centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 897

Perfil de Cumplimiento Específico para la Administración de Justicia



Diciembre 2025

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2025

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.11.03 13:23:46 +01'00'

Fecha de Edición: diciembre de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 5
2. SOBRE LA APLICABILIDAD DEL PERFIL DE CUMPLIMIENTO ESPECÍFICO 5
2.1 ÁMBITO DE APLICACIÓN DEL PCE 5
2.2 ORGANISMOS DE CERTIFICACIÓN DEL ENS 6
3. PLAN DE ADECUACIÓN AL ENS 6
3.1 DETERMINACIÓN DEL ALCANCE 6
3.2 CATEGORIZACIÓN DEL SISTEMA 7
3.2.1 SERVICIOS E INFORMACIÓN EXCLUSIVOS DEL MINISTERIO DE JUSTICIA 8
3.2.2 SERVICIOS E INFORMACIÓN IDENTIFICADOS PARA LOS SERVICIOS COMUNES .9
3.2.3 SERVICIOS E INFORMACIÓN DEL CONSEJO GENERAL DEL PODER JUDICIAL (CGPJ) 12
4. DOCUMENTOS DE APOYO A LA VALORACIÓN DE SERVICIOS E INFORMACIÓN 13
4.1 INSTRUCCIONES PARA CUMPLIMENTAR LOS CUESTIONARIOS 13
4.1.1 INSTRUCCIONES GENERALES 13
4.1.2 CABECERA DEL CUESTIONARIO 14
4.1.3 CUESTIONARIO RELATIVO A LA CATEGORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN 14
4.1.4 FINALIZACIÓN Y CUESTIONARIO PARA VALORACIONES FINAL DE ALTO 14
5. DECLARACIÓN DE APLICABILIDAD 15
5.1 DECLARACIÓN DE APLICABILIDAD MINISTERIO DE JUSTICIA 15
5.1.1 MEDIDAS DE APLICACIÓN 17
5.2 DECLARACIÓN DE APLICABILIDAD SERVICIOS COMUNES 20
5.2.1 MEDIDAS DE APLICACIÓN 22
5.3 DECLARACIÓN DE APLICABILIDAD CONSEJO GENERAL DEL PODER JUDICIAL 25
5.4 MEDIDAS DE APLICACIÓN 27
6. CRITERIOS DE APLICACIÓN DE MEDIDAS 29
6.1 CRITERIOS DE APLICACIÓN DE MEDIDAS PARA MINISTERIO DE JUSTICIA 29
6.1.1 [ORG.4] PROCESO DE AUTORIZACIÓN 29
6.1.2 [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES 29
6.1.3 [OP.ACC.1] IDENTIFICACIÓN 30
6.1.4 [OP.ACC.5] MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS) 30
6.1.5 [OP.ACC.6] MECANISMO DE AUTENTICACIÓN (USUARIOS INTERNOS) 30
6.1.6 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD 30
6.1.7 [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES 30
6.1.8 [MP.PER.3] CONCIENCIACIÓN 31
6.1.9 [MP.PER.4] FORMACIÓN 31
6.1.10 [MP.SI.5] BORRADO Y DESTRUCCIÓN 31
6.1.11 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN 31
6.1.12 [MP.INFO.3] FIRMA ELECTRÓNICA 32
6.1.13 [MP.INFO.4] SELLOS DE TIEMPO 32
6.1.14 [MP.INFO.5] LIMPIEZA DE DOCUMENTOS 32
6.2 CRITERIOS DE APLICACIÓN DE MEDIDAS PARA SERVICIOS COMUNES 33
6.2.1 [ORG.4] PROCESO DE AUTORIZACIÓN 33

6.2.2 [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES 33
6.2.3 [OP.ACC.1] IDENTIFICACIÓN 33
6.2.4 [OP.ACC.5] MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS) 33
6.2.5 [OP.ACC.6] MECANISMO DE AUTENTICACIÓN (USUARIOS INTERNOS) 33
6.2.6 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD 33
6.2.7 [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES 34
6.2.8 [MP.PER.3] CONCIENCIACIÓN 34
6.2.9 [MP.PER.4] FORMACIÓN 34
6.2.10 [MP.SI.5] BORRADO Y DESTRUCCIÓN 34
6.2.11 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN 35
6.2.12 [MP.INFO.3] FIRMA ELECTRÓNICA 35
6.2.13 [MP.INFO.4] SELLOS DE TIEMPO 36
6.2.14 [MP.INFO.5] LIMPIEZA DE DOCUMENTOS 36
6.3 CRITERIOS DE APLICACIÓN DE MEDIDAS PARA EL CONSEJO GENERAL DEL PODER JUDICIAL 36
6.3.1 [ORG.4] PROCESO DE AUTORIZACIÓN 36
6.3.2 [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES 36
6.3.3 [OP.ACC.1] IDENTIFICACIÓN 36
6.3.4 [OP.ACC.5] MECANISMO DE AUTENTICACIÓN (USUARIOS EXTERNOS) 36
6.3.5 [OP.ACC.6] MECANISMO DE AUTENTICACIÓN (USUARIOS INTERNOS) 37
6.3.6 [OP.EXP.6] PROTECCIÓN FRENTE A CÓDIGO DAÑINO 37
6.3.7 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD 37
6.3.8 [OP.CONT.2] PLAN DE CONTINUIDAD 37
6.3.9 [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES 37
6.3.10 [MP.PER.3] CONCIENCIACIÓN 38
6.3.11 [MP.PER.4] FORMACIÓN 38
6.3.12 [MP.COM.3] PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD 38
6.3.13 [MP.SI.5] BORRADO Y DESTRUCCIÓN 38
6.3.14 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN 39
6.3.15 [MP.INFO.3] FIRMA ELECTRÓNICA 39
6.3.16 [MP.INFO.4] SELLOS DE TIEMPO 39
6.3.17 [MP.INFO.5] LIMPIEZA DE DOCUMENTOS 40

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar Perfiles de Cumplimiento Específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Un perfil de cumplimiento específico determina una postura de seguridad conforme a un conjunto de medidas de seguridad, comprendidas o no en el Esquema Nacional de Seguridad que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Para su desarrollo, se ha tenido en cuenta el Esquema de Seguridad de la Administración de Justicia (ESAJ), aprobado en el seno del Comité Técnico Estatal de la Administración de Justicia (CTEAJE). Asimismo, se tendrán en cuenta todos los procedimientos, políticas e instrucciones desarrollados en el marco de dicho esquema, que serán de aplicación sin perjuicio de este perfil.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, ha validado el presente Perfil de Cumplimiento Específico, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, garantizando que las medidas de seguridad implementadas son las necesarias y proporcionales en relación con el contexto de la amenaza, nivel de madurez, riesgo residual asumible y recursos disponibles.

A tal fin, tras un análisis de riesgos contemplando las dificultades, brechas de seguridad, riesgos asociados y las potenciales amenazas a las que se ven expuestas las entidades, organismos u organizaciones; y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente Perfil de Cumplimiento Específico (en adelante, PCE).

2. SOBRE LA APLICABILIDAD DEL PERFIL DE CUMPLIMIENTO ESPECÍFICO

2.1 Ámbito de aplicación del PCE

El alcance de este Perfil de Cumplimiento Específico comprende los sistemas de información de Tribunales y Fiscalías, así como los sistemas de apoyo o auxiliares de la Administración de Justicia, de conformidad con la Política de Seguridad de la Información de la Administración Judicial Electrónica.

Atendiendo al artículo 88 del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, el ENS es de obligado cumplimiento para la administración de justicia, teniendo en cuenta las particularidades del sector. Después de realizar un análisis exhaustivo del ESAJ, parte integrante del Esquema Judicial de Interoperabilidad

y Seguridad (EJIS) contando con la colaboración del sector, se aprueba este PCE. La adecuación de la seguridad de los sistemas de información de las administraciones prestacionales del servicio de justicia mediante este PCE garantiza el cumplimiento tanto del ENS como del propio ESAJ ya que contempla las particularidades del mismo.

