Política de seguridad criptográfica de la Universitat Oberta de Catalunya

Texto aprobado por el Comité de Dirección Ejecutivo el 5 de febrero de 2015, actuando por delegación del Consejo de Gobierno

Universitat Oberta de Catalunya

SUMARIO

I. Introducción

Este documento contiene las normas de seguridad criptográfica aplicables a los sistemas de información que ofrecen apoyo a procedimientos académicos y de gestión electrónicos de la Universitat Oberta de Catalunya (UOC).

Una política de seguridad criptográfica es un documento que especifica normas de uso en relación con la criptografía, e incluye estándares para su implantación en la organización. Algunos de los usos de la criptografía incluyen los mecanismos de autenticación, firma electrónica e irrefutabilidad, confidencialidad o integridad.

Esta política es conforme con los requisitos de seguridad y proporcionalidad correspondientes a los sistemas electrónicos de apoyo a procedimientos administrativos, establecidos en las normas que regulan el uso de los medios electrónicos en los servicios públicos.

Los contenidos de esta política de seguridad criptográfica se han estructurado para cubrir los controles previstos en la norma internacional ISO/IEC 27002:2006 y las recomendaciones contenidas en las Guías de Seguridad de las TIC CCN-STIC-405 y CCN-STIC-807 del Centro Criptológico Nacional.

II. Contenidos generales de la Política de seguridad criptográfica

1. Identificación

Esta política de seguridad criptográfica se identifica con el siguiente identificador de objeto (OID): 1.3.6.1.4.1.43653.1.1.

2. Fecha de emisión

Esta política ha sido emitida en fecha de 5 de febrero de 2015, momento a partir del cual entrará en vigor.

3. Identificación del emisor de la Política de seguridad criptográfica

Esta política ha sido emitida por el Comité de Dirección Ejecutivo, actuando por delegación del Consejo de Gobierno de acuerdo con lo establecido en el artículo 13.2 de las NOF (Acuerdo GOV /140/2010, de 3 de agosto), el artículo 4 del Reglamento del Consejo de Gobierno y el Acuerdo de Consejo de Gobierno de 15 de julio de 2013.

4. Ámbito de aplicación de la Política de seguridad criptográfica

Esta política es aplicable a todos los sistemas de información de apoyo a procedimientos y actividades académicos y de gestión electrónicos, y también a las relaciones por medios electrónicos con terceros que no forman parte de la comunidad universitaria.

III. Utilización de la criptografía en la UOC

1. Servicios de seguridad basados en criptografía

La UOC empleará 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 usan los algoritmos criptográficos aprobados en esta política.

Las normativas de desarrollo de esta política deben indicar la aplicación de criptografía en cada caso y escenario concretos:

- Firma electrónica
- Autenticación electrónica
- Cifrado
- Prueba electrónica

2. Algoritmos criptográficos aprobados

Los algoritmos criptográficos aprobados para el uso por la UOC son los siguientes.

- Algoritmos de resumen aprobados

  - SHA-1,[1] 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».

    SHA-1 es el algoritmo más usado actualmente, aunque se recomienda no utilizarlo, siempre que la infraestructura tecnológica lo permita.

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

  - SHA-256,[3] 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».

[1]Sección 1.2.1k) CCN STIC 807

[2]Sección 1.2.1 k) CCN STIC 807

- SHA-384,[4] definido en la norma FIPS 180-2 (2002): «Secure Hash Standard».
- SHA-512,[5] definido en la norma FIPS 180-2 (2002): «Secure Hash Standard».

- Algoritmos simétricos aprobados

  - AES,[6] definido en la norma FIPS 197 (2001): «Specification for the Advanced Encryption Standard (AES)».
  - TDEA[7] (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 emplear 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,[8] definido en la especificación técnica IETF RFC 3447 (2003): «Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1».
  - DSA,[9] 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,[10] en sus dos variantes E(Fp) y 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».
  - EC-GDSA, en sus dos variantes E(Fp) y E(F2m), definido en la norma internacional ISO/IEC 15946-2 (2002): «Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures».

- 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».

---

[3]Sección 1.2.1 k) CCN STIC 807
[4]Sección 1.2.1 k) CCN STIC 807
[5]Sección 1.2.1 k) CCN STIC 807
[6]Sección 1.2.1 b) CNN STIC 807
[7]Sección 1.2.1 a) CNN STIC 807
[8]Sección 1.2.1 i) CNN STIC 807
[9]Sección 1.2.1 g) CNN STIC 807
[10] Sección 1.2.1 h) CNN STIC 807

- Algoritmo de transporte de claves RSA.

