



SERVICIOS EN LOS ARCHIVOS UNIVERSITARIOS, PRESERVACIÓN Y SEGURIDAD: ANÁLISIS DE LA SITUACIÓN EN LAS UNIVERSIDADES PÚBLICAS ESPAÑOLAS

SERVICES IN UNIVERSITY ARCHIVES, PRESERVATION AND SECURITY: ANALYSIS OF THE SITUATION IN SPANISH PUBLIC UNIVERSITIES

Autoras:

Esther Ovejero Ruiz. ODILO. eovejero@odilo.us ORCID 0000-0003-1702-6728

María García González. ODILO. mgarcia@odilo.us ORCID 0000-0002-9577-8434

Resumen:

Este trabajo analiza los requisitos normativos y legales que exigen a las universidades públicas y a sus respectivos archivos la implantación de servicios disponibles a través de medios electrónicos con garantías de seguridad y de preservación digital. A continuación, para analizar la situación en las universidades públicas españolas, se realiza la revisión de sus sedes electrónicas y sitios web en lo relativo a disponibilidad de los servicios de archivo y los criterios de seguridad y preservación digital.

Abstract:

This paper analyzes the regulatory and legal requirements that require public universities and their respective archives to implement services available through electronic means with guarantees of security and digital preservation. From the above, the situation in Spanish public universities is analyzed from the review of their electronic websites in relation to the availability of archiving services, and security and digital preservation criteria.

Palabras clave:

Ciberseguridad; Preservación digital; Archivos universitarios

Keywords:

Cybersecurity; Digital Preservation; Academic Archives

1. INTRODUCCIÓN AL OBJETO DE ESTUDIO Y METODOLOGÍA EMPLEADA

Los archivos universitarios públicos en particular, y las universidades en las que se circunscriben en general, están considerados como sector público institucional según la legislación administrativa vigente. Tienen, además, la plena consideración de administraciones, hecho que tiene una repercusión directa en el conjunto de preceptos que les son de aplicación y por tanto están obligados a cumplir con una serie de requisitos legales equiparándolos a otras administraciones como la Administración General del Estado o las autonómicas, por poner algunos ejemplos. El más importante de los preceptos aplicables a los archivos universitarios es el de la obligatoriedad de proporcionar sus servicios a través de medios electrónicos, para lo que deben poner a disposición de la comunidad universitaria y ciudadanos en general los canales de acceso que sean necesarios, así como los sistemas y aplicaciones para el acceso a estos servicios (artículo 12 de la Ley 39/2015).

Por si esto no fuera de por sí bastante, entre los elementos que conforman la panoplia de la administración electrónica y que son también extensibles al archivo universitario encontramos el concepto (y servicio) de «archivo electrónico único». Su entrada en vigor, esto es, su obligatoriedad, se ha pospuesto en varias ocasiones sin, al parecer, haber tenido en cuenta que el funcionamiento completo y coordinado de un sistema de gestión documental dentro de cualquier administración es inseparable del de su archivo. En cualquier caso, los preceptos relativos al «archivo electrónico único» entraron en vigor el 2 de abril de 2021 de modo que, desde entonces, «cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable [...]». Cabe hacer algún comentario acerca de la entrada en vigor que se produjo tras la modificación de la Ley 39/2015 vía Real Decreto-Ley 28/2020, lo que supone una extravagancia cada vez más habitual, esto es, la de los reales decretos-leyes cajones de sastre utilizados aludiendo a razones de extraordinaria y urgente necesidad. Nótese que, en este caso, el objetivo no era otro que el de prorrogar (con extraordinaria y urgente necesidad) la no aplicación de las disposiciones de archivo electrónico único durante 6 meses más. Por si esto fuera poco, el Real Decreto-Ley y la modificación del plazo de aplicación del

«archivo electrónico único» quedaron subsumidos en la Ley 10/2021, de 9 de julio, de trabajo a distancia, otra extravagancia más ya que esta ha dejado para la posteridad la prolongación de la prórroga de la no aplicación con carácter retroactivo: la Ley es de 9 de julio de 2021 y la prórroga era válida hasta el 2 de abril de 2022.

