CONSEJERÍA DE ECONOMÍA, EMPLEO Y TRANSFORMACIÓN DIGITAL

RESOLUCIÓN de 15 de julio de 2025, del Consejero, 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 1 de julio de 2025, por el que se establece una nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura. (2025062843)

El Consejo de Gobierno de la Junta de Extremadura el día 1 de julio de 2025, ha aprobado el Acuerdo por el que se establece una nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura, teniendo en cuenta el contenido del mismo y lo dispuesto en el apartado 2 del artículo 11 del Decreto 17/2025, de 1 de abril, por el que se regula el Diario Oficial de Extremadura,

RESUELVO:

Ordenar la publicación en el Diario Oficial de Extremadura del Acuerdo del Consejo de Gobierno de la Junta de Extremadura, de 1 de julio de 2025, por el que se establece una nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura, el cual se incorpora como anexo a la presente resolución.

Mérida, 15 de julio de 2025.

El Consejero,

GUILLERMO SANTAMARÍA GALDÓN

ACUERDO DEL CONSEJO DE GOBIERNO DE LA JUNTA DE EXTREMADURA DE 1 DE JULIO DE 2025 POR EL QUE SE ESTABLECE UNA NUEVA 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 el Estatuto de Autonomía de la Comunidad Autónoma de Extremadura, en la redacción dada al mismo por la Ley Orgánica 1/2011, de 28 de enero, 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 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 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS), establece la necesidad de disponer de Política de Seguridad en la utilización de medios electrónicos por parte de las entidades públicas, asegurando la protección adecuada de la información y los servicios electrónicos, y siendo necesaria su aprobación por el órgano competente.

A nivel autonómico, el Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura establece las bases para el uso de medios electrónicos en la Administración pública de Extremadura, facilitando la relación entre la Administración y los ciudadanos, así como las relaciones con otras Administraciones Públicas. Dicho decreto, 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, con 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 con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que adapta dicho Reglamento General de Protección de Datos al ámbito nacional, reconociendo y recopilando, además, un catálogo de derechos digitales.

El 26 de junio de 2018, se aprobó por Acuerdo de Consejo de Gobierno de la Junta de Extremadura, la actual Política de Privacidad y Seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura, que cumple con las obligaciones recogidas en la normativa vigente hasta esa fecha. Resultó oportuno e idóneo establecer dicha Política, que define las directrices de la Administración para garantizar la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad de los datos personales que dispone, conserva y obtiene en la prestación de los servicios de interés público para preservar e incrementar la confianza de la ciudadanía, pero que se ha quedado obsoleta.

A estos efectos, a propuesta de la Comisión de Coordinación de Administración Electrónica, previa iniciativa de la Dirección General de Digitalización de la Administración, 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 8 del Decreto 234/2023, de 12 de septiembre, que establece la estructura orgánica de laConsejería de Economía, Empleo y Transformación Digitalde la Comunidad Autónoma de Extremadura, se establece por Acuerdo del Consejo de Gobierno, una

nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura.

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 ENS, en su Anexo II, Sección 3. Marco organizativo [ORG], 3.1 Política de seguridad [org.1], precisa que "La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

— [org.1.1] Los objetivos o misión de la organización.

— [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.

— [org.1.3] 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.

— [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

— [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

".

La disposición adicional séptima del Decreto 225/2014, de 14 de octubre, indica que la Política de Seguridad de la Información de la Comunidad Autónoma de Extremadura cumplirá los principios básicos y los requerimientos mínimos recogidos en el ENS.

Con estas premisas, la Política que sea de aplicación en nuestra administración pública, necesariamente tiene que cumplir con el contenido prescrito en el ENS, que además de lo indicado en el anexo II ya enunciado, en su artículo 11 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 12 que todas las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el órgano competente 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 transversal, por la Dirección

General de Digitalización de la Administración y, coordinada por la Secretaría General de Transformación Digital y Ciberseguridad, 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 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura.

