III OTRAS RESOLUCIONES

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

RESOLUCIÓN de 3 de julio de 2018, de la Vicepresidenta y Consejera, por la que se ordena la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Junta de Extremadura de 26 de junio de 2018 por el que se establece la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura. (2018061663)

Habiéndose aprobado el Acuerdo del Consejo de Gobierno de la Junta de Extremadura de 26 de junio de 2018 por el que se establece la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura, y teniendo en cuenta que en su apartado segundo se indica que este acuerdo empezará a surtir efectos el mismo día de su publicación en el Diario Oficial de Extremadura, se

R E S U E L V E :

Ordenar la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Junta de Extremadura de 26 de junio de 2018 por el que se establece la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura.

Mérida, 3 de julio de 2018.

La Vicepresidenta y Consejera de Hacienda
y Administración Pública,

PILAR BLANCO-MORALES LIMONES

A N E X O

ACUERDO DEL CONSEJO DE GOBIERNO DE LA JUNTA DE EXTREMADURA DE 26 DE JUNIO DE 2018 POR EL QUE SE ESTABLECE LA POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA

La Junta de Extremadura tiene como misión servir con objetividad a los intereses generales y procurar satisfacer, con eficacia y eficiencia, las necesidades públicas, de conformidad con los principios constitucionales y estatutarios, para beneficio de la ciudadanía.

En la Ley Orgánica 1/2011, de 28 de enero, de reforma del Estatuto de Autonomía de la Comunidad Autónoma de Extremadura se impone, entre otros, "facilitar el acceso a las nuevas tecnologías de la información y comunicación a los ciudadanos y empresas" (artículo 7), ajustar su actuación a "los principios de buena fe, confianza legítima, transparencia, calidad en el servicio a los ciudadanos" (artículo 37.2) y como medidas de buena administración "regular los procedimientos administrativos propios y adaptar los procedimientos generales para dar celeridad y transparencia a la tramitación administrativa, para extender las relaciones interadministrativas y con los ciudadanos por medios telemáticos y para la simplificación de trámites" (artículo 39.2).

De acuerdo con ello, la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura, previene que la buena administración y el buen gobierno administrativo deberán ser informados por los principios previstos en la normativa básica del Estado y otros tales como de modernización, accesibilidad y prevención dirigidos a impulsar el proceso de transformación digital de la Administración pública.

Dichas previsiones deben ser contextualizadas en el nuevo marco de actuación del sector público definido por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que imponen el funcionamiento de las Administraciones Públicas, por medios electrónicos, para satisfacción de la ciudadanía preservando la protección de datos de carácter personal y, en particular, la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones que dispongan para prestar servicios públicos.

En relación con este ámbito, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, establece la necesidad que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política de seguridad que cumpla los principios básicos y requisitos mínimos que precisa para procurar una protección adecuada de la información y requiere así como la necesidad de que se apruebe por el titular del órgano superior.

A nivel autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura, cuyo ámbito de aplicación se

extiende a la Administración de la Comunidad Autónoma, los organismos públicos vinculados o dependientes de la misma sujeto a derecho público y los restantes organismos cuando ejerzan potestades públicas, a la ciudadanía y a las relaciones con otras Administraciones Públicas establece en su disposición adicional séptima que el Consejo de Gobierno establecerá una Política de Seguridad de la Información, "donde se marcarán las directrices de la Administración para garantizar el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias". "La Política de Privacidad y Seguridad de la Información será reglamentariamente desarrollada por la Consejería competente en materia de administración electrónica, a través del órgano directivo competente conforme al apartado tercero de la disposición adicional séptima del Decreto 225/2014".

Dicha Política debe ser coherente con la Estrategia de Ciberseguridad de la Unión Europea y las exigencias del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que sienta las bases de una normativa de privacidad, en el auge de la economía digital, para garantía de los derechos de la ciudadanía y cuyas previsiones superan a las que se desprenden de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos y del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo.

Por todo lo anterior, resulta oportuno e idóneo establecer la Política de Privacidad y Seguridad de la Información de la Comunidad Autónoma de Extremadura que define la directrices de la Administración para garantizar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad de los datos que dispone, conserva y obtiene en la prestación de los servicios de interés público para preservar e incrementar la confianza de la ciudadanía.

A estos efectos, a propuesta de la Comisión de Coordinación de Administración Electrónica, previa iniciativa de la Secretaria General de Administración Pública conforme a lo dispuesto en la disposición adicional séptima del Decreto 225/2014, de 14 de octubre, de régimen jurídico de la administración electrónica de la Comunidad Autónoma de Extremadura en relación con el artículo 5 del Decreto 261/2015, por el que se aprueba la estructura orgánica de la Consejería de Hacienda y Administración Pública de la Comunidad Autónoma de Extremadura, se establece, por Acuerdo del Consejo de Gobierno, la Política de Privacidad y Seguridad. Todo ello conforme al artículo 11.2 del citado Real Decreto 3/2010, de 8 de enero, que considera que son órganos superiores, los responsables directos de la ejecución de la acción del gobierno de acuerdo con lo establecido en sus propias normas de organización.

En este sentido, el contenido del documento que se somete a aprobación del Consejo de Gobierno está determinado por la normativa básica estatal y autonómica. Así, el Real Decreto 3/2010 regulador del Esquema Nacional de Seguridad, en su anexo II, Sección 3.1 precisa que "la política de seguridad se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente: a) Los objetivos o misión de la organización; b) El

marco legal y regulatorio en el que se desarrollarán las actividades; c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación; d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización; y e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso".

La disposición adicional séptima de Decreto 225/2014 indica en su apartado segundo "la Política de Seguridad de la Información de la Comunidad Autónoma de Extremadura cumplirá los principios básicos y los requerimientos mínimos recogidos en Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad".

Con estas premisas, la Política que sea de aplicación en nuestra administración pública, necesariamente tiene que cumplir con el contenido prescrito en el Esquema Nacional de Seguridad, que además de lo indicado en el anexo II ya enunciado, en su artículo 10 configura la seguridad como función diferenciada en la que se contemplan varios roles posibles, debiendo detallar la correspondiente política de la seguridad las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos, exigiendo el artículo 11 que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente.