El alcance del concepto del «archivo electrónico único» ha suscitado un gran debate y análisis desde su aparición. Buena cuenta de ello son los trabajos, publicados (desde la perspectiva jurídica más que archivística, aunque no solo) desde entonces. Cabe resaltar las aportaciones de Lluís-Esteve Casellas Serra (2016), Gerardo Bustos (2018, 2021) o de Francisco Fernández Cuesta (2016, 2017) por citar solo algunos.

La presente aportación trata de complementar estos trabajos desde una perspectiva paralela y, a nuestro parecer, insuficientemente estudiada: preservación digital y ciberseguridad en relación con el concepto particular de «archivo electrónico único» y general de los servicios de archivo, centrado, además, en el ámbito universitario, aunque extensible a otras administraciones.

Vista ya la obligatoriedad de los servicios de «archivo electrónico único» y atendiendo a los otros dos temas de estudio de este trabajo (preservación y seguridad), podemos afirmar que existen tres vías para la puesta en marcha de los servicios del archivo: los medios y recursos de la propia administración, los medios de un proveedor externo de servicios o una combinación de las dos cosas. El análisis realizado tiene en cuenta esta cuestión en el sentido en el que se presumen las mismas garantías para estos conjuntos de servicios y gozan, por lo tanto, de plena validez y aplicación.

La metodología, utilizada se ha basado, por una parte, en el análisis normativo y legislativo de los preceptos relacionados con los servicios prestados por los archivos universitarios y con la seguridad y preservación de la información y documentación custodiadas. A continuación, sobre esta base, se ha realizado un análisis de los sitios web institucionales de universidades públicas (CRUE, 2022), de sus archivos y de sus respectivas sedes electrónicas, con el objetivo de valorar la información disponible sobre los temas de estudio. No se ha contactado con ninguna universidad o archivo para recabar información adicional.

2. SE SUPONE LA EXISTENCIA DE LOS SERVICIOS DE ARCHIVO Y SE INTUYE QUE DEBE HABER UNOS REQUISITOS DE SEGURIDAD Y PRESERVACIÓN PARA LOS ARCHIVOS, PERO ¿ESTÁN REGULADOS?

2.1. Servicios públicos accesibles a través de medios electrónicos: disponibilidad de servicios de archivo

Más allá de la citada obligatoriedad de la existencia de servicios accesibles a través de medios electrónicos y del «archivo electrónico único» de la normativa española, cabe destacar que la tendencia comunitaria de la Unión Europea se dirige, asimismo, hacia la existencia de un conjunto amplio de servicios públicos digitales en línea para todos los ciudadanos europeos (Fernández, 2022). Cabe decir que, en esta línea, la Comisión Europea ha publicado una declaración de principios y derechos digitales (Declaración europea sobre..., 2022) que dispone como un derecho fundamental el acceso a todos los servicios públicos clave a través de internet. Lo cual plantea serias dificultades a las reticencias relativamente habituales sobre la puesta a disposición en línea de determinados servicios públicos, y especialmente los que se proveen a través de los archivos. La ausencia de alternativas al acceso en línea a los servicios públicos estaba ya vetada en nuestro ordenamiento, pero, por si fuera poco, con estas declaraciones la legislación comunitaria no hace sino reforzar esta visión. Aun así es mucho el camino que queda por recorrer hasta contar con un conjunto de servicios plenamente accesibles y disponibles a través de vías exclusivamente electrónicas.

Conviene, llegados a este punto, que realicemos un repaso a la legislación y normativa nacional que, en relación con el concepto de «archivo electrónico único», afecta a los archivos universitarios en los aspectos de la preservación y la seguridad. En este sentido, hay tres textos legales más o menos recientes en los que se tratan los aspectos objeto de estudio, preservación y seguridad, estos son la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 40, de 1 de octubre, de Régimen Jurídico del Sector Público¹; y el

¹ Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>

Real Decreto 203/2021, de 30 de marzo², por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, este último orientado al desarrollo de las dos normas anteriores.

