CTEAJE

Comité Técnico Estatal de la Administración Judicial Electrónica

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA

CTEAJE
Comité Técnico Estatal de la Administración Judicial Electrónica

Ficha del Documento

NOMBRE DEL DOCUMENTO	Política de Seguridad de la Información de la Administración Judicial Electrónica
CÓDIGO DEL DOCUMENTO	CTEAJE - Política de Seguridad de la Información de la Administración Judicial Electrónica
VERSIÓN	2.0

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	GT BIS Seguridad	Aprobada en Pleno 30/10/2019	Política de Seguridad de la Información Judicial Electrónica. Aprobada en Pleno 30/10/2019
2.0	Oficina de Seguridad CTEAJE	Aprobada en Pleno 21/06/2024	• Cambios normativos: Principalmente por la Ley Orgánica 7/2021, de 26 de mayo), que modifica la LOPJ. • Asignación de los roles de seguridad de la información y protección de datos. • Diferenciación de tipos de sistemas de la Administración de Justicia: - Juzgados y Tribunales - Fiscalías - Auxiliares de la Administración de Justicia • Aprobación de normativa de desarrollo de la PSIJE en cada ámbito específico de aplicación. • Cambio de referencias normativas derivadas 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. • Cambio de denominación de la Política conforme al art. 93 del Real Decreto-ley 6/2023 • Se eliminan las funciones del Subcomité de Seguridad, reservado al futuro desarrollo reglamentario del Real Decreto-ley 6/2023

Índice

INTRODUCCIÓN

En cumplimiento del mandato contenido en el artículo 93 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 que deberá observarse en los sistemas y aplicaciones que prestan servicio a la Administración de Justicia, se desarrolla el contenido de la Política de Seguridad de la Información de la Administración Judicial Electrónica (PSIAJE).

La PSIAJE se ha elaborado de acuerdo con lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones competentes en materia de justicia y los servicios electrónicos e infraestructuras ya existentes, así como demás normativa concurrente en la materia, para el mejor cumplimiento de lo establecido en relación a las Bases del Esquema Judicial de Interoperabilidad y Seguridad, aprobadas por el Comité técnico estatal de la Administración judicial electrónica.

Asimismo, y respecto al tratamiento de datos personales también se ha considerado lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE, para las jurisdicciones civil, contencioso administrativo y social, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales.

En el ámbito penal en materia de protección de datos y a su libre circulación es de aplicación 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, que transpone al Derecho español la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

También se tendrán en cuenta las normas especiales contenidas en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables, así como, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal, en el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal.

Dado que la seguridad de la información debe responder a múltiples requisitos y abarca todos los aspectos de una organización, es fundamental abordarla de acuerdo con los estándares facilitados por normas nacionales e internacionales, y en particular, los facilitados por el Esquema Nacional de Seguridad, así como el Esquema Judicial de Interoperabilidad y Seguridad (EJIS). También se tendrá en consideración las normas UNE/ISO como la 22301

o la 27001, así como la normativa que pueda afectar a la custodia y conservación de archivos judiciales.

Todo ello sin perjuicio de que en la Administración de Justicia intervienen diversas administraciones en base a un sistema de reparto competencial, por lo que se ha procedido a adaptar la normativa referida en los párrafos anteriores a la realidad existente.

La transformación digital de la Administración de Justicia facilitará la relación entre los diferentes operadores jurídicos y, principalmente, con la ciudadanía, conciliando las actuaciones telemáticas con la seguridad jurídica digital.

Asimismo, la colaboración con las Comunidades Autónomas y la cooperación jurídica internacional, principalmente en el ámbito europeo, serán ámbitos comunes que exigirán la adopción de estándares de interoperabilidad y seguridad.

