de fuerza bruta, podrían llegar a adivinarse. A continuación, se presenta un listado (no exhaustivo) de contraseñas prohibidas[1]:

a) Contraseñas obtenidas en brechas de seguridad anteriores.

b) El nombre de host del sistema o razón social de la propia organización.

c) Cualquier palabra que aparezca en un diccionario, incluidos también diccionarios de otros idiomas distintos al español (inglés, francés…).

d) Matrículas de vehículos propios, fecha de nacimiento, fecha de boda, nombre de mascota, etc.

e) Nombres propios, títulos de películas, series televisivas, etc.

f) Secuencias de caracteres, caracteres repetitivos, patrones de teclado (i.e.: "aaaa", "12345", "abcde", "zaq12wsx".

g) Permutaciones de todo lo anterior. Por ejemplo, una palabra del diccionario cuyas vocales se hayan sustituido por números (i.e.: f00t) o a la que se añadan números al final.

[1] Para más información sobre la creación y uso de contraseñas, véase el Apéndice V – Normas de Creación y Uso de Contraseñas, de la Guía CCN-STIC 821.

94. Si, por el contrario, las contraseñas son generadas de forma aleatoria o pseudoaleatoria, deberán poseer la suficiente seguridad como para evitar repeticiones o hipótesis acerca de su posible valor.

5.4.2. PROTOCOLOS DE AUTENTICACIÓN

95. En cuanto a protocolos de autenticación, serán aceptables los siguientes:

a) Kerberos.

b) RADIUS (Remote Authentication Dial-In User Server) con EAP-TLS.

c) WPA3 (Wi-Fi Protected Access).

5.5 MECANISMOS DE AUTENTICACIÓN (USUARIOS INTERNOS) [OP.ACC.6]

96. Para la autenticación de usuarios internos, es decir, personal del organismo propio o contratado que pueda tener acceso a la información contenida en el sistema bajo el alcance del ENS se considerarán los siguientes métodos de autenticación:

e) **Contraseña (1 factor "algo que se sabe")**: Orientado a sistemas de categoría BÁSICA, consiste en una cadena de caracteres alfanuméricos empleada como mecanismo de autenticación. Para estas contraseñas se define una robustez, periodicidad mínima y un número de intentos fallidos de autenticación, a partir de los cuales el sistema debe:

1. Bloquearse y requerir una intervención específica para reactivar la cuenta

   o

2. Incluir un retardo cada vez mayor entre intentos de autenticación, de cara a evitar ataques de autenticación por fuerza bruta.

f) **Contraseñas + OTP (2 factores: "algo que se sabe" + "algo que se tiene")**: Además de emplear una contraseña, este mecanismo requerirá una contraseña de un solo uso (OTP, en inglés) como complemento.

g) **Certificados cualificados (de acuerdo a lo establecido en el Reglamento eIDAS), cuyo uso esté protegido por un segundo factor, del tipo PIN ("algo que se tiene" + algo que se sabe") o biométrico ("algo que se tiene" + "algo que se es")**. Además, las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

h) **Certificados cualificados en dispositivo físico que permita la creación de firma cualificada. El uso del certificado estará también protegido por un segundo factor del tipo PIN ("algo que se tiene" + algo que se sabe") o biométrico ("algo que se tiene" + "algo que se es")**. Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

97. A diferencia de los usuarios externos [OP.ACC.5], **no es necesario** que las credenciales de autenticación a las entidades, usuarios o procesos internos deban haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, aunque sí ante el órgano que, a tales efectos, haya determinado la organización usuaria.

98. Se considerarán distintos niveles de seguridad para los mecanismos de autenticación de usuarios internos, dependiendo del máximo nivel de seguridad exigido por el sistema para cualquiera de las dimensiones de Confidencialidad [C], Integridad [I], Trazabilidad [T] o Autenticidad [A]. La siguiente tabla muestra los métodos de autenticación recomendados para cada uno de los niveles, así como los requisitos de robustez para cada uno de ellos:

	Métodos de autenticación permitidos	Requisitos
Nivel BAJO (1 o 2 factores)	**Contraseñas**	El acceso debe ser desde una "*zona controlada*", entendiendo como tal aquella que no es de acceso público, y que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema Longitud mínima: 9 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5 Prohibición de reutilizar 5 contraseñas anteriores.
	Contraseñas + OTP	Longitud mínima: 9 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5 Prohibición de reutilizar 5 contraseñas anteriores.