Además de la obligatoriedad ya comentada de la creación de un «archivo electrónico único» para cada administración, de modo que parecen diluirse o integrarse las tradicionales etapas del ciclo de vida del documento y los diferentes estadios archivísticos, la citada normativa y legislación nos presenta un archivo que, por supuesto, debe ser capaz de asegurar la integridad, autenticidad, confidencialidad, calidad, protección, conservación y acceso de los documentos que custodia. Aquí quedan apuntadas las exigencias de seguridad y preservación a las que nos referimos.

Estos tres textos legales guardan bastantes similitudes entre ellos, las definiciones que ofrecen son, prácticamente, copias con pequeños matices. En los tres se habla de la necesidad de conservar los datos de los expedientes, independientemente de su soporte asegurando el acceso a los mismos a lo largo del tiempo (preservación); y de garantizar la seguridad de los datos. Veámoslo con más detalle:

2.2. Seguridad

Como no podía ser de otro modo, la seguridad de la información es un aspecto clave tanto en el Real Decreto 203/2021, como en las leyes 39/2015 y 40/2015. El término «seguridad» se repite más de cien veces en estas normas, lo que nos induce a pensar que se están imponiendo medidas de ciberseguridad que responden a la realidad actual. Efectivamente, si analizamos el contenido, averiguamos que el marco de seguridad al que se está recurriendo constantemente es el del Esquema Nacional de Seguridad (ENS).

¿Es este marco del ENS suficiente para abordar las contingencias actuales? ¿y de cara al futuro? El Esquema Nacional de Seguridad tiene por objeto garantizar la

² Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032>

seguridad en el uso de los medios electrónicos, definiendo los principios y los requisitos orientados a salvaguardar la seguridad de la información y la protección de los datos personales. En el ámbito de los archivos universitarios (de los archivos en general), dadas las características de la información y documentación que conservan, especialmente en lo que tiene que ver con la protección de datos personales, y dadas las exigencias de disponibilidad del servicio como esencial en el contexto de la administración electrónica institucional, la categoría del ENS aplicable, y de los requisitos y obligaciones asociados, es la alta.

Mientras que la mayor parte del marco de las normas técnicas de interoperabilidad ha permanecido inalterado desde su publicación, en el caso del ENS, la última actualización fue en el año 2015, cuando en el Real Decreto 951/2015, se modificó el Real Decreto 3/2010, de 8 de enero. Esta actualización que tuvo como objetivo actualizar el marco normativo de acuerdo con la evolución tecnológica, las ciberamenazas y el contexto regulatorio internacional y europeo, no puede considerarse una modificación reciente aunque las guías de aplicación publicadas por el Centro Criptológico Nacional (CCN-CERT) y la evolución de la materia han sido constantes. Puede asegurarse que el marco que ofrece el ENS está plenamente vigente aunque no hay que descuidar su adecuación al contexto tecnológico actual.

Además, no se plantea como una recomendación, sino que queda clara su obligatoriedad cuando el artículo 38 del ENS, indica que la seguridad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos (entiéndanse incluidos los servicios de archivo), se regirán por lo establecido en el propio Esquema Nacional de Seguridad. Siendo además una obligación la acreditación de estos servicios en la línea de lo que indica el artículo 41: los órganos y entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

Por otra parte, ¿qué ocurre con la seguridad de los servicios prestados por terceros? La respuesta es que es igualmente obligatoria y su acreditación igualmente exigible. Así lo indica la «Guía de Seguridad de las TIC CCN-STIC 809» (CCN-CERT, 2019)

en sus apartados 41 y 42: «cuando las organizaciones del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del ENS, deberán estar en condiciones de exhibir [...] la Certificación de Conformidad con el ENS (obligatoriamente, cuando se trate de sistemas de categorías MEDIA o ALTA [...]), utilizando los mismos procedimientos que los exigidos para las entidades públicas. Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad [...]».

