I. DISPOSICIONES Y ACUERDOS GENERALES

I.2. Consejo de Gobierno

Acuerdo 5.1/CG 23-5-17, por el que se aprueba la Política de firma y sello electrónicos y de certificados.

Acuerdo 5.1/CG 23-5-17, por el que se conviene, por asentimiento, aprobar la Política de firma y sello electrónicos y de certificados, en los términos del documento que se anexa.

ANEXO

POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS

Índice

1. Introducción.

2. Propuesta de Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla.

1. 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 establecida a tal efecto en la disposición adicional primera. En particular, la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración se aprobó mediante Resolución de 19 de julio de 2011 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. Por Resolución de 27 de octubre de 2016 de la Secretaría de Estado para la Función Pública ha sido aprobada la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración General del Estado, que entiende que la definición de política de firma establecida en el Esquema Nacional de Interoperabilidad es también aplicable a los sellos electrónicos.

   Por otra parte, 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». Esta Norma ya cumple con el Reglamento (UE) Nº 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS).

7. Examinada la Política de Firma Electrónica y de certificados de la Administración General del Estado, se considera que es coherente con el ordenamiento de la Universidad de Sevilla y plenamente asumible en sus aspectos técnicos, por lo que, con su adopción, la Universidad de Sevilla pretende dar un paso claro para favorecer la interoperabilidad entre Administraciones Públicas.

La Universidad de Sevilla tiene en cuenta también las especificaciones de la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónico y de Certificados de la Administración, aprobada por Resolución de 27 de octubre de 2016, de la Secretaría de Estado de la Función Pública, que sustituye la anterior Norma técnica de 2011.

La adopción de la Política de Firma Electrónica y Certificados de la Administración del Estado[1] simplifica la relación de la Universidad de Sevilla con otras administraciones y da seguridad jurídica a los interesados.

2. Propuesta de Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla

Teniendo en cuenta lo anterior, se propone el siguiente articulado para la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla, acompañada de un anexo para Reglas particulares de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla:

Primero. — Aprobación de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla.

1. Aprobar la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla, adoptando la Política de firma electrónica y de certificados de la Administración General del Estado (OID 2.16.724.1.3.1.1.2.1.9).

2. Aprobar las Reglas particulares de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla que podrán ser modificadas mediante Resolución Rectoral a propuesta de la Comisión de Administración Electrónica, salvo aquellos aspectos que puedan ser actualizables automáticamente. Estos aspectos serán incluidos en anexos incorporados al presente documento y actualizados, previa aprobación de la Comisión de Administración Electrónica de la Universidad de Sevilla, por el gestor de la Política sin necesidad de que sea sustituido por una nueva versión.

Segundo. — Ámbito de aplicación.

La Política de Firma y Sello electrónicos y de Certificados aprobada será de aplicación, en el ámbito competencial de la Universidad de Sevilla, a los siguientes casos:

1 https://sede.administracion.gob.es/PAG_Sede/dms/sedePAG/documentos/politica_de_firma_anexo_1.pdf

a. Las relaciones electrónicas entre la Universidad de Sevilla y los ciudadanos (miembros o no de la Comunidad Universitaria) y proveedores, en todos los servicios y procedimientos puestos a su disposición en la sede electrónica, siempre que sea obligada o se permita la firma electrónica con certificado digital.
b. Las relaciones electrónicas entre las distintas unidades y empleados de la Universidad de Sevilla, siempre que sea obligada o se permita la firma electrónica con certificado digital.
c. Las relaciones electrónicas de la Universidad de Sevilla con el resto de Administraciones y entidades públicas y privadas.

Tercero. — Identificador del gestor de la Política.

Nombre del gestor	Vicerrectorado de Desarrollo Digital y Evaluación
Dirección de contacto	Rectorado, C/San Fernando s/n
Identificador del gestor[1]	U01700190

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

Cuarto. — Atribuciones del gestor de la Política.

1. Adoptará las medidas y dictará las instrucciones necesarias para el desarrollo, ejecución y aplicación de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla.
2. Será responsable del mantenimiento, actualización y publicación electrónica de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla.

Quinto. — Adaptación de los sistemas existentes.

Los sistemas de información existentes que requieran adaptaciones específicas dispondrán de un plazo de 18 meses para efectuarlas y dar cumplimiento a lo dispuesto en esta resolución.

Sexto. — Efectos

La presente Política de Firma y Sello electrónicos y de Certificados surtirá efectos a partir del día siguiente de su publicación en el Boletín Oficial de la Universidad de Sevilla y será válida mientras no sea sustituida o derogada por otra política.