2.2 Organismos de certificación del ENS

Las Certificaciones de Conformidad con el ENS, incluidas las que se rijan por este Perfil de Cumplimiento Específico, las pueden otorgar los siguientes organismos de certificación que se basarán internamente entre otras, en la norma ISO/IEC 17065:2012:

- Una Entidad de Certificación (EC) acreditada por la Entidad Nacional de Acreditación (ENAC).
- Un Órgano de Auditoría Técnica (OAT) del Sector Público, reconocido por el Centro Criptológico Nacional (CCN), en su ámbito de competencias.
- En determinados casos específicos, directamente el CCN.

3. PLAN DE ADECUACIÓN AL ENS

Para llevar a cabo el proceso de adecuación, será necesario elaborar un Plan de Adecuación, que es un documento que contendrá información sobre la identificación del Alcance del Sistema, la Categorización del Sistema, la Declaración de Aplicabilidad Provisional, el Análisis de Riesgos, la Declaración de Aplicabilidad Definitiva - Perfil de Cumplimiento específico validado.

Dado que el objetivo es proporcionar un Perfil de Cumplimiento Específico para Justicia, con un conjunto de medidas que, junto con sus criterios de aplicación, permitirán que estas se adecuen al ENS, únicamente será necesario realizar los siguientes pasos en el Plan de Adecuación:

- Identificación del Alcance de los sistemas a certificar.
- Categorizar del Sistema.
- Declaración de Aplicabilidad Provisional- Aplicación del Perfil de Cumplimiento Específico.
- Análisis de riesgos. Declaración de aplicabilidad definitiva- Perfil de Cumplimiento Específico Validado.

Una vez realizado el Plan de Adecuación, se pasará a la fase de Implantación de la Seguridad, mediante la definición del plan de implantación que contendrá los documentos a elaborar y las medidas técnicas a implementar de forma priorizada.

3.1 Determinación del alcance

Para determinar el alcance de los sistemas a certificar es necesario elaborar un catálogo identificando los activos esenciales, servicios e información, y el sistema en el

que se alojan. Se recomienda, en la medida de lo posible, englobar los activos esenciales en el menor número de sistemas posibles.

En este marco, se han desarrollado tres tipologías de catálogos de servicios:

1. **Catálogo específico de servicios**, que abarca los servicios prestados exclusivamente por el **Ministerio de Justicia.**
2. **Catálogo de servicios comunes**, que incluye los servicios prestados por todas las administraciones prestacionales en todos los territorios.
3. **Catálogo específico de servicios, que abarca los servicios prestados exclusivamente por el Consejo General del Poder Judicial (CGPJ).**

3.2 Categorización del sistema

Atendiendo a las especialidades de los activos esenciales relacionadas con la prestación del servicio público de justicia y a las distintas entidades con competencias en la materia, contando con el apoyo del Ministerio de Justicia, el Consejo General del Poder Judicial, Fiscalía General del Estado, Secretaría General de la Administración de Justicia y la participación de algunas Comunidades Autónomas, se ha elaborado un inventario de servicios e información valorándolo de conformidad con el Anexo I del ENS, atendiendo también las indicaciones de los procedimientos de valoración aprobados por el CTEAJE en el ámbito de las competencias de dicho organismo.

Si bien se ha tratado de realizar una síntesis de los principales activos, es posible que las entidades en el alcance de este PCE presten otros no identificados en este Anexo o que consideren necesario hacer una modificación de estos por lo que se pone a su disposición unos modelos de cuestionarios orientativos de uso voluntario, incluidos como anexos, basados en el Anexo I del ENS, la Guía CCN-STIC 803 y la Guía de criterios de valoración de referencia de dimensiones de seguridad , que faciliten la labor de la valoración de dichos servicios e información. En caso de que alguna categorización difiera de las propuestas en los siguientes apartados, se aplicarán los criterios específicos de aplicabilidad correspondientes a las categorías resultantes.

La aprobación de las valoraciones se realizará siguiendo el apartado 6.2.5, punto 2 de la Política de Seguridad de la Información de la Administración Judicial Electrónica (en adelante, PSIAJE).

La valoración de las dimensiones de seguridad se realizará siguiendo el siguiente procedimiento:

- Se valorarán conjuntamente las 5 dimensiones de seguridad CITAD (Confidencialidad [C], Integridad [I], Trazabilidad [T], Autenticidad [A] y Disponibilidad [D]), teniendo en cuenta que las cuatro primeras (CITA) hacen alusión a la información manejada y la última [D] a la disponibilidad del Servicio que da acceso a la información.
- En el caso de que un activo esencial no se vea afectado por alguna de las dimensiones, en el apartado de valoración se indicará: “No Aplica” [NA].

- Los criterios de valoración de las dimensiones de seguridad, y la asignación de sus niveles, se realizará conforme a lo descrito en la Guía CCN-STIC 803 de Valoración de Sistemas y la Guía de criterios de valoración de referencia de dimensiones de seguridad.

3.2.1 Servicios e información exclusivos del Ministerio de Justicia

3.2.1.1 Inventario de servicios e información exclusivos del Ministerio de Justicia

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
Servicios finalistas			
S01	GESTIÓN DE REGISTROS JUDICIALES Y REQUISITORIAS	Servicios que constituyen un sistema de información único de carácter no público, que permite la conexión entre los distintos registros del territorio Nacional facilitando el trabajo a Tribunales. Su objetivo fundamental es servir de apoyo a la actividad de los órganos judiciales, a la del Ministerio Fiscal, a las Fuerzas y Cuerpos de Seguridad del Estado y a la de otros órganos administrativos de acuerdo con sus competencias. Acceso a toda la documentación necesaria para que el órgano judicial, ante el que se presenta el requisitorio, pueda decidir sobre la situación personal de éste en los Registros de Violencia y medidas cautelares.	**Expediente judicial:** **- Datos de infracciones penales, condenas y medias cautelares.** **- Datos relativos a órdenes judiciales para la localización, detención o presentación de personas ante los tribunales.**
S02	GESTIÓN DE EXPEDIENTE ADMINISTRATIVOS Y GUBERNATIVOS (FISCALÍA)	El Servicio permite el registro y tramitación de Expedientes Gubernativos a todas las Fiscalías Territoriales, a las Fiscalías de órganos centrales, Fiscalía de la Audiencia Nacional y Antidroga y Fiscalía Anticorrupción, y a las diferentes Unidades de la Fiscalía General de Estado como son Secretaría Técnica y Unidad de Apoyo. Además, permite el intercambio electrónico de información entre las diferentes Fiscalías y Unidades de la FGE.	**Información relativa a expedientes gubernativos y/o administrativos.**
S03	CONSULTA DE DATOS DE ADN	Servicio con la base de datos para almacenar los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas.	**Datos de ADN.**
S04	GESTIÓN DE LABORATORIOS	Servicio para la gestión de la información de los laboratorios del Instituto Nacional de Toxicología y Ciencias Forenses que permite: - La gestión diaria de todos los análisis realizados por los distintos servicios del instituto, así como obtener datos estadísticos a través de su cuadro de mando. - El acceso controlado a la información, la realización de cálculos relacionados con las muestras, el uso de códigos de barras y la conexión con los instrumentos	**Expedientes forenses: pericias, informes, solicitudes, colaboraciones, interconsultas y análisis de laboratorio.**

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
		de laboratorio, así como el control de la cadena de custodia de las muestras recibidas.	
S05	OTORGAMIENTO DE APODERAMIENTOS JUDICIALES	El Servicio de otorgamiento de apoderamientos judiciales permite al ciudadano dar de alta apoderamientos de manera telemática. Además, el órgano judicial puede consultar estos apoderamientos.	**Expediente judicial: Datos poderdantes y apoderados.**

3.2.1.2 Valoración de información y servicios exclusivos del Ministerio de Justicia

Cod.	SERVICIO	Cod.	INFORMACION	Dimensiones ENS				
				[C]	[I]	[T]	[A]	[D]
S01	GESTIÓN DE REGISTROS JUDICIALES Y REQUISITORIAS	I01	**Expediente judicial:** **- Datos de infracciones penales, condenas y medias cautelares.** **- Datos relativos a órdenes judiciales para la localización, detención o presentación de personas ante los tribunales.**	[A]	[A]	[A]	[A]	[A]
S02	GESTIÓN DE EXPEDIENTE ADMINISTRATIVOS Y GUBERNATIVOS (FISCALÍA)	I02	**Información relativa a expedientes gubernativos y/o administrativos.**	[A]	[A]	[A]	[A]	[M]
S03	CONSULTA DE DATOS DE ADN	I03	**Datos usados en el Sistema de Índice combinado de ADN.**	[B]	[A]	[A]	[A]	[M]
S04	GESTIÓN DE LABORATORIOS	I04	**Expedientes forenses: pericias, informes, solicitudes, colaboraciones, interconsultas y análisis de laboratorio.**	[A]	[A]	[A]	[A]	[A]
S05	OTORGAMIENTO DE APODERAMIENTOS JUDICIALES	I05	**Expediente judicial: Datos poderdantes y apoderados.**	[B]	[M]	[M]	[M]	[M]

