

POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE LA UNIVERSIDAD DE ALCALÁ

Universidad de Alcalá

Elaborado por	Comisión de Administración Electrónica y Seguridad	01/12/2023
Aprobado por	Consejo de Gobierno	18/07/2024

ACUERDO DE 18 DE JULIO DE 2024, DEL CONSEJO DE GOBIERNO DE LA UAH POR EL QUE SE APRUEBA LA
POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE LA UNIVERSIDAD DE ALCALÁ

TÍTULO I	4
Definición del alcance y ámbito de aplicación	4
Artículo 1. Alcance	4
Artículo 2. Datos identificativos de la Política	5
Artículo 3. Período de Validez	5
Artículo 4. Identificador del gestor de la política	5
TÍTULO II	6
Roles de los actores implicados	6
Artículo 5. Roles y Responsabilidades	6
TÍTULO III	7
Directrices para la estructuración y desarrollo de los procedimientos de gestión documental	7
Artículo 6. Procesos de gestión documental	7
Artículo 7. Captura	8
Artículo 8. Registro	19
Artículo 9. Clasificación	21
Artículo 10. Descripción	24
Artículo 11. Acceso	27
Artículo 12. Calificación	30
Artículo 13. Conservación	33
Artículo 14. Transferencia	36
Artículo 15. Destrucción o eliminación	41
TÍTULO III	41
Formación	41
Artículo 16. Formación sobre Gestión Documental	42
TÍTULO IV	42
Supervisión y auditoría de los procesos de gestión de documentos	42
Artículo 17. Auditoría de la gestión documental	42
TÍTULO IV	43
GESTIÓN DE LA POLÍTICA	43
Artículo 18. Mantenimiento, actualización y publicación	43
ANEXO I	43
Terminología	43
ANEXO II	44
Instrucciones para la digitalización de expedientes de la Universidad de Alcalá	44

Alcance y contenido	44
Requisitos básicos en los procesos de digitalización	45
Descripción del proceso de digitalización.....	46
Definición de proyectos de digitalización.....	46
Contenido del proyecto de digitalización	47
Contratación de la digitalización.....	47
Fase de Preparación de la Documentación	48
Fase de Preparación de las herramientas y sistemas informáticos	48

TÍTULO I

Definición del alcance y ámbito de aplicación

Artículo 1. Alcance

1. La presente política de gestión de documentos electrónicos está integrada en el contexto de la Universidad de Alcalá junto al resto de las políticas implantadas para el desempeño de sus actividades. En particular, esta política está integrada en el marco general de la gestión de documentos de la Universidad de Alcalá, con independencia del soporte en el que puedan estar materializados dichos documentos.
2. Esta política de gestión de documentos electrónicos tiene por objeto establecer el conjunto de criterios comunes asumidos por la Universidad de Alcalá, así como documentar los mismos, en relación con la gestión de los documentos y expedientes producidos y custodiados por ésta.
3. Esta política persigue garantizar la creación, disponibilidad e integridad de los metadatos mínimos obligatorios y, en su caso, los complementarios o necesarios (metadatos de contenido, contexto y estructura) para asegurar la gestión, recuperación y conservación de los documentos y expedientes electrónicos de la Universidad de Alcalá manteniendo permanentemente su relación.
4. En particular, se integrará con la política de seguridad que establece el Esquema Nacional de Seguridad, publicado en el Real Decreto 311/2022, de 3 de mayo, que ha sido adaptado en la Política de Seguridad de la Información de la Universidad de Alcalá, aprobada por Acuerdo de 15 de julio de 2020. Asimismo, se integrará con la política de interoperabilidad que establece el Esquema Nacional de Interoperabilidad, publicado en el Real Decreto 4/2010, de 2 de enero, con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y se integrará con el 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.

5. Esta política se aplicará tanto a los documentos analógicos como a los documentos electrónicos de la Universidad. Debido a que la Universidad es un entorno híbrido, será de aplicación lo indicado en el Esquema Nacional de Seguridad: “toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente Real Decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos”.

Artículo 2. Datos identificativos de la Política

Nombre del Documento	Política de Gestión de Documentos Electrónicos de la Universidad de Alcalá
Versión	1.0
Identificador de la Política	U02900001 v1
URI de referencia de la política	
Fecha de publicación	
Ámbito de aplicación	Gestión de los documentos producidos y/o bien custodiados por la Universidad de Alcalá

Artículo 3. Período de Validez

La presente política de gestión del Documento electrónico entrará en vigor en la fecha de su expedición y será válida hasta que no sea sustituida o derogada por una política posterior, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar los diferentes sistemas de gestión de documentos a las especificaciones de la nueva versión.

Debido al cambio continuo de las tecnologías y la legislación de administración digital aquellos aspectos que puedan ser actualizables automáticamente, sobre todo, en el caso de relaciones por modificaciones normativas, cambios estructurales, etc. serán incluidos en anexos incorporados al presente documento y actualizables automáticamente por el gestor del documento sin necesidad de que sea sustituido por una nueva versión.

Artículo 4. Identificador del gestor de la política

Nombre del gestor	Comisión de Administración Electrónica
Dirección de contacto	Secretaría de la CAE. Colegio de San Pablo y San Pedro, s/n. Alcalá
Identificador del gestor	U02900094 v1

TÍTULO II

Roles de los actores implicados

Artículo 5. Roles y Responsabilidades

1. Los actores involucrados en los procesos de gestión documental contemplados en la presente política serán como mínimo los siguientes:
 - a. El Consejo de Gobierno, como órgano colegiado de la Universidad de Alcalá es el encargado de aprobar la política de gestión documental y sus modificaciones, así como el resto de las políticas de la Universidad, alineándolas con la misma, con el asesoramiento de la Comisión de Reglamentos.
 - b. La Comisión de Administración Electrónica, como órgano asesor de la Universidad de Alcalá en materia de Administración Electrónica, que tiene entre sus funciones la definición y actualización de la política de gestión documental y preservación digital de los documentos de la Universidad. Dicha Comisión contará con la Secretaría de la Comisión, para la coordinación en la implementación de la política de gestión documental.
 - c. Los responsables de los servicios y unidades, como encargados de la gestión de sus correspondientes competencias y funciones, adoptarán la política de gestión documental empleando los medios funcionales, electrónicos y tecnológicos puestos a su disposición que mejor se adapten a esta política y las normas de administración electrónica, facilitando en todo caso su implementación.
 - d. Los responsables de los Servicios Informáticos se encargan del ámbito tecnológico y de la organización general de los sistemas y tecnologías de la información en la Universidad, implementando las soluciones técnicas específicas para el cumplimiento de esta política, según las directrices de la Comisión de Administración Electrónica
 - e. La Gerencia a través del Servicio de Nuevos Procesos Administrativos y Administración Electrónica es la encargada de la implementación de las políticas y procedimientos en la gestión de los expedientes administrativos, facilitando la simplificación de procesos, la automatización y la formación en la aplicación de la política de gestión documental.
 - f. La Gerencia a través de la unidad que corresponda a la administración electrónica y archivo digitales la encargada de la gestión, organización y conservación del patrimonio documental analógico y digital de la Universidad, y participa en la planificación y la implementación de las políticas y los procedimientos de gestión de documentos.
 - g. El Personal Docente e Investigador, Personal de Administración y Servicios y los estudiantes matriculados en la Universidad de Alcalá participarán en la ejecución de esta Política, relacionándose con medios electrónicos con la universidad y generando documentos electrónicos, así como empleando y actualizando los programas, equipos, herramientas informáticas y dispositivos de seguridad indicados o recomendados por la Universidad de Alcalá.
 - h. La unidad encargada de la gestión de la calidad de los servicios de la UAH, será el encargado de la supervisión y auditoría de la política de gestión documental con la colaboración del resto de unidades.
2. A continuación, se describen los roles y responsabilidades de los actores antes mencionados:

- a. Aprobación, Modificación e impulso de la Política:
 - i. Consejo de Gobierno
 - ii. Comisión de Administración Electrónica
- b. Aplicación de la política: responsables de procesos de gestión de la entidad:
 - i. Los responsables de los Servicios y Unidades
- c. Planificación, implantación y administración del programa de tratamiento de documentos electrónicos y gestión de expedientes:
 - i. Gerencia
 - ii. Servicios Informáticos
 - iii. Unidad de Archivo y Registro
 - iv. Unidad de Administración Electrónica
- d. Ejecución: personal implicado en tareas de tratamiento de documentos, es decir, personal que crea, recibe y mantiene documentos como parte de su labor diaria:
 - i. Personal PDI/PAS
- e. Supervisión y control de la ejecución de la política: personal encargado de la gestión de la calidad mediante auditorías internas y externas:
 - i. Unidad encargada de la gestión de la calidad
- f. Formación de usuarios en materia de gestión de documentos:
 - i. Unidad Administración Electrónica
 - ii. Unidad Archivo y Registro

TÍTULO III

Directrices para la estructuración y desarrollo de los procedimientos de gestión documental

Artículo 6. Procesos de gestión documental

Los procesos de gestión que generen documentos y expedientes electrónicos de la Universidad deben aplicar esta política, procesos que se realizarán a través de la implementación de la administración electrónica que garantice su materialización, con la creación de entornos automatizados que cumplan los requisitos exigidos por la legislación.

La gestión documental de la UAH, según la normativa vigente, no deberá de realizarse en ningún caso en soporte papel, sólo en soporte electrónico o digital, que deberán de seguir los requisitos de la administración electrónica y la presente política de gestión documental, mediante su integración en herramientas de administración electrónica.

El tratamiento electrónico se aplicará de manera continua sobre todas las etapas o fases del ciclo de vida de los documentos y los expedientes electrónicos con el objetivo de garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad; permitiendo la protección, recuperación y conservación física y lógica de los documentos y de su contexto de creación.

Para la implementación de la administración electrónica la Universidad de Alcalá dispone de una sede electrónica, un sistema de gestión de expedientes electrónicos o escritorio de tramitación, conectado a los sistemas de planificación de recursos empresariales (ERP) de la

EJEMPLO DE EXPEDIENTE DE LA UNIVERSIDAD DE ALCALÁ:
 ES_U02900001_2022_EXP_REGSED_000000000000000000000002 (ET)
 ES_U02900001_2021_EXP_UXXI-2021-003386 (UXXI)

Tabla 2. MODELO DE IDENTIFICADOR PARA DOCUMENTO ELECTRÓNICO

<IDIOMA>	Código del idioma o lengua cooficial del documento: - ES: español - CA: catalán - GL: gallego - EU: vasco - VA: valenciano
<ÓRGANO>	U02900001 (DIR3 de la Universidad de Alcalá)
<AÑO DE FECHA DE CAPTURA>	Año de la fecha de captura del documento
<ID_ESPECIFICO>	Código específico siguiendo lo establecido en el modelo del escritorio de tramitación:00000000000000000000000000000000(Número correlativo empezando en 1) Código específico siguiendo lo establecidos en el modelo de UXXI: DOC-Año-NumSecuencial

EJEMPLO DE DOCUMENTO DE LA UNIVERSIDAD DE ALCALÁ:
 ES_U02900001_2022_000000000000000000000000000012 (ET)
 ES_U02900001_2023_DOC-2022-00026623 (UXXI)

Los documentos y expedientes electrónicos contendrán los siguientes metadatos para las entidades “documento” y “expediente”, que serán cumplimentados en el momento de la captura o en el proceso de tramitación, dependiendo si la captura es en registro o si es en fase de digitalización.