A la vista de esta situación, tanto si los servicios de archivo y la construcción del «archivo electrónico único» se desarrollan utilizando medios propios, como si se emplean proveedores de servicios o alternativas que combinan las dos categorías, no debería resultar descabellado, aplicar criterios de seguridad adicionales pero compatibles con el ENS especialmente en un ámbito, el del archivo, en el que pretendemos garantizar la conservación de la información pensando a muy largo plazo. No basta con afirmar que existen garantías, estas deberían ser acreditadas. Así, la certificación de los servicios del archivo bajo el paraguas del ENS debería completarse a través de normas como la ISO 27001 de seguridad de la información, la ISO 27701 de privacidad de la información acompañadas de las normas ISO 27017 y 27018 que garantizan la seguridad de los entornos *cloud computing* (en el caso de que este sea el modelo de prestación de servicios). La garantía de la continuidad de los servicios de archivo, que son críticos aunque la legislación se haya empeñado en prorrogarlos, se podría acreditar a través de normas como la ISO 22301, seguridad y resiliencia-sistema de gestión de la continuidad del negocio.

2.3. Preservación digital

En relación con la preservación digital, observamos referencias muy generales. La Ley 39/2015, indica en su artículo 17 que los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, la integridad y la conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar

los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. Y en la Ley 40/2015, en su artículo 46, se traslada la obligatoriedad de conservar la información generada por la administración, independientemente de su soporte.

Por su parte, el mucho más reciente Real Decreto 203/2021, en su artículo 54 puntualiza que se tratarán las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los propios documentos y de su contexto. Además, incide en que se planificarán las actuaciones de preservación digital que garanticen la conservación a largo plazo de los documentos digitales y permitan de esta forma dar cumplimiento a lo establecido.

En un contexto ya no circunscrito exclusivamente a la documentación generada en el marco de la administración electrónica, como indicaban las leyes 39/2015 y 40/2015, sino ampliado a un concepto de documentación en soporte electrónico más amplio, el del Real Decreto 203/2021, el objetivo parece estar claro: la preservación de la documentación (entiéndase en soporte electrónico) en un marco que en el que se asegure la autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad. Las regulaciones a las que aludimos nos alertan, asimismo, de la volatilidad de los soportes entendemos que con el fin de que las administraciones promuevan la definición de mecanismos de preservación de la información, que no son especificados. La externalización de estos mecanismos no está vetada a proveedores de servicios, pero, igualmente, los límites y criterios no son definidos.

A la vista de esta falta de especificidad en los conceptos, ¿podemos afirmar que es suficiente para dotar a las administraciones de herramientas que aseguren la preservación? ¿dónde se definen las características de las herramientas que han de utilizarse para asegurar los criterios de preservación? Y, si hay intermediarios o prestadores de servicios, ¿qué garantías deberían recabarse? ¿Por qué no se define con más detalle el papel que deben llevar a cabo las diferentes administraciones? ¿no sería interesante disponer de un modelo básico de referencia? ¿estos pocos apuntes legales acerca de la preservación digital son suficientes?

Quizá esas referencias, aunque necesarias, son realmente escasas. No proporcionan medios para acreditar la conservación a largo plazo de los documentos electrónicos y tampoco obligan a las administraciones a asegurar que prestan un servicio de preservación digital con unas mínimas garantías.

La preservación digital es cada vez más un reto para las administraciones públicas, pero también para los terceros que desarrollan herramientas de preservación y prestan sus servicios en esta materia. El ENS tiene en cuenta la posibilidad de la obsolescencia de los formatos y soportes, de ahí que incida que se debe asegurar, en todo caso, el traslado de los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. Si bien en ningún momento refleja la posibilidad de que los servicios de preservación no sean directamente gestionados por la administración pública. Sin duda, no todas las administraciones públicas en la actualidad tienen recursos para asumir con medios propios todo lo que implica la preservación.

Existen administraciones públicas que confían la preservación digital de terceros, sin embargo, no existen regulaciones (más allá del ENS) que exijan garantías de preservación digital. A nuestro entender, deberían regularse los requisitos y características que debe acreditar un tercero para gestionar la preservación digital de una administración pública: ¿a quién si no estamos confiando los fondos de los archivos? ¿quién acredita que se cumplen las garantías adecuadas en cuanto a seguridad y preservación digital?