	Certificados	Utilización de certificados X509v3. Fortaleza mínima de mecanismos criptográficos: 112. Se permite la utilización de algoritmos *Legacy*. Máximo número de intentos fallidos de autenticación: 10
	Certificados en dispositivo físico	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: criptográficos: 112. Se permite la utilización de algoritmos *Legacy*. Máximo número de intentos fallidos de autenticación: 10
Nivel MEDIO (2 factores)	**Contraseñas + OTP**	Longitud mínima de contraseña 12 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 5 Prohibición de reutilizar 10 contraseñas anteriores.
	Certificados + pin o biométrico	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: criptográficos: 128. Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: entre 10 y 5
	Certificados en dispositivo físico + pin o biométrico	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: criptográficos: 128. Se permite la utilización de algoritmos Recomendados.

		Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: entre 10 y 5
Nivel ALTO (2 factores)	**Contraseñas + OTP**	Longitud mínima de contraseña 12 caracteres con un mínimo de tres tipos diferentes. Periodicidad de renovación: 2 años, máximo. Máximo número de intentos fallidos de autenticación: 3 Prohibición de reutilizar 10 contraseñas anteriores.
	Certificados	Utilización de certificados X509v3. Fortaleza mínima de mecanismos: 128. Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: 5
	Certificados en dispositivo físico + pin o biométrico	Utilización de certificados X509v3 Fortaleza mínima de mecanismos: 128. Se permite la utilización de algoritmos Recomendados. Mínima longitud del PIN: 6 caracteres alfanuméricos. Máximo número de intentos fallidos de autenticación: 5

Tabla 5-3. [op.acc.6] Requisitos de autenticación para usuarios internos.

5.5.1. PROTOCOLOS DE AUTENTICACIÓN

99. En cuanto a protocolos de autenticación, serán aceptables los siguientes sistemas:

a) Kerberos

b) RADIUS (en inglés, Remote Authentication Dial-In User Server) con EAP-TLS.

c) *WPA3 (Wi-Fi Protected Access).*

5.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS [OP.EXP.10]

100. Las claves criptográficas, independientemente de la seguridad que ofrezcan, estarán protegidas durante todo su ciclo de vida. Esto significa que se deberán arbitrar las medidas de seguridad necesarias tanto en el proceso de generación de las claves, como en su transporte al punto de explotación, en su custodia durante el tiempo que estén en uso y en su posterior almacenamiento después de su vida activa hasta su destrucción final.

101. En la medida de lo posible, se velará porque los dispositivos portátiles no almacenen claves de acceso remoto, es decir, aquellas que permiten acceder a los equipos de la propia Organización o de otras organizaciones vinculadas.

102. Se recomienda que, en caso de que sea necesario almacenar claves en ordenadores portátiles u otros dispositivos removibles, estas estén a su vez cifradas por otras claves que solo el propietario de la solución que las tiene almacenadas sea capaz de generar y utilizar.

103. En general, los procesos de generación de claves deberán estar aislados de los medios de explotación. De igual modo, las claves archivadas por haber sido retiradas y en espera de ser destruidas, también deberán estar almacenadas en dispositivos aislados de los de explotación.

104. La siguiente tabla muestra la fortaleza mínima de los mecanismos criptográficos requerida para el acceso a los procesos tanto de generación de claves, como de transporte, custodia y almacenamiento de acuerdo a la categoría del ENS de la información que va a manejar el sistema.

Categoría ENS		
	BÁSICA	112
	MEDIA	112 o 128, según corresponda dependiendo del nivel de amenaza
	ALTA	128

Tabla 5-4. [op.exp.10] Fortaleza de mecanismos y seguridad equivalente de las claves

105. Además, para sistemas de categoría MEDIA y ALTA se usarán herramientas o dispositivos criptográficos que se encuentren en el catálogo de Productos y Servicios de Seguridad TIC (en adelante, CPSTIC) disponible en la guía CCN-STIC-105, conforme a lo establecido en el ENS ([op.pl.5] Componentes Certificados)

5.7 PROTECCIÓN DE LA CONFIDENCIALIDAD. [MP.COM.2]

106. La confidencialidad de una información consiste en mantener dicha información secreta para todos salvo para los autorizados a conocerla.