Tabla 3. METADATOS PARA EXPEDIENTE ELECTRÓNICO

Metadato (UniversitasXXI/Esquema eEMGDE)	Obligación	Descripción	Posibles valores
EMUXXI/eEMGDE0 Tipo de Entidad	Obligatorio UAH	Especifica el tipo de entidad que se describe.	Documento
EMUXXI/eEMGDE1 Categoría	Obligatorio para la transferencia	Valor del tipo de entidad que se está describiendo.	Expediente
EMUXXI/eEMGDE2. Identificador	Obligatorio ENI	Identificador único asignado a una entidad.	
EMUXXI/eEMGDE2.1 Secuencia Identificador	Obligatorio ENI	Secuencia de caracteres que identifica la entidad	(Ver la secuencia de la UAH en tabla 1 para expediente)

		dentro de un dominio local o global.	
EMUXXI/eEMGDE3. Nombre	Obligatorio para la transferencia	Nombre real que se da al expediente	
EMUXXI/eEMGDE3.1 Nombre Natural	Obligatorio para la transferencia	Nombre real que se da al expediente	Texto Libre
EMUXXI /eEMGDE4. Fecha	Obligatorio ENI	Fecha del expediente	
EMUXXI/eEMGDE4.1 Fecha inicio	Obligatorio ENI	Fecha de apertura del expediente	[<AAAA-MM-DD>T<hh:mm:ss>]
EMUXXI/eEMGDE4.2 Fecha fin	Obligatorio para la transferencia UAH	Fecha de cierre del expediente	[<AAAA-MM-DD>T<hh:mm:ss>]
EMUXXI/eEMGDE8.6 Nivel de confidencialidad de la información	Obligatorio para la transferencia	Evaluación, en cuanto al nivel de la dimensión de seguridad "confidencialidad", de la información recogida en un documento, de acuerdo con el Esquema Nacional de Seguridad.	Alto, Bajo y Medio
EMUXXI/eEMGDE13 Calificación	Obligatorio para la transferencia	Información acerca de los plazos de conservación de los documentos en atención a sus valores, a lo largo de su ciclo de vida, así como acerca de las acciones dictaminadas regladas a emprender sobre los mismos, tomadas a partir de la ponderación de esos valores.	



EMUXXI/eEMGDE13.1.1.1 Tipo de valor	Obligatorio para la transferencia	Identificación de los diferentes valores primarios que poseen los documentos, expedientes y series.	Administrativo, Fiscal, Jurídico y Otros
EMUXXI/eEMGDE13.1.1.2 Plazo	Obligatorio para la transferencia	Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales.	Valor numérico en años
EMUXXI/eEMGDE13.1.2 Valor secundario	Obligatorio para la transferencia	Determinación la existencia de valores secundarios en los documentos	Sí/No/Sin cobertura de calificación
EMUXXI/eEMGDE13.2.1 Dictamen	Obligatorio para la transferencia	Decisiones emitidas por la autoridad calificadora relativas a la conservación o a la eliminación de documentos de acuerdo con la evolución de sus valores conforme avanza su ciclo de vida.	
EMUXXI/eEMGDE13.2.1 Tipo de dictamen	Obligatorio para la transferencia	Tipo de decisión emitida por la autoridad calificadora que debe aplicarse sobre los documentos a lo largo de su ciclo de vida y una vez realizada su valoración.	CP/ET/EP (Conservación permanente, eliminación total o eliminación parcial)
EMUXXI/eEMGDE13.3 Transferencia	Obligatorio para la transferencia	Operación por la que traspasa la custodia de las diferentes fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental	

EMUXXI/eEMGDE13.3.1 Fase de archivo	Obligatorio para la transferencia	Indicación de la fase de archivo correspondiente al momento del ciclo de vida del	Archivo de Oficina Archivo Histórico
EMUXXI/eEMGDE13.3.2 Plazo de transferencia	Obligatorio para la transferencia	Plazo de tiempo en que se traspasa la custodia de las diferentes fracciones de series	
EMUXXI/eEMGDE17 Firma	Obligatorio ENI	Método para fijar las condiciones de fiabilidad y autenticidad de un documento.	
EMUXXI/eEMGDE17.1 Tipo de Firma	Obligatorio ENI	Denominación normalizada del formato de firma utilizado	
EMUXXI/ eEMGDE17.1. Formato de firma	Obligatorio ENI	Formato de firma empleado en una firma con certificado electrónico	TF01 (CSV), TF02 (XAdES internally detached signature), TF03 (XAdES enveloped signature), TF04 (CAAdES detached/explicit signature), TF05 (CAAdES attached/implicit signature), TF06 (PAdES)
EMUXXI/eEMGDE18 Tipo documental	Obligatorio ENI	Modelo estructurado y reconocido que adopta un Documento, en el desarrollo de una competencia concreta, en base a una Regulación y cuyo formato, contenido informativo o soporte son homogéneos.	Las tipologías documentales deben de estar controladas para su creación normalizada. La Norma Técnica de Interoperabilidad de Documento Electrónico contiene una relación genérica pero hay tipos específicos para la Universidad.



EMUXXI/eEMGDE22.1 Código de clasificación	Obligatorio para la transferencia	Identificador único codificado que determina una categoría en un cuadro de clasificación o en el SIA.	Código SIA o código del cuadro de clasificación desarrollado por cada organización.
EMUXXI/eEMGDE22.2 Denominación de clase / Serie documental	Obligatorio para la transferencia	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación.	Texto libre Para series que no forman expedientes
EMUXXI/eEMGDE22.3 Tipo de clasificación	Obligatorio para la transferencia	Término que señala si los valores del elemento corresponden a una clasificación administrativa del procedimiento de acuerdo con el SIA, y en cumplimiento con el metadato obligatorio correspondiente de la NTI de Expediente electrónico, o si se refieren a la adscripción de la entidad a una categoría funcional dentro del cuadro de clasificación funcional de documentos de la organización.	Funcional/SIA
EMUXXI/eEMGDE23 Versión NTI	Obligatorio ENI	Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Documento electrónico conforme a la cual se estructura el documento electrónico.	http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e
EMUXXI/eEMGDE24 Órgano	Obligatorio ENI	Para el Expediente y Serie: Identificador normalizado de la administración	<DIR3Universidad>

		responsable de la tramitación del procedimiento.	
EMUXXI/eEMGDE27 Estado del Expediente	Obligatorio ENI	Estado de tramitación del expediente	Abierto, Cerrado, Pendiente de Iniciar, Anulado, Índice para remisión
EMUXXI/eEMGDE28 Interesado	Obligatorio ENI	DNI/DIR3 del Interesado	a) Si ciudadano o persona jurídica: DNI, NIE, NIF b) Si administración: <Órgano> (DIR3)

Tabla 4. TABLA DE METADATOS PARA DOCUMENTO ELECTRÓNICO

Metadatos	Obligación	Descripción	Posibles valores
EMUXXI/eEMGDE0 Tipo de Entidad	Obligatorio UAH	Especifica el tipo de entidad que se describe.	Documento
EMUXXI/eEMGDE1 Categoría	Obligatorio para la transferencia	Valor del tipo de entidad que se está describiendo.	Documento
EMUXXI/eEMGDE2 Identificador	Obligatorio ENI	Identificador único asignado a una entidad.	EMUXXI/eEMGDE2.1 Secuencia del Identificador (Ver como se forma en tabla 1)
EMUXXI/eEMGDE2.1 Secuencia del Identificador (Ver como se forma en tabla 1)	Obligatorio ENI	Secuencia de caracteres que identifica la entidad dentro de un dominio local o global.	(Ver la secuencia de la UAH en tabla 2 para documento)
EMUXXI/eEMGDE3 Nombre	Obligatorio para la transferencia	Nombre real que se da al documento	
EMUXXI/eEMGDE3.1 Nombre Natural	Obligatorio para la transferencia	Nombre real que se da al documento	Texto Libre
EMUXXI/eEMGDE4 Fecha	Obligatorio ENI	Fecha de captura del documento	
EMUXXI/eEMGDE4.1 Fecha de inicio	Obligatorio ENI	Fecha de captura del documento en el escritorio de tramitación	[<AAAA-MM-DD>T<hh:mm:ss>]
EMUXXI/eEMGDE8.6 Nivel de confidencialidad de la información	Obligatorio para la transferencia	Evaluación, en cuanto al nivel de la dimensión de seguridad	Alto, Bajo y Medio



		"confidencialidad", de la información recogida en un documento, de acuerdo con el Esquema Nacional de Seguridad.	
EMUXXI/eEMGDE9.1 Tipo de Acceso	Obligatorio para la transferencia	Indica si el documento se rige por el régimen general de libre acceso o si, por el contrario, está sujeto a alguna de las limitaciones recogidas en la legislación o normativa de aplicación.	Libre, Parcialmente Restringido, Restringido
EMUXXI/eEMGDE13 Calificación	Obligatorio para la transferencia	Información acerca de los plazos de conservación de los documentos en atención a sus valores, a lo largo de su ciclo de vida, así como acerca de las acciones dictaminadas regladas a emprender sobre los mismos, tomadas a partir de la ponderación de esos valores.	
EMUXXI /eEMGDE13.1.1.1 Tipo de valor	Obligatorio para la transferencia	Identificación de los diferentes valores primarios que poseen los documentos, expedientes y series.	Administrativo, Fiscal, Jurídico y Otros
EMUXXI /eEMGDE13.1.1.2 Plazo	Obligatorio para la transferencia	Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales.	Valor numérico en años
EMUXXI/eEMGDE13.1.2 Valor secundario	Obligatorio para la transferencia	Determinación la existencia de valores secundarios en los documentos	Sí/No/Sin cobertura de calificación
EMUXXI/eEMGDE13.2.1 Tipo de dictamen	Obligatorio para la transferencia	Tipo de decisión emitida por la autoridad calificadora que debe aplicarse sobre los documentos a lo largo de su ciclo de	CP/EP/ET (Conservación Permanente/ Eliminación Parcial/ Eliminación total)



		vida y una vez realizada su valoración.	
EMUXXI/eEMGDE13.3 Transferencia	Obligatorio para la transferencia	Operación por la que traspasa la custodia de las diferentes fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental	
EMUXXI/eEMGDE13.3.1 Fase de archivo	Obligatorio para la transferencia	Indicación de la fase de archivo correspondiente al momento del ciclo de vida del	Archivo de Oficina Archivo Histórico
EMUXXI/eEMGDE13.3.2 Plazo de transferencia	Obligatorio para la transferencia	Plazo de tiempo en que se traspasa la custodia de las diferentes fracciones de series	Se indica el valor numérico en años
EMUXXI/eEMGDE13.4 Documento esencial	Obligatorio para la transferencia	Calificación de un documento como esencial para el desarrollo de las actividades de la organización y que, por ello, debe ser objeto de medidas especiales de protección, que incluyen su duplicado y almacenamiento en un repositorio diferente.	Si/No
EMUXXI/eEMGDE14 Características Técnicas	Obligatorio ENI	Información acerca de la forma lógica y otras características técnicas lógicas y físicas de un documento digital o digitalizado.	
EMUXXI/eEMGDE14. Formato	Obligatorio ENI	Formato lógico del fichero contenido en el documento electrónico	
EMUXXI/eEMGDE14.1.1 Nombre del Formato	Obligatorio ENI	Denominación del formato lógico del fichero contenido en el documento electrónico	Valores definidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares en la columna "Extensión" de la