Un nuevo escenario de cogobernanza y de relaciones auspiciadas por la transformación digital, donde los datos se convierten en activos esenciales para una Administración de Justicia ágil y cercana a la ciudadanía, hace necesaria una estrategia de ciberseguridad, a desarrollar mediante una política de seguridad de la información, común para todos los operadores jurídicos, como pieza clave de la protección de los servicios digitales y la información.

ARTÍCULO 1. OBJETO Y ÁMBITO DE APLICACIÓN.

1. La finalidad de este documento consiste en definir la Política de Seguridad de la Información de la Administración Judicial Electrónica (PSIAJE) en la utilización de medios electrónicos en el ámbito de la Administración de Justicia, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. Esta política se 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.

3. Esta política afectará a la información, tanto de carácter jurisdiccional como no jurisdiccional, tratada por medios electrónicos, así como a toda la información en soporte no electrónico que haya sido causa o consecuencia directa de la citada información electrónica en la Administración de Justicia.

4. La PSIAJE será de obligado cumplimiento en el desarrollo de la actividad de los órganos y oficinas judiciales, y de las fiscalías por parte de todos sus integrantes.

También será de obligado cumplimiento para todo el personal destinado en los órganos, departamentos y unidades citados en el apartado 2, así como para aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso tanto a sus sistemas de información como a la propia información que sea gestionada por dichos órganos, departamentos y unidades, con independencia de cuál sea su destino, adscripción o relación.

ARTÍCULO 2. MISIÓN DE LA ORGANIZACIÓN.

La Administración de Justicia desarrolla las funciones encomendadas al Poder Judicial en la Constitución Española, al amparo de lo dispuesto en la Ley Orgánica 1/1985, de 6 de julio, del Poder Judicial, y en las correspondientes normas procesales.

El Consejo General del Poder Judicial es el órgano de gobierno del mismo, según el artículo 122.2 de la Constitución española, cuyas atribuciones vienen reguladas en los artículos 558 a 565 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Asimismo, e incardinado con autonomía funcional en el Poder Judicial, el Ministerio Fiscal tiene por misión promover la acción de la justicia en defensa de la legalidad, de los derechos de los ciudadanos y del interés público tutelado por la ley, de oficio o a petición de los interesados, así como velar por la independencia de los Tribunales, y procurar ante éstos la satisfacción del interés social.

Al Ministerio de Justicia y a las Comunidades Autónomas con competencias transferidas en materia de justicia les corresponde proveer a los juzgados, tribunales y fiscalías de los medios precisos para el desarrollo de su función.

ARTÍCULO 3. MARCO NORMATIVO.

En la toma de decisiones en materia de seguridad se deben tener en cuenta, entre otras, las siguientes normas:

a. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ).
b. Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.
c. 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.
d. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).
e. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD).
f. 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.

g. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las Instrucciones Técnicas de Seguridad publicadas en su desarrollo, sin perjuicio de las particularidades de la Administración de Justicia que requieran una concreta regulación.
h. Bases del Esquema Judicial de Interoperabilidad y Seguridad.
i. Normativa reguladora referente a la custodia y conservación de archivos judiciales.

ARTÍCULO 4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN.

1. Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a. Protección de los derechos fundamentales de los ciudadanos: La seguridad de la información contenida en los sistemas de la Administración de Justicia y los servicios prestados a través de ellos, deben tener como principio básico la protección de los derechos fundamentales de los ciudadanos, y en particular el derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión, la protección de las víctimas de delitos, menores y otras personas vulnerables, el respeto al derecho al honor, a la intimidad personal y familiar y a la propia imagen, a la protección de datos personales, y en general cualquier derecho que pueda verse afectado por un incidente de seguridad en los sistemas de información de la Administración de Justicia.

b. Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de las Instituciones y Administraciones competentes que participan en la Administración de Justicia para conformar un todo coherente y eficaz.

c. Responsabilidad diferenciada: en relación con los sistemas de información, cada una de las entidades a las que se le aplica esta política de seguridad será responsable en relación con las funciones contempladas en el artículo 6.

