Instrucción general

Seguridad criptográfica

Normativa de Seguridad Documental del Sector Público de Cataluña.

Información general

Control documental

Proyecto:	**BIBLIOTECA NORMATIVA**
Entidad de destino:	**Administraciones públicas catalanas y entidades que forman parte del sector público de Cataluña.**
Código de referencia:	1.3.6.1.4.1.36142.1.1
Versión:	**1.0**
Fecha de la edición:	**21/12/2010**
Fichero:	**IG-Seg-Criptografica-v1r0**
Formato:	**Edición: Word 97-2003** **Publicación: ISO 32000-1 PDF 1.7**
Autores:	

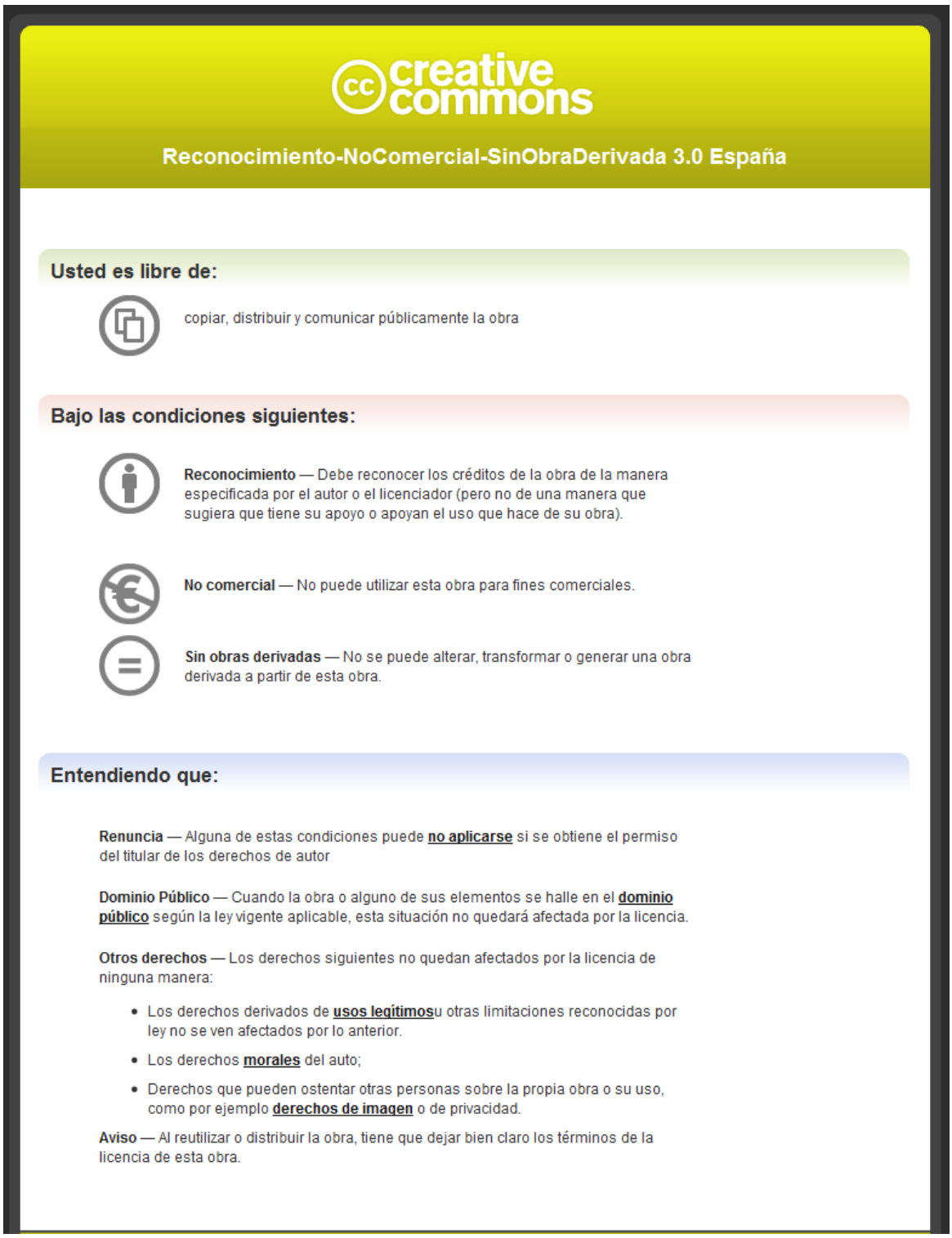
Estado formal

Preparado	Revisado	Aprobado
Nombre: Equipo ASTREA Fecha: 21/12/2010	Nombre: CATCert Fecha:	Nombre: Dirección ASTREA Fecha:

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Equipo Astrea	21/12/2010

Licencia



creative commons

Reconocimiento-NoComercial-SinObraDerivada 3.0 España

Usted es libre de:

copiar, distribuir y comunicar públicamente la obra

Bajo las condiciones siguientes:

Reconocimiento — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).