			tabla recogida en su anexo.
EMUXXI/eEMGDE14.1.2 Extensión del fichero	Obligatorio ENI	Extensión del formato lógico del fichero contenido en el documento electrónico	Valores definidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares en la columna "Extensión" de la tabla recogida en su anexo.
EMUXXI/eEMGDE17.1.1 Tipo de firma	Obligatorio	Denominación normalizada del formato de firma utilizado	(CSV) (XAdES internally detached signature) (XAdES enveloped signature) (CAAdES detached/explicit signatura) (CAAdES attached/implicit signature), (PAdES)
EMUXXI/eEMGDE18 Tipo documental	Obligatorio ENI	Modelo estructurado y reconocido que adopta un Documento, en el desarrollo de una competencia concreta, en base a una Regulación y cuyo formato, contenido informativo o soporte son homogéneos.	Las tipologías documentales deben de estar controladas para su creación normalizada. La Norma Técnica de Interoperabilidad de Documento Electrónico contiene una relación genérica, pero hay tipos específicos para la Universidad.
EMUXXI/eEMGDE22.1 Código de clasificación	Si	Identificador único codificado que determina una categoría en un cuadro de clasificación de la UAH	Código del cuadro de clasificación de la UAH
EMUXXI/eEMGDE22.2 Denominación de clase / Serie documental	Obligatorio para la transferencia	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación de la UAH	Texto libre
EMUXXI/eEMGDE23 Versión NTI	Obligatorio	Identificador normalizado de la	http://administracionelectronica.gob.es/



		versión de la Norma Técnica de Interoperabilidad de Documento electrónico conforme a la cual se estructura el documento electrónico.	ENI/XSD/v1.0/expediente-e
EMUXXI/eEMGDE24 Órgano	Obligatorio ENI	Para el Documento simple: identificador normalizado de la administración generadora del documento o que realiza la captura del mismo. Para el Expediente y Serie: Identificador normalizado de la administración responsable de la tramitación del procedimiento.	<DIR3Universidad>
EMUXXI/eEMGDE25 Origen	Obligatorio	Indica si el contenido del documento fue creado por el ciudadano o por una administración.	Ninguno, Ciudadano, Administración
EMUXXI/eEMGDE26 Identificador del Documento origen	Condiciona Completar en caso de que el metadato eEMGDE20 - Estado de elaboración, contenga los valores EE02, EE03 o EE04 (EE02 (Copia electrónica auténtica con cambio de formato) EE03 (Copia electrónica auténtica de documento papel) EE04 (Copia electrónica	Identificador normalizado del documento origen al que corresponde la copia.	Sin definir

	parcial auténtica)		
--	-----------------------	--	--

Tabla 5. METADATOS DE LA UAH			
Metadato (UniversitasXXI/Esquema eEMGDE)	Obligación	Descripción	Posibles valores
Código clasificación SIA	Si	Código SIA	Por ejemplo: 2348206
Denominación de clase SIA	Obligatorio para la transferencia	Nombre en SIA o catálogo de procedimientos	Quejas y Sugerencias
Código clasificación Funcional	Si (Desde el momento de la creación del cuadro)	Código Funcional	El valor se extraerá del cuadro de clasificación funcional de la UAH
Denominación de clase Funcional	Obligatorio para la transferencia (Desde el momento de creación del cuadro)	Nombre en el Cuadro de Clasificación Funcional	El valor se extraerá del cuadro de clasificación funcional de la UAH

Artículo 8. Registro

El registro y tramitación de los documentos y expedientes electrónicos presentados en el registro electrónico de la entidad Universidad de Alcalá, con DIR3 U02900001 se realizará conforme al siguiente procedimiento:

- Los documentos y expedientes electrónicos registrados por Sede Electrónica siguen el siguiente procedimiento. Los ciudadanos, empresas, y miembros de la comunidad universitaria presentan documentos electrónicos en la Sede Electrónica de la Universidad de Alcalá a través de los formularios del catálogo de procedimientos o bien, a través de la solicitud genérica o registro electrónico para los procedimientos que no están dados de alta en el catálogo. Rellenan el formulario, adjuntan la documentación solicitada en el procedimiento en formato electrónico en soporte PDF y proceden a firmar la solicitud, se genera entonces la solicitud firmada y un recibo de registro. Este procedimiento genera un expediente ENI. La solicitud aparece con un sello de registro de entrada de la Universidad (fecha/hora/número de REGAGE/número de expediente) y CSV (Código Seguro de Verificación). Esta plataforma conecta con la gestión integral del procedimiento administrativo, no sólo con la solicitud, permite guardar los documentos en la carpeta ciudadana para facilitar el acceso al registro al solicitante, permite anexionar documentos por parte del solicitante a lo largo del procedimiento enlazando con el expediente de la solicitud presentada y permite realizar notificaciones

a los solicitantes, generando un acuse de registro. En todo caso genera, documentos originales auténticos.

- Los documentos y expedientes electrónicos llegan a través de la plataforma GEISER (Gestión Integrada de Servicios de Registro) es una solución integral de registro que funciona en modo nube para prestar el servicio para cualquier organismo público, que cubre tanto la gestión de sus oficinas de registro de entrada/salida como la recepción y envío de registros en las unidades tramitadoras destinatarias de la documentación. Esta plataforma no genera un expediente ENI, y no conecta con la plataforma de gestión integral del procedimiento administrativo. No enlaza con la carpeta ciudadana de la Universidad de Alcalá. Si que aparece con un CSV (Código Seguro de Verificación). Por ello, se han derivado los registros generados por esta plataforma con el escritorio de tramitación para generar un expediente ENI.

Si la Universidad de Alcalá recibe documentación en soporte papel en las oficinas de asistencia en materia de registro se seguirá el siguiente procedimiento para el registro y digitalización segura de la documentación presentada:

Un funcionario habilitado procederá al registro de la documentación en la plataforma.

La plataforma permite introducir los datos de contacto de la persona (interesado o representante) que quiera realizar el registro de documentación en papel en la Universidad de Alcalá, estos datos se emplearán para identificar a la persona en el área personal o carpeta ciudadana de la Sede Electrónica de la Universidad de Alcalá, para que pueda acceder a la documentación que ha registrado y al acuse de registro. El propio interesado podrá modificar sus propios datos de contacto en el área personal o carpeta ciudadana de la Sede Electrónica.

En el registro de la documentación el funcionario deberá de rellenar los siguientes campos de manera obligatoria:

- Tipo de Asunto
- Resumen
- Unidad de destino

Separará la documentación, para subirla al registro, fundamentalmente, la solicitud de los anexos. Y en la medida que sea posible separará los anexos por originalidad y tipología documental.

En cuanto a la tradición documental de los documentos presentados en la oficina de registro:

- Las solicitudes en papel firmadas que se presenten son originales, que es lo que se indicará en “estado del documento” en la fase de registro del documento y el proceso de conversión que hace el funcionario al digitalizarlas y al registrarlas es “copia electrónica auténtica de documento papel”.
- Los anexos en papel presentados pueden ser más variados en cuanto a tradición documental, pueden ser originales, o no. El cotejo de la documentación con los originales se hace por la unidad tramitadora de la documentación, no en la fase de registro, quien podrá solicitar los originales para su validación en el trámite de gestión del expediente. Pudiendo cambiar la tradición documental de “otros”, que será el que se indique en la oficina de registro, a copia electrónica auténtica de documento en papel o electrónico.

En el registro se incluye:

- El sistema genera una solicitud con CSV (el Código Seguro de Verificación, que se puede verificar en Verificación de la Sede Electrónica), un número de expediente, fecha de registro y hora de registro.
- El sistema integra los documentos en un expediente con fecha de apertura, interesado, estado de elaboración, fecha de vencimiento.
- Se genera un expediente con metadatos obligatorios ENI, automatizados y con otros metadatos obligatorios para la transferencia con posibilidad de cubrir en la fase de envío al archivo.

Artículo 9. Clasificación

En la fase de oficina es de obligado cumplimiento que toda la Administración de la Universidad de Alcalá, remita sus procedimientos y servicios antes de integrarlos en sistemas de gestión automatizados que incorporen sistemas de gestión documental, con la finalidad de incluirlos en el Sistema de Información Administrativa (SIA), que es el inventario de información administrativa de la AGE. Deberán remitir los procedimientos anualmente a la Unidad de Administración Electrónica para actualizar el Catálogo de la UAH.

Este sistema viene reglado por el artículo 9 del Esquema Nacional de Interoperabilidad, y actualizado de forma corresponsable por todos los Organismos participantes. El Catálogo SIA contiene la relación de procedimientos y servicios de la AGE y las diferentes Administraciones Públicas participantes, en este sistema cada procedimiento tiene asignado un código y una denominación.

Es importante diferenciar el código y denominación del procedimiento, del código y denominación de la serie documental. El código y denominación de procedimiento se tomará del Catálogo SIA. El código y denominación de serie documental se tomará del cuadro de clasificación de la Universidad. (Tabla 3. METADATOS DE LA UAH).

El código de procedimiento se establece en la fase de archivo de oficina para gestionar los expedientes electrónicos. El código de serie documental se establece en la fase de transferencia al archivo.

La diferencia entre procedimiento y serie la vemos reflejada la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, en la diferencia entre procedimiento y expediente administrativo.

Cuando se define procedimiento administrativo como: el conjunto ordenado de trámites y actuaciones formalmente realizadas, según el cauce legalmente previsto, para dictar un acto administrativo o expresar la voluntad de la Administración.

Y cuando se define le expediente administrativo en el artículo 70:

“1. Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

2. Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que

contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.

3. Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autenticado y acompañado de un índice, asimismo autenticado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

4. No formará parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo, como la contenida en aplicaciones, ficheros y bases de datos informáticas, notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, así como los juicios de valor emitidos por las Administraciones Públicas, salvo que se trate de informes, preceptivos y facultativos, solicitados antes de la resolución administrativa que ponga fin al procedimiento”.

El procedimiento administrativo genera informaciones auxiliares o de apoyo, como notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, que no formaría parte del expediente.

Los expedientes administrativos en los que se plasma la actuación administrativa se agrupan en series documentales, que son conjuntos de expedientes, dossiers, unidades de expedientes, o documentos individuales que son agrupados de acuerdo con una clasificación o sistema de clasificación, o que son conservados como una unidad porque son el resultado de la misma acumulación o proceso de archivo, la misma función o la misma actividad, y que tienen una forma particular o una relación motivada por su producción, recepción o uso. O bien: un conjunto de documentos generados por un sujeto productor en el desarrollo de una misma actividad administrativa y regulado por la misma norma de procedimiento.

Ambos tipos de clasificación estarán incluidos en los sistemas de gestión documental de la administración electrónica tanto a nivel de sede electrónica como en el escritorio de tramitación de los documentos y expedientes electrónicos de la Universidad.

En todo caso, se tomará como referencia el cuadro de clasificación de la UAH, que irá reflejando los cambios que se generen en la gestión automatizada de expedientes, para su uso por la totalidad de las unidades administrativas de la Universidad de Alcalá. Dicho cuadro de clasificación será actualizado sistemáticamente siempre que haya alguna modificación normativa, estructural o funcional que le afecte, sin necesidad de modificar el documento de política de gestión de documentos electrónica. Asimismo, dicha modificación se realizará en la Universidad de Alcalá en los sistemas en los que haya una vinculación con el cuadro de clasificación. A medida que avance la tramitación electrónica se caminará hacia un cuadro de clasificación más funcional.

El cuadro de clasificación de los expedientes que es propio de los sistemas automatizados es el funcional, al emplear en su estructura como elemento definidor la funciones que tiene cada organismo, en la medida en que éstas son permanentes y garantizan, en consecuencia, un Cuadro de Clasificación sólido, consistente y de larga duración frente a los órganos que son más inestables en su estructura. Cualquier alteración en el organigrama universitario y, en

consecuencia, en la estructura orgánica obligaría a frecuentes cambios del cuadro y reclasificaciones de los expedientes.

La necesidad de contar con un cuadro de clasificación funcional se desprende asimismo de lo dispuesto en la Norma Técnica de Política de gestión de documentos electrónicos, al contemplar en su Apartado VI.3 la clasificación de los documentos como uno de los procesos de gestión de los mismos: "Clasificación de documentos, que incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la Norma Técnica de Interoperabilidad de Expediente Electrónico, así como la clasificación funcional de acuerdo con el cuadro de clasificación de la organización".