107. Para mantener la confidencialidad de la información se utilizarán redes privadas virtuales o canales de acceso seguro, cuando la comunicación discurra por redes fuera del propio dominio de seguridad. En particular se hará uso del protocolo IPsec (en inglés, *Internet Protocol Security*) y TLS (en inglés, *Transport Layer Security*).

108. IPsec es un protocolo, que posibilita proteger las comunicaciones sobre una red IP, de modo que cada uno de los paquetes de datos que se transmite es cifrado y autenticado. Dado que IPsec incluye protocolos para el establecimiento de claves de cifrado, estas deberán garantizar, al menos, una seguridad equivalente a la fortaleza de mecanismos requerida.

109. Por su parte TLS (sucesor de SSL, por lo que las VPN con dicho protocolo siguen llamándose VPN SSL), es un protocolo criptográfico que proporciona autenticidad y privacidad en una red, es decir, comunicaciones seguras, haciendo uso de métodos criptográficos. Por defecto, en estos protocolos únicamente se autentica el servidor, quedando el cliente sin autenticar. Al igual que con IPsec, las claves que se utilicen en estos protocolos deberán tener un nivel de seguridad equivalente a la fortaleza de mecanismos requerida.

110. Para las categorías MEDIA y ALTA del ENS se emplearán productos que se encuentren en el CPSTIC, conforme a lo establecido en el ENS ([op.pl.5] componentes certificados). Además, para categoría ALTA se emplearán, preferentemente, dispositivos *hardware* para establecer dichas VPN.

111. La siguiente tabla muestra la fortaleza mínima requerida para los mecanismos criptográficos autorizados (**L**egacy/**R**ecomendado) que se utilicen, atendiendo al nivel de amenaza considerado y al nivel de confidencialidad [C] requerido por el sistema para la información transmitida.

		Nivel de amenaza		
		BAJO	**MEDIO**	**ALTO**
Nivel de seguridad ENS [C]	**BAJO**	N/A	N/A	N/A
	MEDIO	112 (**L**) 128 (**R**)	112 (**L**) 128 (**R**)	128 (**R**)
	ALTO	112 (**L**) 128 (**R**)	128 (**R**)	128 (**R**)

Tabla 5-5. [mp.com.2] Fortaleza de mecanismos autorizados

112. Como hemos visto en la sección 3, un nivel de seguridad equivalente a 112 bits se traduce en:

a) claves de 112 bits (o superiores) para los sistemas de cifrado simétrico.

b) claves de longitud 2048 bits (o superiores) para el criptosistema RSA.

c) claves de longitudes comprendidas entre los 224 y 255 bits para criptosistemas basados en curvas elípticas.

113. Un nivel de seguridad equivalente a 128 bits supone el uso de:

    a) claves de 128 bits (o superiores) para el sistema de cifrado simétrico AES.

    b) claves de entre 256 y 283 bits para los sistemas basados en curvas elípticas.

    c) claves de al menos 3072 bits para el criptosistema RSA.

5.8 PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD [MP.COM.3]

114. Se entiende por autenticidad de una información la corroboración de la fuente de la información, es decir, la verificación de que quien la elaboró o el remitente de la misma es quien dice ser. Por su parte, la integridad de una información hace referencia a la comprobación de que la información recibida no ha sido alterada por entidades no autorizadas o por medios no conocidos.

115. Para cualquier nivel de seguridad requerido, se asegurará, al menos, la autenticidad de modo que se prevengan posibles ataques activos, que serán, como mínimo, detectados.

116. Se consideran ataques activos (por contraposición a los ataques pasivos en los que sólo se monitoriza la comunicación con el fin de obtener información de la misma o de lo intercambiado en ella) a aquellos ataques en los que se altere la información en tránsito, se inserte información engañosa, o el secuestro de la sesión por una tercera parte.

117. Para las categorías MEDIA y ALTA del ENS se emplearán productos que se encuentren en el CPSTIC, conforme a lo establecido en el ENS ([op.pl.5] componentes certificados). Además, para categoría ALTA se emplearán, preferentemente, dispositivos hardware para establecer Redes Privadas Virtuales.

118. La siguiente tabla muestra la fortaleza mínima requerida para los mecanismos criptográficos autorizados (Legacy/Recomendado) que se utilicen, atendiendo al nivel de amenaza considerado y al máximo nivel de seguridad requerido por el sistema para las dimensiones de integridad y autenticidad de la información transmitida.

