Esquema de Seguridad de la Administración de Justicia

Ficha del Documento

NOMBRE DEL DOCUMENTO	Esquema de Seguridad de la Administración de Justicia
CÓDIGO DEL DOCUMENTO	CTEAJE-BIS-INF-MPJRC-ESAJ
VERSIÓN	2.00
CLASIFICACIÓN [1]	B

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
V 1.00		07/07/2015	Texto inicial aprobado por el Pleno del CTEAJE
V 1.01		27/06/2017	Versión actualizada debido a cambios legislativos
V 2.00	Oficina de Seguridad CTEAJE	26/02/2025	Versión actualizada debido a: -cambios legislativos derivados 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. -separación de los ámbitos de Interoperabilidad y Seguridad en documentos diferentes, autorizado por el Pleno del CTEAJE de 21 de noviembre de 2024. Versión aprobada en CP 26/02/2025

[1] Los niveles de clasificación son:

A: Rojo - Prioritario: Obligado cumplimiento y clasificado de carácter urgente.

B: Naranja - Necesario: Obligado cumplimiento aún no clasificado urgente.

C: Verde - Recomendación: Cumplimiento conveniente pero no obligado.

ÍNDICE

ÍNDICE 2

DISPOSICIONES GENERALES. 5

I. Del ámbito de aplicación y los principios generales 5

1. Objeto. 5

2. Ámbito de aplicación. 6

3. Mecanismos de control. 7

4. Declaración de Conformidad y Certificación. 7

DE LA SEGURIDAD ELECTRÓNICA DE LA ADMINISTRACIÓN DE JUSTICIA. PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL 8

I. Seguridad, protección de datos personales e inteligencia artificial 8

5. Seguridad electrónica de la Administración de Justicia. 8

6. Protección de datos personales. 8

7. Política de Seguridad y desarrollo normativo. 10

8. Inteligencia Artificial. 10

9. Entidades del sector privado. 10

10. Desarrollo de requisitos específicos. 11

II. Estado de seguridad de los sistemas 12

11. Informe del estado de la seguridad. 12

III. Respuesta a los incidentes de seguridad 13

12. Coordinación frente a incidentes de seguridad de la información. 13

13. Centro de Operaciones de Ciberseguridad. 13

ACTUALIZACIÓN, DESARROLLO Y FORMACIÓN 13

I. Desarrollo del Esquema de Seguridad de la Administración de Justicia 13

14. Actualización permanente. 13

15. Desarrollo. 14
16. Adecuación de sistemas, aplicaciones y servicios. 14
ANEXO. 15
1. TABLA DE MEDIDAS Y APLICACIÓN 15
2. CATEGORÍA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN 17
3. MEDIDAS ESPECÍFICAS DE JUSTICIA 17
3.1 [org.4] Proceso de autorización 17
3.2 [op.pl.3] Adquisición de nuevos componentes 18
3.3 [op.acc.1] Identificación 18
3.4 [op.acc.5] Mecanismo de autenticación (usuarios externos) 18
3.5 [op.acc.6] Mecanismo de autenticación (usuarios de la organización) 19
3.6 [op.exp.8] Registro de la actividad 19
3.7 [mp.if.6] Protección frente a inundaciones 20
3.8 [mp.per.3] Concienciación 20
3.9 [mp.per.4] Formación 20
3.10 [mp.si.5] Borrado y destrucción 20
3.11 [mp.info.2] Calificación de la información 21
3.12 [mp.info.3] Firma electrónica 21
3.13 [mp.info.4] Sellos de tiempo 22
3.14 [mp.info.5] Limpieza de documentos 22
4. MEDIDAS DE PRIVACIDAD 23
4.1 [org.1] Política de seguridad 23
4.2 [org.2] Normativa de seguridad 24
4.3 [org.3] Procedimientos de seguridad 24

4.4 [op.pl.1] Análisis de riesgos 25
4.5 [op.pl.2] Arquitectura de seguridad 25
4.6 [op.exp.5] Gestión de cambios 26
4.7 [op.exp.7] Gestión de incidentes 26
4.8 [op.exp.8] Registro de actividad 26
4.9 [op.ext.1] Contratación y acuerdos de nivel de servicio 27
4.10 [op.ext.4] Interconexión de sistemas 28
4.11 [op.nub.1] Protección de servicios en la nube 28
4.12 [op.mon.2] Sistemas de métricas 28
4.13 [mp.per.1] Caracterización del puesto de trabajo 29
4.14 [mp.per.2] Deberes y obligaciones 29
4.15 [mp.per.3] Concienciación 29
4.16 [mp.per.4] Formación 29
4.17 [mp.sw.1] Desarrollo de aplicaciones 30
4.18 [mp.info.1] Datos personales 31

INTRODUCCIÓN

El presente documento constituye el Esquema de Seguridad de la Administración de Justicia (en adelante, ESAJ o Esquema), y tiene por objeto garantizar la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación de los datos, informaciones y servicios en la Administración de Justicia, de conformidad con el artículo 1, apartado 2 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 (en adelante Real Decreto-ley 6/2023, de 19 de diciembre).

El ESAJ es una pieza imprescindible para la efectividad del derecho de los ciudadanos y ciudadanas a relacionarse con la Administración de Justicia utilizando medios electrónicos, así como, y fundamentalmente, del derecho a la protección de datos de carácter personal, y de la tutela judicial efectiva. A macro nivel, una falta grave de disponibilidad de la información o una pérdida de su integridad podría afectar al Estado de Derecho.

Para la consecución de este objetivo, el Real Decreto-ley 6/2023, de 19 de diciembre, prevé cuatro instrumentos organizativos, el propio Esquema, la Política de Seguridad de la Información de la Administración Judicial Electrónica, el Subcomité de Seguridad como órgano especializado y permanente para la ciberseguridad judicial del Comité técnico estatal de la Administración judicial electrónica, y el Centro de Operaciones de Ciberseguridad de la Administración de Justicia.