La construcción del Cuadro de Clasificación supone integrar en un instrumento sistemático un conjunto de informaciones derivadas de un análisis de la historia del archivo y la institución, la estructura y funciones del organismo, la identificación de la producción documental, el marco legal y jurídico, la compilación de clasificaciones históricas y el conocimiento exhaustivo de los procedimientos administrativos. Añadiendo información contextual de la documentación, aportando información de las diversas entidades del Esquema Nacional de Interoperabilidad: documento, agente, actividad, regulación y relación.

Los metadatos de clasificación que se aplican a nivel de la entidad documento son:

Tabla 5. Tabla de Metadatos para Clasificación			
Metadato (UniversitasXXI/Esquema eEMGDE)	Obligación	Descripción	Posibles valores
EMUXXI/eEMGDE22.1 Código de clasificación	Si	Identificador único codificado que determina una categoría en un cuadro de clasificación de la UAH	Por ejemplo: 2.4.1.12
EMUXXI/eEMGDE22.2. Denominación de clase	Obligatorio para la transferencia	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación.	Por ejemplo: Expediente de personal (Personal Administración y Servicios)
Código clasificación SIA	Si	Código SIA	Por ejemplo: 2348206
Denominación de clase SIA	Obligatorio para la transferencia	Nombre en SIA o catálogo de procedimientos	Quejas y Sugerencias
Código clasificación Funcional	Si (Desde el momento de la creación del cuadro)	Código Funcional	El valor se extraerá del cuadro de clasificación funcional de la UAH

Denominación de clase Funcional	Obligatorio para la transferencia (Desde el momento de creación del cuadro	Nombre en el Cuadro de Clasificación Funcional	El valor se extraerá del cuadro de clasificación funcional de la UAH
---------------------------------	--	--	--

Artículo 10. Descripción

Los sistemas de gestión documental de la Universidad de Alcalá deberán de cumplir en la parte de descripción de los documentos y expedientes electrónico o digitalizados en la fase de oficina se basará el esquema de metadato e-EMGDE, definido por el Real Decreto 4/2010 como “instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida”. Este esquema incluye los metadatos mínimos obligatorios, definidos en las normas técnicas de interoperabilidad de Documento electrónico y Expediente electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos. Se basa como aspectos más destacables en un modelo entidad-relación que reconoce la existencia de diversas entidades: documento, agente, actividad, regulación y relación y en el uso de relaciones y eventos para dejar constancia del contexto.

Este aspecto lo hace compatible entre otras cuestiones con el esquema NEDA-MC: Modelo conceptual de descripción archivística española. El estándar NEDA-MC es un modelo de referencia teórico basado también en el esquema de modelado entidad-relación. Este modelo se ha desarrollado con la intención de identificar los requisitos funcionales que deben tenerse en cuenta en el diseño y configuración de los sistemas de descripción archivística. Como resultado fundamental, se ha obtenido un modelo consistente y lógico a un alto nivel de abstracción que identifica y engloba todos los elementos posibles de la descripción archivística, utilizando elementos de modelado de datos que pueden ser de uso compartido por otras disciplinas (entidades, relaciones y sus correspondientes atributos).

Supone el uso de modelo compatible con otras normas de descripción, como son las normas internacionales del Consejo Internacional de Archivos: ISAD(G), ISAAR (CPF), ISDF, ISDIAH, que se emplean en los sistemas de archivo. Estas normas se pueden complementar con las Normas ISO-UNE de gestión de documento.

La inclusión de metadatos no es incompatible con el uso de otros instrumentos de descripción empleados en la búsqueda y recuperación de documentos como: tesauros, vocabularios, o índices de materias que se emplean en el archivo en los sistemas de gestión documental. Se añadirá el correspondiente metadato, en caso de contar con estos sistemas de clasificación:

Tabla 6. TABLA DE METADATOS PARA MATERIAS		
Metadato	Descripción	Ejemplo
EMUXXI/eEMGDE12.1 - Puntos Acceso	Palabra clave que describe	Ejemplo: Farmacia, Urbanismo,

Termino Punto Acceso	el contenido del documento o de la regulación. Aquellos ya existentes elegidos por cada organización, o los elaborados expresamente por éstas de conformidad con sus necesidades	Administración de Empresas, Siglo XIX, Guerra de Iraq, Madrid, Ley 39/2015, Calificación de documentos
EMUXXI/eEMGDE12.2 - Puntos Acceso Identificador Punto Acceso	Debe utilizarse si se utiliza una taxonomía (tesauro, índice, lista de autoridades, lenguaje o vocabulario controlado, etc.) para proporcionar un valor al sub-elemento	21.3, 72, 636 (si se estuviera usando, por ejemplo, la Clasificación Decimal Universal).
EMUXXI/eEMGDE12.3 - Puntos Acceso Esquema Punto Acceso	Referencia al esquema del que el punto de acceso se ha extraído. eEMGDE12.1 – Término punto de acceso, o eEMGDE12.2 - ID de punto de acceso. Debe utilizarse si se utiliza una taxonomía (tesauro, índice, lista de autoridades, lenguaje o vocabulario controlado, etc.) para proporcionar un valor a los sub-elementos.	Ejemplo: Listado de materias de la Biblioteca Nacional, Clasificación Decimal Universal, listado de puntos de acceso en la plataforma PARES

A efectos de favorecer la interoperabilidad e integración en la fase de archivo de los documentos y expedientes electrónicos, se seguirá el Esquema Nacional de Interoperabilidad, para la asignación de metadatos.

En la fase de archivo de oficina todos los documentos electrónicos deberán incluir los metadatos mínimos obligatorios del ENI (Esquema Nacional de Interoperabilidad):

Tabla 7. ESQUEMA INSTITUCIONAL DE METADATOS DE INTEROPERABILIDAD PARA DOCUMENTO

Metadatos Mínimos Obligatorios de Documento Electrónico	
Metadato	Elemento / Sub-elemento e-EMGDE
Versión NTI	eEMGDE23-Versión NTI (URI) de la Norma Técnica de Interoperabilidad de Documento electrónico.
Identificador	eEMGDE2.1. Secuencia de Identificador-Nota: Siendo el eEMGDE2.2 - Esquema de identificador del "Documento" = ES_<Órgano>_<AAAA>_<ID_especifico>
Órgano	eEMGDE24- Órgano
Fecha de Captura	eEMGDE4.1 - Fecha de inicio del Documento
Origen	EMGDE25 - Origen. Elemento lógico que indicará el tipo de "Agente" que a través de una "Relación" de tipo "crea" está relacionado con el documento: "0": Si es un ciudadano, el "Agente" será de tipo "Persona" con su identificador normalizado (DNI, NIF, CIF, NIE o similar). "1": Si es una Administración, el "Agente" será de tipo "Organización" con su identificador normalizado (<Órgano>).
Estado de Elaboración	Elemento que indicará el estado de elaboración del documento, siendo sus posibles valores: -Si "Original": eEMGDE20 - Estado de elaboración= "EE01". -Si existe una "Relación" de tipo "copia" entre el Documento y otro Documento que actúa de Original eEMGDE20 - Estado de elaboración= "EE02 EE03 EE04".
Nombre de formato	eEMGDE14.1.1 - Nombre de formato lógico de cada fichero de contenido
Tipo Documental	eEMGDE18 - Tipo documental del Documento.
Tipo de firma	Si CSV, 'eEMGDE17.1.1 - Formato de firma="TF01" Si Firma Electrónica basada en certificados: eEMGDE17.1.1 - Formato de firma = "TF02 TF03 TF04 TF05 TF06"
Valor CSV	eEMGDE17.3 - Valor del CSV ="Valor CSV"
Definición generación CSV	eEMGDE17.4 - Definición generación CSV de la "Actividad" que, mediante la "Relación" correspondiente, aplica a la generación del CSV del "Documento".

En la fase de archivo de oficina los expedientes electrónicos deberían incluir los metadatos mínimos obligatorios:

Tabla 8. ESQUEMA INSTITUCIONAL DE METADATOS DE INTEROPERABILIDAD PARA EXPEDIENTE

Metadatos Mínimos Obligatorios de Expediente Electrónico	
Metadato	Elemento / Sub-elemento e-EMGDE
Versión NTI	eEMGDE23 - Versión NTI (URI) de la Norma Técnica de Interoperabilidad de Expediente electrónico.
Identificador	eEMGDE2.1 - Secuencia de identificador. Nota: Siendo el eEMGDE2.2 - Esquema de identificador del "Expediente"= ES_<Órgano>_<AAAA>_<ID_específico>
Órgano	eEMGDE24 - Órgano
Fecha de apertura del expediente	eEMGDE4.1 - Fecha de inicio del Expediente.
Clasificación	eEMGDE22 - Clasificación
Estado	eEMGDE27- Estado del expediente. Elemento que indicará el estado del expediente, siendo sus posibles valores: - "Abierto": Si no existe eEMGDE4.2 - Fecha de fin del expediente. - "Cerrado": Si existe eEMGDE4.2 - Fecha de fin del expediente.
Interesado	eEMGDE28- Interesado
Función resumen foliado	eEMGDE16.1 - Algoritmo empleado para la generación de las huellas de los documentos incluidos en el expediente.
Tipo de firma	Elemento que indicará el tipo de firma del índice del expediente electrónico, siendo sus posibles valores: - Si CSV: eEMGDE17.1.1 - Formato de firma = 'TF01'. - Si Firma electrónica basada en certificados: eEMGDE17.1.1 - Formato de firma = 'TF02 TF03 TF04 TF05 TF06'
Valor CSV	Si eEMGDE17.1.1 - Formato de firma = 'TF01': eEMGDE17.3 - Valor del CSV ="Valor CSV".
Definición generación CSV	eEMGDE17.4 - Definición generación CSV de la "Actividad" que, mediante la "Relación" correspondiente, aplica a la generación del CSV del "Expediente". Nota: Siendo el eEMGDE17.1.1 - Formato de firma = 'TF01'.

Artículo 11. Acceso

En relación con el acceso, a los documentos y expedientes electrónicos les son aplicables las medidas de protección de la información previstas en el anexo II del Esquema Nacional de Seguridad; en particular, de 'Datos de carácter personal' y 'Calificación de la información', sin perjuicio de otras medidas de ese capítulo que se apliquen a la luz de la categorización del sistema y de la calificación de la información, y de las medidas relativas al control de acceso. En consecuencia, el acceso a los documentos y expedientes electrónicos estará sometido a un control de acceso en función de la calificación de la información y de los permisos y responsabilidades del actor en cuestión y contemplará la trazabilidad de las acciones que se realicen sobre cada uno de los documentos y expedientes electrónicos y sus metadatos asociados, siguiendo lo establecido en la Política de Seguridad de la Información de la Universidad de Alcalá, que aprobada por Acuerdo de 15 de julio de 2020.

EL acceso a los documentos y expedientes electrónicos comienza con el control de acceso. Sobre el control de acceso se seguirá lo establecido en la Guía de Adecuación al ENS para Universidades del Centro Criptológico Nacional, de mayo del 2022:

- La identificación de usuarios, entidades o procesos en el sistema se implementará asegurando un identificador singular (cuentas individualizadas) de tal forma que se pueda conocer a quién pertenece, y con qué privilegios se accede y qué acciones realiza.
- La identificación avanzada de los usuarios permitirá al sistema determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos y se mantendrá una lista actualizada de usuarios autorizados para acceder a los diferentes recursos.

Cuando los usuarios dejen la entidad, hayan sido cesados en su función o se les hayan revocado los permisos, se inhabilitarán sus cuentas, manteniendo los registros de actividad asociados durante el periodo de retención que previamente se haya establecido.