		Nivel de amenaza		
		BAJO	**MEDIO**	**ALTO**
Nivel máximo Integridad [I] y autenticidad [A]	**BÁSICO**	112 (L) 128 (R)	112 (L) 128 (R)	112 (L) 128 (R)
	MEDIO	112 (L) 128 (R)	112 (L) 128 (R)	128 (R)
	ALTO	112 (L) 128 (R)	128 (R)	128 (R)

Tabla 5-6. [mp.com.3] Fortaleza de mecanismos

5.9 CRIPTOGRAFÍA [MP.SI.2] Y PROTECCIÓN DE EQUIPOS PORTÁTILES [MP.EQ.3]

119. Cifrar una información consiste en transformarla de modo que pase a ser ininteligible para todos salvo para las entidades autorizadas a acceder a dicha información. En general, el acceso a la información original a partir de su versión cifrada se lleva a cabo mediante el uso de claves y algoritmos.

120. La medida [mp.si.2] se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga. La medida [mp.eq.3] es aplicable aquellos equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo.

121. Para las categorías MEDIA y ALTA del ENS se emplearán productos de cifra fuera de línea (*offline)* o en reposo (*at-rest*) que se encuentren en el CPSTIC, conforme a lo establecido en el ENS ([op.pl.5] componentes certificados).

122. La siguiente tabla muestra la fortaleza mínima de mecanismos criptográficos requerida, atendiendo al nivel de amenaza considerado y al máximo nivel de seguridad requerido por el sistema respecto a la información almacenada en los soportes o en los dispositivos portátiles en las dimensiones de integridad [I] y confidencialidad [C].

		Nivel de amenaza		
		BAJO	**MEDIO**	**ALTO**
Nivel máximo Integridad [I] y Confidencialidad [C]	**BÁSICO**	N/A	N/A	N/A
	MEDIO	112 (L) 128 (R)	112 (L) 128 (R)	128 (R)
	ALTO	112 (L) 128 (R)	128 (R)	128 (R)

Tabla 5-7. [mp.si.2] Fortaleza de mecanismos

123. Es importante destacar que el nivel de amenaza bajo solamente se considerará en el caso de que los soportes y dispositivos portátiles sean accesibles únicamente por personal interno y autorizado, para lo cual deberán establecerse medidas complementarias de vigilancia específicas para dichos dispositivos, dado que, por su naturaleza, los soportes y los dispositivos portátiles están expuestos a un nivel de amenaza alto, especialmente fuera del perímetro físico de la Organización.

124. Estas mismas consideraciones, aunque las medidas de control implementadas sean menos restrictivas, serían aplicables para el nivel de amenaza medio, en el que se considera que los soportes y los dispositivos portátiles únicamente son accesibles por usuarios internos y autorizados dentro del perímetro de la Organización.

5.10 FIRMA ELECTRÓNICA [MP.INFO.3]

125. Una firma electrónica, tal como se encuentra definida en el Reglamento eIDAS, son los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar y tiene como fin enlazar de forma robusta una información electrónica con una entidad, esto es, el firmante, cuando deba acreditarse la voluntad y consentimiento del interesado respecto del contenido. De este modo, la firma electrónica previene el hecho de que un firmante pueda repudiar ser el autor de la información firmada, además de que la misma, cuando se realiza de determinada forma, permite garantizar la integridad del contenido firmado.

126. Se considerarán distintos niveles de seguridad para los tipos de firma electrónica, dependiendo del máximo nivel de seguridad exigido por el sistema para cualquiera de las dimensiones de Integridad [I] o Autenticidad [A]. La siguiente tabla muestra los tipos de firma permitidos para cada uno de los niveles, así como los requisitos de robustez para cada uno de ellos:

	Tipos de firma permitidas	Requisitos
Nivel BAJO	Cualquier tipo de firma electrónica de los previstos en la legislación vigente, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 40/2015, de 1 de octubre	La fortaleza mínima de mecanismos utilizados deberá ser de **112 bits** y podrán ser *Legacy* [L] o Recomendados [R]. En este sentido, los protocolos de firma electrónica harán uso de certificados digitales con: a) claves RSA (del firmante) de, al menos, **2048 bits.** b) claves de **224-255 bits** si se emplean curvas elípticas. c) Funciones hash **SHA-256** o **superior** .