No comercial — No puede utilizar esta obra para fines comerciales.

Sin obras derivadas — No se puede alterar, transformar o generar una obra derivada a partir de esta obra.

Entendiendo que:

Renuncia — Alguna de estas condiciones puede **no aplicarse** si se obtiene el permiso del titular de los derechos de autor

Dominio Público — Cuando la obra o alguno de sus elementos se halle en el **dominio público** según la ley vigente aplicable, esta situación no quedará afectada por la licencia.

Otros derechos — Los derechos siguientes no quedan afectados por la licencia de ninguna manera:

- Los derechos derivados de **usos legítimos** u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.
- Los derechos **morales** del auto;
- Derechos que pueden ostentar otras personas sobre la propia obra o su uso, como por ejemplo **derechos de imagen** o de privacidad.

Aviso — Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Texto completo de la licencia: http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es

Índex

1. Introducción

Este documento contiene la normativa de seguridad criptográfica aplicable a los sistemas de información que ofrecen soporte a procedimientos administrativos electrónicos.

> **Nota**: Una instrucción general de seguridad criptográfica es un documento que especifica normas de uso en relación con la criptografía, incluyendo estándares para su implementación en la organización. Algunos de los usos de la criptografía incluyen los mecanismos de Autenticación, firma electrónica e irrefutabilidad, confidencialidad o integridad.

Esta Instrucción General es una POLÍTICA DE FIRMA ELECTRÓNICA de acuerdo con el artículo 18.2 del RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica, y ha sido producida de acuerdo con los requisitos de la NTI "Política de firma electrónica y de certificados de la Administración".

Esta instrucción general resulta conforme con los requisitos de seguridad y proporcionalidad correspondientes a los sistemas electrónicos de soporte a procedimientos administrativos, establecidos por las siguientes normas:

- Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

- Ley 11/2007, de 11 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP).

- Ley 26/2010, de 3 de agosto, de régimen jurídico y procedimientos de las administraciones públicas de Cataluña (LRPJCAT).

- Ley 29/2010, de 3 de agosto, de uso de los medios electrónicos en el sector público de Cataluña (LUMESPC).

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

- Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

Los contenidos de esta instrucción general de seguridad criptográfica se han estructurado para cubrir los controles que prevé la norma internacional ISO/IEC 20007:2006 – Tecnología de la Información: Técnicas de seguridad: Código de prácticas para la gestión de la seguridad de la información, secciones 12.3.1 i 15.1.6; y se basan en las recomendaciones de mejores prácticas contenidas en la Publicación Especial 800-57 partes 1[1] y 2[2] del National Institute of Standards and Technology (EEUU), en las recomendaciones de la especificación TS 102 176, partes 1 y 2, del European Telecommunications Standards Institute, y en las recomendaciones contenidas en las Guías de Seguridad de las TIC CCN-STIC-405[3] y CCN-STIC-807[4] del Centro Criptológico Nacional.

[1] Aspectos generales de la gestión de claves criptográficas.

[2] Mejores prácticas para la organización de la gestión de claves.

[3] Algoritmos y parámetros para la firma electrónica segura.

[4] Criptología de empleo en el Esquema Nacional de Seguridad.

2. Contenidos generales de la instrucción general de seguridad criptográfica

2.1. Identificación de la instrucción general de seguridad criptográfica

Esta instrucción general de seguridad criptográfica se identifica con el siguiente identificador de objeto: 1.3.6.1.4.1.36142.1.1

2.2. Fecha de emisión de la instrucción general de seguridad criptográfica

Esta instrucción general de seguridad criptográfica ha sido emitida en fecha [__ de_____ de ____].

2.3. Identificación del emisor de la instrucción general de seguridad criptográfica

Esta instrucción general de seguridad criptográfica ha sido emitida por [_____].

2.4. Ámbito de aplicación de la instrucción general de seguridad criptográfica

Esta instrucción general resulta aplicable a todos los sistemas de información de soporte a procedimientos administrativos electrónicos utilizados por la Administración Pública, sujetos a la LAECSP.