El alcance de la política se extiende a las previsiones y requisitos del ENS y 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, del Procedimiento Administrativo Común de las Administraciones Públicas.

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

En particular se han considerado según 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 (Reglamento general de protección de datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), en el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo en lo que no contradiga a la normativa anteriormente citada, en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) y en 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, de 8 de enero, sin requerir su desarrollo reglamentario.

La normativa básica reguladora del ENS requiere, entre otros aspectos, "Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación" (artículo 12.1 c) ENS), y dichas funciones están determinadas legalmente al precisarse las mismas en el artículo 13 ENS.

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, de 14 de octubre, de régimen jurídico de la Administración electrónica en la Comunidad Autónoma de Extremadura.

A modo de ejemplo, la atribución al Consejo de Gobierno de la competencia para definir la Estrategia de Privacidad y Seguridad de la Información, que habrá de informar la acción de gobierno de la Administración de la Comunidad Autónoma de Extremadura, 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, al 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.

La efectividad de la organización operativa de la privacidad y seguridad de la información contemplada en el texto de la nueva Política de Privacidad y Seguridad de la Información de

la Administración de la Comunidad Autónoma de Extremadura requiere la modificación de la Disposición adicional quinta del Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica básica de la Administración de la Comunidad Autónoma de Extremadura. Esta disposición recoge a los Órganos con competencias en materia de política de privacidad y seguridad de la información, de conformidad con lo establecido en la citada Política Privacidad y Seguridad aprobada por Acuerdo del Consejo de Gobierno de la Junta de Extremadura del año 2018.

No obstante, debido a que como hemos mencionado, con la nueva Política de Privacidad y Seguridad de la información se pretende modificar la organización operativa de la privacidad y seguridad de la información, lo cual requiere la referida modificación del Decreto 77/2023, de 21 de julio, debemos tener en cuenta el carácter de acto administrativo del acuerdo que aprueba la nueva Política de Privacidad y Seguridad de la Información, y asimismo lo dispuesto en el apartado 1 del artículo 37 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, al disponer respecto la inderogabilidad singular de los actos administrativos que "Las resoluciones administrativas de carácter particular no podrán vulnerar lo establecido en una disposición de carácter general, aunque aquéllas procedan de un órgano de igual o superior jerarquía al que dictó la disposición general".

Como consecuencia de lo mencionado anteriormente, el acuerdo del Consejo de Gobierno de la Junta de Extremadura mediante el que se aprueba la Nueva Política de Privacidad y Seguridad no podría modificar lo establecido mediante una norma de carácter general, como es el citado Decreto 77/2023, de 21 de julio. Por este motivo, resulta necesario que lo previsto en el apartado 6 del anexo del acuerdo por el que se establece la actual Política de Privacidad y Seguridad ("DISTRIBUCIÓN ORGÁNICA DE FUNCIONES EN EL ÁMBITO DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN") continue produciendo sus efectos hasta la entrada en vigor de la modificación de la citada Disposición adicional quinta del Decreto 77/2023, de 21 de julio. Asimismo, resulta necesario que el apartado 8 del anexo del acuerdo por el que se establece la nueva política de Privacidad y Seguridad ("DISTRIBUCIÓN ORGÁNICA DE FUNCIONES EN EL ÁMBITO DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN") no empiece a producir sus efectos hasta la entrada en vigor de la modificación de la referida Disposición adicional quinta del Decreto 77/2023, de 21 de julio.

Por ello y, teniendo en cuenta que la actual Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura se aprobó con anterioridad a la entrada en vigor de la LOPDGDD y del vigente ENS, se considera necesaria la aprobación de una nueva Política de Privacidad y Seguridad de la Información de la Administración de la Comunidad Autónoma de Extremadura, la implicación de todos los órganos superiores y centros directivos mencionados en la misma en su implementación y puesta en práctica, y su posterior desarrollo por la Consejería competente en materia de administración electrónica.