	Tipos de firma permitidas	Requisitos
Nivel MEDIO ([I] o [A])	Se empleará **firma electrónica cualificada** incorporando **certificados cualificados**, de acuerdo a lo establecido en el Reglamento eIDAS y a lo dispuesto en las leyes 39/2015 y 40/2015.	Los certificados utilizados deberán estar cualificados. Los mecanismos utilizados deberán ser autorizados y presentar una **fortaleza mínima de 112 bits**. En este sentido, los protocolos de firma electrónica harán uso de certificados digitales con: a) claves RSA (del firmante) de, al menos, **2048 bits**. b) claves de **224-255** bits si se emplean curvas elípticas. c) Funciones hash **SHA-256 o superior**. Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que soporte. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.
Nivel ALTO ([I] o [A])	Se empleará **firma electrónica cualificada** incorporando **certificados cualificados** y **dispositivos cualificados** de creación de firma de acuerdo a lo establecido en el Reglamento eIDAS	Los mecanismos utilizados deberán ser recomendados y presentar una **fortaleza mínima de 128 bits**. Conforme a lo establecido en la [op.pl.5], se utilizarán productos incluidos en el CPSTIC. Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que soporte. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

5.11 SELLOS DE TIEMPO [MP.INFO.4]

127. Atendiendo a la definición dada por el Reglamento eIDAS, un sello de tiempo electrónico son datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante. Así pues, a efectos prácticos, los sellados de tiempo son la asignación por medios electrónicos de una fecha y hora a un documento electrónico, con la intervención de un prestador de servicios de certificación, que asegure la exactitud e integridad de la marca de tiempo del documento a la que va unido, de modo que no se pueda repudiar dicho documento con posterioridad al momento en que se practica el sellado.

128. Se considerarán distintos niveles de seguridad dependiendo de nivel exigido para la dimensión de Trazabilidad [T]. La siguiente tabla los requisitos mínimos establecidos para cada uno de estos niveles:

	Requisitos sellado de tiempo
Nivel BAJO [T]	No aplica
Nivel MEDIO [T]	No aplica
Nivel ALTO [T]	– Se utilizarán **productos certificados** conforme a lo establecido en el ENS ([op.pl.5] Componentes Certificados). – Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo establecido en el **Reglamento eIDAS**. – Se utilizarán mecanismos de firma electrónica recomendados y **fortaleza mínima 128 bits**, es decir: • RSA de, al menos, **3072 bits** (aunque se recomienda el uso de 4096 bits). • Curvas elípticas con claves de, al menos, **256 bits.** • Funciones resumen de las incluidas en la serie **SHA-2 o SHA-3** con una seguridad mayor o igual que SHA-256. – Para los esquemas enlazados, la seguridad recae en la función resumen empleada, por tanto, se empleará cualquiera de las funciones de la serie SHA-2 o SHA-3 con una seguridad mayor o igual que SHA-256.

5.12 EJEMPLO DE APLICACIÓN: TLS

129. Se supone una sede electrónica que ofrece un portal HTTPS para que los ciudadanos realicen trámites con la Administración. La información intercambiada entre el portal web y el ciudadano es información sensible, y tiene requisitos de nivel ALTO para las dimensiones de Confidencialidad [C], Integridad [I] y Autenticidad [A].

130. El intercambio de información debe realizarse a través de un canal de comunicación, aplicándole las medidas relativas a comunicaciones: [mp.com.2] y [mp.com.3] en su nivel ALTO.

131. Esto tendrá las siguientes implicaciones:

    a) Deberá emplearse una VPN (IPsec o TLS), implementada mediante un dispositivo *hardware* certificado conforme a lo establecido en la media [op.pl.5]. En este caso se utilizará el protocolo TLS, y para implementar la VPN TLS podrá usarse, por ejemplo, un dispositivo de los cualificados para nivel ENS ALTO en el catálogo CPSTIC, dentro de la familia "*Redes Virtuales TLS*".

    b) Aunque el ENS no establece como obligatoria ninguna versión de TLS, se debe hacer uso de las versiones de TLS autorizadas TLS 1.2 o TLS 1.3, ya que versiones anteriores son consideradas inseguras.

    c) Los mecanismos criptográficos que utilizará el protocolo TLS, deben encontrarse entre los autorizados en la presente guía, y deben proporcionar un nivel de seguridad equivalente a 128 bits. Para ello:

        - Seleccionar una *ciphersuite* de TLS apropiada (consultar **Tabla 4-1** y **Tabla 4-2**)
        - Verificar que la implementación de TLS utiliza esquemas criptográficos autorizados, y longitudes de clave que proporcionan los 128 bits de seguridad.