3. Utilización de la criptografía en la Administración Pública

3.1. Servicios de seguridad basados en criptografía

La Administración Pública utilizará la criptografía para ofrecer los siguientes servicios de seguridad:

- Servicios de confidencialidad
- Servicios de integridad de datos
- Servicios de Autenticación
- Servicios de autorización.
- Servicios de irrefutabilidad
- Servicios accesorios

Los servicios de seguridad hacen uso de los algoritmos criptográficos aprobados en esta instrucción general.

Las normativas de desarrollo de esta instrucción general deben indicar la aplicación de criptografía en cada caso y el escenario concreto:

- Firma electrónica
- Autenticación electrónica
- Cifrado
- Evidencia electrónica

3.2. Algoritmos criptográficos aprobados

Los algoritmos criptográficos aprobados para el uso por la Administración Pública son los siguientes:

- Algoritmos de resumen aprobados
    - SHA-1[5], definido en la norma internacional ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions" y en la norma FIPS 180-2 (2002): “Secure Hash Standard”.

[5] Sección 1.2.1.k) CCN STIC 807.

SHA-1 es el algoritmo más recomendado actualmente, aunque se recomienda dejarlo de utilizar a partir del 2011, siempre que la infraestructura tecnológica lo permita.

- SHA-224[6], definido en la norma FIPS 180-2 (2002): “Secure Hash Standard” (change notice 1, de 2004).

- SHA-256[7], defindo en la norma internacional ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions" y en la norma FIPS 180-2 (2002): “Secure Hash Standard”.

- SHA-384[8], definido en la norma FIPS 180-2 (2002): “Secure Hash Standard”.

- SHA-512[9], definido en la norma FIPS 180-2 (2002): “Secure Hash Standard”.

- Algoritmos simétricos aprobados

  - AES[10], definido en la norma FIPS 197 (2001): “Specification for the Advanced Encryption Standard (AES)”.

  - TDEA[11] (por ejemplo, Triple DES), definido en la especificación NIST SP 800-67 (2004, revisado en 2008): “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, con la recomendación de utilizar tres claves diferentes.

  Se recomienda utilizar los modos criptográficos de operación definidos en la especificación NIST SP 800-38A (2001): “Recommendation for Block Cipher Modes of Operation - Methods and Techniques”.

- Algoritmos asimétricos aprobados

  - RSA[12], definido en la especificación técnica IETF RFC 3447 (2003): “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”.

[6] Sección 1.2.1.k) CCN STIC 807.
[7] Sección 1.2.1.k) CCN STIC 807.
[8] Sección 1.2.1.k) CCN STIC 807.
[9] Sección 1.2.1.k) CCN STIC 807.
[10] Sección 1.2.1.b) CCN STIC 807.
[11] Sección 1.2.1.a) CCN STIC 807.
[12] Sección 1.2.1.i) CCN STIC 807.

- DSA[13], definido en la norma internacional ISO/IEC 14888-3 (2006): “Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms” y en la norma FIPS 186-2 (2000): “Digital Signature Standard”.

- EC-DSA[14], en sus dos variantes E(Fp) i E(F2m), definido en la norma internacional ISO/IEC 14888-3 (2006): “Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms”.

- Algoritmos de establecimiento de claves aprobados

  - Algoritmos DLC, definidos en la especificación NIST SP 800-56A (2007): “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”.

  - Algoritmo de transporte de claves RSA.

  - Algoritmos contenedores de claves con clave simétrica

[13] Sección 1.2.1.g) CCN STIC 807.
[14] Sección 1.2.1.h) CCN STIC 807.

3.3. Requisitos de protección de claves criptográficas

Las claves criptográficas deben encontrarse disponibles operativamente tanto tiempo como lo requiera el correspondientes servicios criptográfico. Las claves se pueden mantener en un equipamiento criptográfico mientras se utilicen, o se pueden almacenar de forma externa –con las medidas de seguridad adecuadas – y recuperadas cuando sea necesario.

Además, algunas de las claves se deben archivar durante un plazo superior al inicialmente previsto para su uso por su emisor.

La tabla siguiente indica, para cada tipo de clave, los requisitos de protección correspondientes:

Tipo de clave	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Garantía requerida	Período de protección
Clave privada de firma	Autenticación; Integridad; Irrefutabilidad	Integridad; Confidencialidad	Uso o aplicación; Parámetros de dominio; Clave pública de firma	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de firma	Autenticación; Integridad; Irrefutabilidad	Archivo; Integridad	Uso o aplicación; Propietario del par de Claves; Parámetros de dominio; Clave privada de firma; Datos firmados	Validez	Desde su generación hasta que no sea necesario verificar los datos protegidos
Clave simétrica de Autenticación	Autenticación; Integridad	Archivo; Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas; Datos autenticados.	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica
Clave privada de Autenticación	Autenticación; Integridad	Integridad; Confidencialidad	Uso o aplicación; Clave pública de Autenticación; Parámetros de dominio	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de Autenticación	Autenticación; Integridad	Archivo; Integridad	Uso o aplicación; Propietario del par de claves; Datos autenticados; Clave privada de Autenticación; Parámetros de dominio	Validez	Desde su generación hasta que no sea necesario autenticar los datos protegidos