Por todo lo cual, el Consejo de Gobierno de la Junta de Extremadura, a propuesta del Consejero de Economía, Empleo y Transformación Digital, de conformidad con lo establecido en los artículos 23 y 90.3 de la Ley 1/2002, de 28 de febrero, del Gobierno y la Administración de la Comunidad Autónoma de Extremadura

ACUERDA

Primero. Establecer una nueva 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.

Tercero. Disponer que por los órganos competentes se desarrollen las actuaciones correspondientes para proceder a la modificación de la disposición adicional quinta del Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica básica de la Administración de la Comunidad Autónoma de Extremadura, con objeto de proceder a su adecuación a la organización operativa de la privacidad y seguridad de la información contemplada en la nueva Política de Privacidad y Seguridad de la Información administrativa de la Comunidad Autónoma de Extremadura.

Cuarto. Que la nueva Política de Privacidad y Seguridad aprobada surtirá efecto desde el día de publicación de este acuerdo en el Diario Oficial de Extremadura, a excepción de lo establecido en el apartado 8 de la misma ("Distribución orgánica de funciones en el ámbito de la privacidad y seguridad de la información"), que no producirá sus efectos hasta la entrada en vigor de la modificación de la disposición adicional quinta del mencionado Decreto 77/2023, de 21 de julio.

Quinto. Que desde la fecha de su publicación en el Diario Oficial De Extremadura de este acuerdo, quedará sin efecto 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, a excepción de lo previsto en el apartado 6 de dicha Política ("Distribución orgánica de funciones en el ámbito de la privacidad y seguridad de la información") que continuará produciendo sus efectos hasta la entrada en vigor de la modificación del mencionado Decreto 77/2023, de 21 de julio.

JUNTA DE EXTREMADURA

Consejería de Economía, Empleo y Transformación Digital

Política de Privacidad y Seguridad de la Información

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" (Art 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 los datos personales y, en particular, la seguridad y confidencialidad de los mismos que figuren en los registros, sistemas y aplicaciones que dispongan para prestar servicios públicos.

Por todo ello, para la Junta de Extremadura la información constituye un activo de primer nivel ya que resulta esencial para la prestación de los servicios que satisfacen las necesidades de la ciudadanía. La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de la información. Si bien, son estas tecnologías de la información y las comunicaciones imprescindibles, en términos de eficacia y eficiencia, para las administraciones públicas. No obstante, vienen acompañadas de nuevos riesgos y, por lo tanto, es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependan de ellas.

En relación con este ámbito, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, "ENS"), establece la necesidad de que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política

de seguridad aprobada por el titular del órgano superior, que cumpla los principios básicos y requisitos mínimos que precisa para proteger adecuadamente la información.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, establece la obligación en su artículo 9 a que cada Administración Pública disponga de un registro actualizado con el conjunto de sus inventarios de información administrativa y que esta información y documentos electrónicos se aseguren de conformidad con lo establecido en el ENS.

A nivel autonómico, resulta relevante destacar la Ley 8/2019, de 5 de abril, para una Administración más ágil en la Comunidad Autónoma de Extremadura que tiene por objeto el establecimiento de medidas de impulso para facilitar la actividad empresarial en la Comunidad Autónoma de Extremadura y la adopción de medidas de simplificación y mejora de la Administración autonómica, así como la Ley 4/2022, de 27 de julio, de racionalización y simplificación administrativa de Extremadura que entre otras estipulaciones recoge que "el gobierno de los datos está orientado a la consecución de una gestión pública cercana a la ciudadanía, automatizada y segura".

Asimismo, 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 sujetos 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 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), así como Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo en lo que no contradiga a la normativa anteriormente citada, sentando las bases de una normativa de privacidad, en el auge de la economía digital, para garantía de los derechos y libertades de la ciudadanía.

