



SECRETARIA GENERAL

Acuerdo de aprobación de la Política de firma electrónica y de certificados de la Universidad Miguel Hernández de Elche.

Vista la propuesta que formula el Vicerrector de Infraestructuras de la Universidad, **el Consejo de Gobierno, reunido en sesión de 25 de mayo de 2016, ACUERDA:**

Aprobar la Política de firma electrónica y de certificados de la Universidad Miguel Hernández de Elche, en los términos reflejados a continuación:

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

- 0. INTRODUCCIÓN
- 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
 - 1.2 Período de validez
 - 1.3 Identificador del gestor de la Política
- 2. Anexos
 - ANEXO 1. Formatos admitidos
 - ANEXO 2. Algoritmo de firma

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).



SECRETARIA GENERAL

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	Servicios Informáticos
Dirección de contacto	servicios.informaticos@umh.es
Identificador del gestor ¹	U05500058

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



SECRETARIA GENERAL

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).