En este sentido, la exigencia de requisitos basados en el estándar OAIS (Open Archival Information System) de la norma ISO 14721 debería ser el modelo de referencia ya que se ha convertido en el modelo de preservación digital por antonomasia. De nuevo, no debería bastar con decir que se cumple, es necesario buscar acreditaciones que lo garanticen. El modelo de preservación puede completarse con la certificación de otros estándares complementarios que garanticen, por ejemplo, las condiciones de conservación de evidencias de los repositorios de documentación como la ISO 17068 de repositorio de tercero de confianza para documentos electrónicos.

3. OBLIGACIONES DE INFORMACIÓN EN MATERIA DE SERVICIOS EN LÍNEA, PRESERVACIÓN Y SEGURIDAD: ¿CUÁL ES LA SITUACIÓN EN LOS ARCHIVOS UNIVERSITARIOS?

Una vez analizada la legislación y la normativa, desvelados los criterios de seguridad y preservación, y las exigencias de publicidad de los servicios públicos vinculadas al archivo, ha llegado el momento de valorar si están siendo realmente atendidas por los archivos universitarios. Si recopilamos lo tratado hasta ahora tenemos que:

- **En materia de existencia y publicidad de los servicios públicos**, la obligatoriedad de proporcionar sus servicios a través de medios electrónicos y de proporcionar una adecuada publicidad de estos medios. Entre estos servicios destaca el que materializa el concepto de «archivo electrónico único».
- **En materia de preservación digital**, se deben proporcionar condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los propios documentos y de su contexto. Se debe asegurar la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. No se constatan obligaciones de publicidad de las metodologías y herramientas de preservación aplicadas, pero son con certeza recomendables precisamente por los objetivos de conservación a largo plazo.
- **En materia de seguridad**, parafraseamos el contenido anteriormente extraído del ENS y de la guía «Guía de Seguridad de las TIC CCN-STIC 809» (CCN-CERT, 2019): la seguridad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos (tanto si los medios se suministran a través de recursos propios o proporcionados por terceros) se rige por lo establecido en el Esquema Nacional de Seguridad. Siendo además una obligación la acreditación de estos servicios de la conformidad con el ENS, que además serán de categoría alta por las características de la información y de los servicios de los archivos universitarios.

Pretendemos pues, valorar si los archivos universitarios públicos están cumpliendo con las exigencias anteriores y para ello hemos analizado si han dado publicidad a sus servicios y a las cuestiones de preservación y seguridad, independientemente de si se han desarrollado a través de medios y recursos propios o suministrados por terceros.

Buscamos reflejar cuál es la imagen que ofrecen los archivos universitarios públicos de sí mismos en relación con las materias de estudio, esto es, la publicidad que ofrecen acerca de sus servicios y de las cuestiones de preservación y seguridad. El análisis se ha llevado a cabo sin contactar con dichas instituciones, utilizando exclusivamente sus sitios web institucionales y los recursos en línea disponibles. Por este motivo pueden existir resultados que no se correspondieran con la realidad o que, simplemente, aunque el archivo en cuestión responda y cumpla con la cuestión planteada, sin embargo, no lo haya reflejado en su sitio web, sede electrónica, o en los servicios que ofrece a través de medios electrónicos.

Por tanto, utilizando como base los sitios web y sedes electrónicas de las 50 universidades públicas (CRUE, 2022) y de los archivos universitarios (cuando estos sitios específicos estaban disponibles) hemos planteado las cuestiones que se muestran a continuación acerca de la disponibilidad de servicios por parte de los archivos, sobre seguridad y en relación con las medidas de preservación digital existentes. Como podrá observarse en los resultados, los valores han sido anonimizados para no mostrar los resultados específicos de cada universidad.

3.1. Disponibilidad de servicios de archivo

- ¿La Universidad posee una sede electrónica? ¿La sede electrónica incluye y/o permite el acceso a los servicios clave del Archivo o estos servicios se encuentran publicitados y localizables?