d. Seguridad como proceso integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. Se definirá la arquitectura de seguridad y la estructura y componentes que la integran y se mantendrá permanentemente actualizada. La seguridad de la información

debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

e. Gestión de la seguridad basada en Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

f. Proporcionalidad: El establecimiento de medidas de prevención, detección, respuesta y conservación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

g. Existencia de líneas de defensa: con objeto de evitar incidentes de seguridad y reaccionar ante los mismos existirán en los sistemas de información múltiples capas de seguridad que eviten y minimicen el impacto en su conjunto.

h. Vigilancia continua y reevaluación periódica: La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

i. Seguridad desde el diseño y por defecto: Los sistemas de información del ámbito de aplicación de la presente política de seguridad deben diseñarse y configurarse incluyendo medidas técnicas y organizativas que garanticen la seguridad.

2. Directrices fundamentales de seguridad

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSIAJE

y que inspiran las actuaciones de los Órganos, Departamentos y Unidades del ámbito de aplicación de la presente política. Se establecen los siguientes:

a. Protección de datos personales: se aplicarán a los tratamientos de datos personales las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

b. Gestión de activos de información: Los activos y sistemas de información de los Órganos, Departamentos y Unidades se encontrarán inventariados, categorizados y estarán asociados a un responsable. Respecto de los sistemas de información y en la medida que afecte al tratamiento de datos personales, se deberá elaborar un Registro de las actividades de tratamiento de conformidad con el art. 30 del RGPD y se deberá publicar en las sedes electrónicas y en el Punto de acceso general de la Administración de Justicia, previa coordinación y normalización del CTEAJE.

c. Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos. Periódicamente se llevarán a cabo actividades de concienciación y divulgación en materia de seguridad dirigidas a los usuarios, con el fin de que se mantengan permanentemente sensibilizados en sus obligaciones de seguridad. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

d. Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e. Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f. Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la

utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g. Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información; diseño, construcción, puesta en servicio, mantenimiento y retirada del sistema. Con anterioridad a la puesta en servicio de cualquier sistema de información, será obligatorio verificar que cumple los requisitos y especificaciones de seguridad que se hubieran establecido, garantizando su seguridad por defecto.

h. Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. Así como su comunicación con las Autoridades competentes, según corresponda, teniendo en cuenta que dicha comunicación, dependiendo del tipo de incidente, debe ser comunicada a la Dirección de Supervisión y Control de Protección de Datos del CGPJ, a la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado[1], a la Agencia Española de Protección de Datos, a la Agencia Vasca de Protección de Datos, a la Autoridad Catalana de Protección de Datos, al Consejo de Transparencia y Protección de Datos de Andalucía, o al Centro Criptológico Nacional.

i. Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios y se establecerán calendarios de prueba de los planes de continuidad establecidos con el fin de verificar que están correctamente operativos.

j. Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

ARTÍCULO 5. GESTIÓN DE RIESGOS.

Todos los sistemas de información y comunicación utilizados en la Administración de Justicia a los que afecte esta política se someterán a un análisis de riesgos para determinar las medidas de seguridad organizativas y técnicas que deben adoptarse, atendiendo a lo dispuesto en el ENS, el EJIS, la LOPJ, el RGPD, la LOPDGDD, y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención,

[1] Las referencias a la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado, en la presente política, deben entenderse efectuadas, mientras no se constituya dicho órgano, a la Unidad de Apoyo de la Fiscalía General del Estado.

detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Este análisis supondrá evaluar los riesgos y amenazas a los que están expuestos los sistemas de información y comunicación.

Para ello se deberá configurar lo siguiente:

- Plan de análisis.
- Criterios de evaluación de riesgos.
- Directrices de tratamiento.
- Proceso de aceptación del riesgo residual.

