POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA

(PSIJE Versión 0.1.17)

Grupo de trabajo de Bases de interoperabilidad y seguridad del CTEAJE (BIS)

Mayo de 2019

Índice

Introducción

En cumplimiento del mandato contenido en el artículo 47.2.b) y en desarrollo del artículo 54 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia 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 Judicial Electrónica (PSIJE).

La PSIJE se ha elaborado teniendo en cuenta 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 de carácter personal 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, a partir del 25 de mayo de 2018 (RGPD), así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales (LOPDGDD).

En el ámbito penal en materia de protección de datos y a su libre circulación será de aplicación una vez transpuesta 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. Hasta que no se produzca dicha transposición, y en aplicación de la Disposición Transitoria Cuarta de la LOPDGDD, se aplica la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, en particular su artículo 22, así como sus disposiciones de desarrollo.

Dado que la seguridad de la información debe responder a múltiples requisitos y abarca todos los aspectos de una organización, es fundamental abordarla teniendo en cuenta estándares facilitados por normas nacionales e internacionales, y en particular, los facilitados por el Esquema Nacional de Seguridad (ENS) 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.

Artículo 1. Objeto y ámbito de aplicación.

1. La finalidad de este documento consiste en definir la Política de Seguridad de la Información Judicial Electrónica (PSIJE) 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. La PSIJE 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, FGE, Ministerio de Justicia y CCAA que tienen transferidas las competencias en esta materia así como los organismos públicos que dependan de los mismos.

3. La PSIJE 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 PSIJE 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 personales que, aunque no estén destinados 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.

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 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

b) 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.

c) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

d) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en virtud de lo establecido en su Disposición Transitoria Cuarta, principalmente su artículo 22, mientras no se produzca la transposición de la Directiva 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).

e) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de la Seguridad en el ámbito de la Administración Electrónica.

f) Bases del Esquema Judicial de Interoperabilidad y Seguridad.

e) Normativa reguladora referente a la custodia y conservación de archivos judiciales.

Artículo 4. Principios de la seguridad de la información.

4.1. 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) 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.

b) 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.

c) Seguridad 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.

d) Gestión de 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.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: 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.

g) Seguridad desde el diseño y por defecto: Los sistemas de gestión procesal deben diseñarse y configurarse incluyendo medidas técnicas y organizativas que garanticen la seguridad.

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

a) Protección de datos de carácter personal: 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 de carácter personal, 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, previo 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 dirigido 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 al Consejo General del Poder Judicial, a la Agencia Española de Protección de Datos 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 Análisis de riesgos.

Todos los sistemas de información y comunicación utilizados en la Administración de Justicia a los que afecte esta PSIJE se someterán a una análisis de riesgos para determinar las medidas de seguridad organizativas y técnicas que deben adoptarse, atendiendo a lo dispuesto en el ENS, el EJIS, el RGPD y la LOPDGDD.

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:

a) Plan de análisis.
b) Criterios de evaluación de riesgos.
c) Directrices de tratamiento.
d) Proceso de aceptación del riesgo residual.
e) Proceso de revisión de la política de seguridad.

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

a) Cambien la información manejada.
b) Cambien los servicios prestados.
c) Ocurra un incidente grave de seguridad.
d) Se reporten vulnerabilidades graves.

Artículo 6. Funciones.

A los efectos de dar cumplimiento a la PSIJE a cada uno de los sujetos intervinientes se les asigna, al menos, las siguientes funciones:

Consejo General del Poder Judicial:

Elaboración de instrucciones y recomendaciones en materia de seguridad.

Aprobar los niveles de riesgos propuestos por las administraciones prestatarias.

Aprobar la categorización de los sistemas de información de Juzgados y Tribunales.

Promover la seguridad de la información entre Jueces y Magistrados.

Ministerio de Justicia:

Promover la seguridad de la información respecto a los Letrados de la Administración de Justicia.

Fiscalía General del Estado:

Promover la seguridad de la información respecto a los Fiscales.

Aprobar los niveles de riesgos propuestos por las administraciones prestatarias.

Aprobar la Categorización de los sistemas de información Fiscal.

Ministerio de Justicia y Administraciones con competencia en materia de justicia:

De la gestión de seguridad de la información:

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

c) 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 PSIJE.

d) La elaboración de la documentación de tercer nivel, y sucesivos, referida en el artículo 9 de la presente PSIJE y su mantenimiento de forma organizada y actualizada.

Del análisis de riesgos:

a) Proponer la categorización de los sistemas que prestan auxilio a la Administración de Justicia.

b) El impulso y la realización de análisis de riesgos sobre los sistemas de información que se pongan a disposición de la administración de justicia, así como proponer el nivel de riesgo aceptable al Consejo General del Poder Judicial, para que en su condición de Autoridad de Protección de Datos, lo apruebe si así lo considera.