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 las 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 Transformación Digital y Ciberseguridad, 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 7 del Decreto 234/2023, de 12 de septiembre, por el que se establece la estructura orgánica de la Consejería de Economía, Empleo y Transformación Digital, se establece, por Acuerdo del Consejo de Gobierno, la Política de Privacidad y Seguridad. Todo ello conforme al artículo 12.2 del Real Decreto 311/2022, de 3 de mayo, que considera que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente.

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

Contenido

TÉRMINOS Y ACRÓNIMOS.

ACAEx: Administración de la Comunidad Autónoma de Extremadura.

CCN: Centro Criptológico Nacional.

CEPD: Comité Europeo de Protección de Datos.

CPSI: Comité de Privacidad y Seguridad de la Información.

ENS: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (Real Decreto: 3/2010 en su regulación normativa vigente).

FEADER: Fondo Europeo Agrícola de Desarrollo Rural.

FEAGA: Fondo Europeo Agrícola de Garantía.

LGACAEx: Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura.

PPSI: Política de Privacidad y Seguridad de la Información.

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

LOPDGGD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RJAE: Decreto 225/2014, de 14 de octubre, de régimen jurídico de administración electrónica de la Comunidad Autónoma de Extremadura.

RSI: Responsable de Seguridad de la Información.

RSE: Responsable de Seguridad y Enlace.

SGPSI: Sistema de Gestión de Privacidad y Seguridad de la Información.

TIC: Tecnologías de la Información y Comunicación.

PIC: Protección de Infraestructuras Críticas.

CNPIC: Comisión Nacional de Protección de Infraestructuras Críticas.

1. MISIÓN, OBJETO Y ALCANCE.

1.1. MISIÓN.

La 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 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 personales, que gestiona la ACAEx en el ejercicio de sus competencias.

1.3. ALCANCE.

La PPSI se aplicará a los órganos de la ACAEx y a los organismos 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 el de aquellos terceros -entidades externas a la ACAEx- que tengan acceso a los sistemas de información y/o de comunicaciones de la ACAEx para la prestación o ejecución de servicios.

Será de aplicación sobre todos aquellos sistemas de información y a todas las actividades de tratamiento de datos personales de los que sea responsable la ACAEx, 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 e 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 alineada con los principios y requisitos mínimos de esta.

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

El Sector Público Institucional deberá analizar su sujeción al ámbito de aplicación del ENS y ajustarse a esta Política en la medida que les resulte de aplicación, estando obligados a su cumplimiento cuando tengan la consideración de tercero con la ACAEx.

El análisis de los supuestos anteriores corresponderá al CPSI, quién informará a la persona titular de la Consejería con competencias en materia de Administración Electrónica al objeto de que, en su caso, escale la decisión que deba adoptarse al respecto.

La PPSI se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sea responsable la ACAEx en el ámbito descrito. La citada responsabilidad no requerirá, necesariamente, que la plataforma y/o sistemas que soportan los servicios prestados por los sistemas de información responsabilidad de la ACAEx sean gestionados por ésta, pudiendo recogerse los mismos en la correspondiente declaración de alcance y distinguiendo la responsabilidad sobre los distintos elementos en los procesos de análisis y gestión de riesgos que se lleven a cabo.

2. DEFINICIONES.

a) Activos de Información: Toda información y los elementos que la contienen con independencia del soporte y/o infraestructura de almacenamiento. Incluye entre otros: Documentos, Carpetas, Archivadores, Software, hardware y soportes de información en infraestructura local o en la nube.

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: Cualquier suceso, inesperado o no deseado, que pueda afectar a la Privacidad y 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 a mantener el riesgo de la Privacidad y la Seguridad de la Información por debajo de un nivel determinado considerado 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.

m) Sistema de Gestión de la Privacidad y Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que se utilizan en la organización para establecer su política y objetivos de privacidad y seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

3. MARCO REGULADOR DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

Para el cumplimiento de los requisitos aplicables se identifican los siguientes elementos comprensivos del marco regulador de la privacidad y seguridad de la información:

A. Marco Normativo Legislativo aplicable en materia de Seguridad de la Información.

B. La estrategia de Privacidad y Seguridad de la Información.

C. La Política de Privacidad y Seguridad de la Información.

D. Marco documental de desarrollo de la Política de Privacidad y Seguridad de la Información.

E. Disposiciones y resoluciones de los órganos de gobierno de la ACAEx competentes cuyo ámbito afecte a la Privacidad y Seguridad de la Información.