- Los requisitos de acceso a la información se recogerán en una o normativa que identifique quiénes tienen capacidad de otorgar los accesos a los recursos y la forma de solicitarlos. El proceso de gestión de derechos de acceso se realizará en base al cumplimiento de principios tales como, “todo acceso está prohibido, salvo autorización expresa”, “mínimo privilegio”, “necesidad de conocer y responsabilidad de compartir” y “capacidad de autorizar”. Los permisos de acceso se revisarán periódicamente y el acceso remoto debe ser previamente autorizado, contando con una normativa específica de uso. En la definición de la política acceso de los usuarios, se tendrá en cuenta que se debe establecer una segregación de funciones y tareas, asegurando la concurrencia de dos o más personas, para aquellas tareas consideradas como críticas y separando, siempre que sea posible, funciones incompatibles, de tal forma que no recaigan en la misma persona tareas de desarrollo y operación y que las personas que autorizan el acceso y las que controlan el uso sean distintas. Si la falta de personal imposibilita la aplicación de esta segregación, la medida podría ser reemplazada por una medida compensatoria, como por ejemplo la activación de registros de actividad de las actuaciones de estos usuarios sobre el sistema de información, registro que solo podrá ser accesible por personal autorizado. Como apoyo a estas actividades pueden emplearse las Guías “CCNSTIC 819 Medidas compensatorias” y “CCN-STIC 831 Registro de la actividad de los usuarios”.
- Los mecanismos de autenticación (usuarios externos) se adecuarán al nivel de seguridad del sistema, pudiendo usarse los siguientes factores de autenticación: contraseñas, contraseña de usuario + contraseña de un solo uso (OTP), Certificados o bien certificados en dispositivo físico. Antes de proporcionar las credenciales (factores de autenticación) a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre y estarán bajo el control exclusivo del usuario, reconociendo que las ha recibido y que acepta las condiciones que implica su tenencia antes de que se haya activado el mecanismo de autenticación. Se cambiarán con la periodicidad marcada por la política de la universidad y se retirarán e inhabilitarán cuando se termine la relación con el sistema o cuando se detecte que su pérdida o control por parte del usuario. Se establecerá una limitación de intento de accesos que requerirá una intervención específica para reactivar la cuenta. La información suministrada en el acceso será la mínima imprescindible. Una vez otorgado el acceso se informará al usuario de sus obligaciones. Se habilitará el registro de los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad.
- En función de los mecanismos de autenticación usados se tendrá en cuenta lo siguiente:
- Contraseñas o contraseñas + OTP, estas dispondrán de una complejidad mínima y no serán fácilmente adivinables.
- Certificados, las credenciales se obtendrán tras un proceso de registro previo bien sea presencial, telemático, o bien usando certificado electrónico. El uso del certificado estará protegido por un segundo factor (PIN o biométrico).

- Certificados en dispositivo físico (tarjeta o similar), las credenciales se obtendrán tras un proceso de registro previo bien sea presencial, telemático, o bien usando certificado electrónico, se usarán algoritmos, parámetros y dispositivos autorizados por el CCN y su uso estará protegido por un segundo factor (PIN o biométrico).
- En cuanto a los mecanismos de autenticación (usuarios de la organización) del personal propio o contratado estable o circunstancial, que pueda tener acceso a la información contenida en el sistema, se podrá usar los siguientes factores de autenticación: contraseñas (cuando el acceso se realiza desde zonas controladas, en su defecto será necesario doble factor para acceso desde o a través de zonas no controladas), contraseña + otro factor de autenticación (OTP), Certificados o bien certificados en dispositivo físico. Las credenciales estarán bajo el control exclusivo del usuario, reconociendo que las ha recibido y que acepta las condiciones que implica su tenencia antes de que se haya activado el mecanismo de autenticación. Se cambiarán con la periodicidad marcada por la política de la universidad y se retirarán e inhabilitarán cuando se termine la relación con el sistema o cuando se detecte que su pérdida o control por parte del usuario. Se establecerá una limitación de intento de accesos que requerirá una intervención específica para reactivar la cuenta. La información suministrada en el acceso será la mínima imprescindible. Una vez otorgado el acceso se informará al usuario de sus obligaciones. Se habilitará el registro de los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad. En cuanto al acceso remoto (todos los niveles) será de aplicación la ITS de interconexión de sistemas de información, deberá ser autorizado previamente, el tráfico deberá estar cifrado, se inhabilitará cuando su uso no sea constante y se activarán los registros de auditoría de las conexiones.

En los sistemas de información de la Universidad que traten datos personales, se seguirá lo establecido en el artículo 3 del ENS (Esquema Nacional de Seguridad):

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.
2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.
3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto”.

Artículo 12. Calificación

Confluyen aquí dos acepciones de 'calificación'; una desde la perspectiva archivística y otra desde la perspectiva de la seguridad (ENS). También será aplicable la norma ISO 27001, de Gestión de la Seguridad de la Información. En general, el nivel de confidencialidad asignado a un documento en este metadato no tendrá por qué coincidir con el nivel de seguridad del ENS atribuido a algún sistema de información que lo capture, procese o almacene, ya que el nivel de seguridad del ENS se computa a partir de 5 dimensiones de seguridad.

Valoración

En archivística la calificación es el procedimiento por el cual mediante la aplicación de la metodología de identificación y valoración de series documentales se determinan que documentos y expedientes pueden ser elevados por aprobación por el organismo competente mediante dictamen de la eliminación total, parcial o conservación permanente. En el caso de la Universidad de Alcalá, corresponde elevar el estudio a dictamen de la Comunidad de Madrid. En los estudios de identificación y valoración de documentos se suelen destacar los documentos esenciales de las series documentales, por lo que pueden servir de referencia para determinar que documentos son esenciales en la organización. El estudio se realiza a nivel de serie documental.

A nivel de documento, concretamente a nivel de serie documental, se pueden incluir los siguientes metadatos, algunos de los cuales serán obligatorios para la transferencia a la fase de archivo:

Tabla 9. TABLA DE METADATOS DE VALORACIÓN		
Metadato	Descripción	Valores
eMUXXI/eEMGDE8.6 Nivel de confidencialidad de la información	Evaluación, en cuanto al nivel de la dimensión de seguridad "confidencialidad", de la información recogida en un documento, de acuerdo con el Esquema Nacional de Seguridad.	Bajo, medio y alto
eMUXXI /eEMGDE13.1.1.1 Tipo de valor	Identificación de los diferentes valores primarios que poseen los documentos, expedientes y series	
eMUXXI /eEMGDE13.1.1. Valor Primario	Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales.	Administrativo, legal, jurídico, contable
eMUXXI /eEMGDE13.1.2 Valor secundario	Determinación la existencia de valores secundarios en los documentos	Si, No, sin cobertura de calificación
eMUXXI /eEMGDE13.2.1 Tipo de dictamen	Tipo de decisión emitida por la autoridad calificadora que debe aplicarse sobre los documentos a lo largo de su ciclo de vida y una vez realizada su valoración.	CP Conservación permanente EP Eliminación parcial ET Eliminación total PD Pendiente de dictamen

eMUXXI /eEMGDE13.1.1.2 Plazo	Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales.	Introducir un valor numérico relativo a años
------------------------------------	--	--

Tabla 10. TABLA DE METADATOS DE VALORACIÓN			
Valores primarios		Valores secundarios	
Administrativo	Sirve como testimonio de los procedimientos y actividades de la administración que los ha	Informativo	Aquél que sirve de referencia para la elaboración o reconstrucción de cualquier actividad de la Administración y que también puede ser testimonio de la memoria colectiva
Jurídico / Legal	Aquel del que se derivan derechos u obligaciones legales regulados por el derecho común y que sirve de testimonio ante la Ley	Histórico	El que posee un documento como fuente primaria para la Historia
Fiscal	Es el que sirve de testimonio de obligaciones tributarias		
Contable	El que puede servir de explicación o justificación de operaciones destinadas al control presupuestario		

Los dictámenes de la Universidad de Alcalá, según la legislación de archivos de la Comunidad de Madrid, deberán elevarse al Consejo de Archivos de la Comunidad de Madrid. Para ello, la Universidad elaborará un cuadro de conservación de fondos documentales sea cual sea el formato de los expedientes. La Comunidad de Madrid cuenta con instrucciones específicas para realizar este proceso, que debe de realizarse por expertos de archivos y documentación, ya que supone la aplicación de una procedimiento especializado de gestión documental, para lo cual se puede tomar como referencia la Metodología para la valoración y destrucción física de los documentos que forman parte del patrimonio documental madrileño del Consejo de gobierno de Archivos de la Comunidad de Madrid¹.

¹ Metodología para la valoración y destrucción física de los documentos que forman parte del patrimonio documental madrileño del Consejo de gobierno de Archivos de la Comunidad de Madrid.
http://www.madrid.org/archivos/images/QUIENES_SOMOS/CONSEJO_ARCHIVOS/MetodologiaCACM.pdf

Documentos esenciales de la Universidad de Alcalá

La Universidad de Alcalá, elaborará una relación de documentos de archivo que considere esenciales, y un programa de preservación y conservación de los documentos y expedientes sean en papel o electrónicos, en el que se realizará un análisis de riesgos, se calificará la información, así como se determinarán las medidas de seguridad y nivel requerido aplicable según la importancia de los documentos y expedientes.

Se entiende por documentos esenciales aquéllos que resultan indispensables para que la Universidad pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio, respetar la legalidad vigente y los derechos de las personas. Por otro lado, son aquellos documentos que caso de emergencia o desastre, necesita la Universidad para continuar funcionando, o recuperar su funcionamiento. Estos documentos deben de conservarse con medidas adicionales como realización de copias, diversificarlas en diversas ubicaciones. Para el análisis de riesgos, la calificación de la información, se seguirán entre otras normas el Esquema Nacional de Interoperabilidad.

En líneas generales, los documentos y expedientes que cumplan las siguientes características serán calificados como esenciales:

- Documentos que recogen derechos de la Universidad, como convenios y documentos de propiedad.
- Documentos que informan de políticas, directrices, estrategias y planificación de la Universidad.
- Documentos que dejan constancia de los acuerdos y resoluciones de los órganos de gobierno colegiados y unipersonales.
- Documentos que dan testimonio de las funciones específicas de la Universidad: docencia e investigación.
- Documentos que acreditan y certifican derechos y deberes de estudiantes, personal de administración y personal docente.
- Documentos en cualquier soporte custodiados en el Archivo de la Universidad de Alcalá.

Una vez definida la relación de documentos esenciales de la Universidad de Alcalá, se introducirá el metadato para diferenciarlo en los sistemas de gestión documental, es un metadato obligatorio para la transferencia al archivo, pero es esencial definirlo en la fase de archivo de oficina:

Tabla 11. TABLA DE METADATOS DE DOCUMENTO ESENCIAL		
Metadato	Descripción	Valores
eMUXXI/eEMGDE13.4 – DOCUMENTO ESENCIAL	Calificación de un documento como esencial para el desarrollo de las actividades de la organización y que, por ello, debe ser objeto de medidas especiales de protección, que incluyen su duplicado y almacenamiento en un repositorio diferente	Operador Booleano: SI/NO

Artículo 13. Conservación

Tal y como se señala en la Guía de Aplicación de la Conservación de la Política de Gestión de Documentos Electrónicos: La conservación no es un proceso de gestión documental exclusivo de las últimas fases del ciclo de vida de los documentos, sino un proceso que abarca toda su existencia, concretado en la aplicación de medidas de preservación y conservación a los documentos electrónicos desde el momento de su captura por el sistema de gestión de documentos.

La conservación y su planificación deben plantearse como una parte integral de la política de gestión documental de la organización. Para el desarrollo de un plan de conservación efectivo es necesario que la organización cuente con elementos de la política como un cuadro de clasificación y un calendario de conservación. La Universidad de Alcalá cuenta con un cuadro de clasificación, pero no con un calendario de conservación. Servirán como referencia los estudios de identificación y valoración de la CRUE.