Tras el análisis de estas cuestiones acerca de si la Universidad posee sede electrónica y en relación con si esta incluye y/o permite el acceso a los servicios clave del Archivo, los resultados han sido los que se muestran en la siguiente tabla:

Respuestas	Existencia de la sede electrónica de la Universidad		Servicios de archivo disponibles en la sede electrónica	
	Universidades	% sobre el total	Universidades	% sobre el total
SÍ	50	100,00%	15	30,00%
NO	0	0,00%	35	70,00%

3.2. Seguridad

- ¿El Archivo y/o la Universidad a la que pertenece hacen referencia a las acreditaciones o certificaciones de seguridad? En caso afirmativo, ¿están disponibles para que el ciudadano pueda consultarlas? Las fuentes, ¿son fácilmente localizables?

Se han analizado dos bloques de cuestiones. Por una parte, si el Archivo y/o la Universidad a la que pertenece hacen referencia a las acreditaciones o certificaciones de seguridad. En caso afirmativo se ha evaluado si se encuentran disponibles para que el ciudadano pueda consultarlas y si las fuentes son fácilmente localizables. Estos han sido los resultados.

Respuestas	Referencia a acreditación ENS		Consultables por parte del ciudadano		Fácilmente localizables	
	Universidades	% sobre el total	Universidades	% sobre el total	Universidades	% sobre el total
SÍ	7	14,00%	7	14,00%	7	14,00%
NO	43	86,00%	43	86,00%	43	86,00%

- ¿El Archivo y/o la Universidad a la que pertenece tienen una política propia de protección de datos? ¿existen referencias a la normativa de aplicación? ¿es esta información fácilmente localizable?

En segundo lugar, se ha evaluado si el Archivo y/o la Universidad a la que pertenece tienen una política propia de protección de datos ya que este hecho se encuentra asociado directamente con la seguridad de la información. También se ha analizado si existen referencias a la normativa de aplicación y, en caso de existir, si es esta información fácilmente localizable. Como resultado se ha obtenido la siguiente tabla:

Respuestas	Política de protección de datos		Enlace a la legislación existente		Fácilmente localizables	
	Universidades	% sobre el total	Universidades	% sobre el total	Universidades	% sobre el total
SÍ	37	74,00%	21	42,00%	14	28,00%
NO	13	26,00%	29	58,00%	36	72,00%

3.3. Preservación digital

- ¿El Archivo y/o la Universidad a la que pertenece tienen un plan de preservación y/o proporcionan información sobre las actividades de preservación que se realizan? ¿esta información se encuentra accesible?

Finalmente, en materia de preservación digital se ha evaluado si el Archivo y/o la Universidad a la que pertenece tienen un plan de preservación y/o proporcionan información sobre las actividades de preservación que se realizan. En caso afirmativo se ha evaluado, además, si esta información se encuentra accesible. Estos han sido los resultados:

Respuestas	Existencia de plan de preservación y/o información sobre las actividades de preservación		Fácilmente localizables	
	Universidades	% sobre el total	Universidades	% sobre el total
SÍ	4	8,00%	2	4,00%
NO	46	92,00%	48	96,00%

4. CONCLUSIONES

Tras plantear la situación legal en torno al acceso a través de medios electrónicos a los servicios públicos de los archivos universitarios y en relación con las cuestiones de seguridad y preservación, se ha procedido a realizar una revisión de las sedes electrónicas y sitios web de universidades y archivos. Los resultados obtenidos tras este análisis dejan patente que, mientras que existe un porcentaje apreciable de universidades cuyos servicios de archivo se encuentran publicitados en las sedes electrónicas correspondientes (30%), sin embargo, no existe a penas información accesible por parte del ciudadano que convierta a las universidades en instituciones transparentes en lo relativo a las cuestiones de cumplimiento del ENS (14% de referencias a acreditaciones) o en relación con la existencia de protocolos de preservación (8% de entidades con existencia de plan de preservación o información sobre actividades de preservación digital). El corolario de lo anterior es que la mayoría de las instituciones universitarias no hacen referencia a las certificaciones y acreditaciones de seguridad disponibles (86%).

En relación con los criterios en los que se han extraído resultados más bajos, ¿podría ser que las universidades y por extensión sus archivos, cumplieran con estos criterios de seguridad y preservación, pero que la información no se materialice en las páginas web y sedes electrónicas? No tenemos argumentos para responder a esta cuestión. Para responderla sería necesario ampliar el presente trabajo con una ronda de

cuestionarios que permitieran completar los resultados obtenidos a través de la mera observación que hemos realizado.