Séptimo. — Cita en género femenino de los preceptos de esta Política

La referencia a personas, colectivos o cargos académicos, figuran en la presente Política en género masculino como género gramatical no marcado. Cuando proceda, será válida la cita de los preceptos correspondientes en género femenino.

Anexo: Reglas particulares de la Política de Firma y Sello Electrónicos y de Certificados de la Universidad de Sevilla.

Índice

1. Formatos admitidos.
2. Algoritmo de firma.
3. Certificados admitidos.
4. Tipos de certificados.
5. Certificados de empleado público.

6. Certificado de persona física representante de persona jurídica.

7. Certificados de sede.

8. Certificados de sello electrónico.

9. Sellos de tiempo.

10. Condiciones para salvaguardar la validez de las firmas.

1. Formatos admitidos.

La Universidad de Sevilla empleará los formatos admitidos en la Política de firma y sello electrónicos y de certificados de la Administración general del Estado según los siguientes criterios:

a. El uso preferente de la firma electr ónica 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.
b. El uso obligatorio del formato PDF con firma electrónica PAdES para todos los documentos que tengan como destinatarios a ciudadanos u otras administraciones públicas.
c. 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.

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 de Sevilla 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).

3. Sistemas admitidos para la identificación y firma.

En general se admitirán los sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica y de sello electrónico expedidos por prestadores incluidos en "la lista de confianza de prestadores de servicios de certificación".

La Universidad de Sevilla, en aplicación del principio de proporcionalidad, podrá habilitar sistemas de identificación y firma no basados en el uso de certificados electrónicos reconocidos o cualificados para aquellos trámites administrativos en los que en función de los datos e intereses afectados así se establezcan. En el caso de habilitarse como sistema de firma éste deberá permitir la acreditación de la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

Con el fin de garantizar la interoperabilidad así como para asegurar la integridad, inalterabilidad y el no repudio de los documentos firmados, la US podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.

La Universidad de Sevilla podrá determinar si admite sólo alguno de estos sistemas para realizar determinados trámites.

4. Tipos de certificados.

Se definen las instrucciones de uso general de las distintas tipologías de certificados, en uso de la facultad otorgada a la Universidad de Sevilla dentro de su ámbito de competencias.

Partiendo del documento "Plataforma @Firma. Cambios asociados al reglamento eIDAS" disponible en el Portal de Administración Electrónica (PAE), serán admitidos todos los certificados relacionados en el documento a excepción de los clasificados en el punto 2 (No reconocidos) y que pueden incluir certificados de persona física, de componente y SSL. Igualmente, los certificados clasificados a extinguir se seguirán manteniendo hasta su caducidad o revocación.

Los sistemas de información y servicios electrónicos de la Universidad de Sevilla deberán aceptar y adaptarse a los nuevos tipos de certificados, ya que es posible que reciban certificados con las nuevas clasificaciones. Dicha adaptación deberá ser valorada por la Comisión de Administración Electrónica y su aplicación se ajustará a la normativa de aplicación a este anexo.

5. Certificados de empleado público.

Mediante Resolución Rectoral se procedimentará en qué casos se usará este tipo de certificados.

Las solicitudes de certificados de empleado público para la Universidad de Sevilla se gestionarán través del Vicerrectorado competente en materia de tecnologías de la información y las comunicaciones (en adelante Vicerrectorado TIC), que será el encargado de recibir la solicitud y coordinar la tramitación con el proveedor del certificado. La solicitud deberá incluir el nombre del titular al que se asigna el certificado, su cargo, el tipo de certificado, los motivos de la petición y el uso previsto.

Las solicitudes se canalizarán a través de los miembros del Consejo de Dirección o Decanatos correspondientes, siendo los encargados de la solicitud de nuevos certificados, y de la petición de su renovación o revocación. Estas solicitudes se dirigirán al Vicerrectorado TIC. Esta obligación deberá tenerse en cuenta especialmente durante los procesos de ceses y nombramientos de cargos vinculados a las modificaciones de las estructuras orgánicas, puesto que en los certificados de este personal figura su cargo.

El Vicerrectorado TIC será responsable del Registro de los certificados que adquiera, gestione y custodie, con el objetivo de controlar de forma exhaustiva su uso.