4. MARCO NORMATIVO.

El marco normativo se compone de las normas de ámbito autonómico, estatal y europeo que afecten a la gestión de la Privacidad y Seguridad de la Información. Dicha normativa aplicable se encuentra publicada y actualizada en el Punto de Acceso General de la ACAEx – apartado de Privacidad y Seguridad de la Información.

5. ESTRATEGIA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

De manera periódica, la ACAEX establecerá las líneas de actuación y objetivos en materia de privacidad y seguridad de la información, para un contexto y período determinados y al objeto de garantizar confianza de la ciudadanía en los servicios públicos digitales para el ejercicio de sus derechos y el cumplimiento de las obligaciones de esta Administración.

La estrategia de Privacidad y Seguridad de la Información, como parte de la Estrategia Global de la ACAEx en materia digital, podrá incorporarse en dicho proceso y será aprobada por Acuerdo de Consejo de Gobierno a propuesta de la persona titular de la Consejería con competencias en materia de Administración Electrónica, pudiendo ser sometida, con carácter previo, al análisis y opinión del Comité de Privacidad y Seguridad de la Información en su labor de asistencia a dicha Consejería.

6. POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

La PPSI es el conjunto de directrices que rigen la forma en que la ACAEx gestiona y protege la información que trata y los servicios que presta.

Será aprobada por Acuerdo de Consejo de Gobierno a propuesta de la persona titular de la Consejería con competencias en materia de administración electrónica, oídas las declaraciones del Comité de Privacidad y Seguridad de la Información en su labor de asistencia a la persona titular de dicha Consejería.

7. DESARROLLO DE LA PPSI.

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

— Nivel 1: Políticas y planes específicos.

— Nivel 2: Normas de Privacidad y Seguridad de la Información.

— Nivel 3: Procedimientos y guías e instrucciones técnicas.

Al objeto de contar con un marco documental de desarrollo de la PPSI integrado, se procurará que cada documento, de un nivel determinado esté fundamentado en documentación de niveles superiores. Atendiendo a la necesidad de conocer, se dará acceso a la documentación de desarrollo de la PPSI siguiendo los procesos formales de gestión, acceso, publicación y difusión de la citada documentación.

7.1. 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 en un determinado ámbito.

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 la persona titular de la Consejería con competencia en administración electrónica a propuesta del órgano directivo competente, informando al CPSI.

7.2. NORMATIVA 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 regularizando su cumplimiento.

La Normativa será aprobada por el RPSI y se procederá a informar al CPSI.

7.3. PROCEDIMIENTOS Y GUÍAS E INSTRUCCIONES TÉCNICAS.

Los procedimientos definen formalmente la operativa de la ACAEx desarrollada en los mismos, de manera coherente con las medidas y controles de privacidad y seguridad de información que resulten aplicables al ámbito concreto.

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, mientras que las instrucciones técnicas conducen la operativa de las tareas técnicas definidas en procedimientos.

Los procedimientos de operación deben ser aprobados por el RPSI a propuesta del órgano o unidad administrativa con competencias en la materia.

Las guías e instrucciones técnicas serán, en su caso, aprobadas por la unidad administrativa con competencias en la materia.

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

8.1. ÓRGANOS COMPETENTES.

8.1.1. Consejo de Gobierno.

Corresponde al Consejo de Gobierno aprobar la Política de Seguridad y sus actualizaciones y revisiones.

8.1.2. Comisión de Coordinación de Administración Electrónica.

Esta comisión propone al Consejo de Gobierno la aprobación de la PPSI, sus revisiones y actualizaciones, a iniciativa del titular del órgano directivo con competencias en materia de administración electrónica.

8.1.3. Consejería competente en materia de Administración Electrónica.

La Consejería competente en materia de administración electrónica desarrollará reglamentariamente la PPSI del modo que se determina en la presente Política.

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

La organización operativa se basa en la distribución de competencias realizada en la LGACAEx y complementada en los correspondientes y vigentes Decretos de estructura orgánica básica de la Comunidad Autónoma. Para el caso de los Organismos Autónomos vinculados o dependientes de la ACAEx y en el ámbito de aplicación de esta PPSI, las responsabilidades se distribuirán a un nivel coherente al dispuesto para las Consejerías.

8.2.1. Responsables de la información.

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

Las personas titulares de los Centros Directivos a las que se refiere el artículo 59 de la LGACAEx, ejercerán como Responsables de la Información. Para los Organismos Autónomos vinculados o dependientes de la ACAEx, en el ámbito de aplicación de esta PPSI, las personas titulares de los Centros Directivos dependientes de la correspondiente Dirección Gerencia, asumirán el papel de los Responsables de Información.

8.2.2. Responsable de los Servicios.

Los Responsables de los Servicios tienen la potestad de establecer los requisitos de seguridad sobre los servicios de información que se presten a la ciudadanía o de aquellos otros de soporte a los mismos, contando para ello con el apoyo del Responsable de Información y del Responsable de Privacidad y Seguridad de la Información Sectorial.

Las personas titulares de los órganos de superior nivel funcionarial de las Consejerías u Organismos Autónomos, esto es, las personas responsables de Servicio o Unidad, ejercerán como Responsables de los Servicios.

8.2.3. Responsable del Sistema de Información.

El Responsable del Sistema de Información tiene como competencias operar el sistema de información, atendiendo a las medidas de seguridad y/o acciones correctivas determinadas por el Responsable de Privacidad y Seguridad.

Las personas titulares de los Servicios con competencias en el Desarrollo de Sistemas de Información o que ejerzan la Jefatura de Proyecto de carácter técnico de los mismos, asumirán las funciones y obligaciones del Responsable del Sistema.

8.2.4. Responsable de Privacidad y Seguridad de la Información.

Es quien determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y los servicios, asegurando el Marco Regulador de la ACAEx.

La persona Responsable de Privacidad y Seguridad de la Información se designará, vía Decreto de Estructura, de entre las personas titulares de los Centros Directivos a las que se refiere el artículo 59 de la LGACAEx, de la Consejería con competencias en materia de Administración Electrónica. Asumirá igualmente esta figura para los Organismos y Entes Públicos en el ámbito de aplicación de esta PPSI.

En el ejercicio de sus funciones, el Responsable de Privacidad y Seguridad de la información contará con el apoyo del Servicio con competencias en materia de Seguridad de la Información.

8.2.5. Responsables de Privacidad y Seguridad de la Información Sectoriales.

Los Responsables de Privacidad y Seguridad de la Información Sectoriales velan por la Privacidad y Seguridad de la Información en su ámbito de competencia, el cual se limita a los sistemas de información y servicios que sean competencia y responsabilidad directa de su departamento de pertenencia.

Las personas titulares de las Secretarías Generales a las que se refiere el artículo 58 LGACAEx, ejercerán como Responsables de Privacidad y Seguridad de la Información Sectoriales. Para los Organismos Autónomos vinculados o dependientes de la ACAEx en el ámbito de aplicación de esta PPSI, las personas titulares de los centros directivos asimilables a las Secretarías Generales del citado artículo 58, asumirán el papel de los Responsables de Privacidad y Seguridad Sectorial. En su defecto, dicho papel será asumido por la Dirección Gerencia del Organismo.

