Universidad Rey Juan Carlos

BOLETÍN OFICIAL DE LA UNIVERSIDAD REY JUAN CARLOS

UNIVERSIDAD REY JUAN CARLOS

Política de identificación firma y sello de la Universidad Rey Juan Carlos, aprobada por acuerdo del Consejo de Gobierno de la Universidad, en sesión celebrada el 25 de junio de 2021.

Texto de la Normativa en documento Anexo.

POLÍTICA DE IDENTIFICACIÓN FIRMA Y SELLO DE LA UNIVERSIDAD REY JUAN CARLOS

INTRODUCCIÓN

El 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 explica, en su primer punto, como *la finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.*

Asimismo, en su Capítulo IX, trata sobre la firma electrónica y sus certificados y, en el art. 18 establece:

2. Las Administraciones públicas aprobarán y publicarán su política de firma electrónica y de certificados partiendo de la norma técnica establecida a tal efecto en disposición adicional primera, que podrá convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto.

Esta política será aprobada por el Consejo de Gobierno de la Universidad y entrará en vigor al día siguiente de su publicación en el BOURJC.

Los anexos adjuntos: **ANEXO I, Las políticas de identificación y firma electrónica; ANEXO II, Política de firma manuscrita capturada electrónicamente; ANEXO III, Política de identificación y firma electrónica basada en medios no criptográficos y ANEXO IV, Política de sello electrónico avanzado de actuación automatizada basada en código seguro de verificación**, considerando su alta carga técnica y siendo susceptibles de cambios dados los avances en esta materia, requerirán, para su modificación, de la Resolución Rectoral.

Con estas referencias y atendiendo a la obligación por parte de las administraciones de contar con la política referida a la identificación, firma y sello, es por lo que nuestra Universidad redacta y aprueba el presente documento que pretende contener las directrices de firma electrónica en relación con los documentos de procedimientos administrativos, académicos y de gestión electrónicos de la Universidad Rey Juan Carlos (en lo sucesivo, URJC).

Este documento es una política de firma electrónica de acuerdo con el artículo 18.2 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, y ha sido producida de acuerdo con los requisitos de la Norma Técnica de Interoperabilidad "Política de firma electrónica y de certificados de la Administración".

Este documento contiene las instrucciones de identificación y firma electrónica dictadas por el Consejo de Gobierno de la Universidad, en aplicación de aquello dispuesto en las siguientes normas jurídicas:

- Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones en el mercado interior, y por la que se deroga la Directiva 1999/93/CE.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley 4/1998, de 8 de abril, de Coordinación Universitaria de la Comunidad de Madrid.
- 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.
- Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, de 27 de octubre de 2016.
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

En el marco de aquello que se dispone en el epígrafe II.5.1 de la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, de 27 de octubre de 2016, la URJC ha valorado la conveniencia y oportunidad de desarrollar una política marco propia y se acoge a la política de firma electrónica y de certificados en el ámbito de la Administración General del Estado, aprobada el 30 de mayo de 2012 y publicada por Resolución de 29 de noviembre de 2012, de la Secretaria de Estado de Administraciones Públicas.

Así mismo, la URJC podrá hacer uso de políticas específicas para contextos concretos, en especial las desarrolladas por la Comunidad Autónoma de Madrid la Administración General del Estado y la Conferencia de Rectores de las Universidades Españolas.

En cualquier caso, y en el marco anteriormente indicado, este documento detalla los sistemas de identificación y firma que pueden ser empleados por parte de los interesados y de la propia universidad.

1. Ámbito de aplicación de la política de firma electrónica

Esta política resulta aplicable a todos los sistemas de información de soporte a procedimientos administrativos, académicos y de gestión electrónicos utilizados por la URJC sujetos a la Ley 39/2015, y Ley 40/2015.

Esta política también resulta aplicable a la firma de manifestaciones de documentos y expedientes en el momento de su intercambio con entidades diferentes de esta Universidad, en particular de acuerdo con lo establecido por el Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Identificación y firma electrónica de los interesados

2.1. Reglas generales relativas a la identificación electrónica

1. Los interesados podrán identificarse electrónicamente ante la URJC, empleando cualquier sistema que disponga de un registro previo como usuario que permita garantizar su identidad de manera suficiente en atención al nivel de seguridad exigido para la actuación de qué se trate, en los términos establecidos por la legislación aplicable y, en particular, 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.

2. A estos efectos, se admitirán los sistemas de identificación electrónica aceptados por la Administración General del Estado, de acuerdo con lo que se dispone en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y a las modificaciones introducidas por el RD 203/2021 de 30

de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos .

3. La URJC debe dar publicidad, en su Sede Electrónica, a los sistemas de identificación electrónica admitidos.

2.2. Reglas generales relativas a la firma o al sello electrónico de los interesados

1. Cuando resulte legalmente exigible, los interesados podrán firmar electrónicamente empleando cualquier medio de identificación electrónica, así como cualquier medio previsto en la legislación de servicios de confianza, siempre que éste permita acreditar electrónicamente la autenticidad de su voluntad y consentimiento de forma suficiente en atención al nivel de seguridad exigido para la actuación de qué se trate, en los términos que establece la legislación aplicable y, en particular, 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.

2. Cuando, en aplicación de las normas contenidas 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, la URJC deba exigir al interesado el uso de una firma o un sello electrónico avanzado, una firma o un sello electrónico avanzado basado en certificado cualificado, o de una firma o un sello electrónico cualificado, no se podrá emplear un sistema de identificación electrónica alternativo al medio de firma para esta función.

3. En este caso, cuando se trate de una actuación transfronteriza, se admitirá a los interesados establecidos en el resto de Estados Miembro de la Unión Europea, el uso de un sistema de firma o sello electrónico avanzado, de firma o sello electrónico avanzado basado en certificado cualificado, o de firma o sello electrónico cualificado, exclusivamente en los formatos definidos en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de setiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Los formatos anteriormente indicados también podrán ser empleados, en cualquier caso, por los interesados establecidos en España.

4. La URJC no exigirá, en ningún caso, el uso de un sistema de firma o sello electrónico con un nivel de garantía superior a la firma o al sello electrónico cualificado.

5. Cuando se emplee un sistema de identificación para firmar, que no permita acreditar la integridad e inalterabilidad del documento, la URJC habilita los mecanismos técnicos que garanticen estos aspectos.

6. La URJC debe dar publicidad, en su sede electrónica, a los sistemas de firma electrónica admitidos para cada una de las actuaciones.

2.3. Sistemas específicos de identificación y firma electrónica de las personas físicas

1. Se admite el sistema de clave concertada en el acceso con usuario corporativo de la URJC.

2. Las personas físicas también pueden emplear sistemas de identificación y de firma electrónica avanzada basados en certificado electrónico cualificado, o de firma electrónica cualificada, de acuerdo con lo que prevé el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, expedidos por prestadores cualificados.

De forma expresa se admite el uso de sistema de clave concertada en el acceso con usuario corporativo de la URJC, para la identificación y firma en trámites de nivel de seguridad medio o inferior, conforme a lo que determina el Esquema Nacional de Seguridad, en los trámites que no sea necesario utilizar la firma cualificada y que así se establezca en el correspondiente procedimiento por la Universidad.

3. La URJC admitirá, adicionalmente, los sistemas basados en certificados electrónicos cualificados expedidos a personas físicas representantes de personas jurídicas o de entidades sin personalidad jurídica, cuando los mismos sean conformes a lo que establece el Anexo II de la Política de firma electrónica y certificados de la Administración General del Estado, aprobada de acuerdo con aquello que establece el artículo 18 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.

En este caso, la representación quedará plenamente acreditada, a los efectos legales oportunos.

4. La URJC podrá establecer mecanismos de firma manuscrita con captura electrónica de datos biométricos, para su uso, en relaciones presenciales, por las personas físicas.

Estos mecanismos garantizan, en cualquier supuesto, la confidencialidad de los datos de representación de la firma, así como la no reutilización de los mismos por parte de la URJC o de terceras personas, y la integridad e inalterabilidad de los datos firmados.

2.4. Sistemas de identificación y firma electrónica de las personas jurídicas y entidades sin personalidad jurídica

1. Las personas jurídicas y las entidades sin personalidad jurídica pueden emplear sistemas de identificación y de sello electrónico avanzados basados en certificado electrónico cualificado, o de sello electrónico cualificado, de acuerdo con lo que prevé el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, expedidos por prestadores cualificados.

2. La admisión del sello electrónico está sujeta a las siguientes condiciones:

a) El uso del sello electrónico implica que la actuación se debe atribuir directamente a la persona jurídica o entidad sin personalidad jurídica, sin que haya que acreditar la representación.

b) El sello electrónico no se podrá sujetar a límites, dentro del conjunto de trámites para los cuales sea admitido.

c) El uso del sello electrónico será alternativo al uso del sistema de firma electrónica de la persona física representante, pudiendo emplear los dos sistemas, de forma indistinta, a elección del interesado.

3. El uso del sello electrónico únicamente podrá ser admitido en los casos de firma previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en aquellas actuaciones en que sea suficiente la garantía de la corrección del origen de los datos y de la integridad de los datos sellados por la persona jurídica o la entidad sin personalidad jurídica.

3. Identificación y firma electrónica de la URJC

3.1. Sistemas de identificación y firma electrónica automatizada de la URJC

1. La URJC podrá identificar y firmar electrónicamente de forma automatizada empleando sistemas de sello electrónico avanzados basados en certificado electrónico cualificado, o de sello electrónico cualificado, de acuerdo con lo que prevé el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, expedidos por prestadores cualificados, en atención al nivel de seguridad exigido para la actuación de qué se trate, en los términos que establece la legislación aplicable y, en particular, 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.

2. Los certificados cualificados de sello electrónico de la URJC deben ser expedidos preferentemente a los órganos de la URJC, para el ejercicio por estos de sus competencias legalmente establecidas, sin perjuicio de la posibilidad de que la URJC también disponga de un certificado cualificado de sello electrónico a su nombre.

Los certificados cualificados de sello electrónico expedidos a órganos administrativos deben incluir, en todo caso, los datos de identificación personal de los titulares de estos órganos, con excepción del número del documento nacional de identidad o equivalente, que no será obligatorio.

3. La URJC debe dar publicidad, en su portal de internet, a los certificados cualificados de sello electrónico de que disponga en cada momento.

3.2. Sistemas de identificación y firma electrónica del personal al servicio de la URJC

1. Las personas titulares o miembros de los órganos, así como las restantes personas al servicio de la URJC, podrán emplear sistemas de identificación y de firma electrónica avanzada basados en certificado electrónico cualificado, o de firma electrónica cualificada, de acuerdo con lo que prevé en el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, expedidos por prestadores cualificados, en atención al nivel de seguridad exigido de la actuación de qué se trate, en los términos que establece la legislación aplicable y, en particular, 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.

2. Estos certificados deberán ser facilitados por la URJC a las personas a su servicio, sin perjuicio de la posibilidad de autorizar el uso voluntario de certificados cualificados estrictamente personales de que dispongan dichos individuos.

Los certificados podrán incluir informaciones adicionales para la identificación del órgano, unidad o cargo o puesto de trabajo de la persona, de manera proporcionada y respetando los límites establecidos por la legislación de transparencia y protección de datos personales.

3. Se podrán facilitar certificados cualificados de firma electrónica con pseudónimo en aquellos casos en que sean aplicables límites a la identificación de las personas firmantes de documentos, derivados de la legislación vigente. El pseudónimo se instrumentará mediante el uso de número de identificación profesional o equivalente.

Los órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado cualificado con pseudónimo, en los casos que prevé el artículo 6,1, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

4. La URJC podrá adherirse a sistemas de identificación y firma basados en claves concertadas ofrecidos por otras administraciones públicas, siempre que su nivel de seguridad resulte suficiente.

5. La URJC podrá establecer mecanismos de firma manuscrita, con captura electrónica de datos biométricos, para su uso, en relaciones presenciales, por parte de las personas a su servicio.

Estos mecanismos deben garantizar, en cualquier caso, la confidencialidad de los datos de representación de la firma, así como la no reutilización de los mismos por parte de la URJC o de terceras personas, y la integridad e inalterabilidad de los datos firmados.

3.3. Reglas comunes

1. Los certificados cualificados de sello y firma electrónica de que se dote la URJC serán conformes al Anexo II de la Política de firma electrónica y certificados de la Administración General del Estado, aprobada de acuerdo con lo que establece el artículo 18 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, y el artículo 24 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

2. La URJC debe fomentar la adopción de sistemas de firma o sello electrónico basados en certificados con la gestión centralizada de los dispositivos y datos de creación de firma o sello.

3. Al objeto de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos autenticados con sistemas que no se basan en certificados cualificados, la URJC podrá superponer su propio sello electrónico avanzado basado en certificado electrónico cualificado a los documentos, para posteriormente remitirlos o ponerlos a disposición de otros órganos, organismos públicos, entidades de derecho público o administraciones.

3.4. Relación entre la firma y el documento firmado

1. El formato de la firma debe ser, siempre que sea posible, independiente del formato del documento o registro firmado, con el objetivo de reducir al máximo la dependencia entre los dos objetos de negocio.
2. En relación con los documentos originales que deban estar en poder de la URJC (ejemplo: resoluciones, actos, informes) se procurarán producir con firma independiente del documento, evitando en la medida de lo posible el uso de firmas envueltas en formatos documentales. La relación entre el documento firmado y la firma se establecería en este caso mediante el uso de metadatos del documento.
3. Cuando sea necesario entregar a terceros estos documentos, se debe crear una copia auténtica electrónica, en un formato adecuado al destinatario, que será firmada o sellada electrónicamente, envolviendo la firma o sello en el formato documental.
4. Como excepción, los documentos originales a entregar al ciudadano (ejemplo: una certificación, una notificación) deben incluir la firma envuelta en el propio formato documental (ejemplo: un fichero PDF firmado o sellado). Se recomienda que, adicionalmente, los documentos incorporen un código de verificación electrónica, que permita su consulta en línea y la impresión en concepto de copia auténtica.
5. En relación con los actos de intercambio de datos o acceso a datos entre Universidades o Administraciones, la relación entre la firma electrónica y el documento firmado será típicamente establecida por cada Universidad o Administración que ceda datos o dé acceso a datos, sin perjuicio de establecer estas condiciones por convenio.
6. En relación con los actos de los ciudadanos y estudiantes, siempre que sea posible se deben utilizar formularios con firma electrónica. La firma debería ser independiente del formato del formulario, siempre que sea posible.
7. Respecto a los documentos ofimáticos, firmados o no, que se puedan presentar acompañando a una solicitud administrativa, no se les puede aplicar la política de firma electrónica propia de la Universidad (ya que son documentos previos, que no han sido creados específicamente por el ciudadano para su relación jurídica con la Universidad).
8. En cualquier caso, se deben aceptar –y poder validar- las firmas de los documentos ofimáticos que se determinen en el Esquema Nacional de Interoperabilidad y en el Esquema Nacional de Seguridad.
9. También se deben aceptar las copias digitalizadas de los documentos en soporte papel, producidas por los ciudadanos o estudiantes, en este caso con sujeción al estándar técnico de firma electrónica de la URJC (normalmente, el estándar técnico de firma electrónica de solicitudes).
10. Se recomienda proteger estos ficheros, en todo caso, con la firma electrónica de la solicitud (ejemplo: mediante la inclusión de los resúmenes criptográficos de los documentos en campos ocultos del formulario a firmar). De esta forma, siempre existe una prueba de los documentos que entregó el ciudadano o el estudiante a la URJC, con independencia de la validez de la firma de los documentos, o incluso de que estén firmados o no.

3.5. Formato de la firma

1. En general, el formato de la firma depende del formato del documento firmado (ejemplo: PDF exige firmar de acuerdo con CMS, ODF exige firmar de acuerdo con una variante de XML Digital Signature).

2. La URJC emplea de forma indistinta los formatos de firma XAdES, PAdES o CAdES, en función de la sintaxis correspondiente a los datos a firmar, siempre y cuando el formato del documento o el protocolo correspondiente permitan el empleo de los mismos, con las siguientes restricciones adicionales:
   - La URJC podrá hacer uso de contrafirmas para la producción de sus documentos, en función del caso. En todo caso, la URJC debe validar firmas con atributo de contrafirma.
   - No debe ser utilizada certificación de atributos.
   - Respecto a los atributos de firma electrónica avanzada (AdES), cada estándar técnico de firma electrónica debe identificar los que es necesario incluir en la firma (ver la sección siguiente, relativa al perfil de firma electrónica)
3. Las normas concretas en relación con la firma electrónica de cada formato documental se deben establecer en los correspondientes estándares técnicos de firma electrónica de formato documental.
4. En todo caso, y de acuerdo con lo establecido en la Resolución de la Secretaría de Estado para la Función Pública, de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, se empleará, con carácter general, XAdES internally detached y el formato Facturae con firma XAdES enveloped en, al menos, las facturas en operaciones con las Administraciones Públicas españolas.

3.6. Perfil de la firma

1. Las firmas de los actos administrativos realizados por los órganos administrativos deben ser suficientemente completas para que los ciudadanos o estudiantes las puedan validar sin medios particularmente sofisticados.
2. La URJC debe producir firmas electrónicas de clase EPES explícito, donde el OID de la política de firma coincide con el estándar técnico de firma electrónica de acto jurídico aplicable, siempre que sea técnicamente posible.
3. En general se debe utilizar el perfil AdES-T-LT de acuerdo con ETSI TS T03 171 (XAdES Baseline Profile), TS 103 173 (CAdES Baseline Profile) o ETSI TS 103 172 (PAdES Baseline Profile), para toda firma electrónica de un documento entregado a un ciudadano, siendo recomendable emplear dicho perfil para todos los documentos de la URJC.
4. Las firmas de los actos de trámite pueden ser más básicas, ya que la URJC puede establecer controles adicionales que eviten la necesidad de completar la firma electrónica. En general, se recomienda sellar la firma electrónica, empleando el perfil AdES-T.
5. Las firmas de los actos de intercambio de datos entre Administraciones Públicas o el acceso a datos de otras Administraciones Públicas se deben ajustar al perfil que determine cada Administración que cede o da acceso a datos.
6. Las firmas de los actos de los ciudadanos o estudiantes pueden ser básicas, ya que la URJC dispone de los mecanismos para validar y completar la firma electrónica. En general, la URJC debe admitir documentos externos con firma electrónica de perfil AdES-EPES con política implícita, y debe verificar las firmas conforme el perfil AdES-EPES con política explícita, siempre que la misma sea conforme con lo que establecen los artículos 18 y siguientes del Real Decreto 4/2010.
7. En general, la URJC debe completar la firma de los ciudadanos de acuerdo con el perfil T-LT, o mecanismo de depósito seguro equivalente.

8. En relación con la custodia a largo plazo de las firmas de los documentos, la URJC puede utilizar los siguientes métodos:
   - Completado de las evidencias electrónicas mediante el empleo de formatos AdES-LTA.
   - Técnicas de gestión segura de registros para garantizar la longevidad de los documentos internos.

3.7. Procesos en relación con la firma electrónica

Se deben implantar los siguientes procesos en relación con la firma electrónica:

- Proceso de creación de la firma electrónica:

  Consiste en la sucesión de pasos necesarios para obtener una firma digital para un tipo de contenido concreto. Incluye la posibilidad de seleccionar y visualizar contenidos y atributos de firma, efectuar flujos de firma y ver el estado de una firma realizada.

- Proceso de validación.

  Este proceso se debe basar en el uso de la plataforma de validación de la URJC, que podrá delegar parte del proceso de verificación al servicio @Firma de la Administración General del Estado.

- Proceso de mantenimiento de la validez de la firma electrónica.

  Consiste en la sucesión de pasos necesarios para mantener a través del tiempo la validez de una firma digital para un tipo de contenido concreto, en el momento de su recepción. Se trata de un proceso de adición de garantías criptográficas adicionales (típicamente, informaciones adicionales y sellos de fecha y hora) que permiten acreditar la producción de una firma en un momento concreto del tiempo, incluso en caso de ruptura u obsolescencia matemática de los algoritmos de firma electrónica.

  Este proceso se debe basar en el uso de la plataforma de validación de la URJC, que podrá delegar parte del proceso de verificación al servicio @Firma de la Administración General del Estado.

3.8. Firmas longevas en el expediente y el archivo.

1. Las firmas longevas en expediente electrónico y su ingreso en el archivo deben tener en cuenta:
   - El Archivo definitivo de documentación deberá en todo caso, comprobar la validez de las firmas electrónicas del índice de los expedientes electrónicos, debiendo ser longeva en el momento de su archivado.
   - La actualización de dicha firma a formatos longevos deberá hacerse preferentemente por parte del sistema gestor, aunque podrá realizarse por parte del sistema de archivado.
   - No podrán ingresarse expedientes con firmas del índice inválidas, antes de su pre-ingreso deberá regenerarse y presentar una firma correcta.
2. El resellado de expedientes y documentos archivados, debe tener en cuenta:

- El sistema de archivado deberá controlar la validez y tener actualizadas las firmas de los expedientes electrónicos que custodia.
- Será suficiente con el resellado de la firma longeva del índice del expediente electrónico.
- Toda acción dirigida al mantenimiento de la validez de las firmas deberá quedar reflejada en el sistema de archivado como trazas asociadas al expediente conservadas permanentemente.

3. Las firmas de los documentos electrónicos en el momento del ingreso, deben tener en cuenta:
    - Se recomienda que los documentos electrónicos que forman parte de un expediente electrónico se ingresen en el archivo con formatos longevos de firma.
    - Aquellos documentos electrónicos que presenten firmas válidas en formatos no longevos, podrán:

      a. Ser archivados con la firma original, al considerarse que la firma longeva del índice garantiza su integridad y validez.

      b. Que el sistema de gestión convierta la firma a formatos longevos antes de su remisión al archivo definitivo, actualizando el índice del expediente del que forma parte cuando sea necesario.

      c. Que el sistema de archivado convierta la firma a formato longevo, como parte del archivo definitivo del expediente. En este caso, el sistema de archivado deberá regenerar el índice del expediente original para reflejar los cambios en las funciones resumen de los documentos.

        - el SIP almacenará el expediente y documentos electrónicos originales remitidos por la aplicación, que será distinto al AIP archivado definitivamente.
        - Serán iguales en contenido, pero distintos en los metadatos de las firmas.
        - Aquellos documentos electrónicos que, formando parte de un expediente, presenten una firma inválida o no estén firmados:

          a. Si el expediente no presenta algún otro documento con firma válida que lo referencie y que pueda otorgarle validez jurídica (como, por ejemplo, un justificante de registro):

            - Si se tiene garantía por parte del sistema gestor de la validez del mismo, deberán ser firmados o sellados antes de su ingreso.
            - Si no se tiene dicha garantía, deberá considerarse la conveniencia o no de su inclusión como parte del expediente electrónico. En caso afirmativo, se recomienda esclarecer este extremo mediante metadatos adicionales que expliquen dicha circunstancia.

- Si el expediente presenta algún documento electrónico con firma válida que lo referencie, podrán ser mantenidos en su formato inicial

4. Sobre la transferencia de expedientes y la relación del proceso con la firma electrónica:
   - En los procesos de transferencia de expedientes, sin perjuicio de lo que se defina en normativas que afecten a dicho proceso, se deberá realizar el resellado del expediente antes de su remisión al siguiente archivo, teniendo en cuenta las consideraciones previstas en los puntos anteriores.

4. Admisión de sistemas

1. Esta política aplica los principios de seguridad y proporcionalidad que informan la legislación de procedimiento administrativo y de régimen jurídico del sector público, y que se recogen en el Esquema Nacional de Seguridad.
2. A los efectos de lo que se dispone en esta política, se recogen a continuación los criterios para la determinación de los niveles de seguridad previstos en el Anexo I del Esquema Nacional de Seguridad:

   a) Nivel BAJO. Se utiliza cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

   b) Nivel MEDIO. Se utiliza cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

   c) Nivel ALTO. Se emplea cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

3. Por este motivo, preferentemente se admiten con carácter general todos los sistemas de identificación y firma o sello electrónico de nivel medio, basados en los certificados cualificados incluidos en la "Lista de confianza de prestadores de servicios de certificación" (TSL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Comercio y Turismo, y en aras del principio de proporcionalidad, sistemas de identificación y firma basados en certificados avanzados así como el sistema de clave concertada para el acceso del usuario corporativo para los correspondientes al nivel bajo.

5. Otros servicios de confianza empleados por la URJC

5.1. <u>Validación de la firma o sello electrónico</u>

1. La URJC debe proceder a la validación de cualquier firma o sello electrónico que utilice.

2. Cuando la firma o el sello electrónico sea avanzado y se base en un certificado cualificado, la URJC debe validarlo conforme a lo que disponen los artículos 32 y 40 del Reglamento (UE) nº 910/2014, del Parlamento Europeo y del Consejo, relativo a la

identificación electrónica y los servicios de confianza para las transacciones al mercado interior, y por la que se deroga la Directiva 1999/93/CE, respectivamente.

3. La URJC delega la validación de las firmas y sellos basados en certificados cualificados a la plataforma @firma, que actúa como prestador de servicios de confianza, de acuerdo con lo que disponen los artículos 33 y 40, respectivamente, del Reglamento (UE) nº 910/2014 anteriormente mencionado.

5.2. Sellado de tiempo electrónico

1. La URJC debe proceder a la incorporación, al menos, de un sello de tiempo electrónico a cualquier firma o sello electrónico que haya validado, en los términos definidos por la política marco o específica aplicable.

2. El servicio de sellado de tiempo electrónico es prestado por la Autoridad de Sellado de Tiempo (TSA) de la Administración General del Estado (AGE) que actúa como prestador de servicios de confianza, y producirá los efectos jurídicos previstos en el artículo 41.1 del Reglamento (UE) nº 910/2014 anteriormente mencionado.

5.3. Organización y desarrollo de esta política de firma

1. Corresponde la aprobación de esta política de firma electrónica al Consejo de Gobierno.
2. Esta política se debe desarrollar mediante los siguientes instrumentos:
   - Estándares técnicos de firma electrónica de actos administrativos.
   - Estándares técnicos de firma electrónica de formatos documentales.
   - Guías y recomendaciones de firma electrónica.
   - Procedimientos operativos de firma electrónica.
3. Corresponde a los responsables del área de tecnologías y sistemas de la información el desarrollo de esta Política de Firma por medio de los instrumentos indicados.

ANEXO I

Las políticas de identificación y firma electrónica

La URJC dispone de una clasificación[1] del uso de las diversas políticas de identificación y firma electrónica en relación con los diferentes tipos de documentos que se gestionan. Seguidamente se describe un cuadro resumen.

	Política de Identificación y firma/sello electrónico **basado en certificado**.	Política de Identificación y firma electrónica **basada en medios no criptográficos.**	Política de Firma **manuscrita capturada electróni-camente**.	Política de Sello avanzado con **CSV**.
Documentos de los interesados				
• Solicitud de un ciudadano, alumno o persona jurídica	**SI**	**SI**	**SI**	
• Aportación de nuevos elementos por parte del administrado	**SI**	**SI**	**SI**	
• Presentación electrónica en nombre de terceros interesados	**SI**	**SI**	**SI**	
Documentos de la Administración				
• Producción de documentos administrativos	**SI**	**SI**		**SI**
• Recibo del registro electrónico de entrada	**SI**			**SI**
• Digitalización de documentos que se aportan en formato papel	**SI**			**SI**
• Copia auténtica electrónica de documento electrónico original o de una copia electrónica auténtica	**SI**			**SI**
• Copia auténtica en soporte papel de documento electrónico	**SI**			**SI**
• Copia auténtica en soporte papel de documento electrónico original	**SI**			**SI**
Expedientes electrónicos				
• Cierre, foliado y archivo de expedientes	**SI**			**SI**
• Consulta de documentos y expedientes por parte del administrado	**SI**	**SI**	**SI**	

[1] De acuerdo con el documento "Análisis de trámites en relación al uso de evidencia electrónica y política de firma electrónica"

ANEXO II

Política de firma manuscrita capturada electrónicamente

1.- Reglas generales relativas a la firma manuscrita capturada electrónicamente.

En el caso de que la URJC emplee **firmas electrónicas no basadas en certificado**, sino en la vinculación a los documentos electrónicos de firmas manuscritas captadas con técnicas electrónicas, en adelante (FMCE) se respetarán los siguientes criterios:

- El proceso de creación de las firmas electrónicas manuscritas capturadas electrónicamente (FMCE) *implicará el cifrado de la información biométrica asociada a la realización del trazo de la firma sobre un dispositivo idóneo y su incorporación al propio documento*.
  El cifrado se apoyará sobre una clave pública gestionada por el software de codificación de firmas, asociada con una clave privada custodiada por un notario o un Prestador de Servicios de Confianza Digital.
- En caso de controversia sobre la firma, debe ser posible su cotejo para lo que se podrá recurrir al notario o Prestador de Servicios de Confianza Digital supervisado por el órgano designado (Vicerrector Digitalización-Comité de seguridad de la universidad), que custodia la clave privada, que colaborarán para el descifrado de la información biométrica del documento, lo que podrá utilizar un perito calígrafo para comparar la firma con otras indubitadas del mismo autor.
- La posibilidad de extraer la información dinámica estará disponible sin coste en el Prestador a disposición de los firmantes y terceros con interés legítimo.
- La firma y el contenido del documento se vincularán de forma indisociable, de forma que esta vinculación pueda ser comprobada por quien acceda al documento.
- La imagen estática de la firma será visible en el documento PDF.
- El software de análisis pericial que permita comparar una firma controvertida con otras indubitadas estará disponible sin coste en un tercero depositario a disposición de los firmantes y terceros con interés legítimo.
- Las firmas electrónicas de este tipo pueden ir reforzadas con sellos de tiempo o firmas o sellos automatizados.
- Se preferirán los sistemas que estén respaldados por sellos de calidad que el fabricante o distribuidor haya obtenido tras superar una auditoría de una entidad auditora especializada en sistemas de firma manuscrita digitalizada avanzada.

2.- Reglas particulares relativas a la firma manuscrita capturada electrónicamente

2.1. Introducción

La Firma Manuscrita Capturada Electrónicamente (FMCE) debe recoger las características estáticas (imagen visual) pero también dinámicas (presión, velocidad, vuelo) asociadas a la grafía de un firmante.

La FMCE se trata de una firma manuscrita en la que, únicamente, cambia el soporte en que se produce y, por ello, los mecanismos de prueba deben estar más cerca de la firma tradicional (pericial caligráfica) que de la electrónica basada en certificado electrónico.

2.1.1. Cláusulas en relación a la firma electrónica como manifestación de la voluntad

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la vinculación entre el firmante y el contenido firmado, y de establecer la presunción de que existe intención de firmar, es decir, prestación del consentimiento en el sentido de que se determine por el contexto. Sin embargo, la firma electrónica debe permitir detectar modificaciones del contenido firmado, si se producen.

Un mecanismo para distinguir si el contexto de uso de certificados se lleva a cabo en relación con una firma electrónica, es que el firmante sea consciente de la realización de la firma, del contenido del documento firmado y de las implicaciones de acompañar su firma en el documento.

Siempre que el contexto de uso del certificado implique la realización de una firma, el firmante deberá poder conservar un archivo o documento electrónico en que ha quedado plasmada, de forma que resulte evidente la realización de la firma y el contenido del documento.

En las firmas electrónicas automatizadas y en el uso de sellos electrónicos para la actuación automatizada (si existieran), deberá quedar evidenciado en el procedimiento tecnológico que una persona con acreditación adecuada es consciente de la realización de estas firmas y consiente esta actuación automatizada.

2.1.2. Prestadores de servicios de certificación admitidos

Serán válidos los certificados expedidos por Prestadores de Servicios de Confianza Digital (PSCD) supervisados según el marco definido por el Reglamento Europeo (UE) Nº 910/2014.

En este contexto, se admitirán los prestadores que se incluyan en listas TSL conformes con la norma TS 102 231 administradas por los órganos de supervisión de PSCD de los países miembros de la Unión Europea según se establezca en la TSL colectiva de la UE, tanto PDF como XML. Se considerará válida la versión XML en caso de existir discrepancias entre estas.

Los PSCD deberán cumplir con lo previsto por los organismos de normalización en relación con los estándares y las normas técnicas aplicables, especialmente en lo referente a los requisitos técnicos y operacionales que posibiliten la expedición de certificados cualificados.

Los PSCD, de conformidad con lo descrito en su Declaración de Prácticas de Certificación, deberán:

- Aplicar los estándares relativos a las políticas y prácticas de certificación y de generación de certificados electrónicos; estado de los certificados; dispositivos cualificados de creación de firma; programas controladores; dispositivos criptográficos; interfaces de programación; tarjetas criptográficas; conservación de documentación relativa a los certificados y servicios; y límites de los certificados, conforme a lo establecido en el Reglamento (UE) Nº 910/2014 y en la normativa técnica desarrollada en el marco de su desarrollo. Incluir dentro de los certificados la información relativa a las direcciones de Internet en que se ofrecen servicios de validación del propio certificado sin ningún tipo de coste. Estos servicios de consulta de validez de certificados se basarán en información actualizada y no en mecanismos de consulta de listas de revocación que pudieran requerir tener en cuenta un "periodo de gracia" desde el momento de la firma hasta el momento en que se puede tener la certeza de que el certificado no estaba revocado.
- Opcionalmente pueden contener, además, la dirección electrónica de otro servicio de comprobación de validez que otorgue acceso a la lista de certificados revocados y no caducados del mismo tipo que el cuestionado, igualmente sin coste alguno.
- Cumplir con lo previsto en los apartados 2.2 y 4.2 de la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015.

2.2 Contenidos técnicos

2.2.1 Obligatorios

1) Cumplimiento de ciertas medidas de seguridad consistentes en:

- La captura de los datos biométricos debe realizarse conforme a la norma ISO/IEC 19794-7: 2007, protección frente falsificación con cifrado.
- Debe existir un catálogo de dispositivos homologados.
- El lápiz para la captura de firma debe disponer de capacidad para distinguir el lápiz de la mano.
- La pantalla multitáctil debe detectar 5 puntos y disponer de protección contra fractura y arañazo.
- La tecnología de captura de las medidas de presión durante el proceso de captura debe disponer de un mínimo de 16 niveles de presión.

2) Asegurar que el documento que se muestra en el dispositivo coincide con el documento que firmará.

3) Los datos biométricos nunca deben estar en posesión del prestador del servicio ni del fabricante del software, ya que son datos sensibles que permitirían la falsificación posterior de las firmas.

4) La firma y el contenido del documento se vincularán de forma indisociable, por lo que esta vinculación pueda ser comprobada por aquellos que accedan al documento.

5) La imagen estática de la firma será visible en el documento.

6) Recuperabilidad del documento al cabo de los años.

7) Protección frente falsificación:

- Existencia de un mecanismo de cifrado de la información biométrica asociado a la realización del trazo de la firma, e incorporado al propio documento.
- El cifrado se apoyará sobre una clave pública, gestionada por el software de codificación de firmas, asociada con una clave privada custodiada por un notario, que únicamente se empleará en caso de necesidad (peritaje caligráfico).

2.2.2 Recomendables

1) Intervención de un Tercero de Confianza (según art. 25 de la Ley de Servicios de la Sociedad de la Información, LSSI) para ayudar a asegurar que el documento con la firma manuscrita digitalizada satisface las propiedades de autenticidad e integridad.

El Tercero de Confianza será el Responsable de la custodia de la clave privada de cifrado, así como de la custodia del documento (al menos 5 años).

2) Certificación temporal:

Intervención de un Prestador de Servicios de Confianza Calificado por la emisión de sellos de tiempo (conforme a RFC 3161) que aporte evidencia certificada del momento en que se realiza la firma.

3) Aplicación de la confrontación de firmas:

Que permita ser empleada por un perito calígrafo para comparar la firma (después de ser descifrada con la clave privada en posesión de un notario) con otras indudables del mismo autor.

4) Refuerzo del proceso con firma electrónica:

Incluir una firma al final del proceso con certificado de sello electrónico (emitido a nombre de la empresa) que aporte un nivel de protección adicional sobre el documento final ("plastificación del documento").

5) Auditoría Técnica por parte de una entidad auditora especializada:

Se preferirán los sistemas que estén apoyados por sellos de calidad que el fabricante o distribuidor haya obtenido tras superar una auditoría de una entidad auditora especializada en sistemas de firma manuscrita digitalizada avanzada.

ANEXO III

Política de identificación y firma electrónica basada en medios no criptográficos

1. Mecanismos técnicos para el mantenimiento de la firma electrónica como fuente de prueba.

Este documento tiene por objeto identificar los mecanismos técnicos convenientes para la generación y mantenimiento del valor evidencial de una firma electrónica producida sobre un documento.

Estos mecanismos constituyen pruebas electrónicas que es necesario capturar y gestionar adecuadamente para garantizar el mantenimiento evidencial de la firma electrónica.

En documento aparte se determina un conjunto de vocabularios XSD que permiten la relación entre los contenidos y las firmas electrónicas, específicamente diseñados para la generación de documentos con la máxima calidad probatoria posible.

En este documento se identifican los aspectos relacionados con la firma electrónica avanzada basada en contraseña.

1.1. Contenidos de la evidencia electrónica de firma electrónica

Esta sección recoge los contenidos probatorios que conforman una evidencia de firma electrónica de documento:

- Prueba del contenido firmado.
- Prueba de visualización del contenido firmado.
- Prueba de identidad del firmante.
- Prueba de la fecha y hora de la firma.
- Prueba del rol en que actúa el firmante.

Cada contenido probatorio aporta una cierta credibilidad a la evidencia electrónica producida por la Universidad, de forma que se pueda disponer de una prueba de tipo tecnológico que, en su caso, supere una pericia técnica derivada de una refutación de la firma electrónica y, por tanto, permita a la Universidad sustentar su posición en el proceso judicial.

Una evidencia electrónica de firma electrónica tiene unos contenidos mínimos, y unos contenidos opcionales, en función del caso de uso aplicable (tipo de firma) y en función de la categoría de seguridad del sistema de información (baja, media o alta), de acuerdo con los criterios del Esquema Nacional de Seguridad.

En función del procedimiento de obtención de la evidencia electrónica, se dispondrá de la totalidad o de una parte de los anteriores contenidos probatorios.

1.1.1. Prueba del contenido firmado.

El significado estricto de esta prueba es la presunción, más o menos fuerte, de que la persona ha tenido conocimiento del contenido protegido por la firma electrónica, cosa que depende también de otras pruebas, como la prueba de visualización de la firma.

Metodologías: Uso de la firma electrónica basada en contraseña:

- Verificación del uso de un algoritmo fiable de autenticación de mensaje basado en claves simétricas, como por ejemplo HMAC envuelto en XMLDSig.
- Verificación matemática de la firma electrónica empleando el algoritmo correspondiente, a partir del documento original.

1.1.2. Prueba de visualización del contenido firmado.

El significado estricto de esta prueba es la presunción, más o menos fuerte, de que la persona realmente ha visto esta representación, cosa que realmente depende de su software instalado.

Metodologías:

1) Envío del documento al firmante, para su firma en el equipo local, con garantía de captura y protección a la firma de las condiciones locales de entorno (profundidad de colores, nombre de pantallas, aplicación empleada para la generación de la firma, etc.).
2) Generación de una transformación del documento a firmar, por ejemplo, empleando una plantilla XSLT protegida para la firma electrónica (mediante la incorporación de su resumen criptográfico a la firma), y remisión del resumen criptográfico del documento a firmar.

1.1.3 Prueba de identidad del firmante.

El significado estricto de esta prueba es la presunción, más o menos fuerte, de que la persona ha firmado el documento, ya que, en general, en los actos realizados electrónicamente a distancia no resulta posible acreditar realmente quién lo ha realizado, puesto que puede dejar su dispositivo de firma a un tercero.

Metodologías

1.- Uso de la firma electrónica basada en contraseña:

- Verificación de que el procedimiento de registro y emisión de la contraseña garantiza la identificación de la persona identificada.
- Garantía de la unicidad en las contraseñas asignadas a los usuarios.

2.- Notas técnicas: De acuerdo con aquello que dispone la Norma técnica de interoperabilidad de política de firma electrónica, se deben emplear los formatos XAdES, CAdES o PAdES para la gestión de estas informaciones, en especial cuando las mismas se incorporan a la propia firma.

Cuando se empleen listas de revocación de certificados, la firma debe ser de formato AdES-X, mientras que, si se emplean servicios OCSP, la firma debe ser de formato AdES-A.

1.1.4. Prueba de la fecha y hora de la firma.

El significado estricto de esta prueba es la presunción, más o menos fuerte, de que el documento va a ser firmado en la fecha y hora indicadas, pero realmente no es posible acreditar nada más que el momento en que el documento existe, en la fecha alegada, excepto si el documento ya incorpora previamente una fecha fiable.

Metodologías:

1) Incorporación a la firma de la fecha y hora alegada por el firmante. Se trata de un método de baja fiabilidad, ya que permite al firmante alterar la fecha de su equipo y, por ello, no ofrece garantías reales del momento de firma.

2) Incorporación a la firma de un sello criptográfico de fecha y hora. Para ofrecer garantías, este sello debería ser emitido por un prestador que cumpla los requerimientos de la especificación ETSI TS 102 023 o equivalente. En cualquier caso, cabe tener en cuenta que esta técnica ofrece prueba temporal de existencia del documento (no acredita cuándo se generó la firma, sino que la misma existe en el momento de la incorporación del sello).

- Verificación del certificado que ha expedido el sello de fecha y hora.

- Obtención, verificación y almacenamiento de todos los certificados que avalen el certificado que ha emitido el sello de fecha y hora, y que conforman la ruta de certificación, hasta una raíz fiable.
- Obtención, verificación y almacenamiento de todas las informaciones de revocación de los certificados.
- Gestión de certificados raíz y de listas de confianza de prestadores de servicios de confianza.
- Sellado de fecha y hora de todas las informaciones anteriores, dentro o fuera de la propia firma.

3) Registro de la fecha y hora de la firma a un sistema de marca segura, que permita acreditar la fecha de creación de la firma electrónica, a efectos de la aplicación del algoritmo de verificación de firma electrónica.

1.1.5. Prueba del rol en que actúa el firmante. Este contenido probatorio electrónico acredita el rol en qué actúa la persona que firma el documento.

Metodologías: Alegación del rol de actuación en forma de cadena de texto incorporada a la firma electrónica. Esta información es una simple manifestación del firmante, que generará prueba en su contra, pero que deberá ser verificada si ello procede.

ANEXO IV

Política de sello electrónico avanzado de actuación automatizada basada en código seguro de verificación

1. Casos de uso del código seguro de verificación

I.- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, al regular las reglas para garantizar la identidad y contenido de las copias electrónicas o en papel, y su carácter de copias auténticas, indica lo siguiente en el artículo 27.3.c) "Las copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor".

Igualmente, en el apartado d) de dicho artículo 27.3 se indica que "las Administraciones harán públicos, a través de la sede electrónica correspondiente, los códigos seguros de verificación".

La Ley 40/2015, , de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 42.b) presenta los códigos seguros de verificación como uno de los sistema de firma para la actuación administrativa automatizada "Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente".

II.- Por su parte, el uso del código seguro de verificación igualmente se prevé en el Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión y de inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

En concreto, debe hacerse referencias a los siguientes artículos:

- El artículo 72 prevé que entre el contenido de los certificados tributarios figure el lugar, la fecha y la firma del órgano competente para su expedición y el código seguro de verificación. Asimismo, el artículo 73.3 del RD 1065/2007 determina que "el contenido, autenticidad y validez del certificado se podrá comprobar mediante conexión con la página web de la Administración tributaria, utilizando para esta finalidad el código seguro de verificación que figure en el certificado".
- El artículo 75.3 del RD 1065/2007, determina en relación con los certificados telemáticos, que "la firma escrita será substituida por un código seguro de verificación generado electrónicamente que permita contrastar su contenido, autenticidad y validez mediante el acceso por medios telemáticos a los archivos del órgano o organismo expedidor", y que "los mismos efectos producirán las copias de los certificados cuando las comprobaciones anteriores puedan efectuarse mediante el código de verificación".
- Por su parte, el artículo 83 RD 1065/2007 autoriza a la Administración tributaria a identificarse mediante códigos o firmas electrónicas, lo que incluye el uso del código seguro de verificación. Concreta el artículo 84 que, en caso de actuación automatizada "la Administración tributaria se debe identificar y garantizar la autenticidad del ejercicio de la competencia mediante alguno de los siguientes sistemas de firma electrónica: […] b) Código seguro de verificación vinculado a la Administración pública, órgano o entidad permitiéndose en todo caso la comprobación de la

autenticidad y la integridad del documento accediendo por medios electrónicos a los archivos del órgano u organismo emisor".

- En relación con las copias, el artículo 86.1 del RD 1065/2007 indica que "las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código seguro de verificación generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración pública, órgano u organismo emisor".

Como novedad sobre la regulación legal de esta posibilidad, el segundo apartado del artículo 86 determina que "los interesados podrán conocer que documentos se emiten con un código seguro de verificación u otros sistemas de verificación […] Por esto, serán objeto de publicación en la página web de la Administración tributaria correspondiente".

III.- La resolución de la Agencia Estatal de Administración Tributaria de 3 de mayo de 2000, relativa a la expedición por medios telemáticos de certificados de estar al corriente de las obligaciones tributarias u otras circunstancias de carácter tributario, define el código electrónico seguro de verificación en los siguientes términos: "Es el código formado por 16 caracteres alfanuméricos, generado por la Agencia Estatal de Administración Tributaria mediante un sistema criptográfico (algoritmo de generación de MAC – Message Authentication Code – del algoritmo DES (Data Encryption Standard) basado en la norma del Instituto de los EUA de Estándares Nacionales ANSI X9.9-1) en función de los datos incluidos en la certificación".

En este caso, la garantía de autenticidad y de integridad del certificado viene dada por la formación del código a partir del contenido de los datos de la certificación, de forma que cualquier cambio de estos datos implicará que el código seguro no se verifique correctamente.

Se trata esta de una de las posibilidades para producir códigos seguros de verificación, por lo que es necesario establecer algunos criterios.

IV.- El Real Decreto 1671/2009, de 6 de noviembre, en su artículo 20, indica los aspectos básicos de los sistemas de código seguro de verificación.

El apartado 1 indica la posibilidad de uso: "La Administración General del Estado y sus organismos públicos vinculados o dependientes podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente".

El apartado 2 indica que el Código deberá garantizar: "a) El carácter único del código generado para cada documento. b) Su vinculación con el documento generado y con el firmante. c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

El apartado 3 explica que el sistema "requerirá" (en el ámbito de este proyecto) una "resolución del titular del Organismo Público" y que "se publicará en la sede electrónica correspondiente".

El contenido de la resolución del titular del Organismo Público debe incluir de manera inequívoca: "a) Las actuaciones automatizadas a las que es de aplicación el sistema. b) Los órganos responsables de la aplicación del sistema. c) Las disposiciones que resultan de aplicación a la actuación. d) La Indicación de los mecanismos utilizados para la generación del código. e) La Sede electrónica a la que pueden acceder los interesados para la verificación del contenido de la actuación o documento. f) El plazo de disponibilidad del sistema de verificación respecto a los documentos autorizados mediante este sistema".

El apartado 4 se refiere a la gratuidad del sistema "(la Universidad) dispondrá de un procedimiento directo y gratuito para los interesados" con los "límites que establece la legislación de protección de datos personales u otra legislación específica".

Por último, el apartado 6 de dicho artículo hace mención a la verificación consistente en sumar al CSV una firma electrónica basada en un sello electrónico "Con el fin de mejorar la interoperabilidad electrónica y posibilitar la verificación de la autenticidad de los documentos electrónicos sin necesidad de acceder a la sede electrónica para cotejar el código seguro de verificación, podrá superponerse a éste la firma mediante sello electrónico regulada en el artículo anterior".

2. Criterios en relación con el código seguro de verificación

Para producir un código seguro de verificación se deben aplicar los siguientes criterios:

- El código debe proteger los datos contenidos en un documento, o el documento mismo, de forma que un cambio de los datos protegidos por el código seguro de verificación debe invalidarlo.
    - Por ejemplo, el código se puede formar a partir de los datos de una transacción y ser incorporado en un fichero PDF que representa estos datos, de forma que el tecleo del código recupere la transacción y la muestre en pantalla, para contrastar los datos.
    - Otra posibilidad es generar un documento PDF a partir de un documento Word firmado, por ejemplo, y en este caso que el código sea generado a partir de todo el fichero Word más la firma (si es detached) o bien a partir de un fichero ODF con la firma contenida en su interior.
- El código debe estar basado en un espacio numérico suficientemente grande para que no sea posible obtener documentos a partir del tecleo de datos aleatorios por parte del usuario.
    - Por ejemplo, el uso de un código formado con una función de código de autenticación de mensaje basada en resumen criptográfico robusto (HMAC) garantiza que no haya repeticiones en los códigos de los documentos.
- El código debe asignarse de forma no monótona, de forma que a partir de un código no se puedan obtener otros códigos mediante operaciones simples de adicción o sustracción.
    - Por ejemplo, a partir de un código no se debe poder obtener el documento correspondiente al código siguiente ni al código anterior, sumando o restando un entero al código del que se dispone.

4. Los CSV en los documentos electrónicos

La Norma Técnica de Interoperabilidad de Documento Electrónico dedica el apartado IV a la firma del documento electrónico. La autenticidad e integridad se garantizan con la asociación al menos de una firma electrónica.

Cuando esta firma electrónica exista, se debe incluir:

1) El valor del CSV.
2) La referencia a la orden o resolución que regula su generación.

Ambas indicaciones deben incluirse como metadatos del documento electrónico como se indica a continuación:

Metadato	Descripción / Condiciones de uso	¿Repetible?	Tipo	Esquema de valores

Tipo de firma[2]	Indica el tipo de firma que avala el documento.	1:N	Cadena de caracteres	CSV
Valor CSV	Valor del CSV.	1:N	Cadena de caracteres	n/a
Definición generación CSV	Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente.	1:N	Cadena de caracteres	Si AGE, referencia BOE: BOE-A-YYYY-XXXXX En otro caso, referencia correspondiente.

Además, con el fin de mejorar la interoperabilidad e intercambio de documentos y posibilitar la verificación de la autenticidad de los documentos electrónicos sin necesidad de acceder a la sede electrónica para cotejar el CSV, cabe contemplar la combinación de éste con una firma electrónica basada en certificados.

[2] En este ejemplo solo se indican los valores para CSV obviando las indicaciones para firma con certificados.