Atendiendo a estas previsiones y resultando que en la Administración de la Comunidad Autónoma de Extremadura la competencia sobre administración electrónica y la gestión de los sistemas de información y comunicaciones se ejerce de forma horizontal, por la Secretaria General de Administración Pública y la Dirección General de Tecnologías de la Información respecto a todas las áreas de gobierno, resulta oportuno diseñar un modelo de política que permita definir un marco común en toda nuestra Administración Pública ajustado a las previsiones, no pudiendo desconocer sus requerimientos mínimos ni desarrollarlos de otro modo pues se correría el riesgo de dejar de tener la consideración de política como anteriormente se ha señalado.

Por todo ello, el documento ha sido elaborado cumpliendo dichos requerimientos sin incorporar al ordenamiento organizativo otras funciones o responsabilidades de las definidas por la Ley 1/2002, de Gobierno de la Comunidad Autónoma de Extremadura.

El alcance de la política se extiende de las previsiones y requisitos del Esquema Nacional de Seguridad a la normativa de protección de datos bajo la consideración que esta última forma parte de la seguridad de la información, lo que se desprende de la inclusión de ambas materias en el derecho de la ciudadanía a que refiere el artículo 13 h) de la Ley 39/2015, de 1 de octubre.

De acuerdo con ello, los principios, requisitos mínimos y otras referencias contenidas en la Política de Privacidad y Seguridad de la información se han elaborado considerando el conjunto de normas de dichos ámbitos normativos. En particular se han considerado las

Guías CCN-STIC de Seguridad, que constituyen un cuerpo de normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia, con el fin de mejorar el grado de ciberseguridad de las organizaciones (CCN-STIC-805 Política de Seguridad de la Información, CCN-STIC-830 Ámbito de aplicación del Esquema Nacional de Seguridad, CNN-STIC-800 Glosario de términos y abreviaturas del ENS, CCN-STIC-801 Responsabilidades y Funciones en el ENS).

En este sentido, se ha propuesto describir las directrices con un lenguaje sencillo y simplificado evitando en la medida de lo posible los tecnicismos para facilitar su entendimiento por toda la organización. Por todo ello, se estima que el contenido de la Política cumple sobradamente con el contenido legalmente impuesto.

La aprobación por el Consejo de Gobierno de la Política debe adoptar la forma de acuerdo considerando que su contenido está definido reglamentariamente por la normativa superior de carácter básica y que la necesidad de establecerse por el Consejo de Gobierno está impuesta por la disposición adicional séptima del Decreto 225/2014, aprobado en el momento que estaba vigente el Real Decreto 3/2010, sin requerir su desarrollo reglamentario.

La normativa básica reguladora del Esquema Nacional de Seguridad requiere, entre otros aspecto, "la inclusión de roles y funciones de seguridad con sus correspondientes atribuciones" y dichas funciones están determinadas legalmente al precisarse, por ejemplo, que son "los órganos superiores de las Administraciones Públicas los que deben aprobar la política y asumir la responsabilidad respecto a las áreas específicas" (artículo 11 del Real Decreto 3/2010).

De acuerdo con ello, la propuesta organizativa incluida en la política se realiza de conformidad con los mandatos de la normativa superior (sometida a los trámites de información) consistiendo en una simple contextualización de dichas previsiones en la estructura organizativa de la Administración autonómica considerando lo que se precisa en la Ley 1/2002, de 28 de febrero, de la Administración de la Comunidad Autónoma de Extremadura respecto a las funciones y responsabilidades que deben asumir los respectivos órganos que se estructura la acción de gobierno administrativa tales como Presidente, Consejeros, Secretarias Generales de las Consejerías y órganos directivos.

El documento no contempla funciones distintas de las que legalmente se desprenden del marco normativo de lo que viene impuesto legalmente en leyes, reglamentos europeos, normativa sobre seguridad de la información y preceptos del Decreto 225/2014. A modo de ejemplo la atribución al Consejo de Gobierno de la competencia para definir para la Estrategia de Privacidad y Seguridad de la Información, que habrá de informar la acción de gobierno de la ACAEx estableciendo las condiciones necesarias de confianza en la ciudadanía para el ejercicio de sus derechos y cumplimiento de las obligaciones y que será aprobada a propuesta de la Consejería con competencias en materia de administración electrónica tiene su sede en lo dispuesto en el artículo 12 del Decreto autonómico. Conforme al mismo, el Consejo de Gobierno le corresponde aprobar la política y estrategia de administración electrónica en la que estimamos embebida la estrategia en este ámbito de actuación considerando el régimen de competencias definido reglamentariamente.

Por todo lo cual, el Consejo de Gobierno de la Junta de Extremadura, a propuesta de la Vicepresidenta y Consejera de Hacienda y Administración Pública, de conformidad con lo establecido en los artículos 23 y 90.3 de la Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura,

A C U E R D A :

Primero. Establecer la política de privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura, que se incorpora como anexo.

Segundo. Disponer su publicación en el Diario Oficial de Extremadura.

JUNTA DE EXTREMADURA

Consejería de Hacienda y Administración Pública
Secretaría General de Administración Pública

Política de Privacidad y Seguridad de la Información

Administración de la Comunidad Autónoma de Extremadura

Política de Privacidad y Seguridad de la Información de la Comunidad Autónoma de Extremadura

La Junta de Extremadura tiene como misión servir con objetividad a los intereses generales y procurar satisfacer, con eficacia y eficiencia, las necesidades públicas, de conformidad con los principios constitucionales y estatutarios, para beneficio de la ciudadanía.

En la Ley Orgánica 1/2011, de 28 de enero, de reforma del Estatuto de Autonomía de la Comunidad Autónoma de Extremadura se impone, entre otros, "facilitar el acceso a las nuevas tecnologías de la información y comunicación a los ciudadanos y empresas" (Art 7), ajustar su actuación a "los principios de buena fe, confianza legítima, transparencia, calidad en el servicio a los ciudadanos" (Art. 37.2) y como medidas de buena administración "regular los procedimientos administrativos propios y adaptar los procedimientos generales para dar celeridad y transparencia a la tramitación administrativa, para extender las relaciones interadministrativas y con los ciudadanos por medios telemáticos y para la simplificación de trámites" (artículo 39.2).

De acuerdo con ello, la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura, previene que la buena administración y el buen gobierno administrativo deberán ser informados por los principios previstos en la normativa básica del Estado y otros tales como de modernización, accesibilidad y prevención dirigidos a impulsar el proceso de transformación digital de la Administración pública.