Disponer de una política de gestión documental se desarrollada en base a un análisis riguroso de las necesidades de la organización permite un uso eficiente de los recursos dedicados a la conservación. 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:

1. Se conservan los expedientes necesarios, bajo medidas de protección adecuadas a su valor para la administración.
2. No ingresan en el archivo, individualmente o como parte de un expediente, documentos que no es necesario conservar.
3. Los documentos y expedientes ingresan en el archivo en formatos adecuados, firmados y con los metadatos necesarios para su conservación y recuperación del archivo.
4. Los documentos se transfieren a archivos (central, histórico) con características adecuadas a su estado dentro del ciclo de vida.
5. Se eliminan, de acuerdo con la normativa y los procedimientos aplicables los documentos que han perdido su valor.

De cara a la conservación, son importantes los metadatos de características físicas, almacenamiento, que se podrán cubrir en muchos casos de manera automatizada por los sistemas de digitalización y almacenamiento. Reflejan los cambios de formatos y soportes de cara a la preservación digital a largo plazo, y usar metadatos de integridad y trazabilidad de quién y cuando se han realizado cambios en las entidades.

Tabla 12. TABLA DE METADATOS DE CONSERVACIÓN

Metadatos	Descripción	Valores
eMUXXI/eEMGDE14 CARACTERÍSTICAS TÉCNICAS	Información acerca de la forma lógica y otras características técnicas lógicas y físicas de un documento digital o digitalizado. (La información proporcionada por este elemento puede utilizarse para determinar las estrategias de conservación sobre los documentos digitales y debería ser lo más	



	completa posible para asegurar que las características técnicas se identifican con exactitud).	
eMUXXI /eEMGDE14.1 FORMATO	Formato lógico del fichero contenido en el documento electrónico	
eMUXXI /eEMGDE14.1.1 NOMBRE DEL FORMATO	Denominación del formato lógico del fichero contenido en el documento electrónico	Valores definidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares en la columna "Nombre Común" de la tabla recogida en su anexo. Ejemplos: Strict Open XML ISO/IEC 26300:2006 OASIS 1.2 PDF, PDF/A
eMUXXI /eEMGDE14.1.2 EXTENSIÓN DEL FICHERO	Extensión del formato lógico del fichero contenido en el documento electrónico	Valores definidos en la Norma Técnica de Interoperabilidad de Catálogo de Estándares en la columna "Extensión" de la tabla recogida en su anexo. Ejemplos: docx .xlsx .pptx, .odt, .ods, .pdf, .txt, .csv
eMUXXI /eEMGDE14.2 VERSIÓN DE FORMATO	Versión del formato lógico de fichero del documento	Por ejemplo: PDF 1.7, XHTML 1.0
eMUXXI /eEMGDE14.3 RESOLUCIÓN	Medida de la capacidad para capturar los detalles del documento original, a menudo cuantificada en píxeles por pulgada.	Indicar la resolución para cada una de las dimensiones del documento siguiendo el esquema: Resolución horizontal x resolución vertical. Por ejemplo: 200x200 PPP
eMUXXI /eEMGDE14.4 TAMAÑO	Dimensiones físicas, tamaño lógico o duración del documento	
UXXI/eEMGDE14.4.1 DIMENSIONES FÍSICAS	Dimensiones de un documento físico, incluidas longitud, anchura y profundidad y, si es pertinente, peso y volumen.	Por ejemplo: 20, 12, 5
eMUXXI /eEMGDE14.4.1 TAMAÑO LÓGICO	Tamaño lógico del documento o expediente	Por ejemplo: 20,5
eEMGDE14.4.3 CANTIDAD	Número o cantidad total de elementos contenidos en una determinada entidad	Por ejemplo: 10,4
eMUXXI/eEMGDE14.4.4 UNIDADES	Elemento de medida utilizado para registrar las dimensiones de un documento físico o el tamaño o la	Por ejemplo: cm, Mb, cajas



	duración lógicas de un documento digital y para especificar el tipo de objeto a la que se refiere la cifra de la cantidad.	
eMUXXI /eEMGDE14.5 PROFUNDIDAD DE COLOR	Profundidad de color o escala de grises o resolución cromática de una imagen digitalizada.	Por ejemplo: 8 (bits), 24 (bits)
eMUXXI/eEMGDE15 UBICACIÓN	Localización física y/o lógica donde reside un documento. (El documento no está localizado dentro de un sistema de gestión de documentos, sino que se mantiene en algún otro tipo de almacenamiento virtual o físico)	Debería utilizarse cuando: - El documento no está localizado dentro de un sistema de gestión de documentos, sino que se mantiene en algún otro tipo de almacenamiento virtual o físico. - Sea necesario distinguir la localización del documento a efectos de gestión y de acceso
eMUXXI /eEMGDE15.1 SOPORTE	Objeto físico sobre el que se almacena un documento	Por ejemplo: CD-ROM, DVD, unidad de disco duro externo, caja AGA
eMUXXI /eEMGDE15.2 LOCALIZACIÓN	Localización actual (física o de sistema) del documento	Por ejemplo: http://www.cartagena.es/recursos/urbanismo/132007.pdf \\archivo\deposito\132007.xml ftp://recursos/regla01.txt Archivo Central, caja 12546
eMUXXI /eEMGDE16 VERIFICACIÓN DE INTEGRIDAD	Método para determinar si los bits que conforman un documento digital han sufrido algún cambio en el curso de la transmisión o del almacenamiento. A veces se le denomina "fijeza".	Requerido para documentos/expedientes digitales que se transmiten, transfieren o de alguna otra manera se migran entre sistemas o dentro de un solo sistema.
eMUXXI/eEMGDE16.1 ALGORITMO	Método algorítmico reproducible que transforma la secuencia de caracteres que forma un Documento, en un valor de longitud fija, que representa el valor digital de dicho Documento. Se excluye el caso de CSV.	Por ejemplo: SHA-2, SHA-3
eMUXXI /eEMGDE16.2 VALOR	Valor real, generado por el algoritmo definido en eEMGDE16.1 - Algoritmo que representa el documento simple o conjunto de documentos a que hace referencia.	Por ejemplo: 573066A121BECFDC7B26433 38ED11EB2AAEFD056,

En caso de realizarse cambios a nuevos formatos por migraciones, por ejemplo, deberán de modificarse los metadatos de características técnicas y se reflejarán también los siguientes metadatos:

Tabla 13. TABLA DE METADATOS DE CAMBIOS DE METADATOS		
Metadato	Descripción	Valores
eMUXXI/eEMGDE21.6 HISTORIA DEL CAMBIO	Información que registra el elemento de metadato que ha sido modificado sobre una determinada entidad y su valor anterior.	
eMUXXI/eEMGDE21.6.1 NOMBRE DEL ELEMENTO	Nombre de un elemento o subelemento de metadato cuyo valor ha sufrido algún tipo de modificación.	Por ejemplo: eEMGDE.Formato eEMGDE.Soporte
eMUXXI/eEMGDE21.6.2 VALOR ANTERIOR	Contenido anterior de un elemento o subelemento de metadato de una determinada entidad que ha sido modificado en un momento del tiempo	Por ejemplo: [Cualquier valor de metadato]

Artículo 14. Transferencia

La manera habitual de transferencia de documentos y expedientes electrónicos, y su integración en sistemas de archivo electrónico, se realiza a través de paquetes de información (SIP), que se han incorporado en el Archivo Electrónico de Oficina de UNIVERSITASXXI. El contenido de los paquetes SIP debe contener expedientes y documentos basados en el esquema interoperable ENI, archivos en formato XML, para garantizar la correcta operatividad de los sistemas de intercambio de ficheros y de almacenamiento. La Universidad facilitará en todo caso desde el punto de vista funcional y tecnológico las transferencias de ficheros entre sistemas sin pérdidas documentales o informativas.

Se tendrán que definir a nivel de oficina los plazos de transferencia. El paso entre repositorios de los documentos y expedientes electrónicos estará definido y controlado por reglas en el sistema de gestión de documentos electrónicos, para facilitar el paso entre una fase y otra fase se emplearán calendarios de conservación.

Al realizarse la transferencia a la fase de archivo definitivo, como es un cambio de custodia, se deberá formalizarse a través de una "Relación de entrega":

El receptor verificará el contenido del paquete transferido, confirmando que contiene los expedientes y los documentos acordados, en el formato correcto y con los metadatos complementarios necesarios. Una vez comprobados, deberá enviar constancia de la recepción correcta al organismo que realizó la transferencia.

Deberá quedar constancia tanto de la remisión de los expedientes y documentos por parte del órgano o aplicación emisora de los mismos como de su recepción en el archivo de destino. La

forma concreta en que se exprese dicha constancia dependerá, en cada caso, de las aplicaciones utilizadas para la gestión documental.

Tras verificarse se realizará el “Acta de entrega”:

Al realizarse el ingreso correcto del expediente en el Archivo destino, pasará a estado ‘transferido’ en el Archivo origen. En ese mismo instante y de manera automática, el Archivo destino enviará el Acta de transferencia (en PDF) al Archivo origen. El Acta de entrega implica el traspaso de la responsabilidad de custodia del archivo remitente al archivo receptor. En cualquier caso, la aplicación de archivo deberá tener la funcionalidad necesaria para la redacción de informes comprensivos de los expedientes ingresados en el archivo receptor en un periodo determinado. Dicho informe podrá llevarse a cabo por series documentales y deberá incluir como mínimo la mención del órgano remitente, la identificación de los expedientes, sus fechas extremas y la fecha de ingreso en el Archivo.

En el caso de que la transferencia suponga una duplicación de los documentos que son objeto de esta, el órgano remitente, una vez obtenida la conformidad del nuevo responsable de la custodia, deberá proceder al borrado de sus propios ejemplares.

Con los informes elaborados por la aplicación de archivo se generará un Registro General de entrada de Fondos, como control de la documentación ingresada.

Metadatos: Se asignarán a los documentos y expedientes electrónicos los metadatos mínimos obligatorios ENI y, en su caso, los obligatorios para la transferencia, además de los opcionales si se considera oportuno por el Archivo.

Tabla 14. TABLA DE METADATOS PARA LA TRANSFERENCIA		
METADATOS	DESCRIPCIÓN	VALORES
eMUXXI/ eEMGDE1 CATEGORIA	Tipo de entidad que se está describiendo.	Documento/Expediente
EMUXXI/ eEMGDE3 NOMBRE	Título o nombre dado a una entidad.	
EMUXXI/eEMGDE3.1 NOMBRE NATURAL	Nombre real que se da a la entidad	Para una entidad Documento: Instancia de solicitud de licencia de obras, Expediente de concesión de licencia de obras, Serie de licencias de obras.
eMUXXI/ eEMGDE6 ENTIDAD RELACIONADA	Medio para identificar a otras entidades en una relación	
EMUXXI/ eEMGDE6.1 ID DE ENTIDAD RELACIONADA	Identificador único para una entidad implicada en una relación.	Por ejemplo: DIR3 DE AGENTE
eMUXXI/ eEMGDE6.3 ROL DE LA RELACIÓN	Identificador único para una entidad implicada en una relación	1 La relación se lee desde la entidad. 2 La relación se lee hacia (en dirección a) la entidad.