El análisis de riesgos se realizará al menos cada dos años, así como cuando:

- Se produzcan modificaciones sustanciales en
    - la información manejada.
    - los servicios prestados.
    - los activos de soporte de los sistemas.
- Ocurra un incidente grave de seguridad.
- Se reporten vulnerabilidades graves.

ARTÍCULO 6. ORGANIZACIÓN DE LA SEGURIDAD.

6.1 Responsabilidad diferenciada

Para dar cumplimiento a la diferenciación de responsabilidades, principio básico del Esquema Nacional de Seguridad y de la presente política, se identifican, las figuras de Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema.

Asimismo, se identifican las figuras de Responsable y Encargado del tratamiento de datos personales, en el ámbito de la protección de datos, de acuerdo con la LOPJ y el marco normativo en materia de protección de datos.

Esta identificación de responsabilidades se establecerá con respeto a las competencias de las Instituciones y Administraciones integrantes, en función de los sistemas de información, de acuerdo con los siguientes apartados.

6.1.1 Sistemas de información de Juzgados, Tribunales y Fiscalías

La responsabilidad del tratamiento de datos personales con fines jurisdiccionales, en relación a su respectivo marco de competencias y de facultades de actuación, recae en los órganos, oficinas judiciales y fiscalías, de conformidad con el artículo 236 bis de la LOPJ.

Las administraciones prestacionales asumen la condición de encargado del tratamiento de datos personales, de conformidad con sus competencias establecidas en los artículos 37 de la LOPJ, y disposición adicional segunda de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal, y de conformidad con las obligaciones previstas en los apartados 1 y 2 del artículo 236 sexies de la LOPJ.

La responsabilidad de la seguridad y del sistema recae en las administraciones prestacionales en base a las mismas disposiciones indicadas en el párrafo anterior, y será asumida por las personas físicas, órganos, órganos colegiados, organismos o entidades públicas designadas por las administraciones prestacionales de medios materiales.

6.1.2 Sistemas de información auxiliares de la Administración de Justicia

Están constituidos por aquellos sistemas de apoyo o auxiliares de la Administración de Justicia, cuya competencia y responsabilidad recae en órganos y organismos del Ministerio de Justicia y de las Comunidades Autónomas con competencias transferidas en materia de justicia, o en el CGPJ, en función del sistema.

La responsabilidad de la información y del servicio recaerá en los indicados órganos y organismos, o en el CGPJ.

La responsabilidad del tratamiento de datos personales será asumida por los citados órganos y organismos, o por el CGPJ, de conformidad con la normativa aplicable, sin perjuicio de aquellos supuestos en que se pueda actuar como encargados de tratamiento.

La responsabilidad de la seguridad y del sistema será asumida por la persona física u órgano colegiado designado por la correspondiente administración prestacional de medios materiales, o por el CGPJ.

6.2 Funciones específicas

6.2.1 Consejo General del Poder Judicial

- Elaboración de instrucciones y recomendaciones en materia de seguridad.
- Promover la seguridad de la información entre Jueces y Magistrados.

6.2.2 Ministerio de Justicia

El Ministerio de Justicia, a través del Secretario General de la Administración de Justicia:

- Elaboración de instrucciones y recomendaciones en materia de seguridad.
- Promover la seguridad de la información respecto a los Letrados de la Administración de Justicia.

6.2.3 Fiscalía General del Estado

- Elaboración de instrucciones y recomendaciones en materia de seguridad
- Promover la seguridad de la información respecto a los Fiscales.

6.2.4 Juzgados/Tribunales

- Verificar el cumplimiento de las medidas de seguridad en su ámbito de actuación conforme a sus responsabilidades.

6.2.5 Ministerio de Justicia y Administraciones con competencia en materia de justicia, o CGPJ en función de los sistemas auxiliares

1. En el Ministerio de Justicia, y en las Administraciones con competencias en materia de Justicia, a través de sus órganos y organismos, o en el CGPJ, recae la responsabilidad de la información, servicios, seguridad y sistemas, así como la responsabilidad del tratamiento de datos personales, sin perjuicio de aquellos supuestos en que se pueda actuar como encargado de tratamiento, respecto de los sistemas auxiliares de la Administración de Justicia, de acuerdo con sus competencias y en función del sistema.

Para los sistemas auxiliares de la Administración de Justicia, estas administraciones o el CGPJ asumirán las siguientes funciones:

- Aprobación de la categorización y de los niveles de riesgos, así como la realización de las evaluaciones de impacto relativas a la protección de datos, respecto de los tratamientos de datos efectuados a través de los sistemas.
- Promoverán la seguridad de la información respecto del personal bajo su dependencia orgánica y funcional.

2. Las administraciones prestacionales, de conformidad con sus competencias, y con lo establecido en los apartados 1 y 2 del artículo 236 sexies LOPJ, proveerán de sistemas de información a los órganos y oficinas judiciales y fiscales que garanticen que el tratamiento de datos que se lleve a cabo a través de dichos sistemas cumpla con las obligaciones previstas en el marco normativo aplicable.

A tal efecto, estas administraciones asumirán todas las funciones relativas a la gestión del riesgo que les corresponden como encargados del tratamiento de datos y como entidades prestacionales de sistemas de información, incluyendo la realización de las evaluaciones de impacto de la protección de datos.

La aprobación de las propuestas, que efectúen las administraciones, de valoración de las dimensiones de seguridad, de aceptación de los riesgos residuales resultado de los análisis de riesgos y de las evaluaciones de impacto, será efectuada respecto de la información y del tratamiento de datos efectuados a través de los sistemas puestos a disposición de Juzgados y Tribunales, por las personas designadas por el CGPJ y por el Secretario General de la Administración de Justicia, y respecto de los sistemas del Ministerio Fiscal, por las personas designadas por la FGE.

Con objeto de lograr decisiones consensuadas con los responsables de seguridad, de los sistemas, o en su caso encargados del tratamiento de datos, se adoptarán en el seno de los Comités de Seguridad de las Administraciones prestacionales, primando en todo caso el criterio de las referidas instituciones. No obstante, mientras no se lleven a cabo las designaciones indicadas por el CGPJ, por el Secretario General de la Administración de Justicia y por la FGE, las administraciones asumirán las funciones antes asignadas a estas instituciones.

Para la determinación del nivel de seguridad de cada dimensión de seguridad las administraciones prestacionales deberán aplicar los criterios de valoración que determinen en el Subcomité de Seguridad del CTEAJE.

3. En el Ministerio de Justicia, y en las Administraciones con competencias en materia de Justicia, recaerá la responsabilidad de la seguridad y la responsabilidad del sistema de los sistemas de información puestos al servicio de los Juzgados y Tribunales, Fiscalías, y de los sistemas auxiliares de la Administración de Justicia bajo su competencia. Para los sistemas auxiliares bajo la competencia del CGPJ, estas responsabilidades de la seguridad y del sistema recaerán en el propio CGPJ.

A tal efecto, los órganos internos del Ministerio de Justicia y Administraciones con competencias en materia de Justicia o del CGPJ procederán a la designación del Responsable de Seguridad y del Responsable del Sistema de información, cuyos nombramientos se revisarán cada dos años o cuando el puesto quede vacante, que asumirán las funciones y responsabilidades previstas en el ENS, EJIS, la presente política de seguridad y su desarrollo normativo.