Es el Esquema de Seguridad de la Administración de Justicia objeto de la regulación en el presente documento, conjuntamente con su Anexo de medidas técnicas y organizativas.

DISPOSICIONES GENERALES.

I. Del ámbito de aplicación y los principios generales

1. Objeto.

1.1. Este documento tiene por objeto desarrollar el Esquema de Seguridad de la Administración de Justicia, que constituye la parte de seguridad del Esquema Judicial de Interoperabilidad y Seguridad establecido en el artículo 88 del Real Decreto-ley 6/2023, de 19 de diciembre.

1.2. De conformidad con el indicado Real Decreto-ley, el Esquema será aplicado en la Administración de Justicia para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y la conservación de los datos, informaciones, documentos y servicios, utilizados por medios electrónicos que gestionen los distintos órganos judiciales en el ejercicio de sus competencias. Y todo ello se llevará a efecto con observancia de las prescripciones que en adelante se establecen y de los requisitos funcionales aplicables.

El ESAJ regulará aquellos aspectos relacionados con la seguridad que constituyan particularidades de la Administración de Justicia que requieran una concreta regulación, siendo obligatorio el cumplimiento del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como sus instrucciones técnicas de seguridad, en la medida que no requieran dicha adaptación. Asimismo, para facilitar el cumplimiento del ENS se seguirán las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC) del CCN, particularmente de la serie 800, sin perjuicio de las adaptaciones del ESAJ.

1.4. A estos efectos, albergará la política de seguridad en la utilización de medios electrónicos y el establecimiento de los principios básicos y requisitos mínimos que permitan una protección adecuada de la información de conformidad con el marco jurídico. A través de las guías, tanto de interoperabilidad como de seguridad, se regularán aspectos específicos de requisitos de seguridad en el ámbito de la Administración de Justicia.

1.5. En el ámbito de protección de datos personales recogerá las medidas técnicas y organizativas mínimas que permitan garantizar y poder acreditar que el tratamiento de los datos de carácter personal es conforme con la normativa de protección de datos personales.

1.6. Asimismo, en el CTEAJE podrán establecerse requisitos y criterios mínimos que garanticen un uso responsable, legal y ético de la Inteligencia Artificial en el ámbito de la Administración de Justicia.

2. Ámbito de aplicación.

2.1. El ámbito de aplicación es el ya establecido en el artículo 2 del Real Decreto-ley 6/2023, de 19 de diciembre.

2.2. Aplicará a todos los sistemas de información y comunicación utilizados para la Administración de Justicia por todos los órganos, departamentos y unidades del CGPJ, Ministerio Fiscal, Ministerio de Justicia y CCAA que tienen transferidas las competencias en esta materia, así como los organismos públicos que dependan de los mismos.

Asimismo, se aplicará a los sistemas de información utilizados por las entidades privadas, cuando utilicen sus propios sistemas de información para prestar servicios competenciales a las entidades de la Administración de Justicia.

II. Garantías de Cumplimiento

3. Mecanismos de control.

3.1. El CTEAJE velará por el establecimiento de los mecanismos de control para garantizar de forma efectiva el cumplimiento del Esquema aquí expresado, en cumplimiento de lo dispuesto en el artículo 6.h) del Real Decreto 396/2013, de 7 de junio, regulador del CTEAJE.

4. Declaración de Conformidad y Certificación.

4.1. En las sedes judiciales electrónicas correspondientes, y en su caso, en el portal del Consejo General del Poder Judicial, se publicarán las declaraciones de conformidad, compatibilidad, certificaciones y otros posibles distintivos de seguridad obtenidos respecto al cumplimiento de las exigencias que en materia de seguridad se establecen en el Real Decreto-ley 6/2023, de 19 de diciembre, así como de las desarrolladas en el ESAJ y en su normativa de desarrollo y de acuerdo con los criterios que se adopten en el CTEAJE.

4.2. Las medidas técnicas y organizativas destinadas a garantizar y poder acreditar que el tratamiento de los datos de carácter personal es conforme con la normativa de protección de datos personales que se recogen en el Anexo del Esquema constituyen una guía de ayuda, y no serán objeto de certificación conjuntamente con las medidas de seguridad.

DE LA SEGURIDAD ELECTRÓNICA DE LA ADMINISTRACIÓN DE JUSTICIA. PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL

I. Seguridad, protección de datos personales e inteligencia artificial

5. Seguridad electrónica de la Administración de Justicia.

5.1. El ESAJ adopta el Esquema Nacional de Seguridad, sus principios básicos, requisitos mínimos, la categorización de los sistemas de información, su metodología, con las particularidades específicas de la Administración de Justicia previstas en el Anexo del presente documento, constituyendo la guía técnica de seguridad, sin perjuicio de otras cuestiones específicas previstas en las guías de interoperabilidad y en las guías de seguridad.

Para la determinación del nivel de seguridad de cada dimensión de los sistemas de información, se aplicarán los criterios de valoración que se determinen en el Subcomité de Seguridad del CTEAJE, de conformidad con el artículo 85.2 e) del Real Decreto-ley 6/2023, de 19 de diciembre.

5.2. La Política de Seguridad de la Información de la Administración Judicial Electrónica define el modelo organizativo para garantizar la seguridad de la información y la protección de los datos personales tratados en los diferentes sistemas de información que dan soporte a la Administración de Justicia, con la coordinación, impulso, actualización y mejora permanente del Subcomité de Seguridad del CTEAJE.