Dichas previsiones deben ser contextualizadas en el nuevo marco de actuación del sector público definido por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que imponen el funcionamiento de las Administraciones Públicas, por medios electrónicos, para satisfacción de la ciudadanía preservando la protección de datos de carácter personal y, en particular, la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones que dispongan para prestar servicios públicos.

En relación con este ámbito, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, modificado parcialmente por el Real Decreto 951/2015, de 23 de

octubre, establece la necesidad que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política de seguridad que cumpla los principios básicos y requisitos mínimos que precisa para procurar una protección adecuada de la información y requiere así como la necesidad de que se apruebe por el titular del órgano superior.

En desarrollo de lo anterior, el Anexo II precisa que *"la política de seguridad se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente: a) Los objetivos o misión de la organización; b) El marco legal y regulatorio en el que se desarrollarán las actividades; c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación; d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización; y e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso".*

A nivel autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura, cuyo ámbito de aplicación se extiende a la Administración de la Comunidad Autónoma, los organismos públicos vinculados o dependientes de la misma sujeto a derecho público y los restantes organismos cuando ejerzan potestades públicas, a la ciudadanía y a las relaciones con otras Administraciones Públicas establece en su Disposición Adicional Séptima que "el Consejo de Gobierno establecerá una Política de Seguridad de la Información, "donde se marcarán las directrices de la Administración para garantizar el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias" y añade "la Política de Privacidad y Seguridad de la Información será reglamentariamente desarrollada por la Consejería competente en materia de administración electrónica, a través del órgano directivo competente"..

Dicha Política debe ser coherente con la Estrategia de Ciberseguridad de la Unión Europea y las exigencias del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que sienta las bases de una normativa de privacidad, en el auge de la economía digital, para garantía de los derechos de la ciudadanía y cuyas previsiones superan a las que se desprenden de la Ley Orgánica 15/1999, de 13 de

diciembre, de protección de datos y del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo.

Por todo lo anterior, resulta oportuno e idóneo establecer la Política de Privacidad y Seguridad de la Información de la Comunidad Autónoma de Extremadura que define la directrices de la Administración para garantizar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad de los datos que dispone, conserva y obtiene en la prestación de los servicios de interés público para preservar e incrementar la confianza de la ciudadanía.

A estos efectos, a propuesta de la Comisión de Coordinación de Administración Electrónica, previa iniciativa de la Secretaria General de Administración Pública conforme a lo dispuesto en la Disposición adicional séptima del Decreto 225/2014, de 14 de octubre, de régimen jurídico de la administración electrónica de la Comunidad Autónoma de Extremadura en relación con el artículo 5 del Decreto 261/2015, por el que se aprueba la estructura orgánica de la Consejería de Hacienda y Administración Pública de la Comunidad Autónoma de Extremadura, se establece, por Acuerdo del Consejo de Gobierno, la Política de Privacidad y Seguridad. Todo ello conforme al artículo 11.2 del citado Real Decreto 3/2010, de 8 de enero, que considera que son órganos superiores, los responsables directos de la ejecución de la acción del gobierno de acuerdo con lo establecido en sus propias normas de organización.

1. Misión, objeto y alcance
1.1. Misión
1.2. Objeto
1.3. Alcance
2. Definiciones
3. Acrónimos
4. Marco Regulador de la Seguridad de la Información
4.1. Marco Normativo
4.2. Estrategia Privacidad y Seguridad de la Información
4.3. Política de Privacidad y Seguridad de la Información
4.4. Documentos técnicos de desarrollo
4.4.1. Políticas y planes específicos
4.4.2. Normativas de Privacidad y Seguridad de la Información
4.4.3. Procedimientos y guías técnicas
5. Principios básicos y requisitos mínimos de la Privacidad y Seguridad de la Información
5.1. Principios básicos
5.2. Requisitos mínimos
6. Distribución orgánica de funciones en el ámbito de la Privacidad y Seguridad de la Información
6.1. Órganos competentes
6.1.1. Consejo de Gobierno
6.1.2. Comisión de Coordinación de Administración Electrónica
6.1.3. Consejería competente en materia de Administración Electrónica
6.2. Organización operativa de la Privacidad y Seguridad de la Información
6.2.1. Responsables de la Información
6.2.2. Responsables de los servicios.
6.2.3. Responsable de Privacidad y Seguridad de la Información
6.2.4. Responsables de Privacidad y Seguridad de la Información Sectoriales
6.2.5. Delegado de Protección de Datos de la ACAEx.
6.2.6. Responsables del Tratamiento
6.2.7. Comité de Privacidad y Seguridad de la Información
7. Protección de datos de carácter personal
7.1. Registro de actividades de tratamiento
7.2. Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de los riesgos de seguridad de la información
7.3. Notificación de violaciones de seguridad de los datos de carácter personal .....
8. Revisión y auditoría
9. Medidas de Seguridad
10. Revisión de la Política
11. Organismo Pagador de Extremadura
12. Relación con terceras partes

1. MISIÓN, OBJETO Y ALCANCE

1.1. MISIÓN

La Administración de la Comunidad Autónoma de Extremadura, en adelante ACAEx, tiene como misión servir con objetividad a los intereses generales y procurar satisfacer, con eficacia y eficiencia, las necesidades públicas, de conformidad con los principios constitucionales y estatutarios, respetando los principios de buena fe, confianza legítima, transparencia, seguridad y calidad en el servicio a los ciudadanos y a las organizaciones.

1.2. OBJETO

La Política de Privacidad y Seguridad de la Información, en adelante PPSI, establece el marco de referencia y las directrices para asegurar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones utilizadas y servicios prestados, en especial cuando se traten datos de carácter personal, que gestiona la ACAEx en el ejercicio de sus competencias.

1.3. ALCANCE

La PPSI será de aplicación a los órganos de la ACAEx y a los organismos públicos y entes públicos que utilicen los sistemas de información y/o de comunicaciones dependientes de la ACAEx.

Asimismo deberá de ser observada por todo el personal de los órganos y organismos citados, y por cualquier persona que no perteneciendo a los anteriores tenga acceso a los sistemas de información y/o de comunicaciones de la ACAEx.

Será de aplicación sobre todos aquellos sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable, en especial aquellos relacionados con el ejercicio de derechos por medios electrónicos de la ciudadanía o empleados públicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

Los Organismos Públicos estarán sujetos a la Política en todos sus términos y condiciones de acuerdo con las instrucciones, indicaciones de los órganos superiores de las Consejerías a las que están adscritas a excepción del Servicio Extremeño de Salud, que en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, deberá establecer su propia Política de Privacidad y Seguridad de la Información alineados con los principios y requisitos mínimos de esta política.

No obstante lo anterior, los Organismos Públicos podrán solicitar no adscribirse a la organización que marca esta Política, en cuyo caso deberán disponer de su propia Política de Privacidad y Seguridad de la Información alineada con los principios y requisitos mínimos de esta política.

El Sector Público Institucional deberá analizar su sujeción al ámbito de aplicación del ENS, ajustarse al Marco Regulador de la Política en la medida que les resulte de aplicación y cumplir la política y marco regulador cuando tengan la consideración de tercero.

La PPSI será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable en el ámbito descrito.

2. DEFINICIONES

a) **Activos de Información**: Toda información y los elementos que la contienen, independientemente del soporte, que procesan o manejan información. Incluye entre otros: Documentos, Carpetas, Archivadores, Software (aplicaciones, bases de datos), hardware (ordenadores, impresoras, televisiones, escáneres, fotocopiadoras, teléfonos) y soportes de información (CDs, DVDs, PenDrives, etc).

b) **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

c) **Confidencialidad**: Propiedad o característica de la información de no ponerse a disposición, ni se revela a individuos, entidades o procesos no autorizados.

d) **Disponibilidad**: Propiedad o característica de la información que consiste en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

e) **Incidente de Seguridad**: Cualquier suceso, inesperado o no deseado, que pueda afectar a la Seguridad de la Información.

f) **Integridad**: Propiedad o característica de la información que indica que no ha sido alterada de manera no autorizada.

g) **Medidas de seguridad**: Conjunto de disposiciones encaminadas mantener el riesgo de la Privacidad y la Seguridad de la Información por debajo de un nivel determinado adecuado para la organización.

h) **Riesgo**: Estimación del grado de exposición a que una amenaza se materialice causando una pérdida o daño en un activo de la información.

i) **Sistema de Información**: Conjunto recursos orientados, al tratamiento y administración de datos e información, que permiten que la información se encuentre a disposición de quien la precise, cuando la precise y en el formato establecido, para cubrir una necesidad o un objetivo específicos.

j) **Tratamiento de la información**: Cualquier operación o conjunto de operaciones sobre los datos y la información.

k) **Tecnologías de la Información y Comunicación (TIC)**: Conjunto de recursos necesarios para gestionar la información.

l) **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o una entidad.

3. ACRÓNIMOS

a) **ACAEx**: Administración de la Comunidad Autónoma de Extremadura.

b) **CPSI**: Comité de Privacidad y Seguridad de la Información.

c) **ENS**: Esquema Nacional de Seguridad (Real Decreto: 3/2010).

d) **FEADER**: Fondo Europeo Agrícola de Desarrollo Rural.

e) **FEAGA**: Fondo Europeo Agrícola de Garantía.

f) **LGACAEx**: Ley de Gobierno y Administración de la Comunidad Autónoma de Extremadura.

g) **PPSI**: Política de Privacidad y Seguridad de la Información.

h) **RGPD**: Reglamento General de Protección de Datos (Reglamento (UE) 2016/679).

i) **RJAE**: Régimen Jurídico de Administración Electrónica. (Decreto 225/2014).

j) **TIC**: Tecnologías de la Información y Comunicación.

k) **SGSI**: Sistema de Gestión de Seguridad de la Información.

4. MARCO REGULADOR DE LA SEGURIDAD DE LA INFORMACIÓN

Dada la diversidad de las competencias y funciones de la ACAEX la amplitud de los temas que afectan a la Seguridad de la Información y su rápida evolución, se debe desarrollar un **Marco Regulador de la Seguridad de la Información**, que se compondrá de:

a) Marco Normativo Legislativo aplicable en materia de Seguridad de la Información.

b) La estrategia y la Política de Privacidad y Seguridad de la Información.

c) Documentos técnicos de desarrollo de la Política de Privacidad y Seguridad de la Información.

d) Disposiciones y resoluciones de los órganos competentes del presente acuerdo, cuyo ámbito afecte a la Privacidad y Seguridad de la Información.

4.1. MARCO NORMATIVO

De forma general forman parte del marco normativo las normas de ámbito autonómico, estatal y europeo que afecte a la gestión de la Privacidad y Seguridad de la Información.

De forma específica, se toma como marco normativo de referencia, para el desarrollo de la PPSI, la siguiente normativa legal:

A nivel europeo:

- **Directiva (UE) 2016/1148** del Parlamento Europeo y del Consejo de 6 de Julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que será aplicable a partir del 25 de Mayo de 2018.
- **Reglamento Delegado (UE) núm.907/2014** de la Comisión de 11 de marzo de 2014 que completa el Reglamento (UE) núm.1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, en el anexo I apartado 3 B) ii) dice textualmente *"A partir del 16 de octubre de 2016, la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO/IEC 27001: Information Security management systems Requeriments (ISO) (Sistema de gestión de la Seguridad de la Información-Requisitos) (ISO)".*

A nivel estatal:

- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal o la legislación vigente en cada momento en materia de protección de datos.
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- **Real Decreto 3/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en adelante ENS.
- **Real Decreto 951/2015**, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

A nivel autonómico:

- **Ley 1/2002**, de 28 de febrero de Gobierno y Administración de la Comunidad Autónoma de Extremadura, en adelante LGACAEx.
- **Ley 4/2013**, de 21 de mayo, Gobierno Abierto de Extremadura.
- **Decreto 225/2014**, de 14 de octubre, de régimen jurídico de Administración Electrónica de la Comunidad Autónoma de Extremadura, en adelante RJAE.

4.2. ESTRATEGIA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

La estrategia de Privacidad y Seguridad de la Información informará la acción de gobierno de la ACAEx estableciendo las condiciones necesarias de confianza en la ciudadanía para el ejercicio de sus derechos y cumplimiento de las obligaciones.

La estrategia será aprobada por Acuerdo de Consejo de Gobierno a propuesta de la Consejería con competencias en materia de administración electrónica.

4.3. POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

El presente documento define la Política de Privacidad y Seguridad de la Información que será aprobada conforme a los criterios del punto "*6.1 Órganos competentes*" y revisada conforme al punto "*10.*

Revisión de la política".

4.4. DOCUMENTOS TÉCNICOS DE DESARROLLO

La documentación técnica de desarrollo se estructura jerárquicamente en los siguientes niveles.

- Nivel 1: Políticas y planes específicos
- Nivel 2: Normativas de Privacidad y Seguridad de la Información
- Nivel 3: Procedimientos y guías técnicas

Cada documento técnico, de un nivel determinado, debe estar fundamentado en documentación de nivel superior.

4.4.1. Políticas y planes específicos

Las políticas específicas deben ser entendidas como un conjunto de directrices que rigen la forma en la que esta Administración gestiona la Privacidad y Seguridad de la Información.

Los planes específicos definen las actuaciones a llevar a cabo para el desarrollo de las acciones derivadas del Marco Regulador.

Las políticas y planes específicos serán aprobados por el titular de la Consejería con competencia en administración electrónica a propuesta del órgano directivo competente, previa consulta al CPSI.

4.4.2. Normativas de Privacidad y Seguridad de la Información

El segundo nivel normativo desarrolla la PPSI mediante normas específicas que abarcan un área o aspecto determinado de la Privacidad y Seguridad de la Información.

Las políticas y planes específicos serán aprobados por el titular de la Consejería con competencia en administración electrónica a propuesta del órgano directivo competente en la materia sobre la que se desarrolla el documento, previa consulta al CPSI.

4.4.3. Procedimientos y guías técnicas

Los procedimientos indican lo que hay que hacer paso a paso en tareas o actividades concretas relacionadas con la Privacidad y Seguridad de la Información.

Las guías técnicas tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de Privacidad y Seguridad de la Información.

Los procedimientos y guías técnicas deben ser aprobados por el órgano o unidad administrativa con competencias en la materia sobre la que se desarrolla el documento, previa validación del Responsable de Privacidad y Seguridad de la Información.

5. PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

5.1. PRINCIPIOS BÁSICOS

La ACAEx tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

a) **Licitud, lealtad y transparencia**: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

b) **Legitimación en el tratamiento de datos personales:** Solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.

c) **Limitación de la finalidad**: Los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

d) **Minimización de datos**: Los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

e) **Exactitud**: Los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

f) **Limitación del plazo de conservación**: Los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesaos durante no más tiempo del necesario para los fines que justificaron su tratamiento.

g) **Integridad y confidencialidad**: Los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquel.

h) **Responsabilidad proactiva**: La ACAEX será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.

i) **Atención de los derechos de los afectados**: Se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

j) **Alcance estratégico**: La protección de datos y 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 la ACAEX para conformar un todo coherente y eficaz.

k) **Seguridad integral:** La seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende 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.

l) **Gestión de riesgos**: La gestión del riesgo es el conjunto de actividades coordinadas que la ACAEx desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos que. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información de la ACAEx, de forma que perita 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 la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo la ACAEx tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

m) **Proceso de verificación:** La ACAEx implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la privacidad y seguridad de la información.

n) **Protección de datos y seguridad desde el diseño:** La ACAEX promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información.

o) **Prevención, reacción y recuperación:** La privacidad y seguridad de la información debe contemplar los aspectos de prevención, reacción y recuperación sobre los activos, para conseguir que las amenazas sobre los mismos no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

p) **Líneas de defensa:** Los sistemas de información han de disponer de una estrategia de protección constituida por múltiples capas de seguridad.

q) **Reevaluación periódica**: La gestión de la Privacidad y Seguridad de la Información se revisarán, evaluará y actualizará periódicamente para mantener su eficacia de forma continuada, con la finalidad de hacer frente a la constante evolución de los riesgos y las medidas de seguridad.

r) **Responsabilidad diferenciada:** Los sistemas de información responsabilidad de la ACAEX se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles.

s) **Servicio a la ciudadanía:** La Privacidad y Seguridad de la Información estará orientada a la prestación de servicios de confianza a la ciudadanía en sus relaciones con la Administración.

5.2. REQUISITOS MÍNIMOS

La ACAEx establece los siguientes requisitos mínimos, que han de regir su Marco Regulador:

a) **Organización e implantación del proceso de seguridad:** La seguridad compromete a todo el personal dentro del alcance definido en este documento.

a) **Análisis y gestión de los riesgos:** La ACAEX debe analizar y tratar sus riesgos empleando metodologías reconocidas. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos, en especial cuando se traten datos de carácter personal.

b) **Evaluación de impacto en la privacidad:** Cuando se traten datos de carácter personal que por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas, debe realizarse, antes del tratamiento, una evaluación del impacto en la privacidad.

c) **Gestión de Personal:** El personal de las entidades incluidas en el alcance serán informados de sus deberes y obligaciones en materia de seguridad.

d) **Profesionalidad**: El personal de las entidades incluidas en el alcance que desarrollen funciones en el ámbito de la Privacidad y Seguridad de la Información dispondrán de la capacitación adecuada para la ejecución de las tareas encomendadas.

e) **Autorización y control de los accesos:** El acceso a los sistemas de información estarán controlados y limitados. Cada usuario, proceso, dispositivo y otros sistemas de información que accedan a la información de los sistemas de la ACAEx debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

f) **Protección de las instalaciones**: Las instalaciones de la ACAEx contarán con medidas de seguridad física adecuadas a la información que tratan en su interior.

g) **Adquisición de productos:** En la adquisición de productos de seguridad, se atenderá, de manera proporcionada, a la categoría y el nivel de seguridad determinados para los sistemas de información para los que sus funcionalidades son requeridas, las cuales deberán estar certificadas, salvo en aquellos casos en que las exigencias de proporcionalidad en cuando a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad.

h) **Seguridad por defecto:** Los sistemas de información deben diseñarse y configurarse de forma que proporcionen las mínimas funcionalidades requeridas, incluidas aquellas relacionadas con la operación, administración y registro de actividad, asegurando su disponibilidad y de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

i) **Integridad y actualización del sistema:** Se mantendrá actualizado el estado de seguridad de los sistemas de información, en relación a las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, de forma que dicho estado sirva como entrada a las actividades de gestión de riesgos. Cualquier elemento de los sistemas de información que se considere necesaria su instalación deberá tener la autorización previa por parte del Responsable de Privacidad y Seguridad de la Información.

j) **Protección de la información almacenada y en tránsito:** Se prestará especial atención a la información, en cualquier soporte, almacenada o en tránsito a través de entornos inseguros. Aplicándose las medidas de seguridad que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) **Prevención ante otros sistemas de información interconectados:** Se protegerán adecuadamente tanto las comunicaciones entre los sistemas de información y otros sistemas externos y en particular los puntos de interconexión entre las redes que soporten dichas comunicaciones, especialmente aquellas que se realicen a través de redes públicas.

l) **Registro de actividad:** Con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona, entidad o proceso que actúa.

m) **Incidentes de seguridad:** Se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en el RGPD y el ENS, de los incidentes de seguridad.

n) **Continuidad de la actividad:** Se desarrollarán planes de continuidad de negocio y actividades de recuperación para garantizar la disponibilidad de los servicios.

o) **Mejora continua del proceso de seguridad:** La gestión de Privacidad y Seguridad de la Información estará sometida a un ciclo de mejora continua como resultado de la aplicación del principio de reevaluación periódica.

6. DISTRIBUCIÓN ORGÁNICA DE FUNCIONES EN EL ÁMBITO DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

6.1. ÓRGANOS COMPETENTES

6.1.1. Consejo de Gobierno

Conforme al artículo 12 y la Disposición Adicional Séptima del RJAE corresponde al Consejo de Gobierno aprobar la Política de Seguridad.

Asimismo el Consejo de Gobierno como órgano colegiado integrado por los órganos superiores de la ACAEx aprobará las actualizaciones y revisiones de la PPSI y, en consecuencia, alinearán su acción de gobierno con los objetivos, principios y requisitos que se precisan en este acuerdo.

6.1.2. Comisión de Coordinación de Administración Electrónica

Conforme a la Disposición Adicional Séptima del RJAE, la Comisión de Coordinación de Administración Electrónica debe proponer al Consejo de Gobierno la aprobación de la PPSI, sus revisiones y actualizaciones, a propuesta del titular del órgano directivo con competencias en materia de administración electrónica.

La Comisión de Coordinación de Administración Electrónica la integran los titulares de las Secretarías Generales de todas las Consejerías y de todos los Organismos Públicos, los titulares de los órganos directivos competentes en materia de atención al ciudadano, inspección de servicios y de administración electrónica de acuerdo con el artículo 15 del RJAE.

6.1.3. Consejería competente en materia de Administración Electrónica

Conforme a la Disposición Adicional Séptima del RJAE, la Consejería competente en materia de administración electrónica desarrollará reglamentariamente la PPSI a propuesta del órgano directivo correspondiente.

Le corresponde por tanto las siguientes funciones:

a) Aprobar los documentos técnicos del Marco Regulador de nivel 1 (Políticas y planes específicos) y Nivel 2 (Normativas de Privacidad y Seguridad de la Información), aplicables a toda la ACAEX a propuesta del órgano directivo competente y dictar cuantas disposiciones sean necesarias para su cumplimiento.

b) Velar por una dirección clara y unánime en las actuaciones que den soporte a la Privacidad y Seguridad de la Información promoviendo la adscripción de los recursos necesarios.

c) Resolución, en última instancia, de los conflictos, internos a la ACAEx, que surjan en el ámbito de la Privacidad y Seguridad de la Información.

d) Ejercer una supervisión razonable de la implementación, operación y eficacia de la gestión de la Privacidad y Seguridad de la Información realizada por los gestores que tienen delegada la implementación de las estrategias y políticas para el cumplimiento del propósito de la ACAEx en este ámbito.

e) Promover la implantación, mantenimiento, operación y supervisión del Sistema de Gestión de la Seguridad de la Información (SGSI) y revisar a intervalos planificados la información sobre la operación del mismo y su adecuación a los objetivos establecidos.

f) Proponer al Consejo de Gobierno la aprobación de la Estrategia de Privacidad y Seguridad de la Información.

6.2. ORGANIZACIÓN OPERATIVA DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

6.2.1. Responsables de la Información

Los Responsables de la Información tienen la potestad de establecer los requisitos de seguridad sobre la información que manejan con el apoyo del Responsable de Privacidad y Seguridad de la Información Sectorial. Tienen la responsabilidad última del uso que se haga de la información y, por tanto, de su protección.

Los Responsables de la Información ejercerán las siguientes funciones en su ámbito de actuación y competencia:

a) Evaluar los niveles de Seguridad de la Información tratada.

b) Asegurar el cumplimiento del Marco Regulador de la Privacidad y Seguridad de la Información.

c) Proporcionar los recursos y medios adecuados para el cumplimiento de los principios básicos, requisitos mínimos y Marco regulador en materia de Privacidad y Seguridad de la Información.

d) Asumir las funciones explícitamente atribuidas a la figura del Responsable de la Información en el ENS.

e) Informar al Responsable de la Privacidad y Seguridad de la Información sobre el cumplimiento de los niveles de seguridad y resto de requerimientos que se definan.

Las personas titulares de las Consejerías ejercen como Responsables de la Información conforme al artículo 12 del RD 3/2010 en relación con el artículo 56 de la LGCAEx. En caso de que no existiera Consejería de Presidencia, la responsabilidad recaerá en la persona titular de la Consejería con competencias en administración electrónica con la colaboración de los

órganos directivos que, en su caso, estuvieran adscritos a la Presidencia del Gobierno según el ámbito de responsabilidades definido en este documento.

6.2.2. Responsables de los servicios.

Los Responsables de los Servicios, son aquellos que tienen la potestad de establecer los requisitos de seguridad sobre los servicios de información que se presten a la ciudadanía con el apoyo del Responsable de Privacidad y Seguridad de la Información Sectoriales.

Los Responsables de los Servicios ejercerán las siguientes funciones en su ámbito de actuación y competencia:

a) Evaluar los niveles de seguridad de los servicios prestados.

b) Proporcionar los recursos y medios adecuados para el cumplimiento de los principios básicos, requisitos mínimos y Marco Regulador de la Privacidad y Seguridad de la Información.

c) Asumir las funciones explícitamente atribuidas a la figura del Responsable de los Servicios en el ENS.

Los titulares de los Órganos Directivos a los que se refiere el artículo 59 de la LGACAEx ejercen como Responsable de los Servicios.

6.2.3. Responsable de Privacidad y Seguridad de la Información

El Responsable de Privacidad y Seguridad de la Información vela por la Privacidad de los datos personales y la Seguridad de la Información en la ACAEx.

El Responsable de Privacidad y Seguridad de la Información ejerce las siguientes funciones:

a) Colaborar, cooperar y asistir a los Responsables de Privacidad y Seguridad de la Información en el desarrollo de sus funciones con la asistencia técnica del órgano competente de los sistemas de información que soporten los servicios.

b) Convocar reuniones de coordinación del Comité de Privacidad y Seguridad de la Información para evitar redundancia de acciones, asegurar la reutilización de recursos y unificar criterios en materia de Privacidad y Seguridad de la Información y protección de datos, tales como clausulado, directrices, procedimientos comunes, etc…

c) Desarrollar, operar y mantener el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, apoyado por todos los responsables.

d) Proponer el desarrollo de documentos técnicos del Marco Regulador y elevarlas a la persona titular de la Consejería competente en materia de administración electrónica para su aprobación.

e) Proponer los planes de Privacidad y Seguridad de la Información, auditorías, continuidad de los servicios, formación y concienciación y observar su ejecución, así como su seguimiento.

f) Estar informado e informar al titular de la Consejería competente en materia de administración electrónica del estado de la Privacidad y Seguridad de la Información de la ACAEx. Para ello, de forma anual, le presentará un informe sobre el estado de la Privacidad y Seguridad de la Información en la ACAEx.

g) Mantener informado al Delegado de Protección de Datos de cuantas decisiones tengan relación con la protección de datos que afecten de forma genérica al ámbito de la ACAEx.

h) Difundir la PPSI y el resto del Marco Regulador en la Administración de la Comunidad Autónoma de Extremadura y entidades incluidas en su alcance.

i) Velar por el cumplimiento y observancia del Marco Regulador de Privacidad y Seguridad de la Información.

j) Velar por que la Privacidad y Seguridad de la Información se incorpore en todos los proyectos de los sistemas de información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información que sea requerida tras el cese de sus actividades.

k) Promover la formación y concienciación en materia de Privacidad y Seguridad de la Información.

l) Gestionar los incidentes de seguridad, desde su notificación hasta su resolución y participar en la toma de decisiones en momentos asistido por el órgano directivo competente en materia tecnologías de la información y comunicación.

m) A intervalos planificados, recibir y revisar información sobre el desempeño y cumplimiento del sistema de gestión de la Privacidad y Seguridad de la Información.

n) Asumir las funciones explícitamente atribuidas a la figura del Responsable Seguridad de la Información en el ENS.

El titular del Órgano Directivo al que se refiere el artículo 58 de la LGACAEx con competencias en administración electrónica ejerce como Responsable de Privacidad y Seguridad de la Información con la asistencia técnica del órgano directivo con competencias sobre las tecnologías de la información y comunicación.

6.2.4. Responsables de Privacidad y Seguridad de la Información Sectoriales

Los Responsables de Privacidad y Seguridad de la Información Sectoriales velan por la Privacidad de los datos y Seguridad de la Información en su ámbito de competencia.

El ámbito de actuación de cada Responsable de Privacidad y Seguridad de la Información Sectorial se limita única y exclusivamente a los sistemas de información y servicios que sean competencia y responsabilidad directa del órgano al que pertenezca.

Los Responsables de Privacidad y Seguridad de la Información Sectorial ejercen las siguientes funciones en su ámbito de actuación y responsabilidad:

a) Aprobar los documentos técnicos del Marco Regulador específicos.

b) Asistir a las convocatorias de reuniones de coordinación a propuesta del Responsable de Privacidad y Seguridad de la Información.

c) Estar informado e informar al Responsable de Privacidad y Seguridad de la Información del estado de la Privacidad y Seguridad de la Información, para ello, de forma anual, le presentará un informe sobre el estado de la Privacidad y Seguridad de la Información.

d) Mantener informado al Delegado de Protección de Datos de cuantas decisiones tengan relación con la protección de datos en su ámbito de competencia.

e) Difundir la PPSI y el resto de su Marco Regulador.

f) Asegurar el cumplimiento y observancia del Marco Regulador de Seguridad de la Información.

g) Asegurar que la Privacidad y Seguridad de la Información se incorpore en todos los proyectos de los sistemas de información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información que sea requerida tras el cese de sus actividades.

h) Promover la formación y concienciación en materia de Privacidad y Seguridad de la Información.

i) Gestionar los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta con la asistencia técnica del órgano competente sobre los sistemas de información que soporten los servicios.

Los titulares de las Secretarias Generales al que se refiere el artículo 58 de la LGACAEx ejercerán como Responsables de Privacidad y Seguridad de la Información Sectoriales en su ámbito de actuación y competencias.

6.2.5. **Delegado de Protección de Datos de la ACAEx.**

El Delegado de Protección de Datos es quien debe informar, asesorar y supervisar el cumplimiento en materia de protección de datos y actuar como punto de contacto con las autoridades de control.

El Delegado de Protección de Datos ejerce las siguientes funciones, en el ámbito de la protección de datos:

a) Informar y asesorar a los Encargados de Tratamiento de sus obligaciones.

b) Supervisar el cumplimiento del Marco Regulador relativo a la protección de datos.

c) Cooperar con las autoridades de control.

d) Actuar como punto de contacto de las autoridades de control para cualquier consulta sobre el tratamiento de datos personales.

e) Mantendrá un registro general de todos los incidentes de seguridad de los que sea informado, sean o no objeto de notificación a la Autoridad de Control.

f) Supervisará las auditorías tanto internas como las que realicen los Responsables del Tratamiento a los Encargados de Tratamiento o que se realicen por parte de la Autoridad de Control a la ACAEx.

g) Revisará de forma proactiva la implantación de las clausulas informativas.

h) Apoyar el Responsable del Tratamiento en la toma de decisiones sobre las autorizaciones de cesiones de datos.

i) Supervisará los criterios y procedimientos para evaluar el cumplimiento de garantías por parte de los Encargados de Tratamiento.

j) Revisará de forma proactiva las relaciones con terceros, en especial la existencia o no de cláusulas específicas y los mecanismos que utilizan los Responsables del Tratamiento para evaluar su cumplimiento.

k) Validará los procedimientos de ejecución de derechos en materia de protección de datos.

l) Se mantendrá informado de la gestión de riesgo y evaluación de impacto en la privacidad y dará recomendaciones a los actores en protección de datos sobre estos temas.

m) Dará recomendaciones a los actores en protección de datos sobre las transferencias internacionales

Los Responsables de los Tratamientos pueden, en función de los servicios e información que traten, podrán establecer Delegados de Protección de Datos Sectoriales, que deberán coordinarse a través del Delegado de Protección de Datos de la ACAEx.

El Delegado de Protección de Datos será nombrado por la persona titular de la Consejería con competencias en administración electrónica a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la propia ACAEx.

Todo ello se entiende sin perjuicio de lo dispuesto en normativa en cada caso vigente relativa a la protección de datos.

En el desempeño de sus tareas el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento.

6.2.6. Responsables del Tratamiento

Los Responsables del Tratamiento son quienes determinan los fines y medios del tratamiento de la información, tal como indica el RGPD y ejercerán sus funciones a través de los Responsables de Privacidad y Seguridad Sectoriales.

Las personas titulares de las Consejerías ejercen como Responsables de Tratamiento. En caso de que no existiera Consejería de Presidencia, la responsabilidad recaerá en la persona titular de la Consejería con competencias en administración electrónica con la colaboración de los órganos directivos que, en su caso, estuvieran adscritos a la Presidencia del Gobierno, según el ámbito de responsabilidades definido en este documento.

6.2.7. Comité de Privacidad y Seguridad de la Información

La persona titular de la Consejería con competencias en materia de administración electrónica estará asistida en el ejercicio de sus competencias y funciones por el CPSI.

El CPSI se configura como un grupo de trabajo técnico de asistencia y coordinación entre las distintas entidades incluidas en el alcance de esta Política:

- El Responsable de Privacidad y Seguridad de la Información, o la persona en quien delegue, quien coordinará este Comité.
- Los Responsables de Privacidad y Seguridad Sectoriales, o las personas en quien deleguen.
- El órgano directivo competente en Función Pública, o la persona en quien delegue.
- El órgano directivo competente en Tecnologías de la Información y Comunicación, o la persona en quien delegue.
- El órgano directivo responsable sobre atención al ciudadano, o la persona en quien delegue.
- El órgano directivo responsable sobre la Inspección General de Servicios, o la persona en quien delegue.
- El Delegado de Protección de Datos salvo que las funciones del mismo recaigan en alguno de los órganos anteriormente citados.
- En su caso, los órganos directivos de los organismos públicos, o las personas en quien deleguen.

Puntualmente, podrán formar parte del CPSI, en calidad de asesores, las personas que en cada caso proponga alguno de sus miembros.

El CPSI asumirá, entre otras, las siguientes funciones:

a) El debate, intercambio de experiencias y buenas prácticas en actuaciones dirigidas a garantizar la coordinación entre entidades incluidas en el alcance de esta política para el cumplimiento del Marco Regulador de la Privacidad y Seguridad de la Información.

b) Asistir al Responsable de Privacidad y Seguridad de la Información en la elaboración de los informes y memoria anual para su elevación a la Comisión de Coordinación de Administración Electrónica.

c) Promover planes y programas de concienciación del personal en esta materia

d) Evaluar la idoneidad de los distintos controles de seguridad, facilitar los recursos necesarios y coordinar su implantación efectiva.

e) Estudiar las no conformidades y observaciones detectadas en las auditorías y proponer las acciones correctoras correspondientes.

f) Colaborar con el Consejo de Gobierno en la definición de la estrategia de Privacidad y Seguridad de la Información.

7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

7.1. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

La ACAEx mantendrá actualizado el registro de las actividades de tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD y podrá consultarse en el Portal de Transparencia y Participación Ciudadana de la ACAEx.

7.2. ANÁLISIS DE RIESGOS, EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Cuando la información contenga datos de carácter personal, se estará igualmente a lo señalado en el artículo siguiente, se llevará a cabo, de forma periódica y al menos cada 2 años, un análisis de riesgos que permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo la ACAEx, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

Asimismo, la ACAEx llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del RGPD.

La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

Los Responsables de la Información y los Responsables de los Servicios son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Para el análisis y gestión de riesgos se utilizarán las herramientas facilitadas por el Centro Criptológico Nacional (CCN), en particular las herramientas PILAR o las que se desarrollasen en el futuro, así como las guías, recomendaciones y herramientas elaboradas por la ACAEx en lo que respecta al tratamiento de datos de carácter personal.

7.3. NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL

La ACAEX adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a través del procedimiento establecido al efecto, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

8. REVISIÓN Y AUDITORÍA

La ACAEX llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por los Responsables de Privacidad y Seguridad de la Información, incluidos los sectoriales, y por los delegados de protección de datos competente.

9. MEDIDAS DE SEGURIDAD

Las medidas de seguridad implantadas se corresponderán con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

10. REVISIÓN DE LA POLÍTICA

El Responsable de Privacidad y Seguridad de la Información asegurará la revisión de la PPSI cuando se produzcan cambios significativos en el contexto de la ACAEx o bien con la periodicidad que se determine en el desarrollo del SGSI, la cual se elevará, en su caso, a la Comisión de Coordinación de Administración Electrónica una propuesta de cambio de la PPSI. Su revisión debe garantizar que ésta se encuentra alineada con la estrategia, la misión y visión del Gobierno de la Junta de Extremadura en materia de Privacidad y Seguridad de la Información.

11. ORGANISMO PAGADOR DE EXTREMADURA

El Organismo Pagador para el Fondo Europeo Agrícola de Garantía (FEAGA) y el Fondo Europeo Agrícola de Desarrollo Rural (FEADER), en base a sus requisitos legales y normativos específicos, puede crear una estructura organizativa específica adicional para la gestión de la Privacidad y Seguridad de la Información en lo referente a sus competencias como Organismo Pagador, debiendo estar alineada con esta PPSI.

El Organismo Pagador debe presentar al Responsable de Privacidad y Seguridad de la Información con periodicidad anual y dentro del primer trimestre de cada año, un informe de su estado de la Seguridad de la Información.

12. RELACIÓN CON TERCERAS PARTES

Cuando un tercero preste servicio a la Administración de la Comunidad Autónoma de Extremadura o se cedan activos de información a éstos, se le debe hacer partícipe del Marco Regulador de Privacidad y Seguridad de la Información que ataña a dichos servicios o activos. Las terceras partes quedan sujetas a las obligaciones establecidas en dicho Marco.

Los contratos, encargos o convenios que se suscriban a partir de la entrada en vigor de este acuerdo deben incluir la obligación de cumplir esta Política y el sistema de verificación de su cumplimiento. Las subcontrataciones requerirán el consentimiento expreso del Responsable de la Información para el acceso a los activos de la información.

Cualquier tercero adjudicatario de un contrato, encargo o convenio que conlleve el tratamiento de datos de carácter personal en nombre de la ACAEx, deberá ser constituido como Encargado de Tratamiento.