El Ministerio de Justicia, las Administraciones con competencias en materia de Justicia o el CGPJ asumirán, entre otras, las siguientes funciones:

<u>De la gestión de seguridad de la información:</u>

a. Promover las medidas de seguridad tecnológicas y organizativas en el ámbito de sus competencias prestacionales en materia TIC y de suministros de medios materiales, de conformidad con el marco jurídico de transferencias en materia de medios materiales en la Administración de Justicia. Así como, en su caso, promover el uso y cumplimiento de las medidas de seguridad que corresponda entre el personal de la Administración de Justicia dependiente de cada uno de ellos y del personal que participe en cualquier fase o ciclo de los sistemas de información, que se ponen al servicio de la Administración de Justicia, en los que son competentes.

b. Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

c. Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

d. La coordinación y control del cumplimiento de las medidas de seguridad definidas en los documentos y normas que desarrollen la presente política.

e. El desarrollo, la operación y mantenimiento de los sistemas de información durante su ciclo de vida completo, así como elaborar la normativa de seguridad de tercer nivel a la que se refiere el artículo 9 de la presente política.

f. La elaboración de la documentación de segundo nivel y tercer nivel, referida en el artículo 9 de la presente política y su mantenimiento de forma organizada y actualizada.

Del análisis de riesgos:

Realizar y elevar para su aprobación la categorización y los niveles de riesgos de los sistemas de información puestos al servicio de Juzgados y Tribunales, y Fiscalías, así como, en su caso, las evaluaciones de impacto con el asesoramiento y supervisión del delegado de protección de datos. En el caso de los sistemas auxiliares de la Administración de Justicia, las propuestas serán sometidas a aprobación en la propia administración prestacional, o en el CGPJ, si el sistema auxiliar es de su responsabilidad.

De la gestión de incidencias:

a. La gestión, así como la comunicación y, en su caso, coordinación de gestiones de incidencias, según corresponda, al Centro Criptológico Nacional, Dirección de Supervisión y Control de Protección de Datos del CGPJ, la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado y Agencia Española de Protección de Datos.

b. La comunicación de incidencias de seguridad más relevantes por a las administraciones prestacionales al Subcomité de Seguridad del CTEAJE.

c. La elaboración de informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.

De la mejora continua:

a. Disponer de un sistema de gestión de seguridad de la información que permita la citada mejora continua.

b. La elaboración de un informe de revisión anual sobre el estado de la seguridad.

c. La realización de auditorías periódicas internas o externas para verificar el cumplimiento de las obligaciones con relación a la seguridad de la información.

De la formación y concienciación:

Impulsar la formación y concienciación en materia de seguridad de la información de conformidad con el artículo 12 de la presente política de seguridad.

ARTÍCULO 7. EL DELEGADO DE PROTECCIÓN DE DATOS.

En aquellas Instituciones y Administraciones a las que afecta esta política de seguridad, que hayan procedido a la designación de un Delegado de Protección de Datos, podrán recabar del mismo, el asesoramiento cuando la seguridad afecte al tratamiento de datos personales.

El Delegado de Protección de Datos podrá realizar también funciones de supervisión conforme a lo regulado en el RGPD.

ARTÍCULO 8. COORDINACIÓN DE LAS ACCIONES DERIVADAS DEL CUMPLIMENTO DE LA PSIAJE.

1. De acuerdo con el artículo 85.2 e) del Real Decreto-ley 6/2023, de 19 de diciembre, se establece el marco organizativo en materia de ciberseguridad judicial a través del Subcomité de Seguridad, como un órgano especializado y permanente para la ciberseguridad judicial, en el seno del CTEAJE, integrado por aquellas personas con responsabilidad en materia de seguridad, de cada una de las Instituciones y administraciones integrantes.

3. A través del despliegue del Centro de Operaciones de Ciberseguridad de la Administración de Justicia, de acuerdo con lo establecido en el artículo 96 del Real Decreto-ley 6/2023, de 19 de diciembre, para la prestación de servicios horizontales de ciberseguridad que apoyen las capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y gestión de la ciberseguridad, que permita una mejor eficacia y eficiencia, se llevarán a cabo las siguientes actividades:

    a. Apoyo a la gestión de incidentes de seguridad judicial electrónica de los sistemas de información y de comunicaciones de la Administración de Justicia, sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración con competencias en materia de Justicia e instituciones judiciales sometidas al Real Decreto-ley 6/2023, y de la función de coordinación a nivel nacional e internacional del Equipo de Respuesta para Emergencias Informáticas del Centro Criptológico Nacional (CCN-CERT).
    b. Apoyo a las auditorías técnicas y a la gestión de vulnerabilidades de seguridad judicial electrónica de los sistemas de información y de comunicaciones de la Administración de Justicia.

4. Cada una de las Administraciones e instituciones que hayan designado un Delegado de Protección de Datos, podrán invitarlo a las reuniones de este Subcomité cuando se analicen cuestiones que afecten a la seguridad del tratamiento de datos personales.

5. El Subcomité se reunirá periódicamente y con carácter extraordinario cuando lo decida la Presidencia.

6. El Subcomité podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

ARTÍCULO 9. DESARROLLO NORMATIVO.

1. El cuerpo normativo sobre seguridad de la información, contemplado en la presente política, se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

    a. Primer nivel normativo: constituido por la PSIAJE, las directrices generales de las políticas de seguridad y normas generales aplicables a todas las Instituciones y Administraciones competentes, que conforme al artículo 1, les sea de aplicación la presente política.

    b. Segundo nivel normativo: constituido por las normas de seguridad, desarrolladas por las Instituciones y Administraciones competentes que, conforme al artículo 1, les sea de aplicación la presente política. Estas normas de seguridad deberán cumplir los siguientes requisitos:

        I. Limitarse única y exclusivamente al ámbito específico de las competencias de cada una de esas Instituciones y Administraciones competentes, adscritas a la presente política. Este ámbito vendrá determinado por los sistemas de información, y servicios de tecnologías de la información y de las comunicaciones, que sean prestados y gestionados directamente por dichas Instituciones y Administraciones.

        II. Cumplir estrictamente con lo indicado en el EJIS/ENS y con el primer nivel normativo enunciado en el presente artículo.

        III. Deberán ser aprobadas dentro del ámbito de cada una de las Instituciones y Administraciones competentes adscritas a la presente política.

        IV. El Subcomité de Seguridad verificará que las normas de segundo nivel reúnan los requisitos establecidos en los apartados I y II anteriores.

    c. Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSIAJE, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel normativo deberá cumplir los siguientes requisitos:

        I. Limitarse única y exclusivamente al ámbito específico de las competencias de cada una de las Instituciones y Administraciones competentes adscritas a la presente política. Este ámbito vendrá determinado por los sistemas de información, y servicios de

tecnologías de la información y de las comunicaciones, que sean prestados y gestionados directamente por dicho órgano u organismo.

II. Cumplir estrictamente con lo indicado en el EJIS/ENS y con el primer y segundo nivel normativos enunciados en el presente artículo.

III. Deberán ser aprobados dentro del ámbito de cada una de las Instituciones y Administraciones competentes adscritas a la presente política.

IV. La estructura normativa podrá disponer, a criterio de cada una de las Instituciones y Administraciones competentes adscritas a la presente política, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como estándares de seguridad, buenas prácticas o informes técnicos.

2. El personal de cada una de las Instituciones y Administraciones competentes, adscritos a la presente política, tendrá la obligación de conocer y cumplir todas las directrices generales, normas y procedimientos de seguridad de la información, que sean aprobadas en desarrollo de esta política y que afecten a sus funciones.

3. El Subcomité de Seguridad del CTEAJE establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo, con el propósito de normalizarlo en todo el ámbito de aplicación de la PSIAJE.

4. Este marco normativo estará a disposición de todos los miembros del CTEAJE.

5. El Subcomité de Seguridad del CTEAJE, analizará los desarrollos normativos de aplicación específica a los respectivos ámbitos de competencias con objeto proponer al Pleno del CTEAJE su aplicación a todo el ámbito de la PSIAJE.