- Algoritmos de envoltura de claves con clave simétrica.

3. Requisitos de protección de claves criptográficas

Las claves criptográficas deben estar disponibles operativamente tanto tiempo como lo requiera el servicio criptográfico correspondiente. Las claves pueden mantenerse en un equipamiento criptográfico mientras se utilizan, o pueden almacenarse de manera externa —con las medidas de seguridad adecuadas— y recuperarlas cuando sea necesario.

Además, algunas de las claves se archivarán durante un plazo superior al inicialmente previsto para el uso del 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
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 de envoltura 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 envueltas no necesiten protección, el más largo de los dos períodos
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 períodos
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	Validez	Desde su generación hasta la finalización del período de su validez criptográfica

			Clave privada de transporte de claves		
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 períodos
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 períodos
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 períodos
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
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

4. Requisitos de protección de otro 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 privadas y públicas	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 período 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 procesados en relación con valores únicos de mensaje	Desde su generación hasta que no sean necesarios para procesar datos que dependen de ellos
Resultados intermedios	Soporte	Confidencialidad Integridad	Uso o aplicación	Desde su generación hasta que no sean necesarios, momento en el que tienen que destruirse

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 del uso)	No aplica	Desde su generación hasta que no sea necesario, momento en el que tiene que destruirse
Contraseña	Autenticación	Integridad Confidencialidad	Uso o aplicación Entidad propietaria	Desde su generación hasta que sea sustituida o no sea necesaria para autenticar a la entidad
Información de auditoría	Soporte	Archivo Integridad Autorización de acceso	Eventos auditados Información de control de claves	Desde su generación hasta que no sea necesaria

5. Métodos de protección de seguridad

Las dos tablas anteriores determinan diversas protecciones de seguridad con relación a 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 está en tránsito como cuando está 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 el apartado 5 del punto IV de este documento.

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 el traslado a localizaciones diferentes del lugar de operación. Algunos ejemplos son las claves certificadas 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 manera definitiva en un tercer proveedor de seguridad.

La protección de la integridad de información criptográfica en tránsito debe conseguirse mediante alguno de los siguientes mecanismos:

- En caso de distribución manual, con protección física, puede emplearse 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 a lo que estaba previsto recibir.

Ejemplo: la integridad de una clave privada de firma electrónica reconocida de una persona se garantiza, durante su tránsito, por la protección física de la tarjeta criptográfica que la contiene.

- En caso de distribución electrónica, puede emplearse un mecanismo MAC o de firma digital, sobre la información criptográfica o sobre el mensaje que la transporta, o comprobar que el formato de la información criptográfica recibida corresponde a lo que estaba previsto recibir.

  Ejemplo: la integridad de una clave pública de sello electrónico 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 información criptográfica en tránsito debe conseguirse 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 política 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 su tránsito, para la protección física de la tarjeta criptográfica que la contiene.

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

  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 UOC tiene que hacer lo siguiente:

- No emplear 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.

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

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

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

- Mecanismos físicos, incluyendo el uso de hardware criptográfico validado, de acuerdo con lo dispuesto en el apartado 5 del punto IV de esta política; de ordenadores que no estén conectados a otros sistemas, o depósitos físicos para proteger dispositivos o soportes (como una caja fuerte).

- 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 emplear.

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

- Cifrado de la información utilizando un algoritmo aprobado de acuerdo con esta política, en un hardware criptográfico validado, de acuerdo con lo dispuesto en el apartado 5 del punto IV de esta política.

- Uso de hardware criptográfico validado, de acuerdo con lo dispuesto en el apartado 5 del punto IV de esta política.

- Sistema de almacenamiento físico seguro, con garantía de control de acceso al depósito.

IV. Criterios para el uso de la criptografía

Los servicios criptográficos deben emplearse de acuerdo con las siguientes normas:

- Desarrollo de la Política
- Separación del uso de claves
- Establecimiento de plazos de duración de las claves
- Establecimiento de procedimientos de gestión de claves
- Establecimiento de estándares de implantación de tecnología criptográfica
- Cumplimiento normativo

1. Desarrollo de la Política

Corresponde la aprobación de la Política de seguridad criptográfica al Consejo de Gobierno de la UOC, siendo responsable la Secretaría General.

Esta política de seguridad criptográfica debe desarrollarse mediante las siguientes normativas:

- Política de gestión de claves criptográficas de la UOC
- Política de certificación de la UOC
- Política de autenticación de la UOC
- Política de firma electrónica de la UOC
- Política de cifrado de la UOC

Corresponde al Área de Tecnología de la UOC el desarrollo de la Política de seguridad criptográfica por medio de los instrumentos indicados.

2. Separación del uso de claves

De manera general, una clave solo se utilizará para un uso concreto —por ejemplo, firma electrónica, cifrado de datos o autenticación, etc.— por los siguientes motivos:

- El uso de una misma clave 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 puede utilizarse, de acuerdo con esta directriz, para servicios de integridad, autenticidad e irrefutabilidad.

Se permite de manera expresa el uso de la clave privada para solicitar la certificación digital de la correspondiente clave pública a una entidad de certificación.

3. Plazos de duración de las claves

De manera general, una clave se utilizará durante un plazo concreto, o período criptográfico, por los motivos siguientes:

- Se limita la cantidad de información protegida por una clave que está disponible por 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 puede comprometerse 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	1-4 años	
Clave pública de firma	Varios años (depende de la longitud de la clave)	
Clave simétrica de autenticación	Hasta 2 años	Hasta 3 años adicionales
Clave privada de autenticación	1-4 años	
Clave pública de autenticación	1-4 años	
Clave simétrica de cifrado de datos	Hasta 2 años	Hasta 3 años adicionales
Clave simétrica de envoltura 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
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 de aplicación, debe hacerse un análisis de riesgo, considerando los siguientes factores:

- La fortaleza de los mecanismos criptográficos empleados
- La protección de los mecanismos empleando 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 que hay que 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

Hay que considerar también de manera 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. Procedimientos de gestión de las claves

Se establecerán 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. Almacenamiento de claves, incluyendo cómo obtienen acceso a las claves los usuarios autorizados.
- Cambio o actualización de claves, incluyendo normas sobre cuándo deben cambiarse o actualizarse, y cuál 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 la gestión de claves.

Deben definirse períodos de activación y desactivación de las claves para reducir el riesgo de compromiso, de modo que las claves solo puedan utilizarse durante un plazo concreto, de acuerdo con las circunstancias y el análisis de riesgo.

Deben definirse procedimientos para garantizar la autenticidad de las claves públicas, mediante el uso de las entidades de certificación que sean adecuadas.

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

5. Estándares de implantación de tecnología criptográfica

Debe definirse e implantarse una infraestructura común y adecuada de tecnología criptográfica que preste servicios criptográficos identificados en esta política a las diferentes aplicaciones de la UOC, considerando al menos las siguientes.

- La sede electrónica de la UOC.
- La realización de actos automatizados basados en el uso de sellos de la UOC y de sus órganos.
- La realización de actos manuales y otras acciones que tengan plasmación documental, por parte del personal de la UOC cuando utilicen firma electrónica.
- 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 llevado a cabo.

      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 operaciones 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 certificados 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 llevado a cabo.

    En concreto, se consideran adecuados los 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 deben incluirse 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 política. Debe considerarse de manera particular lo siguiente.
  - El volumen de operaciones y la topología de red interna, a efectos del cálculo del número de equipos criptográficos necesarios.
  - El análisis del cifrado para la protección de informaciones sensibles en tránsito o que estén fuera de las instalaciones de la UOC (transportadas mediante dispositivos móviles, con medios o dispositivos que pueden extraerse 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 las aplicaciones criptográficas durante su ciclo de vida. Su contenido debe considerar lo siguiente.
  - 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 relativas a la gestión de claves de los dispositivos criptográficos
  - La gestión de compromisos y recuperación de los dispositivos criptográficos
  - La recuperación de claves

6. Cumplimiento normativo

Los servicios criptográficos tienen que emplearse de acuerdo con la legislación vigente en cada momento.

V. Roles y responsabilidades en relación con la criptografía

El responsable para la implantación de esta política es el Área de Tecnología de la UOC.

El responsable para la gestión de claves, incluyendo la generación de claves y la operación de la infraestructura criptográfica es el responsable de seguridad. Este puede delegar en otras unidades internas o externas, incluso en empresas, los aspectos de gestión de claves que estén justificados.