132. Existen muchas *ciphersuites* TLS 1.2 que cumplen estos requisitos. Como ejemplo, una *ciphers*uite apropiada sería:

    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

    donde ECDHE se utiliza para acuerdo de claves, AES-256 en modo GMC se usa para cifrado, integridad y autenticación de origen y SHA384 como función hash para PRF (Función pseudoaleatoria).

133. Otras medidas ENS que podrían aplicar a este ejemplo, son:

    a) [op.acc.1] y [op.acc.5] que aplicarían a la identificación y autenticación del ciudadano en el portal web. En caso de que alguno de los factores de autenticación utilice mecanismos criptográficos, estos deberán encontrarse entre los autorizados.

    b) [op.exp.11] que aplicaría a la protección de la clave privada del servidor HTTPS y también del cliente en caso de que este se autentique vía certificado,

o mediante otros mecanismos criptográficos. Para la protección de estas claves deberán emplearse mecanismos criptográficos autorizados, como los de *Key Wrapping* del apartado 3.10 o cualquier otra combinación de mecanismos autorizados (por ejemplo, mecanismos AEAD).

6. REFERENCIAS

[1] American National Standards Institute, ANSI X9.30 Public Key Cryptography for the Financial Services Industry: Part 1: the Digital Signature Algorithm (DSA), 1997.

[2] American National Standards Institute, ANSI X9.42 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 2005.

[3] American National Standards Institute, ANSI X9.62 Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.

[4] American National Standards Institute, ANSI X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011.

[5] International Organization for Standardization, ISO/IEC 10116 Information technology — Security techniques — Modes of operation for an n-bit block cipher, 2017.

[6] International Organization for Standardization, ISO/IEC 10118-3 IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions, 2018.

[7] International Organization for Standardization, ISO/IEC 11770-3 Information security — Key management — Part 3: Mechanisms using asymmetric techniques, 2021.

[8] International Organization for Standardization, ISO/IEC 14888-3 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms, 2018.

[9] International Organization for Standardization, ISO/IEC 18033-2 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, 2006.

[10] International Organization for Standardization, ISO/IEC 18033-3 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers, 2010.

[11] International Organization for Standardization, ISO/IEC 18033-3:2010 Information technology-Security techniques-Encryption algorithms-Part 3: Block ciphers, 2010.

[12] International Organization for Standardization, ISO/IEC 19772 Information security — Authenticated encryption, 2020.

[13] International Organization for Standardization, ISO/IEC 9796-2 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2010.

[14] International Organization for Standardization, ISO/IEC 9797-1 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher, 2011.

[15] International Organization for Standardization, ISO/IEC 9797-2 Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function, 2021.

[16] Institute of Electrical and Electronics Engineers, IEEE 1363-2000 Standard Specifications for Public-Key Cryptography, 2000.

[17] Institute of Electrical and Electronics Engineers, IEEE 1619-2018 Cryptographic Protection of Data on Block-Oriented Storage Devices, 2018.

[18] National Institute of Standards and Technology, Federal Information Processing Standards Publication 180. Secure Hash Standard (SHS), 2015.

[19] National Institute of Standards and Technology, Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2007.

[20] National Institute of Standards and Technology, Special Publication 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, 2012.

[21] National Institute of Standards and Technology, Special Publication 800-56A Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, 2018.

[22] National Institute of Standards and Technology, Spectial Publication 800-56B Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, 2020.

[23] National Institute of Standards and Technology, Spectial Publication 800-38A Recommendation for Block Cipher Modes of Operation, 2001.

[24] National Institute of Standards and Technology, Special Publication 800-38E Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, 2010.

[25] National Institute of Standards and Technology, Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007.

[26] National Institute of Standards and Technology, Special Publication 800-208 Recommendation for Stateful Hash-Based Signature Schemes, 2020.

[27] National Institute of Standards and Technology, Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Applications, 2010.

[28] National Institute of Standards and Technology, Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions, 2009.

[29] National Institute of Standards and Technology, Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, 2019.