6. Protección de datos personales.

6.1. En materia de protección de datos personales tratados con fines jurisdiccionales, con las especialidades establecidas en la Ley Orgánica del Poder Judicial y en las leyes procesales, son de aplicación el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.

En el ámbito penal, sin perjuicio de las especialidades establecidas en Ley Orgánica del Poder Judicial y en las leyes procesales, será de aplicación la Ley Orgánica 7/2021 y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

El tratamiento de datos personales con fines no jurisdiccionales se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.

6.2. En materia de seguridad, con respeto de las medidas de seguridad específicas que pudieran estar previstas en las normas procesales, tanto la Ley Orgánica 3/2018 como la Ley Orgánica 7/2021, obligan a los responsables y encargados, a aplicar las medidas incluidas en el ENS. Entre los responsables y encargados, se encuentran entre otros, los órganos constitucionales o con relevancia constitucional, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las comunidades autónomas, y en el ámbito de la Ley 7/2021 las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

La indicada normativa de protección de datos establece la obligación de adoptar medidas técnicas y organizativas, incluidas las medidas de seguridad, para garantizar que el tratamiento de datos se adecúa a la misma, dentro de un enfoque basado en el riesgo.

6.3. Por su parte, el Esquema, debe incorporar las medidas técnicas y organizativas destinadas a garantizar y poder acreditar que el tratamiento de los datos de carácter personal es conforme con la normativa de protección de datos personales previo análisis de riesgos, de acuerdo con el mandato del artículo 88.5 del Real Decreto-ley 6/2023, de 19 de diciembre. Las medidas de Anexo II del ENS constituyen asimismo medidas de seguridad del tratamiento de datos personales de los artículos 32 RGPD y 33 LO 7/2021, sin perjuicio de otras medidas de seguridad, que, no estando previstas en el ENS, se estimen adecuadas y proporcionadas al nivel de riesgo determinado.

6.4. Siguiendo la estructura del Anexo II del ENS, y propiciando la integración de procesos, se recogen los requisitos en materia de privacidad a nivel organizativo, a nivel de tratamiento u operativo y a nivel de protección de activos específicos. En el Anexo se incorporan las medidas técnicas y organizativas, diferentes a las medidas de seguridad previstas en el ENS o las establecidas de acuerdo con el apartado anterior.

Con ello, se podrá verificar la implantación y el nivel de madurez de las medidas en privacidad acumulándose a las medidas de seguridad naturales del ENS.

7. Política de Seguridad y desarrollo normativo.

7.1. La Política de Seguridad de la Información de la Administración Judicial Electrónica constituye la principal medida de seguridad organizativa y forma parte de la política de privacidad o de protección de datos personales, en caso de existencia de tratamiento de este tipo de datos.

7.2. El contenido de ambas políticas podrá regularse en un único documento, por el que se establezca el marco organizativo y de desarrollo normativo que permita el cumplimiento de los principios y requisitos previstos en los marcos normativos aplicables, en materia de seguridad y privacidad, dentro de su contexto y especialidades de la Administración de Justicia.

7.3. Las administraciones e instituciones integrantes del CTEAJE y sometidas a la política de seguridad y protección de datos desarrollarán la política en su respectivo ámbito competencial, adecuando el cumplimiento de los requisitos a su organización.

No obstante, se propiciarán acuerdos para crear normativa de desarrollo de aplicación general que permitan la homogeneidad en la observación de las diferentes medidas técnicas, organizativas y legales.

8. Inteligencia Artificial.

8.1. Sin perjuicio del cumplimiento de la normativa aplicable, en el ámbito del Derecho Español, en el ámbito del Derecho de la UE, así como otras normas internacionales aplicables, podrán establecerse en el CTEAJE requisitos y criterios mínimos que garanticen un uso responsable, legal y ético de la Inteligencia Artificial en el ámbito de la Administración de Justicia.

9. Entidades del sector privado.

9.1. En la contratación con las entidades del sector privado, así como con empresas públicas, que presten servicios o provean soluciones a las administraciones con competencias en materia de justicia e instituciones sometidas al presente Esquema, se exigirá el cumplimiento de las obligaciones establecidas en el ENS, así como el cumplimiento de las obligaciones exigibles como encargados del tratamiento de conformidad con el marco normativo de protección de datos aplicable.

9.2. La contratación también recogerá aquellos requisitos de seguridad específicos, que prevalecerán sobre los indicados en el apartado anterior, en las correspondientes guías de interoperabilidad y en las guías de seguridad, en la Política de Seguridad de la Información de la Administración Judicial Electrónica, así como aquellos resultados del análisis de riesgos de seguridad de la información y de protección de datos, y en su caso de la evaluación de impacto en protección de datos.

10. Desarrollo de requisitos específicos.

A continuación, se detallan aspectos de seguridad específicos previstos en el Real Decreto-ley 6/2023, de 19 de diciembre, que se desarrollarán a través de los instrumentos de desarrollo normativo del CTEAJE, incluido, en su caso, en el Anexo del presente documento:

10.1. Nivel de Firma: En el marco del CTEAJE podrá determinarse el nivel de firma aplicable en cada una de las actuaciones en el ámbito de la Administración de Justicia. Dicha determinación deberá realizarse en la Guía de Interoperabilidad y Seguridad de autenticación, certificados y firma electrónica, en proporción al nivel de seguridad que se estime necesario para cada clase de actuación. (artículo 20)

10.2. Códigos Seguros de Verificación: determinación de los términos de codificación (artículo 26)

10.3. Sistemas de firma: El CTEAJE determinará los sistemas de firma que deben utilizar los y las fiscales, letrados y letradas de la Administración de Justicia y demás personal al servicio de la Administración de Justicia. Dichos sistemas podrán identificar de forma conjunta al titular y el cargo. (artículo 27)

10.4. Firma electrónica avanzada mediante captura de firma: Requisitos de la Guía de Interoperabilidad y Seguridad de Autenticación, Certificados y Firma Electrónica aprobada por el CTEAJE. (artículo 29)

10.5. Intercambio electrónico de datos en entornos cerrados de comunicación: el CTEAJE determinará las condiciones y garantías por las que se regirán, que al menos comprenderán la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar. (artículo 30)

10.6. Actuaciones automatizadas, proactivas y asistidas: podrá realizarse por el CTEAJE la definición de las especificaciones, programación, mantenimiento, supervisión y

control de calidad y, en su caso, la auditoría del sistema de información y de su código fuente. (artículo 58)

10.7. Firma electrónica en las actuaciones por videoconferencia: El uso de las firmas en cada una de las actuaciones realizadas por videoconferencia se determinará en el marco del CTEAJE. (artículo 60)

10.8. Puntos de acceso seguros: Establecimiento de requisitos que deben reunir los puntos de acceso seguros, además de aquellos establecidos legalmente. (artículo 62)

10.9. Lugares seguros: Establecimiento de requisitos que deben reunir los lugares seguros, además de aquellos establecidos legalmente. (artículo 62);

10.10. Entornos remotos de trabajo: El Esquema Nacional de Seguridad y el Esquema Judicial de Interoperabilidad y Seguridad fijarán los requisitos mínimos que todas las administraciones públicas con competencias en materia de Justicia han de garantizar en relación con los entornos remotos de trabajo. (artículo 68)

II. Estado de seguridad de los sistemas

11. Informe del estado de la seguridad.

11.1. El CTEAJE articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables tecnológicas de la seguridad, en los sistemas de información a los que se ha hecho referencia, de forma que permita elaborar un perfil general del estado de la seguridad de la Administración de Justicia.

11.2. Con este objeto, el CTEAJE recomendará indicadores de la seguridad para dichos sistemas de información que tendrán en cuenta los procedimientos y metodologías que elabore el Centro Criptológico Nacional.

III. Respuesta a los incidentes de seguridad

12. Coordinación frente a incidentes de seguridad de la información.

12.1. Dentro del CTEAJE se fomentará el establecimiento de los protocolos y acuerdos de colaboración con el Centro Criptológico Nacional (CCN) para la coordinación y prestación de servicios de respuesta a incidentes de seguridad.

13. Centro de Operaciones de Ciberseguridad.

13.1. El Centro de Operaciones de Ciberseguridad de la Administración de Justicia prestará un conjunto de servicios horizontales de ciberseguridad a las administraciones públicas prestatarias del servicio público de Justicia, apoyando y facilitando la coordinación con los centros de operaciones de ciberseguridad de las Administraciones con competencias en materia de Justicia e instituciones judiciales en sus capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad.

13.2. El Centro de Operaciones de Ciberseguridad de la Administración de Justicia actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración con competencias en materia de Justicia e instituciones de la Administración de Justicia, y de la función de coordinación a nivel nacional e internacional del Equipo de Respuesta para Emergencias Informáticas del Centro Criptológico Nacional (CCN-CERT).

A tal efecto, se arbitrarán los mecanismos de colaboración necesarios entre el Subcomité de Seguridad y el Centro Criptológico Nacional.

ACTUALIZACIÓN, DESARROLLO Y FORMACIÓN

I. Desarrollo del Esquema de Seguridad de la Administración de Justicia

14. Actualización permanente.

14.1. Para el desarrollo, perfeccionamiento y la actualización del presente Esquema, el CTEAJE elaborará:

a) Las correspondientes guías y normas técnicas de aplicación.

b) En el marco de sus competencias, cualquier otra normativa cuya necesidad venga impuesta por el desarrollo de la Administración judicial electrónica.

15. Desarrollo.

15.1. De conformidad con lo dispuesto en el artículo 88 y concordantes del Real Decreto-ley 6/2023, de 19 de diciembre, y en el Real Decreto 396/2013, de 7 de junio, el CTEAJE elaborará, aprobará y difundirá las guías técnicas de seguridad de las tecnologías de la información y las comunicaciones, en desarrollo del presente Esquema.

16. Adecuación de sistemas, aplicaciones y servicios.

16.1. De conformidad con las competencias del CTEAJE, los sistemas de información de la Administración de Justicia serán objeto de verificación y validación funcional y en materia de seguridad por parte del CTEAJE.

16.2. En materia de seguridad, los sistemas de información de la Administración de Justicia deben someterse a la conformidad con el Esquema Nacional de Seguridad, recogiendo y prevaleciendo las particularidades específicas de la Administración de Justicia.

Con objeto de facilitar la adecuación se promoverán perfiles de cumplimiento específico para la Administración de Justicia, conjuntamente con el Centro Criptológico Nacional.

ANEXO. MEDIDAS

1. TABLA DE MEDIDAS Y APLICACIÓN

En la siguiente tabla, se recogen las medidas del Anexo II del Esquema Nacional de Seguridad, diferenciando aquellas que requieren una adecuación en el Esquema de Seguridad de la Administración de Justicia, de acuerdo con la columna “Justicia”.

Asimismo, se recogen las medidas de privacidad, complementando o ampliando los requisitos o refuerzos de seguridad, con objeto de aprovechar e integrar los procesos existentes.

En ambos casos, se utilizará la nomenclatura (A, M, B) para indicar la categoría (ALTA, MEDIA, BÁSICA) o el nivel (ALTO, MEDIO, BAJO), a partir del cual es exigible la medida.

Dimensiones	CAT B	CAT M	CAT A	Medida	Justicia	Privacidad
Categoría	aplica	aplica	aplica	**org.1**		B
Categoría	aplica	aplica	aplica	**org.2**		B
Categoría	aplica	aplica	aplica	**org.3**		B
Categoría	aplica	aplica	aplica	**org.4**	A	
Categoría	aplica	+ R1	+ R2	**op.pl.1**		B
Categoría	aplica	+ R1	+R1+R2+R3	**op.pl.2**		B
Categoría	aplica	=	=	**op.pl.3**	M	
D	aplica	+R1	+R1	**op.pl.4**		
Categoría	n.a.	aplica	aplica	**op.pl.5**		
T A	aplica	+ R1	+ R1	**op.acc.1**	B	
C I T A	aplica	=	+ R1	**op.acc.2**		
C I T A	n.a.	aplica	+ R1	**op.acc.3**		
C I T A	aplica	aplica	aplica	**op.acc.4**		
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**	B	
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**	B	
Categoría	aplica	aplica	aplica	**op.exp.1**		
Categoría	aplica	aplica	aplica	**op.exp.2**		
Categoría	aplica	+ R1	+R1+R2+R3	**op.exp.3**		
Categoría	aplica	+ R1	+R1+R2	**op.exp.4**		
Categoría	n.a.	aplica	+ R1	**op.exp.5**		M
Categoría	aplica	+ R1+R2	+R1+R2+R3+R4	**op.exp.6**		
Categoría	aplica	+ R1+R2	+ R1+R2+ R3	**op.exp.7**		B
T	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5	**op.exp.8**	B	B
Categoría	aplica	=	=	**op.exp.9**		

Dimensiones	CAT B	CAT M	CAT A	Medida	Justicia	Privacidad
Categoría	aplica	+R1	+R1	**op.exp.10**		
Categoría	n.a.	aplica	aplica	**op.ext.1**		B
Categoría	n.a.	aplica	aplica	**op.ext.2**		
Categoría	n.a.	n.a.	aplica	**op.ext.3**		
Categoría	n.a.	aplica	+R1	**op.ext.4**		M
Categoría	aplica	+R1	+R1+R2	**op.nub.1**		B
D	n.a.	aplica	aplica	**op.cont.1**		
D	n.a.	n.a.	aplica	**op.cont.2**		
D	n.a.	n.a.	aplica	**op.cont.3**		
D	n.a.	n.a.	aplica	**op.cont.4**		
Categoría	aplica	+R1	+R1+R2	**op.mon.1**		
Categoría	aplica	+R1+R2	+R1+R2	**op.mon.2**		B
Categoría	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6	**op.mon.3**		
Categoría	aplica	=	=	**mp.if.1**		
Categoría	aplica	=	=	**mp.if.2**		
Categoría	aplica	=	=	**mp.if.3**		
D	aplica	+ R1	+ R1	**mp.if.4**		
D	aplica	=	=	**mp.if.5**		
D	n.a.	aplica	=	**mp.if.6**	B	
Categoría	aplica	=	=	**mp.if.7**		
Categoría	n.a.	aplica	=	**mp.per.1**		M
Categoría	aplica	+ R1	+ R1	**mp.per.2**		B
Categoría	aplica	=	=	**mp.per.3**	M	B
Categoría	aplica	=	=	**mp.per.4**	M	B
Categoría	aplica	+ R1	+ R1	**mp.eq.1**		
A	n.a.	aplica	+ R1	**mp.eq.2**		
Categoría	aplica	=	+R1+R2	**mp.eq.3**		
C	aplica	+ R1	+ R1	**mp.eq.4**		
Categoría	aplica	=	=	**mp.com.1**		
C	aplica	+ R1	+R1+R2+R3	**mp.com.2**		
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	**mp.com.3**		
Categoría	n.a.	+[R1oR2oR3]	+[R2oR3]+R4	**mp.com.4**		
C	n.a.	aplica	=	**mp.si.1**		
C I	n.a.	aplica	+ R1 + R2	**mp.si.2**		
Categoría	aplica	=	=	**mp.si.3**		
Categoría	aplica	=	=	**mp.si.4**		
C	aplica	+ R1	+ R1	**mp.si.5**	B	

Dimensiones	CAT B	CAT M	CAT A	Medida	Justicia	Privacidad
Categoría	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4	**mp.sw.1**		M
Categoría	aplica	+ R1	+ R1	**mp.sw.2**		
Categoría	aplica	=	=	**mp.info.1**		B
C	n.a.	aplica	=	**mp.info.2**	B	
I A	aplica	+R1+R2+R3	+ R1+R2+R3+R4	**mp.info.3**	B	
T	n.a.	n.a.	aplica	**mp.info.4**	A	
C	aplica	aplica	aplica	**mp.info.5**	B	
D	aplica	+ R1	+ R1 + R2	**mp.info.6**		
Categoría	aplica	aplica	aplica	**mp.s.1**		
Categoría	+[R1oR2]	+[R1oR2]	+R2+R3	**mp.s.2**		
Categoría	aplica	aplica	+ R1	**mp.s.3**		
D	n.a.	aplica	+ R1	**mp.s.4**		

2. CATEGORÍA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El conjunto de medidas aplicables a la Administración de Justicia en materia de seguridad y de privacidad, se obtendrán en función de las valoraciones y categoría, de acuerdo con el presente Anexo.

La valoración de las dimensiones de seguridad de los sistemas de información de la Administración de Justicia que traten datos personales, será efectuada por los responsables del tratamiento, y en su caso, por las personas designadas al efecto de realizar dicha función de acuerdo con la Política de Seguridad, salvo que el sistema no trate datos personales, en cuyo caso las valoraciones serán efectuadas por los responsables de la información y del servicio.

Se aplicarán los criterios específicos que en materia de Administración de Justicia se hubieran establecido en el CTEAJE para dichas valoraciones, que en todo caso priorizarán los riesgos para los derechos y libertades de los interesados titulares de los datos objeto de tratamiento a través de los sistemas de información.

3. MEDIDAS ESPECÍFICAS DE JUSTICIA

Para cada medida que se ve afectada se indica si es un requisito adicional, o si modifica algún requisito o refuerzo del ENS, y a partir de que categoría o nivel de seguridad.

La nomenclatura usada es la siguiente:

- Si modifica un requisito se añade -j
- Si es un requisito adicional se añade -j.1

3.1 [org.4] Proceso de autorización

dimensiones	Todas		
Categoría ENS	BÁSICA aplica	MEDIA aplica	ALTA aplica
Medidas Justicia	=	=	requisito adicional [org.4-j.1]

Se creará para cada proceso una matriz de roles y responsabilidades que delimiten las responsabilidades para cada actuación.

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

dimensiones	Todas		
Categoría ENS	BÁSICA aplica	MEDIA aplica	ALTA aplica
Medidas Justicia	=	requisito adicional [op.pl.3-j.1]	=

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

3.3 [op.acc.1] Identificación

dimensiones	TA		
nivel ENS	BAJO aplica	MEDIO +R1	ALTO +R1
Medidas Justicia	modifica [op.acc.1.1] [op.acc.1.1-j]	=	=

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.

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

dimensiones	CITA		
nivel ENS	BAJO + [R1 o R2 o R3 o R4]	MEDIO + [R2 o R3 o R4] + R5	ALTO + [R2 o R3 o R4] +R5

Medidas Justicia	requisito adicional [op.acc.5-j.1]	=	=

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.

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

dimensiones	CITA		
nivel	BAJO	MEDIO	ALTO
ENS	+ [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
Medidas Justicia	requisito adicional [op.acc.6-j.1]	=	=

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.

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

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
ENS	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5
Medidas Justicia	requisito adicional [op.exp.8-j.1]	=	=

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.

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

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
ENS	n.a.	aplica	aplica
Medidas Justicia	aplica [mp.if.6.1-j]	=	=

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

3.8 [mp.per.3] Concienciación

dimensiones	Todas		
Categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Justicia	=	requisito adicional [mp.per.3-j.1]	=

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.

3.9 [mp.per.4] Formación

dimensiones	Todas		
Categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Justicia	=	requisito adicional [mp.per.4-j.1]	=

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.

3.10 [mp.si.5] Borrado y destrucción

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
ENS	aplica	+ R1	+ R1
Medidas Justicia	modifica [mp.si.5.1] [mp.si.5.1-j]	=	=

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.

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

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
ENS	n.a.	aplica	aplica
Medidas Justicia	modifica [mp.info.2.1] [mp.info.2.1-j]	=	=

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.

3.12 [mp.info.3] Firma electrónica

dimensiones	I A

nivel	BAJO	MEDIO	ALTO
ENS	aplica	+R1+R2+R3	+R1+R2+R3+R4
Medidas Justicia	modifica [mp.info.3.1] [mp.info.3.1-j]	modifica R3 [mp.info.3.r3.1-j]	=

[mp.info.3.1-j] 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.

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.

[mp.info.3.r3.1-j] 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.

3.13 [mp.info.4] Sellos de tiempo

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
ENS	n.a.	n.a.	aplica
Medidas Justicia			modifica [mp.info.4.3.1-j]

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.

3.14 [mp.info.5] Limpieza de documentos

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
ENS	aplica	aplica	aplica
Medidas Justicia	modifica [mp.info.5.1] [mp.info.5.1-j]	=	=

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.

4. MEDIDAS DE PRIVACIDAD

En este apartado se recogen las medidas técnicas y organizativas en materia de protección de datos, de acuerdo con los artículos 24 y 25 del RGPD, y artículo 27 y 28 de la Ley Orgánica 7/2021, de 26 de mayo.

Las medidas de seguridad del artículo 32 RGPD y del artículo 37 de la Ley Orgánica 7/2021, de 26 de mayo, se corresponden con las medidas del Anexo II del ENS, sin perjuicio de otras medidas de seguridad que se establezcan como la anonimización, seudonimización, bloqueo de datos, registro de operaciones, y cualesquiera otras que se estimen adecuadas y proporcionadas al nivel de riesgo determinado.

En resumen, el presente documento trata de recoger los requisitos en materia de protección de datos, llevando a un plano práctico la medida de protección de la información relativa a los Datos personales [mp.info.1] prevista en el ENS.

Para ello, se han distribuido las medidas técnicas y organizativas de privacidad dentro del anexo II del ENS siguiendo su metodología, pudiendo equiparar lo siguiente:

ENS	Seguridad	Privacidad
Marco organizativo	Medidas horizontales	Medidas horizontales
Marco operacional	Medidas del sistema	Medidas del tratamiento
Medidas de protección	Medidas específicas sobre activos	Medidas de privacidad que afectan a determinados activos

Aquellas medidas del ENS que estén supeditadas a la aprobación, verificación o valoración por parte del responsable de la información o por el responsable del servicio, deberá entenderse que dichas funciones serán asumidas por el responsable del tratamiento, con el asesoramiento del delegado de protección de datos.

Para las medidas que se ven afectadas, los requisitos o refuerzos que se indican a continuación son adicionales a los establecidos por el ENS.

La nomenclatura usada ha consistido en añadir al requisito -p.1.

4.1 [org.1] Política de seguridad

dimensiones	Todas

categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	requisito adicional [org.1-p.1]	=	=

La política de privacidad, que podrá formar parte de la política de seguridad de la información, incluirá los siguientes requisitos mínimos:

a) La asignación formal de roles y responsabilidades
b) En su caso, la participación de los roles en órganos colegiados, sin perjuicio de sus competencias y atribuciones.
c) Establecer una estructura de desarrollo de la política que recoja las medidas técnicas y organizativas para garantizar la seguridad y privacidad de los datos personales tratados en la organización.
d) Garantizar la participación de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales del delegado o delegados de protección de datos.
e) Garantizar su enfoque al riesgo para los derechos y libertades de las personas.
f) Establecer auditorías periódicas encaminadas a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas.
g) La revisión de la política de privacidad por el delegado de protección de datos o delegados de protección de datos.

4.2 [org.2] Normativa de seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	adicional [org.2-p.1]	=	=

Se dispondrá de una serie de documentos que describan el cumplimiento del marco normativo de protección de datos aplicable, sus principios y requisitos en la organización, y que integre los procedimientos que garanticen su cumplimiento, y sin perjuicio de otros, aquellos recogidos en [org.3].

4.3 [org.3] Procedimientos de seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	requisito adicional [org.3-p.1]	=	=

Se dispondrá de una serie de documentos que detallen de forma clara y precisa la forma en que se ha de tratar la información en consideración al cumplimiento del marco normativo de protección de datos, precisando cómo efectuar:

-Análisis de riesgos en privacidad.

-Evaluación de impacto en protección de datos personales.

-Gestión de violaciones de seguridad de los datos personales.

-Ejercicio de derechos de protección de datos de los interesados.

-Cumplimiento del deber de información, incluidos los cambios en la actividad de tratamiento que afecten a la información que se debe proporcionar de acuerdo con los artículos 13 y 14 RGPD, y sean comunicados a los interesados.

-Designación de delegado/s de protección de datos, en su caso.

-Llevanza, actualización, revisión del registro de las actividades de tratamiento, así como de la publicación de su inventario.

-Garantizar la seguridad desde el diseño y por defecto, documentando los modelos de datos personales, ciclo de vida, y las medidas utilizadas para garantizar la privacidad.

-Garantizar la protección de datos por los encargados del tratamiento.

-Evaluar los mecanismos de transferencia de datos personales a terceros países.

-Revisión periódica y al menos anual de los tratamientos, o cuando ocurren cambios, incluidos aquellos cambios en los sistemas de información a través de los cuales se tratan dichos datos personales.

4.4 [op.pl.1] Análisis de riesgos

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+ R1	+ R2
Medidas Privacidad	requisito adicional [op.pl.1-p.1]	=	=

Se deberá llevar a cabo un análisis de riesgos sobre la privacidad de los datos personales y la incidencia sobre los derechos y libertades de las personas físicas, que tendrá en cuenta lo establecido en las guías de la Agencia Española de Protección de Datos a estos efectos, que deberá recoger las observaciones del delegado de protección de datos, y ser aprobado por el Responsable del Tratamiento.

Se realizará y se documentará una EIPD en los supuestos de tratamientos de alto riesgo para los derechos y libertades de las personas físicas con carácter previo al inicio del tratamiento.

4.5 [op.pl.2] Arquitectura de seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+ R1	+R1+R2+R3
Medidas Privacidad	requisito adicional [op.pl.2-p.1]	=	=

Se deberá disponer de documentación del sistema relativa a la privacidad, que tenga en cuenta al menos, el modelo de datos personales, su ciclo de vida, evaluación de impacto en protección de datos, en caso de existir, medidas de protección de datos desde el diseño y por defecto.

Sistema de gestión de la seguridad de la información y privacidad, con actualización y aprobación periódica.

4.6 [op.exp.5] Gestión de cambios

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	n.a.	aplica	+R1
Medidas Privacidad	=	requisito adicional [op.exp.5-p.1]	=

Deberá evaluarse el impacto de los cambios en caso de afectar al tratamiento de los datos y a la privacidad. Para ello se dará traslado del análisis de riesgos, para su revisión por el responsable del tratamiento y su delegado de protección de datos, y se recogerán, en su caso, las indicaciones efectuadas por estos últimos, que deberán ser observadas por el Responsable de Seguridad, dejándose evidencia de todo lo anterior.

4.7 [op.exp.7] Gestión de incidentes

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+ R1+R2	+ R1+R2+ R3
Medidas Privacidad	requisito adicional [op.exp.7-p.1]	=	=

Se dispondrá de un proceso para hacer frente a la gestión de violaciones de la seguridad de los datos personales, establecido conforme org.3.

Las violaciones de seguridad de los datos personales, dependiendo del tipo de incidente, deberán ser comunicadas a la autoridad de protección de control correspondiente.

4.8 [op.exp.8] Registro de actividad

dimensiones	T		
nivel	BAJO	MEDIO	ALTO

ENS	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5
Medidas Privacidad	requisito adicional [op.exp.8-p.1]	=	=

En relación con los datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, los responsables y encargados deberán mantener al menos los registros de las operaciones de tratamiento en sistemas de tratamiento automatizados indicados y para las finalidades recogidas en el artículo 33 de 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 responsable del tratamiento determinará el plazo de retención de estos registros.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	n.a.	aplica	aplica
Medidas Privacidad	requisito adicional [op.ext.1-p.1]	=	=

El tratamiento de datos por el encargado requerirá de la suscripción de un contrato de encargo u otro acto jurídico similar, con el contenido del art. 28.3 RGPD, o en su caso del art. 30.3 Ley Orgánica 7/2021, de 26 de mayo.

Las administraciones prestacionales de medios tecnológicos de la Administración de Justicia, respecto de los tratamientos que sean responsables, como de aquellos que sean responsabilidad de los órganos o de las oficinas judiciales o fiscales, mantendrá inventarios permanentemente actualizados de tratamiento de datos efectuados por encargados y por subencargados del tratamiento.