Tipo de clave	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Garantía requerida	Período de protección
Clave simétrica de cifrado de datos	Confidencialidad	Archivo; Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas; Datos cifrados; Datos en claro	No aplica	Desde su generación hasta la finalización de la vida de los datos o la finalización del período de validez criptográfica
Clave simétrica contenedora de Claves	Soporte	Archivo; Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas; Claves cifradas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que las claves contenidas no necesiten protección, el más largo de los dos.
Clave (simétrica y asimétrica) de generación de números aleatorios	Soporte	Integridad; Confidencialidad	Uso o aplicación	Posesión de la Clave privada, cuando se utiliza	Desde su generación hasta su reposición
Clave maestra simétrica	Soporte	Archivo; Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas; Claves derivadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o de las claves derivadas, el más largo de los dos
Clave privada de transporte de Clave	Confidencialidad; Integridad	Archivo; Integridad; Confidencialidad	Uso o aplicación; Claves cifradas; Parámetros de dominio; Clave pública de transporte de claves	Posesión	Desde su generación hasta la finalización del período de protección de todas las claves transportadas
Clave pública de transporte de Clave	Confidencialidad; Integridad	Archivo; Integridad	Uso o aplicación; Propietario del par de Claves; Clave privada de transporte de claves	Validez	Desde su generación hasta la finalización del período de su validez criptográfica

Tipo de clave	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Garantía requerida	Período de protección
Clave simétrica de negociación de Clave	Soporte	Archivo; Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que no sea necesaria en relación con una clave determinada, el más largo de los dos
Clave privada estática de negociación de Clave	Soporte	Archivo; Integridad; Confidencialidad	Uso o aplicación; Parámetros de dominio; Clave pública de negociación de clave estática	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que no sea necesaria en relación con una clave determinada, el más largo de los dos
Clave pública estática de negociación de clave	Soporte	Archivo; Integridad;	Uso o aplicación; Propietario del par de claves; Parámetros de dominio; Clave privada de negociación de Clave estática	Validez	Desde su generación hasta la finalización del período de su validez criptográfica o hasta que no sea necesaria en relación con una clave determinada, el más largo de los dos
Clave privada efímera de negociación de clave	Soporte	Integridad; Confidencialidad	Uso o aplicación; Parámetros de dominio; Clave pública de negociación de clave efímera	No aplica	Desde su generación hasta la finalización del proceso de negociación de claves, con destrucción inmediata
Clave pública efímera de negociación de clave	Soporte	Integridad	Uso o aplicación; Propietario del par de Claves; Parámetros de dominio; Clave privada de negociación de clave efímera	Validez	Desde su generación hasta la finalización del proceso de negociación de claves, con destrucción inmediata
Clave simétrica de autorización	Autorización	Integridad; Confidencialidad	Uso o aplicación; Otras entidades autorizadas	No aplica	Desde su generación hasta la finalización del período de su validez criptográfica

Tipo de clave	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Garantía requerida	Período de protección
Clave privada de Autorización	Autorización	Integridad; Confidencialidad	Uso o aplicación; Parámetros de dominio; Clave pública de Autorización	Posesión	Desde su generación hasta la finalización del período de su validez criptográfica
Clave pública de Autorización	Autorización	Integridad	Uso o aplicación; Propietario del par de claves; Parámetros de dominio; Clave privada de Autorización	Validez	Desde su generación hasta la finalización del período de su validez criptográfica