[30] National Institute of Standards and Technology, Federal Information Processing Standards198. The Keyed-Hash Message Authentication Code (HMAC), 2008.

[31] National Institute of Standards and Technology, Federal Information Processing Standards 186. Digital Signature Standard (DSS), 2013.

[32] National Institute of Standards and Technology, Federal Information Processing Standards 197. Advanced Encryption Standard (AES), 2001.

[33] National Institute of Standards and Technology, Federal Information Processing Standards Publication 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015.

[34] Standards for Efficient Cryptography Group, SEC 1: Elliptic Curve Cryptography, 2009.

[35] H. Krawczyk, M. Bellare y R. Canetti, RFC 2104 HMAC: Keyed-Hashing for Message Authentication, Internet Engineering Task Force (IETF), 1997.

[36] J. Schaad y R. Housley, RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm, Internet Engineering Task Force (IETF), 2002.

[37] J. Jonsson y B. Kaliski, RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force (IETF) , 2003.

[38] K. Igoe y J. Solinas, RFC 5647 AES Galois Counter Mode for the Secure Shell Transport Layer Protocol, Internet Engineering Task Force (IETF) , 2009.

[39] T. Ylonen y C. Lonvick, RFC 4253 The Secure Shell (SSH) Transport Layer Protocol, Internet Engineering Task Force (IETF), 2006.

[40] M. Lochter y J. Merkle, RFC 5639 Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, Internet Engineering Task Force (IETF), 2010.

[41] T. Dierks y E. Rescorla, RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, Internet Engineering Task Force (IETF), 2008.

[42] M. Friedl, N. Provos y W. Simpson, RFC 4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, Internet Engineering Task Force (IETF), 2006.

[43] D. Harkins, RFC 5297 Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES), Internet Engineering Task Force (IETF), 2008.

[44] T. Kivinen y M. Kojo, RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), Internet Engineering Task Force (IETF), 2003.

[45] T. Kohno y C. Namprempre, RFC 4344 The Secure Shell (SSH) Transport Layer Encryption Modes, Internet Engineering Task Force (IETF), 2006.

[46] R. Housley y M. Dworkin, RFC 5649 Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm, Internet Engineering Task Force (IETF) , 2009.

[47] D. Stebila y J. Green, RFC 5656 Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer, Internet Engineering Task Force (IETF) , 2009.

[48] K. Igoe y D. Stebila, RFC 6187 X.509v3 Certificates for Secure Shell Authentication, Internet Engineering Task Force (IETF) , 2011.

[49] D. Bider y M. Baushke, RFC 6668 SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol, Internet Engineering Task Force (IETF) , 2012.

[50] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen y T. Kivinen, RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2), Internet Engineering Task Force (IETF) , 2014.

[51] M.-J. Saarinen y J.-P. Aumasson, RFC 7693 The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC), Internet Engineering Task Force (IETF) , 2015.

[52] A. Langley, W. Chang, N. Mavrogiannopoulos, J. Strombergson y S. Josefsson, RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS), Internet Engineering Task Force (IETF) , 2016.

[53] C. Percival y S. Josefsson, RFC 7914 The scrypt Password-Based Key Derivation Function, Internet Engineering Task Force (IETF) , 2016.

[54] K. Moriarty, B. Kaliski, J. Jonsson y A. Rusch, RFC 8017 PKCS #1: RSA Cryptography Specifications Version 2.2, Internet Engineering Task Force (IETF) , 2016.

[55] K. Moriarty, B. Kaliski y A. Rusch, RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1, Internet Engineering Task Force (IETF) , 2017.

[56] M. Baushke, RFC 8268 More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH), Internet Engineering Task Force (IETF) , 2017.

[57] D. Bider, RFC 8332 Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol, Internet Engineering Task Force (IETF) , 2018.

[58] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld y A. Mohaisen, RFC 8391 XMSS: eXtended Merkle Signature Scheme, Internet Engineering Task Force (IETF) , 2018.

[59] Y. Nir y A. Langley, RFC 8439 ChaCha20 and Poly1305 for IETF Protocols, Internet Engineering Task Force (IETF) , 2018.

[60] National Institute of Standards and Technology, Special Publication 800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths, 2019.

[61] Ministerio de la Presidencia, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema, «BOE» núm. 25, de 29 de enero de 2010 Referencia: BOE-A-2010-1330, 2010.

PUBLICACIONES Pd DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL