Universidad Rey Juan Carlos

**RESOLUCIÓN DE LA SECRETARIA GENERAL DE LA UNIVERSIDAD REY JUAN CARLOS POR LA QUE SE DICTAN LAS INSTRUCCIONES RELATIVAS A LOS PROCESOS DE IMPRESIÓN, DIGITALIZACIÓN DE DOCUMENTOS Y PRESERVACIÓN DE OBJETOS DIGITALES**

## INSTRUCCIÓN DE IMPRESIÓN

### 1. Alcance

Esta instrucción de impresión se encuadra en el marco normativo de la Política de Gestión documental de la URJC, que se publicará en la sede electrónica.

El alcance de esta instrucción es la de la generación y expedición de "copias papel auténticas" de documentos administrativos electrónicos.

Esta instrucción viene motivada por la necesidad de poner a disposición de los usuarios de los procedimientos administrativos electrónicos de la URJC un formato normalizado que permita la impresión cuando sea necesario.

1.1. Validez

Esta instrucción podrá ser publicada en la Sede electrónica de la URJC y su revisión, hasta su sustitución o derogación, corresponde a la Secretaria General.

### 2. Producción de una copia impresa

Los artículos 27.3.c) y 27.3.d) de la ley 39/2015 LPAC dan cobertura al procedimiento de impresión segura, a través del cual se pueden generar copias en papel de documentos originalmente emitidos en soporte electrónico. El requisito legal para que estas copias tengan valor de copia auténtica es que incorporen un código generado electrónicamente u otro mecanismo de verificación.

El apartado VII de la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos explica que para obtener una copia auténtica en soporte papel de documentos públicos administrativos electrónicos "se atenderá a lo previsto en la normativa aplicable y a lo establecido sobre el acceso a documentos electrónicos en la Norma Técnica de Interoperabilidad de Documento electrónico para la verificación de su autenticidad".

El objeto, por tanto, es disponer del uso de un mecanismo de impresión segura al generar una copia, cuando el ciudadano lo necesite, del documento original electrónico de la universidad.

2.1. Procedimiento a seguir

A partir de la reproducción de un documento con calidad de original en formato electrónico o copias auténticas de originales electrónicos se podrán expedir "copias papel auténticas" conforme a lo establecido en la NTI de documento electrónico.

Seguidamente se debe realizar la impresión del contenido del documento original, así como los datos identificativos de la firma, incluyendo el carácter de copia.

Universidad Rey Juan Carlos

Para disponer de trazabilidad del proceso de copiado, generar su traza y el establecimiento de vínculos entre el documento original y la copia, se procederá siempre conforme al marco de gestión documental establecido por cada organización de acuerdo a la NTI de Política de gestión de documentos electrónicos.

2.2. Informaciones a incluir

Las "copias papel auténticas" deben contener los siguientes datos:

- El contenido del documento original en formato electrónico.
- Un Código Seguro de Verificación (CSV).
- Una indicación de que el original ha sido firmado electrónicamente.
- La indicación del cargo y órgano que han realizado la firma electrónica.
- Una dirección web (URL) desde la que poder descargar y verificar el documento electrónico con la "copia papel auténtica".

2.3. Acceso al documento electrónico

La verificación de la "copia papel auténtica" se hará por medio de una dirección web (URL) en la que se podrá descargar y así verificar la autenticidad del documento en papel.

El documento electrónico que descarguemos debe contener:

a) El contenido del documento electrónico cuando éste sea representable conforme a lo recogido sobre formatos en la NT (según sección VI de la NTI de documento electrónico).
b) La información básica de cada una de las firmas del documento definida en la NTI según sección III de la NTI de documento electrónico).

2.4. Limpieza del documento

En general, siempre que se realice un proceso de conversión resulta necesario el borrado de los metadatos que previamente tuviera el documento antes de su edición para generar la copia auténtica.

Este borrado evita la fuga incontrolada de datos sensibles de la Universidad e incrementa la seguridad, así como el cumplimiento de los requisitos del Esquema Nacional de Seguridad.

Universidad Rey Juan Carlos

## INSTRUCCIÓN PARA LA DIGITALIZACIÓN DE DOCUMENTOS

En la política de gestión de documentos electrónicos se encuentran descritos los diferentes procesos de gestión de documentos electrónicos, que conforman el ciclo de vida de este tipo de documentos. En dicho ciclo se encaja este documento en el que se recogen las directrices que seguirán los distintos órganos de la Universidad Rey Juan Carlos cuando procedan a realizar la digitalización de documentos con la finalidad de asegurar la autenticidad, integridad y la preservación de los documentos digitalizados.

**1. Modelo de procesos de digitalización**

Los procesos de digitalización pueden diferir en función de cuál sea su efecto legal, la modalidad de actuación que se siga o del agente que los realice.

1.1. En atención al efecto legal

En atención al efecto legal de la digitalización, este protocolo considera los siguientes tipos de procesos de digitalización:

a) **Proceso de digitalización segura o certificada**, que es un proceso de conversión de documentos en soporte papel a documentos electrónicos con el mismo valor jurídico que los primeros siempre que se garantice la fidelidad, integridad, autenticidad y conservación del documento digitalizado. Los principales objetivos perseguidos a la hora de seleccionar un método de digitalización seguro serán:

- Asegurar un valor probatorio pleno del documento digitalizado sobre los hechos o actos que documente, equivalente al documento original.
- Garantizar la fiabilidad del documento digitalizado como evidencia electrónica de la actividad o procedimiento correspondiente según lo dispuesto en el artículo 21 del RD 4/2010 ENI.
- Avalar la autenticidad del documento digitalizado mediante las medidas de seguridad definidas en el RD 3/2010 ENS y lo dispuesto en el artículo 22 del RD 4/2010 ENI.
-Permitir la destrucción del documento en soporte papel en el momento que se establezca por parte de la autoridad competente, atendiendo a la legislación y normativa aplicable.

Se aplicará a los documentos o series documentales que pertenezcan a las categorías:

1. Documentación administrativa en soporte papel en fase activa, semiactiva o inactiva, así como a documentos aportados por los ciudadanos o de alguna otra forma obtenidos por la URJC para su incorporación a expediente administrativo.
2. Otra documentación pública, interna o externa, que se encuentre en poder de la URJC, que exija la garantía de los requerimientos de seguridad y/o legalidad aplicable.

b) **Proceso de digitalización simple** que, sin garantizar el valor probatorio pleno de la imagen electrónica obtenida, se aplica la digitalización de documentos no prevista en el supuesto anterior, salvo que el responsable o titular de la serie documental lo considere oportuno.

1.2. En atención a la modalidad de actuación

En atención a la modalidad de digitalización, se consideran los siguientes tipos de procesos de digitalización:

**a)** **Proceso de digitalización manual**, en el que interviene una persona al servicio de la URJC que realiza la copia y garantiza su autenticidad e integridad usando su firma electrónica personal. La ley 11/2007 y la ley 39/2015 prevén la posibilidad de que la calidad e integridad de la imagen generada sea validada por un trabajador público habilitado al efecto. El resto de requerimientos relacionados con la seguridad y custodia de la imagen generada se deben cumplir en todo caso.

En este caso, por tanto, no es imprescindible disponer de hardware y software específicamente homologado, pero sí que hay que cumplir con los siguientes requerimientos en el proceso de digitalización:

- El proceso de escaneo se debe realizar por medios fotoeléctricos, utilizando un dispositivo de captura, el cual genera un archivo imagen, al que se aplican los procesos de optimización que se consideren adecuados.
- La imagen se pone a disposición de un usuario habilitado, que la compara con el original en papel para garantizar la identidad. Para garantizar la integridad y autenticidad de la imagen, una vez hecha la comprobación la firma con su certificado digital.
- El documento imagen se deberá completar con los metadatos correspondientes, a fin de generar un documento electrónico completo. Normalmente, en el proceso con intervención humana, esta carga de metadatos se hará manualmente.
- Las condiciones técnicas y requerimientos para la generación y verificación de las firmas serán las establecidas por las normativas correspondientes.
- El certificado digital a emplear será el sello de órgano hechas las habilitaciones correspondientes.

A partir de aquí, el documento sigue el mismo proceso que en la digitalización automatizada, y se deberá incorporar un sistema de gestión documental adecuadamente preparado para garantizar la correcta clasificación y gestión del documento resultante.

**b)** **Proceso de digitalización automatizada**, en la que el sistema garantiza de forma autónoma la autenticidad y la integridad de la copia. Una digitalización segura automatizada se obtiene empleando una plataforma compuesta por un dispositivo de captura de la imagen y un software que sea capaz de generar un archivo que contendrá la imagen digital del documento original en formato papel. Además, para asegurar una reproducción fiel e integra del documento digitalizado, será necesario acreditar que la imagen digital se ha obtenido mediante un proceso automático sin interrupción y sin intervención de ninguna persona física, en línea a lo establecido en la Resolución de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, sobre el procedimiento para la homologación de software de digitalización contemplado en la Orden EHA /962/2007, de 10 de abril de 2007.

Concretamente, la plataforma para la digitalización certificada deberá cumplir los siguientes requerimientos:

- El proceso de escaneo se debe realizar por medios fotoeléctricos, utilizando un dispositivo de captura, el cual genera un fichero.
- A continuación, se aplica el proceso de optimización de la imagen, con el fin de obtener una imagen con mayor calidad; se pueden usar softwares específicos, que deberán estar

firmados digitalmente por el fabricante (para garantizar que no se han producido manipulaciones).
• Firma de la imagen del documento digitalizado, para garantizar su integridad y autenticidad.

• En aquellos casos que sea necesaria la intervención humana, la aplicación deberá disponer de mecanismos estrictos de seguridad que permitan guardar pruebas de todas las acciones realizadas (trazabilidad).
• Hay que vincular el archivo de imagen en los metadatos técnicos, ya sea a través de una estructura de archivo. xml o a través de la inserción de los metadatos en base de datos o en el gestor documental.
• Las condiciones técnicas y requerimientos para la generación y verificación de las firmas serán las establecidas por las normativas correspondientes.
• Los certificados digitales a emplear en procesos automatizados y desatendidos será un sello de órgano o un certificado de hardware, como un sello electrónico.
• El documento digitalizado se deberá incorporar a un sistema de gestión documental adecuadamente preparado para garantizar la correcta clasificación y gestión del documento resultante.

El software deberá cumplir las siguientes características:

• El proceso de captura debe garantizar una imagen fiel e íntegra de cada documento, firmada electrónicamente, así como la organización de la documentación en una base de datos documental.
• El software debe generar documentos en alguno de los formatos incluidos en el catálogo de formatos establecidos en la Política de Identificación, Firma y Sello de la Universidad.
• El nivel de resolución debe ser como mínimo 200 ppp.
• El medio empleado para la digitalización debe ser fotoeléctrico.
• La calidad de la imagen capturada se debe optimizar.

Por tanto, todo proceso de digitalización de documentos podría ser considerado digitalización certificada, siempre que cumpla con los requerimientos enumerados en los párrafos anteriores. Concretamente, la Norma Técnica de Interoperabilidad de "Digitalización de Documentos" establece unos requerimientos mínimos a cumplir por la imagen resultante de la digitalización, a los que se añadirán aquellos que se consideren necesarios para garantizar la fidelidad de la imagen y la integridad del archivo electrónico resultante.

1.3. En atención al agente que realiza la digitalización

En atención al agente que realiza la digitalización, se consideran los siguientes tipos de procesos de digitalización:

a) **Proceso de digitalización interna**, entendido como el proceso de conversión a formato electrónico de documentación en soporte papel que se encuentra en poder de la URJC, realizado por la propia Universidad. Incluye la digitalización, manual o automática, realizada en las oficinas de registro u otros lugares de presentación de documentación, y la digitalización por parte de las unidades administrativas o por los archivos de gestión.

b) **Proceso de digitalización externalizado**, responde a aquellos procesos de digitalización que no se pueden abordar mediante recursos internos, y por tanto se decide contratar a un proveedor externo especializado en este tipo de trabajos, para poder realizarlo. El proceso de conversión a formato electrónico de documentación en soporte papel que se encuentra en poder de la URJC será realizado por un proveedor externo contratado a este efecto. Este proceso debe ser necesariamente ejecutado de forma automatizada. Para obtener unas imágenes electrónicas de los documentos originales en soporte papel, con el máximo de garantías, será necesario redactar un contrato en el que se establecerá un procedimiento estricto y detallado, en el que se describan todas las tareas a realizar concretando al máximo como se llevarán a cabo, incluyendo un riguroso control de calidad y unas medidas de seguridad estrictas para garantizar al máximo la calidad, confidencialidad e integridad. Además, es imprescindible que se mantenga trazabilidad de todo el proceso, anotando el máximo de información de todas y cada una de las tareas realizadas. Se podrá realizar un contrato, en el que la Universidad y la empresa tercera hacen constar por escrito las condiciones que regirán la relación, concretando los derechos y deberes de cada una de las partes, y los aspectos imprescindibles que debería incluir este contrato que se establecen en el punto 2.3.

**2. Modelo organizativo**

2.1. Agentes y responsabilidades

Serán competentes en el ámbito de la digitalización segura los siguientes agentes:

1. La Secretaría General, o el órgano en quien se delegue, que se encargará de:
   i. Autorizar y aprobar los procesos de digitalización segura de carácter horizontal en la URJC.
   ii. Autorizar y aprobar las normas técnicas generales a utilizar en la digitalización segura.
2. La Gerencia General se encargará de:
   i. Proponer al órgano competente la aprobación de procesos de digitalización
   ii. Hacer seguimiento de la aplicación del protocolo y proponer los cambios y las mejoras que se consideres adecuadas.
   iii. Formular las directrices de gestión documental de las copias electrónicas.
   iv. Informar a los órganos y unidades, de los criterios y normas para la digitalización, y en particular sobre los contenidos de esta instrucción.
3. El Consejo de Administración Electrónica se encargará de:
   i. Validar y aprobar el proyecto de digitalización segura y el cumplimiento del plan de calidad.
   ii. Evaluar y valorar los documentos digitalizados según el modelo de gestión documental de la URJC.
   iii. Autorizar las solicitudes de eliminación de documentos originales o copias auténticas en papel cuando las mismas sean objeto de digitalización segura y se den las condiciones exigibles.
4. El responsable de la documentación a digitalizar se encargará de presentar al Consejo de Administración Electrónica, para su validación y aprobación, un proyecto de digitalización segura, que incluya un plan de calidad, con los contenidos que se prevén en esta política. Es responsable de supervisar la ejecución de los procesos de digitalización interna por parte del personal de la URJC.

5. El Área de TI se encargará de:
   i. Gestionar los proyectos tecnológicos y de seguridad para la digitalización segura.
   ii. Establecer normas, guías y estándares técnicos, de seguridad y de firma electrónica que ofrezcan las garantías del proceso de digitalización para el cumplimiento de esta instrucción.
   iii. Establecer la seguridad de los sistemas de información y de protección de datos de la URJC para determinar las medidas suficientes respecto a la confidencialidad, integridad y disponibilidad de los servicios y la información.

2.2. Proyecto de digitalización

2.2.1. Elaboración

Las unidades administrativas que quieran realizar la digitalización segura de documentos en soporte papel deberán elaborar un proyecto de digitalización previo.

Estos proyectos de digitalización segura que impliquen eliminación de soportes en papel deberán llevarse a estudio y aprobación por el Consejo de Administración Electrónica.

El alcance de la responsabilidad del órgano o unidad administrativa que quiera iniciar un proyecto de digitalización incluye la preparación, gestión y control del proceso, así como la preparación de la documentación digitalizada para su transferencia al Archivo Central.

Es también responsabilidad del órgano informar a todas las partes implicadas en el proyecto.

2.2.2. Contenidos mínimos

El proyecto de digitalización debe disponer de los siguientes contenidos mínimos:

a) Justificación del proyecto.
b) Alcance del proyecto:
   a. Identificación detallada del tipo de documentos afectados, y de la fase en la que se encuentran los documentos a digitalizar.
   b. Indicación del tipo de digitalización a aplicar
   c. Identificación de las series documentales correspondientes.
   d. Identificación del valor de los soportes en papel a sustituir, si es necesario.
   e. Análisis de riesgos en caso de eliminación de los soportes a sustituir, con atención especial al tratamiento de datos de carácter personal.
   f. Otros tratamientos a realizar, como la transformación de la imagen en texto y su procesamiento adicional.
c) Si es necesario, la propuesta de eliminación de los soportes originales.
d) Formulario de cumplimiento de los requerimientos contenidos en esta instrucción.
e) Incluir un plan de calidad.
f) Impacto económico del proyecto.

2.3. Digitalización externalizada

La externalización del servicio de obtención de la imagen electrónica a través de medios fotoeléctricos de los documentos en soporte papel deberá ser aprobada por la Gerencia General.

La externalización del servicio deberá formalizarse en un contrato, en el que se debe de prever la actuación del proveedor como encargado del tratamiento de datos de carácter personal, el cual debe implantar las correspondientes medidas de seguridad.

Los licitadores deben presentar un plan de calidad propio que incluya los contenidos requeridos en este documento.

Se nombrará un responsable de la URJC que supervisará los trabajos realizados por el proveedor del servicio. Este responsable comprobará que el proceso cumpla técnicamente lo dispuesto en esta instrucción y validará la calidad del servicio.

En el traslado de la documentación, de ser necesario, se deberán adoptar medidas dirigidas a evitar la sustracción, destrucción, pérdida o acceso indebido a la información y a cubrir los riesgos que se deriven. En el caso de los datos de carácter personal a los que correspondan medidas de seguridad de nivel alto, se deberá de impedir también la manipulación, además de las situaciones antes indicadas.

**3. Normas técnicas**

Los requisitos técnicos a aplicar en los procesos de digitalización serán, para cada tipo de proceso y proyecto, los siguientes:

1) Requisitos del proceso de preparación de la documentación a digitalizar
2) Requisitos de los sistemas informáticos y herramientas a utilizar, en particular respecto la imagen.
3) Requisitos de metadatos del documento electrónico
4) Requisitos de firma del documento electrónico

3.1. Preparación de la documentación a digitalizar

El responsable del proyecto deberá preparar la documentación a digitalizar de acuerdo con los siguientes requerimientos:

a) La documentación tiene que estar evaluada, para conocer los parámetros mínimos necesarios de la digitalización.
b) La documentación tiene que estar ordenada y, si puede ser, paginada.
c) Es necesario incluir referencias de inicio y de final de cada expediente.
d) Es necesario eliminar aquellos elementos que no formen parte de la documentación o que puedan impedir la correcta digitalización y visualización del documento.
e) Es necesario revisar que el estado físico de la documentación sea el adecuado y no se hallen dobleces ni roturas.
f) Es necesario revisar que no se incluyan en los expedientes a digitalizar soportes no digitalizables.

3.2. Sistemas informáticos y herramientas a utilizar

Los programas, herramientas genéricas y aplicaciones a utilizar para cumplir con el procedimiento de digitalización tienen que ser aprobados por el órgano competente indicado en la sección 2.1 de este documento.

Se tiene que establecer un proceso informático que, garantizando en todo momento la integridad de las operaciones, ejecute las siguientes tareas:

a) Digitalización por un medio fotoeléctrico, de forma que se obtenga una imagen electrónica en la memoria del sistema asociado al dispositivo.
b) Si fuera necesario, optimización automática de la imagen electrónica para garantizar su legibilidad, de forma que todo el contenido del documento origen pueda ser apreciado y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros u otros similares).
c) Asignación de los metadatos al documento electrónico digitalizado, de acuerdo con lo que dispone la sección 3.3 de este documento.
d) Firma de la imagen electrónica, en los términos previstos en la sección 3.4 de este documento.
e) Se tiene que garantizar que el documento digitalizado es una copia completa del original al que reemplaza, de acuerdo con el plan de calidad establecido.

La selección de los dispositivos de obtención de la imagen electrónica tendrá en cuenta los siguientes requisitos:

a) Las imágenes electrónicas tienen que representarse usando formatos y resoluciones aprobadas en la política de documento electrónico de la URJC.
b) No se podrá usar compresión excepto si se garantiza que no afecta negativamente a la calidad de la imagen obtenida.
c) Aunque el formato de la resolución se presente en píxeles por pulgada, serán válidos otros formatos que sean equivalentes a estas resoluciones.
d) Se tiene que indicar de forma justificada el nivel de resolución que efectivamente se aplique en función de las necesidades del documento, especialmente desde la perspectiva de prueba (Formato de imagen)
e) La imagen original tiene que ser fiel al documento original, por lo que:
    a. Se tiene que respetar la geometría del documento origen en volumen y proporciones.
    b. No tienen que contener caracteres o gráficos que no figuren en el documento origen.
    c. Se pueden eliminar las páginas de los documentos a digitalizar que se encuentren en blanco, o que no incorporen información con valor administrativo, legal, informativo, cultural o histórico, de lo que es necesario dejar constancia.

Se podrá prescindir de este aspecto cuando el original tenga únicamente un valor informativo, y no jurídico ni cultural, que será necesario justificar.

Los ficheros de imagen se almacenarán en un repositorio documental corporativo de la URJC. Este almacenamiento será en el formato de captura o bien en un contenedor que no incorpore alteraciones en el aspecto de las imágenes, como por ejemplo PDF/A, ISO 19005-1:2005 o ISO 19005-2:2011.

No resulta obligatorio ensobrar los documentos digitalizados usando el formato enidoc definido en la Norma Técnica de Interoperabilidad de Documento Electrónico, si bien este ensobrado se tiene que producir en caso de intercambio del documento digitalizado, por lo que se tiene que garantizar esta posibilidad en todo caso.

El sistema de digitalización tiene que considerar la aplicación de un conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitan garantizar mediante su

cumplimiento que, en todo momento, el estado de la aplicación de digitalización y los dispositivos asociados producirán imágenes fieles al documento en soporte papel.

Estas operaciones se tienen que documentar en el plan de calidad de cada proyecto de digitalización, con los siguientes contenidos mínimos:

a) Descripción y configuración de la infraestructura tecnológica.
b) Procedimientos de digitalización: fiabilidad, márgenes de error, control de calidad…
c) Mantenimiento y actualización de los componentes técnicos.
d) Plan de pruebas y auditoría periódica.

El sistema de digitalización usado tiene que cumplir los requerimientos de la normativa de protección de datos de carácter personal y, en concreto, las obligaciones previstas en la reglamentación en función del nivel de las informaciones contenidas en los documentos a digitalizar.

Para la determinación de este nivel se tiene que tener en cuenta la clasificación en protección de datos de la serie correspondiente.

En cada proyecto es necesario que se defina cómo se identifican de forma unívoca los ficheros que se generan en la digitalización.

3.3. Metadatos del documento electrónico

El documento digitalizado con la consideración de soporte de sustitución tiene que estar identificado individualmente y vinculado al contexto de creación y uso.

La asignación de los metadatos seguirá las indicaciones reflejadas en la política de gestión documental de la URJC. Es posible que se incorporen en la digitalización certificada de copias auténticas en soporte papel los siguientes metadatos.

Metadatos de digitalización segura. Los metadatos que son de aplicación a las copias auténticas de documentos en papel que se generen en el marco de las actividades del Universidad, y que se deberán añadir a los identificados el vocabulario de metadatos se relacionan a continuación:

| Elemento | Metadato | Definición |
|---|---|---|
| eEMGDE14.1 | Soporte origen | Valor: Papel |
| eEMGDE14.4 | Nombre de la aplicación de creación | Denominación del software utilizado para li digitalización del documento papel. |
| eEMGDE 14.5 | Versión de la aplicación de creación | Versión de la aplicación de creación |
| eEMGDE 14.7 | Resolución | Valor de resolución en píxeles per pulgada empleada en la digitalización. |
| eEMGDE 20.2 | Característica de la copia | Información sobre las características de la copia. |
| eEMGDE 20.2.1 | Tipo de copia | Obligatorio en todo caso con el valor: "Copia electrónica auténtica de documento papel" |
| eEMGDE21 | Trazabilidad | Incorporar toda la información referente a la persona o procedimiento administrativo automatizado que ha realizado el proceso de copia |

3.4. Firma del documento electrónico

El documento electrónico digitalizado por medio del proceso de digitalización segura incluirá, al menos, una firma electrónica con sello de fecha y hora:

a) En caso de digitalización segura manual, es necesario que la firma se produzca siguiendo las normas de competencia y procedimiento de la URJC.
b) En caso de digitalización segura automatizada, tanto interna como externa, se tiene que usar un sello electrónico específico para este propósito.

En los dos casos se tendrá en cuenta lo dispuesto en la política de firma electrónica de la URJC.

Universidad Rey Juan Carlos

**INSTRUCCIÓN DE PRESERVACIÓN DE DOCUMENTOS**

**1. Introducción**

La preservación de recursos digitales plantea una serie de problemas relacionados con la gestión técnica y la obsolescencia de la tecnología. Los soportes de almacenamiento pueden ser inestables y se deterioran con los años. Es necesario el mantenimiento de los sistemas, la verificación de la integridad y una garantía de acceso permanente. Los factores de carácter institucional, como cambios en la estructura de la organización o bien en los recursos humanos, materiales y económicos dedicados son también elementos que impactan en la preservación a largo plazo.

La URJC dispone de repositorios que permiten la recopilación, gestión, difusión y preservación de la producción institucional, docente y científica de la Universidad.

Un repositorio digital aporta aspectos beneficiosos como, por ejemplo:

- La custodia de la producción de las autoridades académicas, investigadores, estudiantes y personal propio.
- El cumplimiento de los requisitos legales de accesibilidad, integridad y disponibilidad.
- La accesibilidad a aquellos recursos necesarios para la ejecución de la docencia y la investigación.
- La garantía del acceso a lo largo del tiempo.
- Otorga evidencia de las actividades realizadas por las instituciones que conforman la Universidad, así como las personales.
- La creación de la memoria de la institución ya sea personal o colectiva.

La Gerencia de la Universidad impulsa la creación de esta instrucción de preservación digital para garantizar la continuidad y seguridad del repositorio digital.

La preservación de estos recursos digitales debe tener en cuenta los problemas que plantea su gestión técnica.

Detalles como la inestabilidad de los soportes que almacenan los datos, su posible deterioro, el cambio de los formatos, la intervención humana, las amenazas digitales (virus…) o naturales (exposiciones al fuego o al agua en los centros de procesamiento de datos) pueden modificar o bien destruir finalmente toda la información allí guardada.

**2. Instrucción de preservación**

2.1. Alcance

Este documento quiere facilitar y garantizar el acceso a los contenidos digitales de la URJC.

La URJC dedicará los esfuerzos y recursos necesarios para preservar los documentos creados o gestionados digitalmente, custodiados desde el repositorio corporativo, para permitir su accesibilidad en el tiempo. Las responsabilidades en este aspecto serán las detalladas en el documento de Política Documenta (roles y responsabilidades)

Se podrá almacenar archivos digitales creados mediante las diversas aplicaciones, plataformas informáticas y desde cualquier medio digital, siempre que pertenezcan a personas u organizaciones vinculados con la URJC o bien dispongan de convenios de colaboración.

Se podrá, también, almacenar los archivos de digitalización de los documentos no digitales.

2.2. Objetivos

Esta instrucción de preservación debe servir para conseguir los siguientes objetivos:

- Proteger de la obsolescencia de los elementos físicos que sustentan el servicio.
- Preservar los documentos digitales de la URJC almacenados en los repositorios proporcionados por el Área de TI a lo largo del tiempo.
- Transformar, cuando sea necesario, el formato de los documentos digitales.
- Asegurar el acceso a los materiales por medio de identificadores únicos para los documentos.
- Hacer disponibles los sistemas que captan, gestionan y conservan los documentos digitales.

2.3. Preservación de los documentos electrónicos

La preservación de documentos electrónicos será proactiva. Se deberá monitorizar periódicamente el entorno actual de software y hardware para averiguar si alguno de los formatos en los que se almacenan los ficheros, o los soportes de almacenamiento, tienen problemas.

El programa de vigilancia contemplará los siguientes aspectos:

- Mecanismos para monitorizar la viabilidad de formatos y soportes.
- Criterios de evaluación de formatos: plazo de conservación de los documentos, usuarios y fines de acceso a los documentos, plataformas y tecnologías en que deben de estar accesibles, etc.
- Criterios de evaluación de soportes.
- Dictamen sobre intervención.
- Seguimiento del proceso del cambio y validación de la intervención.

El equipo responsable del programa de preservación digital será multidisciplinar, formado por técnicos informáticos y responsables de Biblioteca y del Archivo General de la URJC.

Para asegurar la accesibilidad de los documentos en el tiempo, se convertirán los formatos si se detecta riesgo de que no sean legibles (riesgo de obsolescencia).

La URJC ofrecerá un servicio que permita la conversión de formatos obsoletos a formatos actuales generando copias autenticadas de los documentos originales.

Para evitar la pérdida de los registros debido a la degradación del soporte de almacenamiento, es necesario establecer un refresco periódico que asegure la legibilidad continuada. El refresco debe realizarse a intervalos regulares que no deben nunca superar los periodos recomendados por los fabricantes de los dispositivos.

Si se determina que el soporte de almacenamiento utilizado para la custodia ya no es el apropiado, debe de establecerse una migración de soportes. La migración difiere del refresco en que los documentos electrónicos son reescritos en un soporte diferente al inicial.

Tras un proceso de refresco o migración se debe de realizar una verificación mediante una comparación de bits entre la versión original y la de destino de cada uno de los ficheros.

La gestión de documentos electrónicos será concretada gracias al desarrollo de un programa continuo de gestión de documentos y expedientes electrónicos que abarca todas las etapas de su ciclo de vida.

2.4. El uso de la firma electrónica

Uno de los retos más importantes de la firma electrónica deriva de la obsolescencia de las cifras criptográficas, que afecta a la validez matemática de las firmas electrónicas generadas en el pasado y, por tanto, genera un problema evidente respecto a la perdurabilidad de los documentos firmados electrónicamente, especialmente en relación con el valor probatorio de los citados documentos.

Para mitigar estos riesgos, es necesario preservar la firma electrónica al menos durante el plazo de vida del documento correspondiente a las fases activa y de vigencia, ya que en estas etapas es cuando el documento puede ser requerido como prueba en un procedimiento judicial.

En este documento se incluye el marco normativo, tanto legal como tecnológico, que regula la preservación de la firma electrónica.

2.5. Funciones y responsabilidades

El Área de TI es la responsable de la preservación de los contenidos digitales del repositorio de la URJC.

El equipo de gobierno da el apoyo necesario desde el punto de vista de gobernanza, así como económico para contribuir activamente en las acciones necesarias para cumplir y hacer cumplir esta instrucción.

Las funciones y responsabilidades que se deben tener en cuenta son:

- El Área productora es la responsable de la captura, difusión y promoción de los contenidos.
- La Biblioteca universitaria será responsable de la revisión y mantenimiento de los registros bibliográficos. También se responsabiliza de la conservación de la documentación necesaria para la trazabilidad futura.
- El Área de Archivo será responsable de la revisión, mantenimiento y conservación de toda la documentación administrativa.
- El Área de TI es la responsable de la instalación de las herramientas tecnológicas necesarias para el mantenimiento y monitorización de los programas y del hardware necesario para el correcto funcionamiento del servicio.
- La Gerencia de la URJC debe de garantizar que el Área de TI dispondrá de la sostenibilidad suficiente tanto a nivel de equipamiento como de recursos humanos.
- Todo el personal de la URJC es responsable de una adecuada custodia de los sistemas de acceso restringido, así como de la confidencialidad de las contraseñas y pines que se les asigne.

Se garantizará en todo momento la autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad de documentos y expedientes, lo que permitirá la protección, recuperación y conservación física y lógica de los documentos y su contexto.

Para el desarrollo de un plan de conservación es necesario que la Universidad cuente con elementos como un cuadro de clasificación y un calendario de conservación, y otros como los formatos y tipos de firma aplicables a los documentos, la definición del esquema de metadatos y la descripción de documentos, la asignación de roles y responsabilidades y las directrices para la definición de los procesos de gestión documental.

La valoración de documentos, su clasificación, calificación y la determinación de los calendarios de conservación, junto a otros aspectos como los requisitos y frecuencia de acceso, asegura que:

i. Se conservan todos los expedientes, bajo medidas de protección adecuadas a su valor para la administración.
ii. Ingresan en el archivo, individualmente o como parte de un expediente, todos los documentos que es necesario conservar.
iii. Los documentos y expedientes ingresan en el archivo en formatos adecuados, firmados y con los metadatos necesarios para su conservación y recuperación del archivo.
iv. Los documentos se transfieren a archivos (central, histórico) con características adecuadas a su estado dentro del ciclo de vida.
v. Se eliminan, de acuerdo con la normativa y los procedimientos aplicables, los documentos que han perdido su valor.

**3. La preservación de las firmas electrónicas**

3.1 Las normas técnicas de interoperabilidad aplicables a la preservación de la firma electrónica

La disposición adicional primera del ENI indica que se despliegan diversas normas técnicas de interoperabilidad (en adelante, NTI) que son de obligado cumplimiento por parte de las administraciones públicas, de las que en este proyecto nos interesan particularmente las siguientes:

- NTI de documento electrónico.
- NTI de política de firma electrónica y de certificados de la Administración.

El epígrafe II.7 de la Norma Técnica sobre archivado y custodia, indica en su regla 1ª que "atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones", para posteriormente autorizar, en su regla 2ª, los siguientes métodos de conservación:

- Las denominadas "firmas longevas".
- Otros métodos, que podemos englobar en la denominación genérica de "repositorio seguro".

La elección de uno u otro mecanismo es responsabilidad de la entidad gestora de la política de firma electrónica, siendo relevante indicar que, de acuerdo con la regla 6ª del epígrafe II.7 de la Norma Técnica, "la definición de medidas y procedimientos para archivado y custodia de firmas electrónicas se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política", lo cual exige un análisis de las necesidades de conservación de los documentos firmados electrónicamente, en los términos dispuestos por la normativa de gestión de documentos de archivo correspondiente, y la aplicación de "lo establecido en la NTI de Política de gestión de documentos electrónicos" (regla 7ª del epígrafe II.7).

Finalmente, la regla 4ª del epígrafe IV.3 de la Norma Técnica insiste en que "las políticas de firma contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable". Todos estos aspectos son recogidos en la Políticas de Identificación, firma y sello electrónico de la Universidad en su apartado 3.8.

3.2 La preservación mediante firmas longevas

La Norma Técnica de Interoperabilidad de política de firma electrónica no define qué es una firma electrónica longeva, si bien la describe en su regla 2ª.a) del epígrafe II.7, en el siguiente sentido: "firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3", caracterización que resulta necesario completar con las restantes previsiones de la norma.

La regla 3ª del epígrafe II.7 indica que "cada política de firma definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas y sellos", de lo cual se desprende la caracterización de la firma electrónica longeva como una firma que ha sido completada. En este sentido, la misma regla 3ª indica que "dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma como los certificados e informaciones de estado utilizadas en su validación", apuntando los elementos que se contienen en la firma electrónica longeva.

La regla 4ª del mismo epígrafe II.7 ofrece algo más de información, cuando indica que "el almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica […]: a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades […] 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.

Sin embargo, es la regla 5ª del epígrafe II.7 la que aclara de forma más completa la finalidad de la firma electrónica longeva, cuando establece que "la protección de la firma electrónica frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos: a) Utilización de mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto", recomendando además "utilizar mecanismos de resellado/refirma en el caso de obsolescencia de los algoritmos o formatos, con un algoritmo más robusto".

En efecto, la longevidad de la firma electrónica se logra mediante la protección técnica de la firma electrónica empleando sellos de fecha y hora, siguiendo lo establecido en las especificaciones técnicas europeas de referencia.

En este sentido, la regla 1ª del epígrafe IV.3 de la Norma Técnica de Interoperabilidad de política de firma electrónica establece que "en el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma", mediante el elemento SignatureTimeStamp.

Si bien la Norma Técnica no explicita en las razones técnicas de esta aproximación, se pueden deducir con facilidad de las citadas especificaciones técnicas, así como de las reglas de validación de firma prevista en la Norma. En concreto, se recordará que el aspecto más relevante en la validación de la firma electrónica era la determinación del momento de producción de la firma, para poder comprobar su corrección empleando certificados que eran válidos en el momento de creación de la firma, pero que ya han perdido su validez por el transcurso del tiempo.

Como las referencias a las informaciones de estado de certificados también se encuentran firmadas, con carácter general, su validez también se puede perder a largo del tiempo y, por tanto, deben ser también protegidas por los sellos de fecha y hora.

Por este motivo, la regla 2ª del epígrafe IV.3 determina que "para la conversión de una firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES y las referencias.
b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:
    a. Certificados: incluyendo los certificados del firmante y de la cadena de certificación, tanto del firmante como del sello de tiempo.
    b. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.
c) Aplicación del sellado a las referencias a los certificados y a las informaciones de estado", mediante diversos elementos disponibles a tal efecto, que convierten la firma al perfil AdES-X (firma electrónica extensa), –XL (firma electrónica súper extensa) o –A (firma electrónica de archivo, que se identifica con la firma electrónica longeva en este epígrafe).

El verdadero problema reside en que también los sellos de fecha y hora son documentos firmados electrónicamente y, por tanto, su validez también es limitada en el tiempo, lo cual exige la incorporación periódica de nuevos sellos de fecha y hora que protejan todas las informaciones anteriormente referidas. A este fenómeno se conoce como "resellado", y para soportarlo técnicamente se emplea el elemento ArchiveTimeStamp definido en las especificaciones técnicas europeas de referencia (existente únicamente en firmas AdES –A).

En principio sería suficiente con incorporar un sello de fecha y hora de archivo de larga duración, para lo cual se precisa que su algoritmo sea ciertamente robusto, y emplear una clave de longitud elevada. Mientras dicho algoritmo y clave se mantengan vigentes, no resultará necesario añadir un nuevo sello de fecha y hora.

3.3. La preservación mediante repositorio seguro

La Norma Técnica permite también la conservación de la firma electrónica, mediante "otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo determinado", según autoriza la regla 2ª.b) del epígrafe II.7, de forma alineada con la previsión equivalente que se encuentra en las normas técnicas europeas de referencia.

La misma regla continúa indicando que "todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada", norma complementaria de la anterior.

Asimismo, se establece que “los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por 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”.

En el caso del repositorio seguro para la conservación de la firma electrónica será aplicable la regla 3ª del epígrafe II.7, que determina que “cada política de firma definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas”, si bien en este caso resulta de extraordinaria importancia su aplicación, al no existir una especificación técnica de referencia que defina estos aspectos.

Por tanto, cobra mayor valor la parte final de dicha regla, que establece que “dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma como los certificados e informaciones de estado utilizadas en su validación”, que realmente deberá describir detalladamente estas cuestiones.

En la regla 4ª del mismo epígrafe II.7 es donde se autoriza que “el almacenamiento de los certificados y las informaciones de estado podrá realizarse […] en un depósito específico: […] b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente”, al objeto de proteger su integridad y autenticidad para uso probatorio.

Por su parte, la regla 5ª del epígrafe II.7 concreta que “la protección de la firma/sello electrónico frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos: […] c) Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica”.

### 3.4. Recomendaciones

Recomendaciones técnicas referentes a la firma electrónica de los expedientes y sus documentos electrónicos archivados definitivamente y en el momento de su preingreso.

Sobre las firmas longevas en expediente electrónico y su ingreso en el archivo.

1. El archivo 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.
2. 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.
3. No podrán ingresarse expedientes con firmas del índice inválidas, antes de su pre-ingreso deberá regenerarse y presentar una firma correcta.

Sobre el resellado de expedientes y documentos archivados.

1. El sistema de archivado deberá controlar la validez y tener actualizadas las firmas de los expedientes electrónicos que custodia.
2. Será suficiente con el resellado de la firma longeva del índice del expediente electrónico.

3. 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.

Sobre las firmas de los documentos electrónicos en el momento del ingreso:

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, 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.
d. 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.

3.5 Mantenimiento y revisión

Se establece un periodo de cinco años para la revisión de esta instrucción que se llevará al Consejo de Administración Electrónica. En caso de cambios importantes desde el punto de vista tecnológico se podrán realizar revisiones extraordinarias.

**Entrada en vigor.**

Esta Resolución entrará en vigor al día siguiente de su publicación en la Sede Electrónica de la Universidad Rey Juan Carlos

Contra la presente Resolución, que no pone fin a la vía administrativa, podrá interponerse recurso de alzada ante el Rector de la Universidad Rey Juan Carlos, en el plazo de un mes contado a partir del día siguiente a su publicación, de conformidad con los artículos 121 y 122 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

LA SECRETARIA GENERAL

Pilar Trinidad Núñez