<p>eMUXXI/ eEMGDE8.4 SENSIBILIDAD DATOS DE CARÁCTER PERSONAL</p>	<p>Término normalizado de acuerdo con los niveles de clasificación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo.</p>	<p>Bajo: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a la entidad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Medio: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a la entidad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Alto: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a la entidad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.</p>
<p>eMUXXI/ eEMGDE8.6 NIVEL DE CONFIDENCIALIDAD DE LA INFORMACIÓN</p>	<p>Evaluación, en cuanto al nivel de la dimensión de seguridad "confidencialidad", de la información recogida en un documento, de acuerdo con el Esquema Nacional de Seguridad Información acerca de los plazos de conservación de los documentos en atención a sus valores, a lo largo de su ciclo de vida, así como acerca de las acciones dictaminadas regladas a emprender sobre los mismos, tomadas a partir de la ponderación de esos valores</p>	<p>Bajo, Medio, Alto</p>
<p>eMUXXI/ eEMGDE13CALIFICACIÓN</p>	<p>Información acerca de los plazos de conservación de los documentos en atención a sus</p>	



	valores, a lo largo de su ciclo de vida, así como acerca de las acciones dictaminadas regladas a emprender sobre los mismos, tomadas a partir de la ponderación de esos valores	
eMUXXI/ VALORACIÓN	eEMGDE13.1 Determinación de los valores y plazos a los que los documentos están sometidos a lo largo de su ciclo de vida	
eMUXXI/ VALOR PRIMARIO	eEMGDE13.1.1 Determinación de los valores primarios de los documentos y expedientes que componen Una determinada serie documental.	Operador booleano: s/n
EMUXXI/ TIPO DE VALOR	eEMGDE13.1.1.1 Identificación de los diferentes valores primarios que poseen los documentos, expedientes y series	Administrativo/Fiscal/ Jurídico/otros
eMUXXI/ PLAZO	eEMGDE13.1.1.2 Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales.	Indicar plazo en años
eMUXXI/ VALOR SECUNDARIO	eEMGDE13.1.2 Determinación la existencia de valores secundarios en los documentos	Valor testimonial o histórico. Operador booleano: S/N
eMUXXI/ DICTAMEN	eEMGDE13.2 Decisiones emitidas por la autoridad calificadoras relativas a la conservación o a la eliminación de documentos de acuerdo con la evolución de sus valores conforme avanza su ciclo de vida	
eMUXXI/ TIPO DE DICTAMEN	eEMGDE13.2.1 Tipo de decisión emitida por la autoridad calificadoras que debe aplicarse sobre los documentos a lo largo de su ciclo de vida y una vez realizada su valoración	CP Conservación permanente EP Eliminación parcial ET Eliminación total PD Pendiente de dictamen
eMUXXI/eEMGDE13.2.2 - ACCIÓN DICTAMINADA	- Condicional: Debe utilizarse para la transferencia a menos que el valor del sub-elemento eEMGDE13.2.1 - Tipo de dictamen, sea PD - Pendiente de dictamen.	Ejemplos: Eliminación de las solicitudes y méritos a los 5 años, y conservación permanente del resto del expediente. Eliminación total dejando una muestra de un expediente por año

eMUXXI/eEMGDE13.2.3 - PLAZO DE EJECUCIÓN DE LA ACCIÓN DICTAMINADA	Plazo en el que se tiene que ejecutar la acción concreta que se aplica al documento y que figura en el sub-elemento eEMGDE13.2.2 - Acción dictaminada	Por ejemplo: 5 años
EMUXXI/ eEMGDE13.3 TRANSFERENCIA	Operación por la que traspasa la custodia de las diferentes fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental	
eMUXXI/ eEMGDE13.3.1 FASE DE ARCHIVO	Indicación de la fase de archivo correspondiente al momento del ciclo de vida del documento que se transfiere	Por ejemplo: Archivo de Oficina/Archivo Histórico
eMUXXI/ eEMGDE13.3.2 PLAZO DE TRANSFERENCIA	Plazo de tiempo en que se traspasa la custodia de las diferentes fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental.	Por ejemplo: 5 años
eMUXXI/ eEMGDE13.4 DOCUMENTO ESENCIAL	Calificación de un documento como esencial para el desarrollo de las actividades de la organización y que, por ello, debe ser objeto de medidas especiales de protección, que incluyen su duplicado y almacenamiento en un repositorio diferente	Operador booleano: s/n
eMUXXI/ eEMGDE22.2 DENOMINACIÓN DE CLASE	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación de la UAH	
DENOMINACIÓN DE CLASE EN SIA	Indicador en lenguaje natural que identifica de forma unívoca la clase en SIA	
DENOMINACIÓN DE CLASE FUNCIONAL	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación Funcional de la UAH	

Se garantizarán la disponibilidad e integridad de los metadatos de los documentos y expedientes electrónicos, manteniendo de manera permanente las relaciones entre cada documento o expediente y sus metadatos.

Con el propósito de equilibrar la carga de trabajo entre los sistemas de gestión de documentos y expedientes y el sistema de gestión de archivos, en el momento del ingreso de expedientes y documentos en el archivo, se ha establecido un conjunto mínimo de metadatos complementarios que son de vital importancia para la gestión archivística, y que no pueden ser deducidos de la serie documental en la que ingresarán dichos datos

Artículo 15. Destrucción o eliminación

Como se ha indicado la Universidad de Alcalá elevará los dictámenes de calificación al Consejo de Archivos de la Comunidad de Madrid, derivado de dichos dictámenes se podrá determinar la conservación o eliminación de sus fondos documentales. No se podrán eliminar documentos, ni expedientes en papel o electrónicos en la fase de oficina, sólo se realizarán tareas de limpieza, no de eliminación, en todo caso, se seguirán las pautas del archivo de la Universidad y de la normativa de la Comunidad de Madrid para realizar las eliminaciones. La Comunidad de Madrid una vez aprobado el dictamen de eliminación, que se publica en el BOCM (Boletín Oficial de la Comunidad de Madrid), se tendrán en cuenta las instrucciones del Archivo de la Universidad para la realización del proceso de destrucción y las de la Comunidad de Madrid, entre otras.

En todo caso, se seguirán las recomendaciones y normas de borrado y destrucción certificada de los soportes de información digitales (discos duros, memorias, flash,...) con la finalidad de proteger tanto la información confidencial de la organización, como la difusión de datos personales que puedan contener dichos soportes. Especialmente las Recomendaciones para el borrado lógico de documentación electrónica y la destrucción física de soportes informáticos que formen parte del patrimonio documental madrileño² o las Recomendaciones para el borrado lógico de documentación electrónica y destrucción física de soportes informáticos de la administración general del estado³

No se eliminará ningún documento o expediente bajo estos supuestos:

1. Esté calificado como de “valor histórico” o de “investigación” de acuerdo con lo previsto en la legislación vigente al respecto.
2. No haya transcurrido el plazo establecido para su conservación, durante el cual pueda subsistir su valor probatorio de derechos y obligaciones de personas físicas o jurídicas.
3. No exista dictamen previo de la autoridad calificadora competente.

TÍTULO III

Formación

² Recomendaciones para el borrado lógico de documentación electrónica y la destrucción física de soportes informáticos que formen parte del patrimonio documental madrileño
http://www.madrid.org/archivos/images/QUIENES_SOMOS/CONSEJO_ARCHIVOS/MetodologiaCACMdo_electronica.pdf

³ Recomendaciones para el borrado lógico de documentación electrónica y destrucción física de soportes informáticos de la administración general del estado
<https://www.culturaydeporte.gob.es/dam/jcr:8a4186d5-73cc-4eb8-b5de-c1272ab8da7c/recomendaciones-destruccion.pdf>

Artículo 16. Formación sobre Gestión Documental

La implantación de la Administración Electrónica supone un cambio de gran importancia en la gestión administrativa tradicional de la Universidad de Alcalá, por ello, se realizarán formaciones continuadas y de capacitación del personal responsable tanto en la ejecución y del control de la gestión, tratamiento y conservación en repositorios o archivos electrónicos.

Se diseñarán, en concreto, acciones formativas específicas para cada uno de los tipos de actores involucrados en los diferentes procesos de gestión documental contemplados en la presente política.

TÍTULO IV

Supervisión y auditoría de los procesos de gestión de documentos

Artículo 17. Auditoría de la gestión documental

La Universidad aplicará normas de supervisión y auditoría de procesos de gestión de documentos. El modelo y política de gestión documental serán objeto de auditorías periódicas que pueden ser internas realizadas por personal certificado en auditorías de gestión documental o externas mediante contratación administrativa, con el objeto garantizar el funcionamiento de los sistemas de gestión documental. Estas auditorías pueden ser simultaneadas con las auditorías de Seguridad.

La normativa ISO15489, ISO 30301, ISO 9001, ISO 14001, ISO/IEC, definen procesos de supervisión y auditoría de los procesos de gestión de documentos. Las auditorías de la gestión de documentos tienen como objetivos:

- Supervisar la eficiencia en la gestión documental (eliminando duplicados, transacciones innecesarias, facilitando el acceso a los datos/información)
- Supervisar el control de los documentos de manera que sean fiable, auténticos, íntegros, conformes con los requisitos, compromisos y objetivos de la gestión documental, además de soporte para la toma de decisiones, la rendición de cuentas y para los procesos de mejora continua de la institución.
- Facilita el control de la información documentada, en relación con las actividades de la institución, aportando consistencia en el control a cambios derivados del incremento de volumen de información y soportes, de la evolución tecnológica y el desarrollo digital, del incremento de la legislación, regulaciones y estándares relacionados con la gestión documental y la dispersión, diversidad y origen de las herramientas de gestión documental.
- Dota de un reconocimiento a la institución al aplicar las normas internacionales y de certificación
- Facilita el cumplimiento de otras normas de Gestión Documental.

En las auditorías se generarán documentos tanto derivados de la gestión documental como derivados de los informes de auditoría que se guardarán formando expedientes custodiados por los responsables de calidad de la Universidad, asimismo, en los procedimientos y acciones

seguidos en los diferentes procesos de gestión documental se generan registros para poder hacer un seguimiento en dichas auditorías.

Las auditorías pueden estar enfocadas o no a la obtención de una certificación. La certificación tendrá como ventajas para la Universidad: una gestión normalizada, el alineamiento de políticas, el ahorro de costes, el control de riesgos; demuestra el cumplimiento de los requisitos (legales, tecnológicos, entre otros), se realizan con auditores independientes y cualificados, generan confianza, credibilidad interna y externa, mejora la imagen y la marca de la institución, y contribuyen a una mejora continua.

TÍTULO IV GESTIÓN DE LA POLÍTICA

Artículo 18. Mantenimiento, actualización y publicación

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá Universidad de Alcalá, y en concreto al Gestor de la Política identificado en el apartado 1.3.2.

La Universidad de Alcalá creará una comisión técnica con el objeto de evaluar y hacer un seguimiento de su cumplimiento, proponer la aprobación de los requisitos, medios y normas técnicas para su aplicación, y tomar las medidas adecuadas para la correcta implantación de esta Política y su desarrollo.

Los miembros que integrarán esta Comisión serán designados por Resolución de un órgano de gobierno y se regirá por las reglas de funcionamiento que se establecen para los órganos colegiados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

ANEXO I

Terminología

Copia electrónica auténtica con cambio de formato: Copia auténtica en la que tanto el origen como el nuevo documento generado destino tienen naturaleza electrónica y además, para la obtención de la copia se requiere un cambio de formato.

Copia electrónica auténtica de documento papel: Copia resultante de un original en soporte papel sobre el que se crea un nuevo documento electrónico con calidad de copia auténtica para lo que es necesario aplicar un proceso de digitalización.

Copia electrónica parcial auténtica: Copia auténtica en la que tanto el documento origen como la copia generada tienen naturaleza electrónica, pero su contenido, por motivos de confidencialidad, representa sólo parcialmente el del documento original.

Copia papel auténtica de documento público administrativo electrónico: Copia cuyo origen es un documento público administrativo electrónico y la copia se manifiesta en soporte papel.

Clasificación: De acuerdo con la norma ISO 15489, la clasificación es “la identificación y estructuración sistemática de las actividades de las organizaciones o de los documentos generados por éstas en categorías, de acuerdo con convenciones, métodos y normas de procedimiento, lógicamente estructurados y representados en un cuadro de clasificación”.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado

Expediente electrónico: El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo.