3.4. Requisitos de protección de material criptográfico

Tipo de material	Servicio de seguridad	Protección de seguridad	Datos asociados a proteger	Período de protección
Parámetros de dominio	Depende de la clave asociada a los parámetros de dominio	Archivo; Integridad	Uso o aplicación; Claves privada y pública	Desde su generación hasta que no sean necesarios para generar claves o verificar firmas
Vectores de inicialización	Depende del algoritmo	Archivo; Integridad	Datos protegidos	Desde su generación hasta que no sean necesarios para procesar datos protegidos
Secretos compartidos	Soporte	Confidencialidad; Integridad	No aplica	Desde su generación hasta la finalización de la transacción. Serán destruidos al finalizar el periodo de protección.
Semillas de generadores de números aleatorios	Soporte	Confidencialidad; Integridad	Uso o aplicación	Se utilizan una vez y se destruyen
Otra información pública	Soporte	Archivo; Integridad	Uso o aplicación; Otras entidades autorizadas; Datos procesado en relación con valores únicos de mensaje	Desde su generación hasta que no sean necesarios para procesar datos dependientes
Resultados intermedios	Soporte	Confidencialidad; Integridad	Uso o aplicación	Desde su generación hasta que no sean necesarios, momento en que se deben destruir.
Información de control de Claves	Soporte	Archivo; Integridad	Clave	Desde su generación hasta que la clave asociada es destruida
Número aleatorio	Soporte	Integridad; Confidencialidad (depende de uso)	No aplica	Desde su generación hasta que no sea necesario, momento en que se debe destruir
Contraseña	Autenticación	Integridad; Confidencialidad	Uso o aplicación; Entidad propietaria	Desde su generación hasta que sea substituida o no sea necesaria para autenticar a la entidad
Información de auditoría	Soporte	Archivo; Integridad; Autorización d'accés	Acontecimientos auditados; Información de control de claves	Desde su generación hasta que no sea necesaria

3.5. Métodos de protección de seguridad

Las dos tablas anteriores determinan diversas protecciones de seguridad en relación con las claves criptográficas y otros materiales:

- Integridad.
- Confidencialidad.
- Archivo.

A continuación se determinan los métodos aceptables para conseguir las protecciones de integridad y de confidencialidad, tanto cuando la información criptográfica se encuentra en tránsito como cuando se encuentra en su lugar de operación. Los estándares de infraestructura para la protección en la custodia y el archivo de las claves y el resto de material criptográfico se detallan en la sección 4.5 de este documento.

3.5.1. Protección de la información criptográfica en tránsito

La información criptográfica en tránsito incluye toda la información en procesos de distribución de claves o de copia de seguridad y traslado a localizaciones diferentes del lugar de operación. Algunos ejemplos son las claves certificados por terceras Entidades de Certificación, que viajan desde esta Entidad hasta el destino de operación, o las claves que ya han llegado al fin de su período de operación, y que son archivadas de forma definitiva en un tercer proveedor de seguridad.

La protección de la Integridad de información criptográfica en tránsito se debe conseguir mediante alguno de los siguientes mecanismos:

- En caso de distribución manual, con protección física, se puede utilizar un mecanismo de control CRC de la información criptográfica, pactado entre emisor y receptor; o comprobar que el formato de la información criptográfica recibida corresponde al que estaba previsto recibir.

  Ejemplo: La integridad de una clave privada de firma electrónica reconocida de una persona se garantiza, durante su tránsito, para la protección física de la tarjeta T-CAT que la contiene.

- En caso de distribución electrónica, se puede utilizar un mecanismo MAC o de firma digital, ya sea sobre la información criptográfica o sobre el mensaje que la transporta; o comprobar que el formato de la información criptográfica recibida corresponde al que estaba previsto recibir.

  Ejemplo: La integridad de una clave pública de sello de órgano que se transmite a una Entidad de Certificación para la generación del correspondiente certificado digital, se garantiza mediante la firma del mensaje de solicitud con la clave privada del solicitante.

La protección de la confidencialidad de la información criptográfica en tránsito se debe conseguir mediante alguno de los siguientes mecanismos:

- En caso de distribución manual, mediante protección física, cifrando la información criptográfica con un algoritmo aprobado de acuerdo con esta instrucción general o dividiendo la información criptográfica en componentes distribuidos por agentes o vías independientes.

  Ejemplo: La confidencialidad de una clave privada de firma electrónica reconocida de una persona se garantiza, durante el tránsito, por la protección física de la tarjeta T-CAT que la contiene.

- En caso de distribución electrónica, cifrando la información criptográfica con un algoritmo aprobado de acuerdo con esta instrucción general.

  Ejemplo: La confidencialidad de una clave privada de un certificado de firma de software, generada por la Entidad de Certificación se garantiza, durante su tránsito, mediante su entrega en un contenedor cifrado.

Si se detecta un fallo en la protección de la seguridad de la información criptográfica en tránsito, la Administración Pública debe hacer lo siguiente:

- No utilizar la información criptográfica recibida
- Reintentar la operación, con un número máximo de tres veces.
- Generar una incidencia, en su caso con la Entidad de Certificación participante.

3.5.2. Protección de la información criptográfica en el lugar de la operación

La información criptográfica en el lugar de operación incluye toda la información en dispositivos y hardware en el lugar de operación, y también la información custodiada en espacios de archivo o copia de seguridad. Algunos ejemplos son el hardware y software que dan soporte a las sedes electrónicas y aplicaciones de la Administración Pública.