3.2.2 Servicios e información identificados para los servicios comunes

3.2.2.1 Inventario de servicios e información para los servicios comunes

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
Servicios finalistas			

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
S01	REGISTRO DE ASUNTOS	Servicio que facilita los registros de expedientes judiciales en todo tipo de jurisdicciones e instancias: - Registro electrónico de causas y procedimientos. - Registros de escritos de trámite. - Registros de partes de lesiones. - Registros de atestados. - Registro de dictámenes. - Acuses de recibo. - Otros escritos que se puedan presentar con destino órganos judiciales. .	**Expediente judicial:** **- Datos de víctimas** **- Datos preprocesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación.** **- Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos.** **- Información de los procedimientos de cualquier orden, incluido el orden penal, con datos de víctimas, menores, secretos de sumario, etc.**
S02	TRAMITACIÓN DE EXPEDIENTES JUDICIALES	Servicio que facilita la gestión digital integral de expedientes judiciales en todo tipo de jurisdicciones e instancias del ordenamiento jurídico español.	**Expediente judicial:** **- Datos de víctimas** **- Datos procesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación.** **- Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos.** **- Información de los procedimientos de cualquier orden, incluido el orden penal, con datos de víctimas, menores, secretos de sumario, etc.**
S03	GESTIÓN DE ACTOS DE COMUNICACIÓN ELECTRÓNICA	Los principales servicios que ofrece a sus usuarios son: - Notificaciones de los órganos judiciales a los operadores jurídicos. - Presentación de escritos iniciadores de demanda de los operadores jurídicos en los órganos judiciales. - Presentación de escritos de inicio de ejecución de los operadores jurídicos en los órganos judiciales. - Presentación de atestados de las Fuerzas y Cuerpos de Seguridad de Estado en los órganos judiciales. - Presentación de partes de lesión de los centros hospitalarios en los órganos judiciales. ...	**Expediente judicial:** **- Datos de víctimas** **- Datos pre- y procesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación.** **- Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos.**
S04	GESTIÓN DE AGENDA	Servicio destinado a los Partidos Judiciales con un número importante de salas de vistas. Este servicio facilita la gestión de los señalamientos que realizan los Tribunales en las salas de vistas.	**Expediente judicial:** **- Datos de las personas intervinientes en las vistas.**
S05	GESTIÓN DE GRABACIONES AUDIOVISUALES	Servicio de grabación de vistas, declaraciones y otros actos de interés procesal, de forma que se levanta acta sin necesitad de asistencia física del Letrado de Administración de Justicia de la sala.	**Expediente judicial:** **- Grabaciones de las vistas, declaraciones…(datos identificativos, imagen, voz)**
S06	DIGITALIZACIÓN Y CATALOGACIÓN	El servicio permite al usuario: - La digitalización de los escritos registrados. - La catalogación documental.	**Expediente judicial:** **- Datos de víctimas** **- Datos procesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación.** **- Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos.** **- Información de los procedimientos de cualquier orden, incluido el orden penal,**

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
			con datos de víctimas, menores, secretos de sumario, etc.
S07	TRAMITACIÓN DE EXPEDIENTES FISCALES	Servicio de expediente electrónico para las Fiscalías.	Expediente fiscal: - Datos procesales de todos los órdenes en los que interviene la Fiscalía. - Datos de víctimas.
S08	TRAMITACIÓN DE EXPEDIENTES FACULTATIVOS	Servicio para la gestión de expedientes electrónicos para los Institutos de Medicina Legal.	Datos jurisdiccionales de los expedientes del IML.
S09	ACCESO AL EXPEDIENTE	Este servicio permite a la ciudadanía y a los profesionales de justicia acceder a expedientes en los que se encuentren incursos. Permite a las partes solicitar, al órgano judicial correspondiente, el acceso al expediente judicial electrónico, de manera íntegramente telemática.	Expediente judicial: - Datos de víctimas. - Datos procesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación. - Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos. - Información de los procedimientos de cualquier orden, incluido el orden penal, con datos de víctimas, menores, secretos de sumario, etc.
S10	PRESENTACIÓN DE ESCRITOS Y RECEPCIÓN DE NOTIFICACIONES	El Servicio de Presentación de escritos permite a cualquier persona física o jurídica realizar la presentación telemática de escritos (iniciadores, de trámite, o iniciadores de ejecución) dirigidos a los órganos de la Administración. Además, cualquier persona física o jurídica recibir, por vía electrónica, las notificaciones de la Administración de Justicia.	Expediente judicial: - Datos de víctimas. - Datos procesales: Nombre y apellidos, documento de identidad, teléfono y/o correo electrónico y/o postal, nacionalidad, edad, parentesco filiación. - Categorías especiales de datos: aquellos que, en su caso, pudieran derivarse de los propios expedientes o procedimientos. - Información de los procedimientos de cualquier orden, incluido el orden penal, con datos de víctimas, menores, secretos de sumario, etc.

3.2.2.2 Valoración de información y servicios para los servicios comunes

Cod.	SERVICIO	Cod.	INFORMACION	Dimensiones ENS				
				[C]	[I]	[T]	[A]	[D]
S01	REGISTRO DE ASUNTOS	I01	Expediente judicial	[A]	[A]	[A]	[A]	[A]
S02	TRAMITACIÓN DE EXPEDIENTES JUDICIALES	I02	Expediente judicial	[A]	[A]	[A]	[A]	[A]

S03	GESTIÓN DE ACTOS DE COMUNICACIÓN ELECTRÓNICA	I03	Expediente judicial	[A]	[A]	[A]	[A]	[A]
S04	GESTIÓN DE AGENDA	I04	Expediente judicial: - Datos de las personas intervinientes en las vistas.	[A]	[A]	[A]	[A]	[A]
S05	GESTIÓN DE GRABACIONES AUDIOVISUALES	I05	Expediente judicial: - Grabaciones de las vistas, declaraciones…(datos identificativos, imagen, voz)	[A]	[A]	[A]	[A]	[A]
S06	DIGITALIZACIÓN Y CATALOGACIÓN	I06	Expediente judicial	[A]	[A]	[A]	[A]	[A]
S07	TRAMITACIÓN DE EXPEDIENTES FISCALES	I07	Expediente fiscal	[A]	[A]	[A]	[A]	[A]
S08	TRAMITACIÓN DE EXPEDIENTES FACULTATIVOS	I08	Datos jurisdiccionales de los expedientes del IML	[A]	[A]	[A]	[A]	[M]
S09	ACCESO AL EXPEDIENTE	I09	Expediente judicial	[A]	[A]	[A]	[A]	[A]
S10	PRESENTACIÓN DE ESCRITOS Y RECEPCIÓN DE NOTIFICACIONES	I10	Expediente judicial	[A]	[A]	[A]	[A]	[A]

3.2.3 Servicios e información del Consejo General del Poder Judicial (CGPJ)

3.2.3.1 Inventario de servicios e información para el Consejo General del Poder Judicial (CGPJ)

COD	SERVICIO ALCANCE PCE	Descripción del servicio	INFORMACIÓN IDENTIFICADA
Servicios finalistas			
S01	CONSULTA ENTIDADES	Consultas a entidades externas acordadas en el procedimiento judicial	Consultas a organismos públicos y privados al amparo de una resolución judicial para obtención de datos y documentos.
S02	INTEROPERABILIDAD EJE	Servicios de intercambio de datos y documentos del EJE entre órganos Judiciales, Ministerio Fiscal y otros organismos	Información en la plataforma de interoperabilidad del CGPJ para la realización de exhortos y comunicaciones seguras intra AJU y AJU con AGE.
S03	EJECUCIÓN DE EMBARGOS	Ejecución de los embargos ordenados por los órganos judiciales	Intercambios entre CGPJ / Entidades Financieras / MJU (Cuentas de Depósitos y Consignación Judicial).

3.2.3.2 Valoración de información y servicios exclusivos del Consejo General del Poder Judicial (CGPJ)

Cod.	SERVICIO	Cod.	INFORMACION	Dimensiones ENS				
				[C]	[I]	[T]	[A]	[D]
S01	CONSULTA ENTIDADES	I01	Consultas a organismos públicos y privados al amparo de una resolución judicial para obtención de datos y documentos.	[M]	[M]	[M]	[M]	[B]
S02	INTEROPERABILIDAD EJE	I02	Información la plataforma de interoperabilidad del CGPJ para la realización de exhortos y comunicaciones seguras intra AJU y AJU con AGE.	[M]	[A]	[M]	[A]	[B]
S03	EJECUCIÓN DE EMBARGOS	I03	Intercambios entre CGPJ / Entidades Financieras / MJU (Cuentas de Depósitos y Consignación Judicial) .	[M]	[M]	[M]	[M]	[B]

4. DOCUMENTOS DE APOYO A LA VALORACIÓN DE SERVICIOS E INFORMACIÓN

Para apoyar en la categorización de los servicios y sistemas de información el presente PCE incluye dos anexos en formato Excel que podrán ser utilizados por las organizaciones que se encuentren dentro del ámbito de aplicación del presente PCE. Estos anexos de apoyo son meramente orientativos y su uso es voluntario por parte de las organizaciones que se encuentre dentro del ámbito de aplicación de este PCE, además, están confeccionadas únicamente para la ayuda a la valoración de los activos (servicios e información) propios de la Administración de Justicia, proponiendo una categorización del sistema.

4.1 Instrucciones para cumplimentar los cuestionarios

4.1.1 Instrucciones generales

Para la orientación en la realización de las valoraciones de los sistemas de información de la Administración de Justicia, los responsables de la información y los responsables de los servicios podrán que establecer la valoración respondiendo a una serie de preguntas del cuestionario. En la primera parte del cuestionario se tratan las dimensiones de seguridad relacionadas con la información y en la parte final, denominada, cuestionario relativo al análisis de impacto (disponibilidad), se establecen las preguntas dirigidas al responsable del servicio. Los campos que cumplimentar por el usuario son los siguientes:

- Nombre del sistema de información.
- Respuesta a cada una de las situaciones planteadas (elección simple).

4.1.2 Cabecera del cuestionario

En primer lugar, se tiene que rellenar la cabecera del cuestionario en la que se indicará el nombre del sistema de información.

La celda "CATEGORÍA DEL SI" servirá de indicador para conocer si hemos completado el cuestionario en su totalidad.

Si quedasen preguntas por contestar, la celda mostrará el mensaje de error, debiendo revisarse qué preguntas se han quedado sin contestar.

Por el contrario, en caso de haber completado el cuestionario correctamente, la celda mostrará la categoría del sistema de acuerdo con las valoraciones finales orientativas calculadas en base a las respuestas marcadas en el cuestionario.

4.1.3 Cuestionario relativo a la categorización de los sistemas de información

A continuación, se pasará a valorar cada una de las dimensiones de seguridad del sistema de información, respondiendo a las preguntas planteadas. Para cada dimensión de la información se exponen una o varias situaciones a las que habrá que responder según los efectos que se produjesen si se llegase a materializar o, al menos, los que más se ajustarían a la realidad. Los efectos provocados se agrupan en temáticas de diversa índole. El método de respuesta es el de selección simple, de manera que solo se permitirá una respuesta para cada una de las situaciones. El usuario deberá elegir la respuesta que mejor se ajuste a la pregunta planteada.

Por último, se debe rellenar el cuestionario relativo al Análisis de Impacto (disponibilidad), que pretende orientar en la evaluación de los efectos que supondría para la continuidad de las operaciones de la organización un incidente que afectase a la disponibilidad del sistema de información. Para ello, se han dispuesto diversas preguntas con selección simple de respuesta, por lo que el usuario deberá seleccionar únicamente una de las opciones, la que más se ajuste a la realidad del sistema de información a evaluar.

4.1.4 Finalización y cuestionario para valoraciones final de ALTO

Una vez respondidas todas las preguntas, se recomienda volver al inicio del cuestionario. En caso de que el cuestionario se haya contestado correctamente, la casilla de "Categoría del SI" indicará la propuesta de categoría resultante de la valoración en función de las respuestas aportadas.

Si apareciese el mensaje "Aún quedan preguntas por contestar", será necesario que se revise el cuestionario, pues significa que hay preguntas que no han sido contestadas. En el supuesto en el cual el resultado final de la valoración sea ALTO, será necesario completar el segundo cuestionario "Cuestionario de valoración ALTO" con el objetivo de corroborar que esta valoración es la adecuada.

5. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad es el conjunto de medidas que son de aplicación para el cumplimiento del ENS. El conjunto de medidas dependerá de los niveles asociados a las dimensiones de seguridad.

Se ha determinado que, para garantizar la seguridad en los sistemas a los que hace referencia este Perfil de Cumplimiento Especifico, la relación de medidas que son de aplicación y la exigencia en el nivel de seguridad de cada medida aplicada, es la que se indica en la siguiente tabla. El "*" indica que disponen de criterios específicos de aplicación, los cuales se detallan en el apartado "6. CRITERIOS DE APLICACIÓN DE MEDIDAS".

5.1 Declaración de aplicabilidad Ministerio de Justicia

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicabilidad	Ref
Categoría	aplica	aplica	Aplica	org.1	BÁSICA	
Categoría	aplica	aplica	Aplica	org.2	BÁSICA	
Categoría	aplica	aplica	Aplica	org.3	BÁSICA	
Categoría	aplica	aplica	Aplica	org.4	BÁSICA*	**6.1.1**
Categoría	aplica	+ R1	+ R2	op.pl.1	ALTA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	ALTA	
Categoría	aplica	aplica	Aplica	op.pl.3	BÁSICA*	**6.1.2**
D	aplica	+ R1	+ R1	op.pl.4	MEDIA	
Categoría	n.a.	aplica	Aplica	op.pl.5	MEDIA	
T A	aplica	+ R1	+ R1	op.acc.1	MEDIA*	**6.1.3**
C I T A	aplica	aplica	+ R1	op.acc.2	ALTA	
C I T A	n.a.	aplica	+ R1	op.acc.3	ALTA	
C I T A	aplica	aplica	Aplica	op.acc.4	BAJO	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	MEDIA*	**6.1.4**
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	ALTA*	**6.1.5**
Categoría	aplica	aplica	Aplica	op.exp.1	BÁSICA	
Categoría	aplica	aplica	Aplica	op.exp.2	BÁSICA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	ALTA	
Categoría	n.a.	aplica	+ R1	op.exp.5	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	ALTA	
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	ALTA*	**6.1.6**
Categoría	aplica	aplica	Aplica	op.exp.9	BÁSICA	

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicabilidad	Ref
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.1	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.2	MEDIA	
Categoría	n.a.	n.a.	Aplica	op.ext.3	ALTA	
Categoría	n.a.	aplica	+ R1	op.ext.4	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	ALTA	
D	n.a.	aplica	Aplica	op.cont.1	MEDIA	
D	n.a.	n.a.	Aplica	op.cont.2	ALTA	
D	n.a.	n.a.	Aplica	op.cont.3	ALTA	
D	n.a.	n.a.	Aplica	op.cont.4	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	ALTA	
Categoría	aplica	aplica	Aplica	mp.if.1	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.2	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.3	BÁSICA	
D	aplica	+ R1	+ R1	mp.if.4	MEDIA	
D	aplica	aplica	Aplica	mp.if.5	BÁSICA	
D	n.a.	aplica	Aplica	mp.if.6	MEDIA*	**6.1.7**
Categoría	aplica	aplica	Aplica	mp.if.7	BÁSICA	
Categoría	n.a.	aplica	Aplica	mp.per.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.per.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.per.3	BÁSICA*	**6.1.8**
Categoría	aplica	aplica	Aplica	mp.per.4	BÁSICA*	**6.1.9**
Categoría	aplica	+ R1	+ R1	mp.eq.1	MEDIA	
A	n.a.	aplica	+ R1	mp.eq.2	ALTA	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	ALTA	
C	aplica	+ R1	+ R1	mp.eq.4	MEDIA	
Categoría	aplica	aplica	Aplica	mp.com.1	BÁSICA	
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	ALTA	
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	ALTA	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	ALTA	
C	n.a.	aplica	Aplica	mp.si.1	MEDIA	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	ALTA	
Categoría	aplica	aplica	Aplica	mp.si.3	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.si.4	BÁSICA	
C	aplica	+ R1	+ R1	mp.si.5	MEDIA*	**6.1.10**
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.sw.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.info.1	BÁSICA	
C	n.a.	aplica	Aplica	mp.info.2	MEDIA*	**6.1.11**
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	ALTA*	