Cabe, finalmente, una última reflexión, dada la regulación acerca de la preservación de la información en soportes electrónicos, debemos suponer que esta está protegida, aunque los resultados obtenidos nos ofrezcan poca información acerca del tipo de políticas de preservación y medidas de conservación que se están aplicando (solo un 4% de las universidades proporcionan información al respecto). En general, la información relacionada con los procesos de preservación digital aplicados en los archivos (ese conjunto de procesos que garantizan la continuidad de la documentación a lo largo del tiempo) debería ser pública, conocida por los ciudadanos que son los que en última instancia tienen el poder sobre la información. ¿No debería ser entonces el plan de preservación (esos principios, políticas, estrategias y acciones específicas para garantizar la estabilidad física y tecnológica de los datos, la permanencia y el acceso de la información de los documentos digitales) y las medidas de preservación aplicadas, públicas? Como dueños de la información, los ciudadanos deberían poder saber cómo o qué acciones se están acometiendo para proteger sus datos y su información, la información de su comunidad universitaria y que en un tiempo se convertirá en HISTORIA de la institución y de la sociedad.

5. BIBLIOGRAFÍA Y FUENTES

- BUSTOS PRETEL, Gerardo (2018). El archivo electrónico único es una idea digital. En *La gestión del documento electrónico*. Wolters Kluwer.
- BUSTOS PRETEL, Gerardo (2021). ...Y el archivo electrónico único perdió su aroma jacobino. En *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n. extra 3.
- CASELLAS SERRA, Lluís-Esteve. (2016). El archivo electrónico único, una visión sesgada. En: *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n. 24, p. 2785-2788.

- CCN-CERT. CENTRO CRIPTOLÓGICO NACIONAL. (2019). *Guía de Seguridad de las TIC CCN-STIC 809: Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento*. Disponible en <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html>
- CRUE. (2022). *Universidades*. Disponible en <https://www.crue.org/universidades/>
- *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*. (2022). Comisión Europea. Disponible en <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration>
- FERNÁNDEZ, C. B. (2022). La Comisión presenta una declaración de principios y derechos digitales para todos en la UE. En *Wolters Kluwer CISS: Portal de Actualidad*. Disponible en https://cissactualidad.ciss.es/Content/Documento.aspx?params=H4sIAAAAAA AEAC2NQQvCIBhA_41ndXPNw3dwTUbuUFgzZoZs0B0KI-K2F_76ijg_e4_l5hkFTSjmry7IWZHMJfXgAp5xTxivyRJeg66TYVaJvRxlt4gum4iKb6Wv7JbfhanJ0sNgbOnK36_pJ9ufBqOak_3x0GXpl9HhQxKOKMYXNzb9NwRmTTLwBVm8c94wAAAA=WKE
- FERNÁNDEZ CUESTA, Francisco. (2016). Un Archivo único para gobernarlos a todos: El tortuoso camino hacia el Monte del Destino de los documentos electrónicos. En *Archivamos: Boletín ACAL*, n. 99, p. 39-41.
- FERNÁNDEZ CUESTA, Francisco. (2017). Un mar de preguntas sobre el archivo electrónico único: (a propósito de un artículo de Gerardo Bustos). En *Archivamos: Boletín ACAL*, n. 104, 2017, p. 38-40.
- *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*. Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>

- *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.* Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>
- *Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.* Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043&p=20210710&tn=1>
- *Ley 10/2021, de 9 de julio, de trabajo a distancia.* Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2021-11472>
- *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.* Disponible en <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330>
- *Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.* Disponible en <https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032>
- *UNE-ISO 14721:2015. Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.*
- *UNE-ISO 17068:2020. Información y documentación. Repositorio de tercero de confianza para documentos electrónicos.*
- *UNE-ISO 22301:2020. Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio. Requisitos.*
- *UNE-ISO 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015).*
- *UNE-ISO 27017:2021. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en nube.*



- *UNE-ISO 27018:2020. Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII.*
- *UNE-ISO 27701:2021. Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices.*