Anualmente, deberá darse traslado de los inventarios al delegado de protección de datos de la administración prestacional para su supervisión. Respecto de los tratamientos por cuenta de los órganos o de las oficinas judiciales o fiscales, se pondrá respectivamente a disposición de CGPJ, FGE y del Secretario General de la Administración de Justicia a su requerimiento.

Lo previsto en el presente requisito será sin perjuicio de las obligaciones relativas al registro de actividades de tratamiento.

En el caso de tratamiento de datos por contratistas encargados del tratamiento o subcontratistas, que requieran la transferencia internacional de datos, incluida la posibilidad de que los datos puedan ser accesibles desde terceros países u organizaciones internacionales, requerirán su autorización previa por el responsable del tratamiento, y el previo asesoramiento documentado del delegado de protección de datos.

4.10 [op.ext.4] Interconexión de sistemas

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	n.a.	aplica	+R1
Medidas Privacidad	=	requisito adicional [op.ext.4-p.1]	=

Las interconexiones que impliquen tratamiento de datos, incluida la comunicación, serán recogidas en el documento de ciclo de vida de los datos personales.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+R1	+R1+R2
Medidas Privacidad	requisito adicional [op.nub.1-p.1]	=	=

El tratamiento de datos por encargado que preste servicio en la nube requerirá del cumplimiento de los requisitos previstos en la medida [op.ext.1].

La Administración prestacional de la Administración de Justicia analizará y documentará la necesidad de llevar a cabo una evaluación de impacto en protección de datos, con el asesoramiento del delegado de protección de datos, y, en su caso, se llevará a cabo.

4.12 [op.mon.2] Sistemas de métricas

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+R1+R2	+R1+R2
Medidas Privacidad	requisito adicional [op.mon.2-p.1]	=	=

El grado de implantación de las medidas de seguridad formarán parte y se acumularán al resto de medidas recogidas en este anexo en materia de protección de datos, que en conjunto garantizan la privacidad.

A partir de categoría media, se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de violaciones de la seguridad de los datos personales.

A partir de categoría media, se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad y privacidad, en relación con los recursos consumidos, en términos de horas y presupuesto.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	n.a.	aplica	aplica
Medidas Privacidad	=	requisito adicional [mp.per.1-p.1]	=

Para cada puesto de trabajo, relacionado directamente con el tratamiento de datos personales, se definirán las responsabilidades en materia de protección de datos, que estarán basadas en el análisis de riesgos.

4.14 [mp.per.2] Deberes y obligaciones

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	+ R1	+ R1
Medidas Privacidad	requisito adicional [mp.per.2-p.1]	=	=

Los requisitos en seguridad serán extensibles en materia de protección de datos personales.

A partir de categoría media, se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones en materia de protección de datos necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

4.15 [mp.per.3] Concienciación

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	requisito adicional [mp.per.3-p.1]	=	=

Entre las acciones necesarias para concienciar regularmente, se considerarán acciones en materia de protección de datos, del personal que participa en las operaciones de tratamiento de datos personales.

4.16 [mp.per.4] Formación

dimensiones	Todas

categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	requisito adicional [mp.per.4-p.1]	=	=

Entre las acciones necesarias para formar regularmente, se considerarán acciones en materia de protección de datos, del personal que participa en las operaciones de tratamiento de datos personales.

4.17 [mp.sw.1] Desarrollo de aplicaciones

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4
Medidas Privacidad	=	requisito adicional [mp.sw.1-p.1]	=

Formarán parte del desarrollo de aplicaciones los siguientes elementos:

a) Modelo de datos personales suscrito por el responsable del tratamiento con las observaciones del delegado de protección de datos, para garantizar el principio de minimización de datos, con la necesidad de cada campo en relación a la finalidad del tratamiento.
b) Ciclo de vida de los datos personales, que recogerá los plazos de conservación de los datos personales, que será objeto de análisis documentado, por el responsable del tratamiento con el asesoramiento del delegado de protección de datos, asimismo documentado.
c) Requisitos que, en su caso, deban implantarse en el sistema relativos a:
    a. Cumplimiento del deber de información
    b. Recabar el consentimiento
    c. Ejercicio de derechos
    d. Revisión de datos inexactos o incompletos
    e. Control de los plazos de conservación de los datos personales
    f. Bloqueo de los datos personales
    g. Anonimización
    h. Seudonimización
d) Los requisitos recogidos en el plan de acción resultante del análisis de riesgos en privacidad, o en su caso, de la evaluación de impacto en protección de datos, que sean diferentes a los recogidos en el análisis de riesgos de seguridad de la información conforme a [op.pl.1], y que deban implementarse en el sistema de información.
   Entre ellos, los requisitos de privacidad desde el diseño y por defecto, diferentes de los indicados en los apartados anteriores, con objeto de integrar las garantías para la protección de los derechos y libertados de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas y productos.

En caso de utilizarse la anonimización, se efectuará un análisis de riesgos de reidentificación de las personas titulares de los datos, que será, en su caso, aceptado por el Responsable del Tratamiento, con asesoramiento del delegado de protección de datos.

En caso de no ser posible la anonimización o la utilización de datos ficticios, y no sea estrictamente necesario el uso de datos personales, se aplicarán técnicas de seudonimización, con la verificación por el responsable del tratamiento, con el asesoramiento del delegado de protección de datos, que impida la reidentificación sin disponer de la información adicional que estará sujeta a medidas técnicas y organizativas para garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

4.18 [mp.info.1] Datos personales

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
ENS	aplica	aplica	aplica
Medidas Privacidad	requisito adicional [mp.info.1-p.1]	=	=

Los requisitos de protección de datos serán como mínimo los establecidos en el presente Anexo, identificados como medidas de privacidad.