Dimensiones						
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicabilidad	Ref
						6.1.12
T	n.a.	n.a.	Aplica	mp.info.4	ALTA*	**6.1.13**
C	aplica	aplica	Aplica	mp.info.5	BAJO*	**6.1.14**
D	aplica	+ R1	+ R1 + R2	mp.info.6	ALTA	
Categoría	aplica	aplica	Aplica	mp.s.1	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	ALTA	
Categoría	aplica	aplica	+ R1	mp.s.3	ALTA	
D	n.a.	aplica	+ R1	mp.s.4	ALTA	

5.1.1 Medidas de aplicación

De las 73 medidas de seguridad definidas en el Anexo II del RD 311/2022, **aplican un total de 73*[1] medidas.**

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (33):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento/ gestión de la capacidad

[op.pl.5] Componentes certificados

[op.acc] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

[1] De estas 73 medidas, 31 aplican en categoría ALTA, 22 en categoría BÁSICA/BAJO y 20 en categoría MEDIA.

[op.acc.5] Mecanismo de autenticación (usuarios externos)
[op.acc.6] Mecanismo de autenticación (usuarios de la organización)
[op.exp] Explotación
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.3] Gestión de la configuración de seguridad
[op.exp.4] Mantenimiento y actualizaciones de seguridad
[op.exp.5] Gestión de cambios
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad
[op.exp.9] Registro de la gestión de incidentes
[op.exp.10] Protección de claves criptográficas
[op.ext] Recursos externos
[op.ext.1] Contratación y acuerdos de nivel de servicio
[op.ext.2] Gestión diaria
[op.ext.3] Protección de la cadena de suministro
[op.ext.4] Interconexión de sistemas
[op.nub] Servicios en la nube
[op.nub.1] Protección de servicios en la nube
[op.cont] Continuidad del servicio
[op.cont.1] Análisis de impacto
[op.cont.2] Plan de continuidad
[op.cont.3] Pruebas periódicas
[op.cont.4] Medios alternativos
[op.mon] Monitorización del sistema
[op.mon.1] Monitorización
[op.mon.2] Sistema de métricas
[op.mon.3] Vigilancia

Medidas de Protección (36):

[mp.if] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y control de acceso

[mp.if.2] Identificación de las personas
[mp.if.3] Acondicionamiento de los locales
[mp.if.4] Energía eléctrica
[mp.if.5] Protección frente a incendios
[mp.if.6] Protección frente a inundaciones
[mp.if.7] Registro de entrada y salida de equipamiento
[mp.per] Gestión del personal
[mp.per.1] Caracterización del puesto de trabajo
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de dispositivos portátiles
[mp.eq.4] Otros dispositivos conectados a la red.
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la integridad y de la autenticidad
[mp.si] Protección de los soportes de información
[mp.si.1] Marcado de soportes
[mp.si.2] Criptografía
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.2] Calificación de la información
[mp.info.3] Firma electrónica
[mp.info.4] Sellos de tiempo
[mp.info.5] Limpieza de documentos

[mp.info.6] Copias de seguridad (backup)

[mp.s] Protección de los servicios

[mp.s.1] Protección del correo electrónico

[mp.s.2] Protección de los servicios y aplicaciones web

[mp.s.3] Protección de la navegación web

[mp.s.4] Protección frente a denegación de servicio

5.2 Declaración de aplicabilidad Servicios Comunes

Dimensiones						
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicabilidad	Ref
Categoría	aplica	aplica	Aplica	org.1	BÁSICA	
Categoría	aplica	aplica	Aplica	org.2	BÁSICA	
Categoría	aplica	aplica	Aplica	org.3	BÁSICA	
Categoría	aplica	aplica	Aplica	org.4	BÁSICA*	**6.2.1**
Categoría	aplica	+ R1	+ R2	op.pl.1	MEDIA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	MEDIA	
Categoría	aplica	aplica	Aplica	op.pl.3	BÁSICA*	**6.2.2**
D	aplica	+ R1	+ R1	op.pl.4	MEDIA	
Categoría	n.a.	aplica	Aplica	op.pl.5	MEDIA	
T A	aplica	+ R1	+ R1	op.acc.1	MEDIA*	**6.2.3**
C I T A	aplica	aplica	+ R1	op.acc.2	ALTA	
C I T A	n.a.	aplica	+ R1	op.acc.3	ALTA	
C I T A	aplica	aplica	Aplica	op.acc.4	BAJO	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	MEDIA*	**6.2.4**
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	ALTA*	**6.2.5**
Categoría	aplica	aplica	Aplica	op.exp.1	BÁSICA	
Categoría	aplica	aplica	Aplica	op.exp.2	BÁSICA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	ALTA	
Categoría	n.a.	aplica	+ R1	op.exp.5	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIA	
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	ALTA*	**6.2.6**
Categoría	aplica	aplica	Aplica	op.exp.9	BÁSICA	
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.1	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.2	MEDIA	
Categoría	n.a.	n.a.	Aplica	op.ext.3	ALTA	

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicabilidad	Ref
Categoría	n.a.	aplica	+ R1	op.ext.4	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	ALTA	
D	n.a.	aplica	Aplica	op.cont.1	MEDIA	
D	n.a.	n.a.	Aplica	op.cont.2	ALTA	
D	n.a.	n.a.	Aplica	op.cont.3	ALTA	
D	n.a.	n.a.	Aplica	op.cont.4	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	MEDIA	
Categoría	aplica	aplica	Aplica	mp.if.1	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.2	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.3	BÁSICA	
D	aplica	+ R1	+ R1	mp.if.4	MEDIA	
D	aplica	aplica	Aplica	mp.if.5	BÁSICA	
D	n.a.	aplica	Aplica	mp.if.6	MEDIA*	**6.2.7**
Categoría	aplica	aplica	Aplica	mp.if.7	BÁSICA	
Categoría	n.a.	aplica	Aplica	mp.per.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.per.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.per.3	BÁSICA*	**6.2.8**
Categoría	aplica	aplica	Aplica	mp.per.4	BÁSICA*	**6.2.9**
Categoría	aplica	+ R1	+ R1	mp.eq.1	MEDIA	
A	n.a.	aplica	+ R1	mp.eq.2	ALTA	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	ALTA	
C	aplica	+ R1	+ R1	mp.eq.4	MEDIA	
Categoría	aplica	aplica	Aplica	mp.com.1	BÁSICA	
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	ALTA	
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	ALTA	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	ALTA	
C	n.a.	aplica	Aplica	mp.si.1	MEDIA	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	ALTA	
Categoría	aplica	aplica	Aplica	mp.si.3	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.si.4	BÁSICA	
C	aplica	+ R1	+ R1	mp.si.5	MEDIA*	**6.2.10**
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.sw.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.info.1	BÁSICA	
C	n.a.	aplica	Aplica	mp.info.2	MEDIA*	**6.2.11**
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	ALTA*	**6.2.12**
T	n.a.	n.a.	Aplica	mp.info.4	ALTA*	**6.2.13**
C	aplica	aplica	Aplica	mp.info.5	BAJO*	**6.2.14**
D	aplica	+ R1	+ R1 + R2	mp.info.6	ALTA	
Categoría	aplica	aplica	Aplica	mp.s.1	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	MEDIA	

Dimensiones						
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicabilidad	Ref
Categoría	aplica	aplica	+ R1	mp.s.3	ALTA	
D	n.a.	aplica	+ R1	mp.s.4	ALTA	

5.2.1 Medidas de aplicación

De las 73 medidas de seguridad definidas en el Anexo II del RD 311/2022, **aplican un total de 73*[2] medidas.**

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (33):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento/ gestión de la capacidad

[op.pl.5] Componentes certificados

[op.acc] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

[op.acc.5] Mecanismo de autenticación (usuarios externos)

[op.acc.6] Mecanismo de autenticación (usuarios de la organización)

[op.exp] Explotación

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de seguridad

[op.exp.3] Gestión de la configuración de seguridad

[2] De estas 73 medidas, 25 aplican en categoría ALTA, 22 en categoría BÁSICA/BAJO y 26 en categoría MEDIA.