6. Certificado de persona física representante de persona jurídica.

Mediante Resolución Rectoral se procedimentará en qué casos se usará este tipo de certificado. Las solicitudes de certificados de persona física representante de persona jurídica se gestionarán a través del Vicerrectorado competente en materia de tecnologías de la información y las comunicaciones, que será el encargado de recibir la solicitud y coordinar la tramitación con el proveedor del certificado. La solicitud deberá incluir el nombre de la persona física a la que se le asigna la representación y los motivos de la petición. Se llevará un Registro de este tipo de certificados.

7. Certificados de sede.

En la Universidad de Sevilla los certificados de sede electrónica sólo podrán utilizarse para la identificación de la sede electrónica. De esta forma, queda prohibido su uso para la firma de contenido de documentos electrónicos.

Para la correcta identificación de la sede electrónica, el certificado deberá hacer referencia al nombre “sede.us.es”

8. Certificados de sello electrónico.

Los certificados de sello electrónico se utilizarán exclusivamente para la actuación administrativa automatizada definida en la normativa vigente.

La creación de sellos electrónicos se realizará mediante resolución de Secretaria General y se publicará en la sede electrónica.

El Vicerrectorado TIC será el encargado de gestionar y coordinar la tramitación con el proveedor del certificado. Los certificados se anotarán en un Registro que deberá incluir el Órgano titular del certificado de sello, el nombre de la persona titular del mismo, los motivos de la petición, el uso previsto y la resolución de creación.

Para nuevas actuaciones de los certificados de sello electrónico aprobados, la Secretaría General deberá enviar al Vicerrectorado TIC la aprobación, indicando la actuación específica que se realizará, sus principales características así como la propuesta de modificación de la resolución que afecta al sello.

Secretaría General comunicará la necesidad de renovación o revocación de los certificados existentes a Vicerrectorado TIC. A partir de esa comunicación el Vicerrectorado TIC procederá a gestionar con la entidad certificadora su renovación o revocación.

9. Sellos de tiempo.

La Universidad de Sevilla deberá según la normativa de aplicación asociar a los documentos administrativos firmados con certificados electrónicos una de las siguientes modalidades de referencia temporal:

a. "Marca de tiempo" entendiendo como tal la asignación de medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.
b. "Sello de tiempo", entendiendo por tal 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.

Para ello en la Universidad de Sevilla se tomará como autoridad de sellado de tiempo (TSA) corporativa, la plataforma de Sellado de Tiempo TS@ de @firma (en su versión basada en servicios web) ofrecida por el actual Ministerio de Hacienda y Administraciones Públicas y accesible a través de la red SARA.

La utilización de sellos de tiempo prevendrá de la posibilidad de repudio posterior. Los casos en los que se debe aplicar un sello de tiempo a la actuación administrativa son:

1. Cuando lo establezca una norma de rango legal o reglamentaria.
2. Cuando así esté definido para el procedimiento administrativo de que se trate.
3. Cuando el sistema afectado esté clasificado como de nivel alto según el Esquema Nacional de Seguridad.

10. Condiciones para salvaguardar la validez de las firmas.

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características a lo largo del tiempo, se deberán seguir los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas de tipo CAdES, XAdES o PAdES:

- Las plataformas de firma electrónica adoptadas en el ámbito de la Universidad de Sevilla deberán disponer de mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo utilizando un algoritmo robusto en el momento de ser firmado.
- Los sistemas de información deberán contemplar las funcionalidades necesarias para garantizar la validez en el tiempo de los documentos firmados por el sistema hasta su archivo. Para ello se tendrá en cuenta lo establecido en la Política de Gestión de Documentos Electrónicos y el

Esquema Nacional de Interoperabilidad para la transferencia de documentos y expedientes al Sistema de Información y Gestión de Archivos de la Universidad de Sevilla.

- Se almacenarán los documentos firmados con los formatos de firma mencionados en el presente anexo.
- La Política de Gestión de Documentos Electrónicos de la Universidad de Sevilla establecerá los criterios de archivo y custodia aplicable a los documentos, con independencia de su formato electrónico o físico.
- El tratamiento de los documentos y sus firmas podrán ser auditados en el marco del cumplimiento del Esquema Nacional de Seguridad.
- El almacenamiento de los certificados y las informaciones de estado se realizará en un depósito específico en el entorno de gestión de documentos, debidamente relacionados. Se incluirán metadatos específicos adecuados a la fase de conservación en que se encuentren. Asimismo, podrán producirse procesos de conversión o migración de formatos de documentos para preservar su longevidad.
- Todo documento que salga del entorno seguro de administración de documentos, para que mantenga su validez jurídica en el tiempo, deberá incluir una firma electrónica con sellado de tiempo con carácter de copia auténtica del original.

***