ARTÍCULO 10. TERCERAS PARTES.

1. Cuando se utilicen servicios de terceros se les hará partícipes de esta política y de la Normativa de Seguridad que ataña a dichos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en la presente normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política.

   Si estos servicios de terceros consistiesen en el tratamiento de datos personales, deberán adoptar, a los efectos de lo dispuesto en la Disposición Adicional Primera de la LOPDGDD, el Esquema Nacional de Seguridad.

2. Cuando algún aspecto de la PSIAJE no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se requerirá un informe, por parte de quien tenga asignadas funciones de responsabilidad en materia de seguridad, que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por aquellos a los que les pueda afectar el contenido del mismo.

ARTÍCULO 11. PROTECCIÓN DE DATOS PERSONALES Y AUTORIDADES DE CONTROL.

1. En lo referente a los datos personales, que sean objeto de tratamiento por los sistemas de información y comunicación de la Administración de Justicia, se adoptarán las medidas técnicas y organizativas que corresponda implantar, derivadas de los riesgos generados por el tratamiento, una vez llevado a cabo el análisis de riesgos exigido por el RGPD, y sin perjuicio de aquellas situaciones en las que se requiera con carácter previo realizar una Evaluación de Impacto de la Protección de Datos.

2. El Ministerio de Justicia y las Administraciones con competencias transferidas en la dotación de medios materiales, velarán por el mantenimiento de un nivel óptimo de seguridad en la gestión de los sistemas de información e infraestructuras tecnológicas puestos al servicio de la Administración de Justicia, en calidad de responsables o encargados del tratamiento, así como para la Fiscalía General del Estado, a través de su Comisión Nacional de informática y comunicaciones electrónicas.

3. En todo caso, la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial, y la Unidad de Supervisión y Control de Protección de Datos de la Fiscalía General del Estado, en ejercicio de las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizados respectivamente por Juzgados, Tribunales y oficinas judiciales, y por el Ministerio Fiscal u oficinas fiscales, ostentan la facultad de dictar las instrucciones que estime necesarias en el ejercicio de sus funciones y poderes atribuidos por la LOPJ, el RGPD, LOPDGDD y Ley Orgánica 7/2021, en aquellos supuestos que sean de aplicación.

4. A los efectos de realizar el análisis de riesgos en los tratamientos de datos personal de la Administración de Justicia, con la finalidad de adoptar las correspondientes medidas de seguridad, se seguirá para tal fin lo dispuesto en el Esquema Judicial de Interoperabilidad y Seguridad, y en el Esquema Nacional de Seguridad.

ARTÍCULO 12. FORMACIÓN Y CONCIENCIACIÓN.

1. La seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo al principio de seguridad como proceso integral recogido en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como en la presente política, lo que exige el desarrollo de actividades formativas específicas orientadas a la concienciación y formación de los

empleados públicos adscritos a la Administración de Justicia, así como la difusión entre los mismos de la PSIAJE y su desarrollo normativo.

2. El Subcomité de Seguridad del CTEAJE podrá encargarse de promover, a través de las Instituciones y Administraciones competentes, la realización de actividades de formación y concienciación en materia de seguridad judicial, que incluyan la difusión y conocimiento del contenido de esta política, así como de aquellas normas, guías o instrucciones que se dicten en desarrollo de la misma. Este tipo de actividades se planificarán al menos con una periodicidad anual.

3. En todo caso, cada una de las Instituciones y Administraciones afectadas realizarán las actividades formativas propuestas en relación con el personal dependiente de cada una de ellas.

ARTÍCULO 13. ACTUALIZACIÓN.

1. Esta política deberá mantenerse actualizada para adecuarla al progreso de los servicios de la Administración de Justicia, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares nacionales e internacionales de seguridad.

2. Las propuestas de las sucesivas revisiones de esta política las hará el Subcomité de Seguridad del CTEAJE.