[op.exp.4] Mantenimiento y actualizaciones de seguridad
[op.exp.5] Gestión de cambios
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad
[op.exp.9] Registro de la gestión de incidentes
[op.exp.10] Protección de claves criptográficas
[op.ext] Recursos externos
[op.ext.1] Contratación y acuerdos de nivel de servicio
[op.ext.2] Gestión diaria
[op.ext.3] Protección de la cadena de suministro
[op.ext.4] Interconexión de sistemas
[op.nub] Servicios en la nube
[op.nub.1] Protección de servicios en la nube
[op.cont] Continuidad del servicio
[op.cont.1] Análisis de impacto
[op.cont.2] Plan de continuidad
[op.cont.3] Pruebas periódicas
[op.cont.4] Medios alternativos
[op.mon] Monitorización del sistema
[op.mon.1] Monitorización
[op.mon.2] Sistema de métricas
[op.mon.3] Vigilancia

Medidas de Protección (36):

[mp.if] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y control de acceso
[mp.if.2] Identificación de las personas
[mp.if.3] Acondicionamiento de los locales
[mp.if.4] Energía eléctrica
[mp.if.5] Protección frente a incendios
[mp.if.6] Protección frente a inundaciones
[mp.if.7] Registro de entrada y salida de equipamiento

[mp.per] Gestión del personal
[mp.per.1] Caracterización del puesto de trabajo
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de dispositivos portátiles
[mp.eq.4] Otros dispositivos conectados a la red.
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la integridad y de la autenticidad
[mp.si] Protección de los soportes de información
[mp.si.1] Marcado de soportes
[mp.si.2] Criptografía
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.2] Calificación de la información
[mp.info.3] Firma electrónica
[mp.info.4] Sellos de tiempo
[mp.info.5] Limpieza de documentos
[mp.info.6] Copias de seguridad (backup)
[mp.s] Protección de los servicios
[mp.s.1] Protección del correo electrónico
[mp.s.2] Protección de los servicios y aplicaciones web
[mp.s.3] Protección de la navegación web
[mp.s.4] Protección frente a denegación de servicio

5.3 Declaración de aplicabilidad Consejo General del Poder Judicial

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicabilidad	Ref
Categoría	aplica	aplica	Aplica	org.1	BÁSICA	
Categoría	aplica	aplica	Aplica	org.2	BÁSICA	
Categoría	aplica	aplica	Aplica	org.3	BÁSICA	
Categoría	aplica	aplica	Aplica	org.4	BÁSICA*	**6.3.1**
Categoría	aplica	+ R1	+ R2	op.pl.1	ALTA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	ALTA	
Categoría	aplica	aplica	Aplica	op.pl.3	BÁSICA*	**6.3.2**
D	aplica	+ R1	+ R1	op.pl.4	BAJO	
Categoría	n.a.	aplica	Aplica	op.pl.5	MEDIA	
T A	aplica	+ R1	+ R1	op.acc.1	MEDIA*	**6.3.3**
C I T A	aplica	aplica	+ R1	op.acc.2	ALTA	
C I T A	n.a.	aplica	+ R1	op.acc.3	ALTA	
C I T A	aplica	aplica	Aplica	op.acc.4	BAJO	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	MEDIA*	**6.3.4**
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	MEDIA*	**6.3.5**
Categoría	aplica	aplica	Aplica	op.exp.1	BÁSICA	
Categoría	aplica	aplica	Aplica	op.exp.2	BÁSICA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	ALTA	
Categoría	n.a.	aplica	+ R1	op.exp.5	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	MEDIA (+R4)*	**6.3.6**
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIA	
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	MEDIA*	**6.3.7**
Categoría	aplica	aplica	Aplica	op.exp.9	BÁSICA	
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.1	MEDIA	
Categoría	n.a.	aplica	Aplica	op.ext.2	MEDIA	
Categoría	n.a.	n.a.	Aplica	op.ext.3	N/A	
Categoría	n.a.	aplica	+ R1	op.ext.4	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	ALTA	
D	n.a.	aplica	Aplica	op.cont.1	N/A	
D	n.a.	n.a.	Aplica	op.cont.2	(N/A)*	**6.3.8**
D	n.a.	n.a.	Aplica	op.cont.3	N/A	
D	n.a.	n.a.	Aplica	op.cont.4	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	MEDIA	

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicabilidad	Ref
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	ALTA	
Categoría	aplica	aplica	Aplica	mp.if.1	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.2	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.if.3	BÁSICA	
D	aplica	+ R1	+ R1	mp.if.4	BÁSICA	
D	aplica	aplica	Aplica	mp.if.5	BÁSICA	
D	n.a.	aplica	Aplica	mp.if.6	MEDIA*	**6.3.9**
Categoría	aplica	aplica	Aplica	mp.if.7	BÁSICA	
Categoría	n.a.	aplica	Aplica	mp.per.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.per.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.per.3	BÁSICA*	**6.3.10**
Categoría	aplica	aplica	Aplica	mp.per.4	BÁSICA	**6.3.11**
Categoría	aplica	+ R1	+ R1	mp.eq.1	MEDIA	
A	n.a.	aplica	+ R1	mp.eq.2	ALTA	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	ALTA	
C	aplica	+ R1	+ R1	mp.eq.4	MEDIA	
Categoría	aplica	aplica	Aplica	mp.com.1	BÁSICA	
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	MEDIA	
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	MEDIA (+R4) *	**6.3.12**
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	MEDIA	
C	n.a.	aplica	Aplica	mp.si.1	MEDIA	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	ALTA	
Categoría	aplica	aplica	Aplica	mp.si.3	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.si.4	BÁSICA	
C	aplica	+ R1	+ R1	mp.si.5	MEDIA*	**6.3.13**
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.sw.2	MEDIA	
Categoría	aplica	aplica	Aplica	mp.info.1	BÁSICA	
C	n.a.	aplica	Aplica	mp.info.2	MEDIA*	**6.3.14**
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	ALTA*	**6.3.15**
T	n.a.	n.a.	Aplica	mp.info.4	ALTA*	**6.3.16**
C	aplica	aplica	Aplica	mp.info.5	BAJO*	**6.3.17**
D	aplica	+ R1	+ R1 + R2	mp.info.6	BAJO	
Categoría	aplica	aplica	Aplica	mp.s.1	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	ALTA	
Categoría	aplica	aplica	+ R1	mp.s.3	BÁSICA	
D	n.a.	aplica	+ R1	mp.s.4	N/A	

5.4 Medidas de aplicación

De las 73 medidas de seguridad definidas en el Anexo II del RD 311/2022, **aplican un total de 67*[3] medidas.**

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (28):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento/ gestión de la capacidad

[op.pl.5] Componentes certificados

[op.acc] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

[op.acc.5] Mecanismo de autenticación (usuarios externos)

[op.acc.6] Mecanismo de autenticación (usuarios de la organización)

[op.exp] Explotación

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de seguridad

[op.exp.3] Gestión de la configuración de seguridad

[op.exp.4] Mantenimiento y actualizaciones de seguridad

[op.exp.5] Gestión de cambios

[op.exp.6] Protección frente a código dañino

[op.exp.7] Gestión de incidentes

[3] De estas 67 medidas, 16 aplican en categoría ALTA, 26 en categoría BÁSICA/BAJO y 25 en categoría MEDIA.