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, Consejo General del Poder Judicial y Agencia Española de Protección de Datos.

b) La comunicación de incidencias de seguridad a sus respectivos Comités de Seguridad de las administraciones prestacionales, así como las más relevantes al Subcomité de Seguridad del CTEAJE.

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.

Juzgados/Tribunales:

Verificar el cumplimiento de las medidas de seguridad en su ámbito de actuación.

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 de carácter personal.

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 PSIJE del CTEAJE.

1. Se crea el Subcomité de Seguridad como un órgano especializado y permanente para la seguridad judicial electrónica en el seno del CTEAJE, integrado por aquellas personas con responsabilidad en materia de seguridad de cada una de las instituciones integrantes o en su caso por aquellos designados en representación de cada Comité de Seguridad de la Información, así como por las personas que se designe por el CGPJ y la FGE.

2. Entre las actividades a llevar a cabo por este Subcomité de Seguridad destacar las siguientes:

a) Actualización y mantenimiento de la PSIJE y elevarla para su aprobación en su caso al Pleno del CTEAJE.

b) Elaboración, actualización y mantenimiento de la Guía Técnica de Seguridad para su posterior elevación al Pleno para su aprobación.

c) Recabar las propuestas de normas de desarrollo de la PSIJE de segundo nivel, según lo previsto en el apartado 9, por parte de cada una de las Instituciones Judiciales, para su posterior elevación al Pleno del CTEAJE.

d) Crear un marco de trabajo para recoger las posibles iniciativas de seguridad que se lleven a cabo en los sistemas informáticos y de comunicaciones que dan soporte a los sistemas de la Administración de Justicia, por parte del Ministerio de Justicia, CGPJ, FGE y de las CC.AA. que tienen las competencias transferidas en esta materia, con el objetivo de crear estándares comunes en seguridad judicial electrónica.

d) Participar activamente en la elaboración y revisión de las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones en la parte que afecte a la seguridad judicial.

e) Impulsar la mejora permanente del proceso de seguridad en los sistemas utilizados por la Administración de Justicia.

f) Poner a disposición del Ministerio de Justicia, Fiscalía General del Estado, Consejo General del Poder Judicial y de las CC.AA. con las competencias transferidas en esta materia, la información disponible en el presente Subcomité de Seguridad.

g) Participar en eventos, foros, seminarios y cursos relacionados con la seguridad de la información con el fin de que el Subcomité de Seguridad esté al día en este ámbito.

h) Cualquier otra actividad que se considere de interés en el ámbito de la seguridad judicial electrónica.

3. 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 de carácter personal.

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

5. 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 contemplada en la presente PSIJE 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 PSIJE, las directrices generales de las

políticas de seguridad aplicables a las instituciones y Administraciones competentes, conforme al artículo 1, sea de aplicación la presente PSIJE del CTEAJE.

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 PSIJE. 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 adscritos a la presente PSIJE. 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 y con el primer nivel normativo enunciado en el presente artículo.

iii. Ser aprobadas conjuntamente tanto por el ámbito de cada una de las instituciones y Administraciones competentes adscritas a la presente PSIJE, como por el Subcomité de Seguridad, informando de esta aprobación al Pleno del CTEAJE. No obstante, en aquellos supuestos que así se considere, se podrá elevar al Pleno del CTEAJE su aprobación.

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSIJE, 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 PSIJE. 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 y con el primer y segundo nivel normativos enunciados en el presente artículo.

iii. Deberá ser aprobado dentro del ámbito de cada una de las instituciones y Administraciones competentes adscritas a la presente PSIJE por el Comité de seguridad de la información.

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

El personal de cada una de las Instituciones y Administraciones competentes adscritos a la presente PSIJE 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 PSIJE 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 PSIJE.

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

Artículo 10. Terceras partes.

1.Cuando se utilicen servicios de terceros se les hará partícipes de esta PSIJE 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 PSIJE.

Si estos servicios de terceros consistiesen en el tratamiento de datos de carácter personal, 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 PSIJE 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 de carácter personal y Autoridad de Control.

1. En lo referente a los datos de carácter personal 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 atendidos los riesgos generados por el tratamiento una vez llevada 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 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, el CGPJ como autoridad de protección de datos de los tratamientos jurisdiccionales podrá dictar las instrucciones que estime necesarias en el ejercicio de sus funciones y poderes atribuidos tanto por la LOPJ, el RGPD y la LOPDGDD.

4. A los efectos de realizar el análisis de riesgos en los tratamientos de datos de carácter 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 /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 Integral recogido en el Artículo 53 de la Ley 18/2011 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 PSIJE y su desarrollo normativo.

2. El Subcomité de Seguridad del CTEAJE podrá encargarse de promover, a través de los comités de seguridad 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 PSIJE 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 PSIJE 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 PSIJE las hará el Subcomité de Seguridad del CTEAJE.