La protección de la integridad de información criptográfica en el lugar de operación se debe conseguir mediante alguno de los siguientes mecanismos:

- Mediante mecanismos físicos, incluyendo el uso de hardware criptográfico validado, de acuerdo con lo que dispone la sección 4.5 de esta instrucción general; o de ordenadores que no estén conectados a otros sistemas; o depósitos físicos para proteger dispositivos o soportes (como una caja fuerte).

- Mediante mecanismos criptográficos, como por ejemplo el uso de mecanismos MAC o de firma digital de la información criptográfica almacenada; o la comprobación de formato de la información criptográfica a utilizar.

La protección de confidencialidad de información criptográfica en el lugar de operación se debe conseguir mediante alguno de los siguientes mecanismos:

- Cifrado de la información utilizando un algoritmo aprobado de acuerdo con esta instrucción general, en un hardware criptográfico validado, de acuerdo con lo que dispone la sección 4.5 de esta instrucción general.

- Mediante el uso de hardware criptográfico validado, de acuerdo con lo dispuesto en la sección 4.5 de esta instrucción general.

- Mediante un sistema de almacenamiento físico seguro, con garantía de control de acceso en el depósito.

4. Criterios para el uso de la criptografía

Los servicios criptográficos se deben utilizar de acuerdo con las siguientes normas:

- Desarrollo de la instrucción general.
- Separación del uso de claves
- Establecimiento de plazos de duración de las claves
- Establecimiento de procedimientos de gestión de claves
- Establecimientos de estándares de implementación de tecnología criptográfica.
- Cumplimiento normativo.

4.1. Desarrollo de la instrucción general

Esta instrucción general de seguridad criptográfica se debe desplegar mediante las siguientes normativas:

- Instrucción general de gestión de claves criptográficas de la Administración Pública.
- Instrucción general de certificación de la Administración Pública.
- Instrucción general de autenticación de la Administración Pública.
- Instrucción general de firma electrónica de la Administración Pública.
- Instrucción general de cifrado de la Administración Pública.

4.2. Separación del uso de claves

De forma general, una clave solo se debe utilizar para un uso concreto –por ejemplo: firma electrónica, o cifrado de datos, o autenticación, etc. - por los siguientes motivos:

- El uso de una misma clava para dos procesos criptográficos diferentes puede debilitar la seguridad de alguno de estos procesos.
- La limitación de uso de una clave permite controlar los daños causados en caso de compromiso de la clave.
- Algunos usos de las claves generan problemas colaterales, porque tienen períodos de duración o conservación diferentes.

Esta directriz no impide el uso de una misma clave para procesos que ofrecen más de un servicio criptográfico. Por ejemplo: una clave de firma digital se puede utilizar, de acuerdo con esta directriz, para servicios de integridad, autenticidad e irrefutabilidad.

Se permite de forma expresa el uso de la clave privada para solicitar la certificación digital de la correspondiente clave pública en una Entidad de Certificación.

4.3. Plazos de duración de las claves

De forma general, una clave se debe utilizar durante un plazo concreto, o período criptográfico, por los siguientes motivos:

- Se limita la cantidad de información protegida por una clave que se encuentra disponible para análisis criptográfico.
- Se limita la exposición en caso de compromiso de una clave.
- Se limita el uso de un algoritmo particular a su período estimado de uso eficiente
- Se limita el tiempo disponible para intentar penetrar los mecanismos de acceso lógico, físico y de procedimiento que protegen una clave de su divulgación no autorizada.
- Se limita el período durante el cual la información se puede comprometer por divulgación accidental de claves o material criptográfico a entidades no autorizadas.

Se establecen los siguientes períodos criptográficos recomendados:

Tipo de Clave	Período de uso del emisor	Período de uso del receptor
Clave privada de firma	1 – 3 años	
Clave pública de firma	Diversos años (depende de la longitud de la clave)	
Clave simétrica de Autenticación	Hasta 2 años	Hasta 3 años adicionales
Clave privada de Autenticación	1 – 2 años	
Clave pública de Autenticación	1 – 2 años	
Clave simétrica de cifrado de datos	Hasta 2 años	Hasta 3 años adicionales
Clave simétrica contenedora de claves	Hasta 2 años	Hasta 3 años adicionales
Clave (simétrica y asimétrica) de generación de números aleatorios	Hasta la generación de nuevas semillas	
Clave maestra simétrica	Hasta 1 año	
Clave privada de transporte de clave	Hasta 2 años	
Clave pública de transporte de Clave	1 – 2 años	
Clave simétrica de negociación de Clave	1 – 2 años	
Clave privada estática de negociación de clave	1 – 2 años	
Clave pública estática de negociación de Clave	1 – 2 años	

Tipo de Clave	Período de uso del emisor	Período de uso del receptor
Clave privada efímera de negociación de Clave	Una transacción	
Clave pública efímera de negociación de Clave	Una transacción	
Clave simétrica de Autorización	Hasta 2 años	
Clave privada de Autorización	Hasta 2 años	
Clave pública de Autorización	Hasta 2 años	

Para la decisión concreta de los períodos aplicables, se debe hacer un análisis de riesgo, considerando los siguientes factores:

- La fortaleza de los mecanismos criptográficos utilizados.
- La protección de los mecanismos utilizando equipamiento criptográfico seguro.
- El entorno de operación (instalaciones de acceso controlado, equipamiento de oficina o terminal de acceso público).
- El volumen de información o el número de transacciones a proteger.
- La clasificación de seguridad de los datos.
- La función de seguridad involucrada (cifrado de datos, firma digital, producción, negociación o protección de claves)
- El método de regeneración de las claves
- El método de actualización o de derivación de las claves.
- El número de nodos de red que eventualmente comparten una clave
- El número de copias de una clave y de distribución de las copias.
- Las amenazas a la seguridad de las claves.

Es necesario considerar de forma particular las restricciones derivadas de las normas y políticas de las Entidades de Certificación externas, ya que en muchos casos son las Entidades de Certificación las que fijan los períodos criptográficos.

En este sentido, se autoriza la aceptación de períodos criptográficos superiores a los recomendados, siempre que se trate de claves garantizadas en certificados reconocidos emitidos cumpliendo la legislación de firma electrónica.

4.4. Procedimientos de gestión de las claves

Se deben establecer los siguientes procedimientos en relación con los siguientes aspectos:

- Generación de claves para diferentes sistemas criptográficos y aplicaciones.
- Generación y obtención de certificados de clave pública.

- Distribución de claves a los usuarios, incluyendo la activación una vez hayan sido recibidas.
- Almacenaje de claves, incluyendo como obtienen acceso a las claves los usuarios autorizados.
- Cambio o actualización de claves, incluyendo normas sobre cuando las claves deben ser cambiadas o actualizadas, y cual es el procedimiento aplicable.
- Gestión de claves comprometidas.
- Revocación de claves, incluyendo su retirada o desactivación.
- Archivo de claves, especialmente en caso de información cifrada que haya sido archivada.
- Destrucción de claves.
- Registro y auditoría de operaciones relativas a gestión de claves.

Se deben definir períodos de activación y desactivación de las claves, para reducir el riesgo de compromiso, de forma que las claves solo se puedan utilizar durante un plazo concreto, de acuerdo con las circunstancias y el análisis de riesgo.

Se deben definir procedimientos para garantizar la autenticidad de las claves públicas, mediante el uso de las Entidades de Certificación que resulten adecuadas.

En caso que haya terceros prestadores de servicios relacionados con la criptografía, se deben establecer acuerdos de nivel de servicios que consideren de forma específica las cuestiones de responsabilidad, la fiabilidad de los servicios y los tiempos de respuesta garantizados.

4.5. Estándares de implementación de tecnología criptográfica

Se debe definir e implantar una infraestructura común y adecuada de tecnología criptográfica que preste los servicios criptográficos identificados en esta instrucción general en las diferentes aplicaciones de la Administración Pública, considerando al menos las siguientes:

- La sede electrónica de la Administración Pública.
- La realización de actos administrativos automatizados basados en el uso de sellos de la Administración Pública y de sus órganos.
- La realización de actos administrativos manuales, y de otras acciones que tengan plasmación documental, por parte de los órganos y del personal al servicio de la Administración Pública.

La infraestructura criptográfica debe utilizar hardware y software fiable, certificado de acuerdo con las siguientes especificaciones técnicas:

- Hardware criptográfico dedicado:

    - ISO 15408 (2005): “Information technology – Security techniques - Evaluation criteria for IT security”, nivel EAL 4 o superior, de acuerdo con un objetivo de evaluación o perfil de protección adecuado al análisis de riesgo realizada.

      En concreto, se consideran adecuados los siguientes perfiles de protección:

        - CEN CWA 14167-2 (2004): “Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP”, en relación con las operacioens de firma de certificados y otros documentos, con copia de seguridad.
        - CEN CWA 14167-3 (2004): “Cryptographic module for CSP key generation services - Protection profile - CMCKG-PP”, en relación con las operaciones de generación de claves.
        - CEN CWA 14167-4 (2003): “Cryptographic module for CSP signing operations - Protection profile - CMCSO PP”, en relación con las operaciones de firma de certificacos y otros documentos.