Metadato: La definición genérica de ‘metadato’, según figura en el Esquema Nacional de Interoperabilidad, es “dato que define y describe otros datos”. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean gestionan, mantienen y utilizan. (Igual definición en Ley 18/2011 y RD 4/2010)

Tipo documental: 1) Agrupa documentos en relación con caracteres externos e internos. Externos: haciendo referencia a como es el documento físicamente: clase y tipo documental, formato, etc. Internos: que se refieren a las partes de las que consta un documento: productor o entidad, fecha,... Según la NTI de Documento Electrónico (Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de documento electrónico), los tipos documentales son:

- Documentos de decisión: Resolución, Acuerdo, Contrato, Convenio, Declaración
- Documentos de transmisión: Comunicación, Notificación, Publicación, Acuse de recibo
- Documentos de constancia: Acta, Certificado, Diligencia
- Documentos de juicio: Informe
- Documentos de ciudadano: Solicitud, Denuncia, Alegación, Recursos, Comunicación ciudadano, Factura, Otros incautados
- Otros.

Para la consulta de más términos está disponible en Web el Diccionario de Conceptos y Términos de la Administración Electrónica (8ª edición). Ministerio de Hacienda y Función Pública.

ANEXO II

Instrucciones para la digitalización de expedientes de la Universidad de Alcalá

Alcance y contenido

Para llevar a cabo un procedimiento de digitalización de expedientes la Universidad se seguirá las normas y recomendaciones nacionales e internacionales.

La digitalización se ha convertido en una forma de preservación documental, los documentos en papel sufren procesos de deterioro intrínseco y extrínseco que limitan su vida y hace que la preservación y su restauración en caso de deterioro sean costosas. Son muchas las ventajas de los procesos de digitalización para la oficina: trabajo en entornos compartidos, gestión más eficiente y eficaz, favorece el teletrabajo, evita la duplicidad y simplifica las tareas, mejora el control, acceso y seguridad de los documentos y expedientes, permite la generación de un archivo electrónico único, y una mayor transparencia de la organización, así como la mejora de la toma de decisiones, así como ahorros de costes.

Es importante diferenciar entre el procedimiento de digitalización tradicional que se define como la conversión de objetos analógicos (documentos en papel) en digitales (expediente electrónico), y el proceso de conversión digital de la administración y sus procesos, mediante la introducción de nuevas tecnologías y la simplificación de procedimientos, orientando el conjunto de las unidades administrativas a la atención a la ciudadanía y la resolución de sus problemas.

Estas instrucciones no se aplicarán para la digitalización de los documentos en papel conservados en el Archivo de la Universidad, ya que será el Servicio de Registro y Archivo quien determine estos procesos de digitalización en el ámbito de la preservación digital y la difusión del archivo.

Estas instrucciones se aplicarán en la digitalización certificada de documentos, que es el proceso realizado en el marco de la conversión de documentos en papel en documentos electrónicos válidos desde el punto de vista administrativo, jurídico, técnico y legal. Esta digitalización genera documentos con pleno valor probatorio equivalentes al original, garantiza la fiabilidad del documento digitalizado como evidencia electrónica de la actividad o procedimiento correspondiente, avalar la autenticidad del documento digitalizado, permite obtener una copia de seguridad auténtica y válida para la oficina. Y en su caso, puede permitir la destrucción del documento en soporte papel tras el proceso de identificación y valoración según la legislación y normativa aplicable, elevando la propuesta de dictamen a la autoridad competente.

Para ello, deberá de obtenerse en el proceso final un objeto digital formado por una imagen electrónica codificada, fiel e íntegra del documento original, con sus metadatos y las firmas asociadas al proceso de digitalización, de este modo, garantizaremos la autenticidad, integridad y preservación a largo plazo.

Estas instrucciones serán empleadas en todo caso para los siguientes procesos de digitalización:

- Procesos de digitalización interna, cuando se realice el proceso de digitalización por las oficinas de registros o por las unidades administrativas de la Universidad d Alcalá.
- Procesos de digitalización externa, cuando por falta de recursos humanos, se decida contratar a un proveedor externo, que deberá de estar especializado en estos procedimientos, y se realizará mediante contratación.

Requisitos básicos en los procesos de digitalización

Las imágenes electrónicas aplicarán los formatos admitidos en cada uno de los sistemas en los que se integren, el formato más habitual es el PDF/A, en su defecto se tendrá en cuenta la Norma Técnica de Interoperabilidad de Catálogo de Estándares, en cuanto a estándares válidos para la preservación digital.

El nivel de resolución mínimo para imágenes electrónicas será de 200 píxeles por pulgada, tanto para imágenes obtenidas en blanco y negro, color o escala de grises.

La imagen electrónica será fiel al documento origen, para lo cual:

- a) Respetará la geometría del documento origen en tamaños y proporciones.
- b) No contendrá caracteres o gráficos que no figurasen en el documento origen.
- c) No se utilizará compresión, excepto si se garantiza que no afecta a la calidad de la imagen obtenida.

Descripción del proceso de digitalización

La digitalización de un soporte papel o en otros soportes susceptibles de digitalización se realizará por medios fotoeléctricos, y se realizará a través de un procedimiento informático automático.

1. Se realizará a través de un proceso informático en el que, garantizando la integridad de cada uno de los pasos, se realizarán las siguientes tareas:

- a) Digitalización por un medio fotoeléctrico, de modo que se obtenga una imagen electrónica en la memoria del sistema asociado al dispositivo.
- b) Si procede, optimización automática de la imagen electrónica para garantizar su legibilidad, de modo que todo contenido del documento origen pueda apreciarse y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros, eliminación de documentos en blanco, u otros de naturaleza análoga).
- c) Asignación de los metadatos al documento electrónico digitalizados

Definición de proyectos de digitalización

El proyecto de digitalización es el documento básico para la digitalización masiva. Aquellas unidades y servicios administrativos que quieran realizar un proyecto de digitalización de expedientes en papel, deberán de presentar por escrito un proyecto a la CAES (Comisión de Administración Electrónica y Seguridad). Dichos proyectos deben de ser elevados al Consejo de Administración Electrónica y Seguridad para su estudio y aprobación, fundamentalmente, si se va a generar una digitalización certificada de documentos.

En el caso de que implique el cambio de soporte, con la destrucción total o parcial del soporte en papel deberá de ser estudiada por la Comisión de Administración Electrónica y Seguridad con la finalidad de ser elevada a Dictamen del Consejo de Archivos de la Comunidad de Madrid.

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. Para este proyecto contará en todo caso con la supervisión del Servicio de Registro y Archivo y Nuevos Procesos Administrativos y Administración Electrónica.

Contenido del proyecto de digitalización

- 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.

Contratación de la digitalización

La externalización del servicio de obtención de la imagen electrónica a través de medios fotoeléctricos de los documentos en soporte papel deberá de elevarse a la Comisión de Administración Electrónica y Seguridad.

La externalización deberá de realizarse a través de un contrato público y deberá de tenerse en cuenta en la formalización del contrato:

- El proveedor al ser el encargado de datos de carácter personal y de la información confidencial de los documentos y expedientes, deberá de implantar las correspondientes medidas de seguridad, sobre todo, si la documentación tiene que salir de las instalaciones de la Universidad a otras instalaciones y a efectos de informar a los trabajadores del manejo de los datos de carácter personal y de la información confidencial, sus riesgos y consecuencias.

- La documentación deberá de estar en todo momento en un entorno de seguridad en el proceso de digitalización, sobre todo, lo que comprenderá entradas y salidas de personal sólo autorizado, cierre de las instalaciones en el momento de que no haya personal, guarda de la documentación en cajas tras los trabajos de digitalización, sin dejar documentación visible encima de mesa o escáneres en los momentos de inactividad,... Las medidas de seguridad serán más rigurosas en los traslados de documentos de unas instalaciones a otras, para evitar la sustracción, pérdida, acceso o sustracción indebida a la información y evitar riesgos derivados.
- Es un requisito imprescindible que los licitadores presenten un plan de calidad que incluya los requisitos establecidos en la presenta instrucción, de manera que sirva para evaluar la capacitación técnica y profesional en las tareas de digitalización.
- Es necesario nombrar un responsable de la Universidad de Alcalá que supervise los trabajos que realice el proveedor, desde el punto de vista de que se cumplan los requisitos técnicos de estas instrucciones y las que se definan para cada proyecto, así como comprobar la calidad técnica del servicio, desde el punto de vista de la calidad de la digitalización y del servicio.

Fase de Preparación de la Documentación

Prevía a la digitalización habrá que preparar la documentación a digitalizar, el responsable del proyecto debe de ayudar a la preparación de la documentación en cuanto a:

- a) Parámetros mínimos a tener en cuenta en la digitalización
- b) Preparación de la documentación para que esté ordenada, y pueda ser fácilmente paginada.
- c) Incluir referencias de inicio y final de cada expediente.
- d) Limpieza de los expedientes de los elementos que impidan el proceso de digitalización: clips, grapas, y otros elementos de sujeción, post-its, documentos duplicados, documentos que no tengan que ser digitalizados.
- e) Comprobación de que el estado de conservación de los documentos no impide la digitalización.
- f) Extraer soportes no digitalizables.
- g) Atender a las diversas incidencias de digitalización que se pueden plantear a lo largo del proceso.

Fase de Preparación de las herramientas y sistemas informáticos

Los programas y aplicaciones que se emplean en la digitalización y en el procesado de los documentos y su gestión documental debe de ser supervisada por los Servicios Informáticos y por el Servicio de Nuevos Procesos Administrativos y Administración Electrónica.

En todo caso el proceso informático que se establezca para la digitalización deberá de garantizar las siguientes tareas:

- a) Digitalización por un medio fotoeléctrico, de modo que se obtenga una imagen electrónica en la memoria del sistema asociado al dispositivo.

b) Si procede, optimización automática de la imagen electrónica para garantizar su legibilidad, de modo que todo contenido del documento origen pueda apreciarse y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros, eliminación de documentos en blanco, u otros de naturaleza análoga).

c) Asignación de los metadatos al documento electrónico digitalizados, en la política de gestión de documentos electrónicos de la UAH se definen los metadatos mínimos obligatorios para los documentos, se asignarán metadatos específicos para la digitalización, como es el caso de los metadatos de conservación, trazabilidad, nombre de la aplicación de creación, versión de la aplicación de creación, características de la copia, tipo de copia, soporte de origen, entre otros.

d) Para obtener una digitalización certificada de documentos o copia auténtica de los documentos originales en papel y al realizarse por personal externo a la UAH por medios automáticos, se podrá emplear el sello electrónico de la UAH habilitado para los procedimientos de digitalización.

e) El sistema de digitalización tienen que cumplir en todo caso los requisitos de la normativa de protección de datos de carácter personal y de la política de seguridad de la información de la Universidad de Alcalá, por lo cual, deberán de identificar de forma unívoca los ficheros que se generen el proceso de digitalización.

f) Los dispositivos empleados para la obtención de la imagen electrónica tendrán los siguientes requisitos:

1. Las imágenes electrónicas aplicarán los formatos admitidos en cada uno de los sistemas en los que se integren, el formato más habitual es el PDF/A, en su defecto se tendrá en cuenta la Norma Técnica de Interoperabilidad de Catálogo de Estándares, en cuanto a estándares válidos para la preservación digital.
2. El nivel de resolución mínimo para imágenes electrónicas será de 200 píxeles por pulgada, tanto para imágenes obtenidas en blanco y negro, color o escala de grises.
3. La imagen electrónica será fiel al documento origen.
4. Respetará la geometría del documento origen en tamaños y proporciones.
5. No contendrá caracteres o gráficos que no figurasen en el documento origen.
6. No se utilizará compresión, excepto si se garantiza que no afecta a la calidad de la imagen obtenida.
7. Se podrán eliminar páginas de los documentos en blanco, siempre y cuando no aporten información administrativa a los documentos o expedientes.

Se definirá un plan de calidad de cada proyecto de digitalización, con los siguientes contenidos:

- 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.