POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

0. INTRODUCCIÓN

1. Según la definición del 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, una política de firma electrónica y de certificados es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, se verifican y se gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma».

2. Con carácter general, una política de firma electrónica es un documento legal que contiene una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal), definiendo las reglas y obligaciones de todos los actores involucrados en el proceso. El objetivo es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que debe incluir la persona firmante en el proceso de generación de la firma y la información que se debe comprobar en el proceso de validación de la misma.

3. El artículo 18 del citado Real decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, establece que las administraciones públicas aprobarán y publicarán una política de firma electrónica y de certificados partiendo de la norma técnica aprobada por la Resolución de 19 de julio de 2011 (BOE de 30 de julio) de la Secretaría de Estado para la Función Pública.

4. En desarrollo de dicha norma, con fecha 30 de mayo de 2012, la Comisión Permanente del Consejo Superior de Administración Electrónica aprobó la versión 1.9 de la política de firma electrónica y de certificados (OID 2.16.724.1.3.1.1.2.1.9).

5. Posteriormente, el *Boletín Oficial del Estado* número 299, de 13 de diciembre, recogió la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la política de firma electrónica y de certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.

6. En este contexto normativo, la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados de la Administración General del Estado, aprobada por la Resolución de 19 de julio de 2011 de la Secretaría de Estado para la Función Pública, en su sección II.5 sobre interacción con otras políticas, establece que «cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente».

1. POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS

1.1 Adhesión a la política de firma electrónica y de certificados de la Administración General del Estado

Examinada la política de firma electrónica y de certificados de la Administración General del Estado, se considera que es coherente con la normativa de administración electrónica de la Universidad Miguel Hernández, en adelante UMH, y plenamente asumible en sus aspectos técnicos, por lo que, con su adopción, la UMH pretende dar un paso claro para favorecer la interoperabilidad entre administraciones públicas, lo que redundará de una manera inmediata en la simplificación de trámites para los ciudadanos.

Por todo ello, la Universidad Miguel Hernández de Elche adoptará, como política de firma electrónica y de certificados, la política de firma electrónica y de certificados de la Administración General del Estado, de fecha 29 de noviembre de 2012 y publicada en el BOE de 13 de diciembre de 2012, (OID 2.16.724.1.3.1.1.2.1.9) con las especificidades que se indican en los anexos incorporados a esta política.

1.2 Período de validez

La presente Política de firma electrónica y de certificados entrará en vigor en la fecha de entrada en vigor del Reglamento de Administración Electrónica de la UMH y será válida mientras no sea sustituida o derogada por una política posterior.

Aquellos aspectos que puedan ser actualizables automáticamente serán incluidos en anexos incorporados al presente documento y actualizables, previa aprobación de la Comisión Técnica de Administración Electrónica de la UMH, por el gestor del documento sin necesidad de que sea sustituido por una nueva versión.

1.3 Identificador del gestor de la Política

Nombre del gestor	Servicio de Innovación y Planificación Tecnológica
Dirección de contacto	sipt@umh.es
Identificador del gestor[1]	U05500145

[1] Código extraído del Directorio Común de Unidades Orgánicas y Oficinas (DIR3).

2. Anexos

ANEXO 1. Formatos admitidos

La Universidad Miguel Hernández empleará los formatos admitidos en la política de firma electrónica y de certificados de la Administración general del Estado según los siguientes criterios:

(i) El uso obligatorio de la firma electrónica con formato XAdES-T para todos los documentos generados por actuaciones administrativas automatizadas y para todos los documentos generados por el personal de la administración, salvo restricciones de formato o por la utilización de otros estándares de interoperabilidad ya establecidos.

(ii) El uso obligatorio del formato PDF con firma electrónica PAdES para todas las copias de documentos (con cambio de formato) que tengan como destinatarios a ciudadanos u otras administraciones públicas, salvo restricciones de formato o por la utilización de otros estándares de interoperabilidad ya establecidos.

(iii) El uso del formato CAdES solo en aquellos supuestos en los que aspectos relacionados con el volumen de los ficheros o el rendimiento de los sistemas que los gestionan desaconsejen el uso de los formatos PAdES y XAdES.

ANEXO 2. Algoritmo de firma

Respecto a la recomendación establecida en el apartado 3.6 «Reglas de uso algoritmos» de la política de la Administración General del Estado, la Universidad Miguel Hernández de Elche determina que para la creación de la firma electrónica se utilizará el algoritmo de firma RSA/SHA2, con un hash mínimo de 256 bits (RSA/SHA2-256 o RSA /SHA2-512). En el caso de documentos de archivo y custodia se deberá utilizar el algoritmo de firma RSA/SHA2, con un hash mínimo de 512 bits (RSA/SHA2-512).

ANEXO 3. Validez y preservación de la firma

Para garantizar la validez jurídica de las firmas, proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo de validez, la Universidad Miguel Hernández de Elche seguirá las recomendaciones establecidas en la política de la Administración General del Estado, con las siguientes especificaciones:

1) Promoción a firmas longevas

(i) En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.

(ii) Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:

a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.

b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.

(iii) Al menos, deberán sellarse las referencias a los certificados y a las informaciones de estado.

(iv) En caso de almacenar los certificados y las informaciones de estado dentro de la firma se sellarán también estas informaciones, siguiendo las modalidades de firmas AdES –X o -A.

El sistema de gestión de expedientes convertirá la firma de los documentos electrónicos que formen parte de un expediente electrónico a formatos longevos antes de su archivo definitivo.

Aquellos documentos electrónicos que presenten una firma no válida, no pueda validarse la misma o no estén firmados:

(i) Se firmarán con formato XAdES utilizando el certificado digital del tramitador que incorpore el documento al sistema de gestión de expedientes. La firma se promocionará a formato longevo.

(ii) Si no se ha podido evidenciar la validez jurídica del documento, deberá consignarse el metadato obligatorio "Estado de elaboración" con el valor EE99 (Otros).
En cualquier caso, se consignará un metadato adicional indicando el motivo de la validación y las circunstancias que han llevado a firmarlo.

2) Proceso de resellado

Se aplicará un mecanismo de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.

Partiremos, tal y como se ha establecido en el punto anterior, del supuesto de que los documentos tendrán ya una firma del tipo longeva.

Sobre estas firmas se incorporará un nuevo sello de tiempo que estará ya generado con un certificado reciente, con un periodo de validez superior al actual en la firma a resellar, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.