[op.exp.8] Registro de la actividad

[op.exp.9] Registro de la gestión de incidentes

[op.exp.10] Protección de claves criptográficas

[op.ext] Recursos externos

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

[op.ext.4] Interconexión de sistemas

[op.nub] Servicios en la nube

[op.nub.1] Protección de servicios en la nube

[op.mon] Monitorización del sistema

[op.mon.1] Monitorización

[op.mon.2] Sistema de métricas

[op.mon.3] Vigilancia

Medidas de Protección (35):

[mp.if] Protección de las instalaciones e infraestructuras

[mp.if.1] Áreas separadas y control de acceso

[mp.if.2] Identificación de las personas

[mp.if.3] Acondicionamiento de los locales

[mp.if.4] Energía eléctrica

[mp.if.5] Protección frente a incendios

[mp.if.6] Protección frente a inundaciones

[mp.if.7] Registro de entrada y salida de equipamiento

[mp.per] Gestión del personal

[mp.per.1] Caracterización del puesto de trabajo

[mp.per.2] Deberes y obligaciones

[mp.per.3] Concienciación

[mp.per.4] Formación

[mp.eq] Protección de los equipos

[mp.eq.1] Puesto de trabajo despejado

[mp.eq.2] Bloqueo de puesto de trabajo

[mp.eq.3] Protección de dispositivos portátiles

[mp.eq.4] Otros dispositivos conectados a la red.

[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la integridad y de la autenticidad
[mp.si] Protección de los soportes de información
[mp.si.1] Marcado de soportes
[mp.si.2] Criptografía
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.2] Calificación de la información
[mp.info.3] Firma electrónica
[mp.info.4] Sellos de tiempo
[mp.info.5] Limpieza de documentos
[mp.info.6] Copias de seguridad (backup)
[mp.s] Protección de los servicios
[mp.s.1] Protección del correo electrónico
[mp.s.2] Protección de los servicios y aplicaciones web
[mp.s.3] Protección de la navegación web

6. CRITERIOS DE APLICACIÓN DE MEDIDAS

6.1 Criterios de aplicación de medidas para Ministerio de Justicia

6.1.1 [org.4] Proceso de autorización

Se creará para cada proceso una matriz de roles y responsabilidades que delimiten las responsabilidades para cada actuación. Se deberán tener en cuenta los requisitos establecidos en el control de **Segregación de funciones y tareas [op.acc.3].**

6.1.2 [op.pl.3] Adquisición de nuevos componentes

Los productos adquiridos deberán seguir un proceso formal de pruebas y compra.

6.1.3 [op.acc.1] Identificación

Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

6.1.4 [op.acc.5] Mecanismo de autenticación (usuarios externos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros, en aquello que difiera o sea contradictorio con el resto de los requisitos o refuerzos establecidos en el Anexo II del ENS.

6.1.5 [op.acc.6] Mecanismo de autenticación (usuarios internos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros, en aquello que difiera o sea contradictorio con el resto de los requisitos o refuerzos establecidos en el Anexo II del ENS.

6.1.6 [op.exp.8] Registro de la actividad

Los sistemas de información y comunicación empleados por la Administración de Justicia deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros harán posible determinar la justificación, la fecha y la hora de tales operaciones, así como la persona que realiza la consulta o comunicación de los datos personales y la identidad de los destinatarios o destinatarias de dichos datos.

Se aplicarán a todo aquel o aquella que interactúe con el sistema, inclusive al personal en labores de administración, mantenimiento y soporte de los sistemas de información, o de inspección de los sistemas, así como a las actuaciones automatizadas y al personal de los centros de atención y soporte a usuarios y usuarias de las administraciones públicas.

El responsable del tratamiento determinará el plazo de retención de estos registros.

6.1.7 [mp.if.6] Protección frente a inundaciones

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Protección frente a inundaciones no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.1.8 [mp.per.3] Concienciación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de concienciación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.1.9 [mp.per.4] Formación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de formación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.1.10 [mp.si.5] Borrado y destrucción

Con pleno respeto a las normas procesales sobre conservación de la información, custodia de las actuaciones y expurgo de los archivos, se aplicará en su caso la medida de borrado y destrucción de soportes de información a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

a) Se destruirán de forma segura los soportes, en los siguientes casos:
   1. Cuando la naturaleza del soporte no permita un borrado seguro.
   2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.
b) Se llevará un registro de la destrucción de soportes con información confidencial, a efectos de auditoría.
c) Se procederá a retirar los soportes con autorización escrita expresa, manteniendo el registro actualizado (registro de salida).
d) La destrucción de los soportes se puede llevar a cabo mediante una empresa externa protegiendo su información a través de un acuerdo de confidencialidad. En tal caso, será obligatorio que dicha empresa realice un certificado de destrucción que garantice las obligaciones contractuales que ha adquirido.

6.1.11 [mp.info.2] Calificación de la información

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. Los procedimientos de calificación estarán también a lo que se

establezca en la política de gestión de documentos de cada entidad de la Administración de Justicia.

La calificación de la información formará parte de la política de gestión documental que se siga dentro de cada entidad de la Administración de Justicia, estando incluida en las primeras fases de dicha gestión, donde se estructurará la información en base a la finalidad de la misma.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Calificación de la Información no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.1.12 [mp.info.3] Firma electrónica

En el ámbito de la Administración de Justicia se emplearán los sistemas de firma, en los términos y condiciones establecidos en Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Se utilizarán los sistemas de firma que garanticen el nivel de seguridad de la actuación de conformidad con el artículo 20 del Real Decreto-ley 6/2023, de 19 de diciembre.

En caso de que la entidad adopte una categorización distinta de la propuesta, a partir de nivel MEDIO, cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad procesal o judicial que aquélla soporte. Una vez bajo la custodia del sistema de gestión procesal la firma electrónica se considerará válida indefinidamente sin ulteriores comprobaciones tecnológicas. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

6.1.13 [mp.info.4] Sellos de tiempo

Cuando se gestionen sellos de tiempo se comprobará su validez y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidos indefinidamente sin ulteriores comprobaciones tecnológicas.

6.1.14 [mp.info.5] Limpieza de documentos

En el proceso de limpieza de documentos, se retirará de los mismos, toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento y el emisor muestre su conformidad, siguiendo los procedimientos que

se establezcan en la política de gestión de documentos de cada entidad de la Administración de Justicia.

6.2 Criterios de aplicación de medidas para Servicios comunes

6.2.1 [org.4] Proceso de autorización

Se creará para cada proceso una matriz de roles y responsabilidades que delimiten las responsabilidades para cada actuación. Se deberán tener en cuenta los requisitos establecidos en el control de **Segregación de funciones y tareas [op.acc.3].**

6.2.2 [op.pl.3] Adquisición de nuevos componentes

Los productos adquiridos deberán seguir un proceso formal de pruebas y compra.

6.2.3 [op.acc.1] Identificación

Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

6.2.4 [op.acc.5] Mecanismo de autenticación (usuarios externos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros, en aquello que difiera o sea contradictorio con el resto de requisitos o refuerzos establecidos en el Anexo II del ENS.

6.2.5 [op.acc.6] Mecanismo de autenticación (usuarios internos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros, en aquello que difiera o sea contradictorio con el resto de los requisitos o refuerzos establecidos en el Anexo II del ENS.

6.2.6 [op.exp.8] Registro de la actividad

Los sistemas de información y comunicación empleados por la Administración de Justicia deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros harán posible determinar la justificación, la fecha y la hora de tales operaciones, así

como la persona que realiza la consulta o comunicación de los datos personales y la identidad de los destinatarios o destinatarias de dichos datos.

Se aplicarán a todo aquel o aquella que interactúe con el sistema, inclusive al personal en labores de administración, mantenimiento y soporte de los sistemas de información, o de inspección de los sistemas, así como a las actuaciones automatizadas y al personal de los centros de atención y soporte a usuarios y usuarias de las administraciones públicas.

El responsable del tratamiento determinará el plazo de retención de estos registros.

6.2.7 [mp.if.6] Protección frente a inundaciones

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Protección frente a inundaciones no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.2.8 [mp.per.3] Concienciación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de concienciación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.2.9 [mp.per.4] Formación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de formación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.2.10 [mp.si.5] Borrado y destrucción

Con pleno respeto a las normas procesales sobre conservación de la información, custodia de las actuaciones y expurgo de los archivos, se aplicará en su caso la medida de borrado y destrucción de soportes de información a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

e) Se destruirán de forma segura los soportes, en los siguientes casos:
   1. Cuando la naturaleza del soporte no permita un borrado seguro.