    - FIPS 140-2, nivel 3 o superior.

- Tarjetas y otros dispositivos criptográficos móviles, y software criptográfico:

    - FIPS 140-2, nivel 3 o superior.

    - ISO 15408 (2005): “Information technology – Security techniques - Evaluation criteria for IT security”, nivel EAL 4 o superior, de acuerdo con un objetivo de evaluación o perfil de protección adecuado al análisis de riesgo realizado.

      En concreto, se consideran adecuados los siguientes perfiles de protección:

        - CEN CWA 14169 (2004): “Secure signature-creation devices “EAL 4+”, en relación con los dispositivos de firma electrónica.
        - CEN CWA 14365-2 (2004): “Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices”, en relación con el software de firma electrónica.

En la definición de la infraestructura se deben incluir los siguientes aspectos:

- Identificación detallada de aplicaciones y servicios específicos que necesitan servicios criptográficos.
- Identificación del catálogo de requisitos criptográficos, que debe garantizar el cumplimiento de esta instrucción general. Se debe considerar de forma particular:

    - El volumen de operaciones y la topología de red interna, a efectos del cálculo del número de equipamientos criptográficos necesarios.
    - El análisis del cifrado para la protección de informaciones sensibles en tránsito o que se encuentren fuera de las instalaciones de la Administración Pública (transportadas mediante dispositivos móviles, con medios o dispositivos que se pueden remover o por líneas de comunicación).
    - El análisis del impacto del uso de la criptografía sobre los controles basados en la inspección de contenidos, como por ejemplo los programas antivirus.

- Desarrollo de una especificación de gestión de claves, que debe describir los componentes de gestión de claves requeridos para operar los dispositivos y aplicaciones criptográficas durante su ciclo de vida. Su contenido debe considerar:

    - La aplicación criptográfica para los dispositivos criptográficos
    - El entorno de comunicaciones de los dispositivos criptográficos
    - Los requisitos de los componentes de gestión de claves de los dispositivos criptográficos.
    - La distribución de los componentes de gestión de claves de los dispositivos criptográficos.
    - El control de acceso a los dispositivos criptográficos.
    - El registro de actividades relativa a gestión de claves para los dispositivos criptográficos.
    - La gestión de compromisos y recuperación de los dispositivos criptográficos.
    - La recuperación de claves.

4.6. Cumplimiento normativo

Los servicios criptográficos se deben utilizar de acuerdo con la legislación vigente en cada momento, y en concreto, de acuerdo con los siguientes aspectos:

- Se deben aplicar los controles de seguridad criptográficos establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y en las Guías de desarrollo que dicte en Centro Criptológico

Nacional, adscrito al Centro Nacional de Inteligencia, de acuerdo con lo establecido en la Ley 11/2002, de 6 de mayo y el Real Decreto 421/2004, de 12 de marzo, que la desarrolla.

- Se deben evaluar y cumplir las posibles restricciones sobre la importación y/o exportación de hardware y software que ejecuta operaciones criptográficas, de acuerdo con lo que determina el Reglamento (CE) nº 1334/2000 del Consejo, de 22 de junio de 2000, por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnología de doble uso.

- Se debe evaluar y cumplir las posibles restricciones sobre la importación y/o exportación de hardware y software diseñado para que se le incorporen funciones criptográficas, de acuerdo con lo que determina el Reglamento (CE) nº 1334/2000 del Consejo, de 22 de junio de 2000, por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnología de doble uso.

- Se deben evaluar y cumplir las posibles restricciones sobre el uso del cifrado. En ningún caso se pueden almacenar claves privada utilizadas para generar firmas digitales, de acuerdo con lo que determina la Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Se deben evaluar los métodos obligatorios que permiten a las autoridades públicas el acceso a informaciones cifradas, utilizando hardware o software para garantizar la confidencialidad, de acuerdo con lo que determina la Ley 27/2008, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

5. Roles y responsabilidades en relación con la criptografía

La unidad administrativa responsable para la implementación de esta instrucción general es [_____].

La unidad administrativa responsable para la gestión de claves, incluyendo la generación de claves y la operación de la infraestructura criptográfica es [_____]. Esta unidad puede delegar en otras unidades internas o externas, hasta en empresas, los aspectos de gestión de claves que se encuentren justificados.

La unidad administrativa responsable para la auditoría de las políticas y operaciones criptográficas es [_____]