2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.

f) Se llevará un registro de la destrucción de soportes con información confidencial, a efectos de auditoría.

g) Se procederá a retirar los soportes con autorización escrita expresa, manteniendo el registro actualizado (registro de salida).

h) La destrucción de los soportes se puede llevar a cabo mediante una empresa externa protegiendo su información a través de un acuerdo de confidencialidad. En tal caso, será obligatorio que dicha empresa realice un certificado de destrucción que garantice las obligaciones contractuales que ha adquirido.

6.2.11 [mp.info.2] Calificación de la información

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. Los procedimientos de calificación estarán también a lo que se establezca en la política de gestión de documentos de cada entidad de la Administración de Justicia.

La calificación de la información formará parte de la política de gestión documental que se siga dentro de cada entidad de la Administración de Justicia, estando incluida en las primeras fases de dicha gestión, donde se estructurará la información en base a la finalidad de la misma.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Calificación de la Información no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.2.12 [mp.info.3] Firma electrónica

En el ámbito de la Administración de Justicia se emplearán los sistemas de firma, en los términos y condiciones establecidos en Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Se utilizarán los sistemas de firma que garanticen el nivel de seguridad de la actuación de conformidad con el artículo 20 del Real Decreto-ley 6/2023, de 19 de diciembre.

En caso de que la entidad adopte una categorización distinta de la propuesta, a partir de nivel MEDIO, cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad procesal o judicial que aquélla soporte. Una vez bajo la custodia del sistema de gestión procesal la firma electrónica se considerará válida indefinidamente sin ulteriores comprobaciones tecnológicas. Para tal fin se adjuntará a la firma, o se referenciará, toda la información

pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

6.2.13 [mp.info.4] Sellos de tiempo

Cuando se gestionen sellos de tiempo se comprobará su validez y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidos indefinidamente sin ulteriores comprobaciones tecnológicas.

6.2.14 [mp.info.5] Limpieza de documentos

En el proceso de limpieza de documentos, se retirará de los mismos, toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento y el emisor muestre su conformidad, siguiendo los procedimientos que se establezcan en la política de gestión de documentos de cada entidad de la Administración de Justicia.

6.3 Criterios de aplicación de medidas para el Consejo General del Poder Judicial

6.3.1 [org.4] Proceso de autorización

Se creará para cada proceso una matriz de roles y responsabilidades que delimiten las responsabilidades para cada actuación. Se deberán tener en cuenta los requisitos establecidos en el control de **Segregación de funciones y tareas [op.acc.3].**

6.3.2 [op.pl.3] Adquisición de nuevos componentes

Los productos adquiridos deberán seguir un proceso formal de pruebas y compra.

6.3.3 [op.acc.1] Identificación

Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

6.3.4 [op.acc.5] Mecanismo de autenticación (usuarios externos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares

Seguros, en aquello que difiera o sea contradictorio con el resto de requisitos o refuerzos establecidos en el Anexo II del ENS.

6.3.5 [op.acc.6] Mecanismo de autenticación (usuarios internos)

Se cumplirá en todo caso con lo establecido en la Guía Técnica de Interoperabilidad y Seguridad sobre Requisitos de Puntos de Acceso Seguro y Lugares Seguros, en aquello que difiera o sea contradictorio con el resto de los requisitos o refuerzos establecidos en el Anexo II del ENS.

6.3.6 [op.exp.6] Protección frente a código dañino

Se aplicarán los requisitos correspondientes a la categoría MEDIA añadiendo además el refuerzo R4, que implica tener capacidad de respuesta en caso de incidente. Para ello, se deberán utilizar herramientas de seguridad que permitan detectar, investigar y resolver actividades sospechosas tanto en los puestos de trabajo como en los servidores, como por ejemplo soluciones EDR (Endpoint Detection and Response).

6.3.7 [op.exp.8] Registro de la actividad

Los sistemas de información y comunicación empleados por la Administración de Justicia deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros harán posible determinar la justificación, la fecha y la hora de tales operaciones, así como la persona que realiza la consulta o comunicación de los datos personales y la identidad de los destinatarios o destinatarias de dichos datos.

Se aplicarán a todo aquel o aquella que interactúe con el sistema, inclusive al personal en labores de administración, mantenimiento y soporte de los sistemas de información, o de inspección de los sistemas, así como a las actuaciones automatizadas y al personal de los centros de atención y soporte a usuarios y usuarias de las administraciones públicas.

El responsable del tratamiento determinará el plazo de retención de estos registros.

6.3.8 [op.cont.2] Plan de continuidad

Aunque no sea de aplicación, es recomendable implementar mecanismos efectivos de continuidad que garanticen la disponibilidad y resiliencia de dichos servicios ante incidentes que puedan comprometer su operatividad.

6.3.9 [mp.if.6] Protección frente a inundaciones

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Protección frente a inundaciones no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.3.10 [mp.per.3] Concienciación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de concienciación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.3.11 [mp.per.4] Formación

Teniendo en cuenta que en el ENS esta medida es de obligado cumplimiento para todas las categorías, debe elaborarse un plan anual de formación que tendrá que materializarse. Las Instituciones y Administraciones prestacionales de medios personales y materiales de la Administración de Justicia realizarán las actividades derivadas de dicho plan en relación con el personal dependiente de cada una de ellas.

6.3.12 [mp.com.3] Protección de la integridad y de la autenticidad

Se aplicarán los requisitos correspondientes a la categoría MEDIA, añadiendo además el refuerzo R4, siendo necesario el empleo de productos certificados conforme a lo establecido en [op.pl.5].

6.3.13 [mp.si.5] Borrado y destrucción

Con pleno respeto a las normas procesales sobre conservación de la información, custodia de las actuaciones y expurgo de los archivos, se aplicará en su caso la medida de borrado y destrucción de soportes de información a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

i) Se destruirán de forma segura los soportes, en los siguientes casos:
   1. Cuando la naturaleza del soporte no permita un borrado seguro.
   2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.
j) Se llevará un registro de la destrucción de soportes con información confidencial, a efectos de auditoría.
k) Se procederá a retirar los soportes con autorización escrita expresa, manteniendo el registro actualizado (registro de salida).
l) La destrucción de los soportes se puede llevar a cabo mediante una empresa externa protegiendo su información a través de un acuerdo de confidencialidad. En tal caso, será obligatorio que dicha empresa realice un certificado de destrucción que garantice las obligaciones contractuales que ha adquirido.

6.3.14 [mp.info.2] Calificación de la información

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. Los procedimientos de calificación estarán también a lo que se establezca en la política de gestión de documentos de cada entidad de la Administración de Justicia.

La calificación de la información formará parte de la política de gestión documental que se siga dentro de cada entidad de la Administración de Justicia, estando incluida en las primeras fases de dicha gestión, donde se estructurará la información en base a la finalidad de la misma.

En caso de que la entidad adopte una categorización distinta de la propuesta y la medida de Calificación de la Información no fuera aplicable por estar prevista solo a partir de la categoría MEDIA, dicha medida deberá implementarse igualmente a fin de cumplir con los requisitos establecidos por el ESAJ.

6.3.15 [mp.info.3] Firma electrónica

En el ámbito de la Administración de Justicia se emplearán los sistemas de firma, en los términos y condiciones establecidos en Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Se utilizarán los sistemas de firma que garanticen el nivel de seguridad de la actuación de conformidad con el artículo 20 del Real Decreto-ley 6/2023, de 19 de diciembre.

En caso de que la entidad adopte una categorización distinta de la propuesta, a partir de nivel MEDIO, cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad procesal o judicial que aquélla soporte. Una vez bajo la custodia del sistema de gestión procesal la firma electrónica se considerará válida indefinidamente sin ulteriores comprobaciones tecnológicas. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

6.3.16 [mp.info.4] Sellos de tiempo

Cuando se gestionen sellos de tiempo se comprobará su validez y, una vez bajo la custodia del sistema de gestión procesal se considerarán válidos indefinidamente sin ulteriores comprobaciones tecnológicas.

6.3.17 [mp.info.5] Limpieza de documentos

En el proceso de limpieza de documentos, se retirará de los mismos, toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento y el emisor muestre su conformidad, siguiendo los procedimientos que se establezcan en la política de gestión de documentos de cada entidad de la Administración de Justicia.