8.2.6. Administrador de la Seguridad.

El Administrador de Seguridad tiene como competencias ejecutar las acciones de operación del sistema de información, implementando, gestionar y mantener las medidas de seguridad aplicables al sistema y asegurar que éstas se cumplan estrictamente.

Asimismo, le corresponde reportar al Responsable de Privacidad y Seguridad de la Información los incidentes relativos a la seguridad del sistema y de las acciones de configuración, actualización o corrección, así como recopilar información sobre el desempeño del sistema de información en materia de seguridad.

Las personas titulares de la Unidad o Unidades Administrativas adscritas a la Consejería con competencias en materia de Administración Electrónica y que desarrollen funciones en seguridad de la información y seguridad operativa de los sistemas de información, ejercerán como Administrador de Seguridad.

8.2.7. Responsables del Tratamiento.

Los Responsables del Tratamiento son quienes determinan los fines y medios del tratamiento de los datos personales en sus respectivos ámbitos de competencia, esto es, en sus respectivas Consejerías u Organismos de adscripción, tal como indica el RGPD.

En el ámbito de la Presidencia y de las Consejerías de la Junta de Extremadura, las personas titulares de las Secretarías Generales a las que se refiere el artículo 58 de la LGACAEx ejercerán como Responsables de Tratamiento. Para los Organismos Autónomos vinculados o dependientes de la ACAEx en el ámbito de aplicación de esta PPSI, las personas titulares de los centros directivos asimilables a las Secretarías Generales del citado artículo 58, asumirán el papel de los Responsables del Tratamiento. En su defecto, dicho papel será asumido por la Dirección Gerencia del Organismo. En ambos casos, actuarán bajo la supervisión de las personas titulares de las correspondientes Consejerías de adscripción.

En el ejercicio de las funciones de Responsable del Tratamiento, contará con el apoyo de los Centros Directivos de la Consejería u Organismo Autónomo de adscripción.

8.2.8. 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 personales y actuar como punto de contacto con la autoridad de control y resto de autoridades en materia de protección de datos personales.

La persona que ejerce las funciones del Delegado de Protección de Datos en la ACAEx en el ámbito de aplicación de esta PPSI se designará, vía Decreto de Estructura orgánica básica, de entre las personas titulares de los Centros Directivos a las que se refiere el artículo 59 de la LGACAEx.

Asimismo, los Responsables de los Tratamientos de datos personales pueden, en función de los servicios e información que traten y escuchando la opinión del Delegado de Protección de Datos de la ACAEx, establecer o proponer, según corresponda, Delegados de Protección de Datos Sectoriales, que deberán coordinarse a través del Delegado de Protección de Datos de la ACAEx, por ser ésta figura el único punto de contacto con las autoridad de control y resto de autoridades en materia de protección de datos personales. En cualquier caso y, sobre todo, en caso de discrepancia, prevalecerá el criterio del DPD de la ACAEx sobre el de aquellos DPD sectoriales designados por los distintos responsables de tratamiento.

En el desempeño de sus tareas el delegado de protección de datos tendrá acceso a los datos personales y actividades de tratamiento llevadas a cabo en el ámbito de aplicación de esta PPSI, debiendo facilitarse dicho acceso por los distintos responsables de las Consejerías y Organismos. El DPD de la ACAEx contará con el apoyo de los DPD sectoriales para aquellas tareas provenientes de o relacionadas con sus respectivos departamentos.

8.2.9. Comité de Privacidad y Seguridad de la Información.

La persona titular de la Consejería con competencias en materia de administración electrónica estará asistida, en materia de protección de datos personales y seguridad de la información por el CPSI.

El CPSI se configura como un grupo de trabajo técnico que, además, prestará asistencia y coordinación en estas materias entre las distintas entidades incluidas en el alcance de esta Política. Está formado por:

— La persona titular de la Consejería con competencias en materia de administración electrónica, que presidirá el Comité.

— El Responsable de Privacidad y Seguridad de la Información, quien coordinará este Comité.

— Los Responsables de Privacidad y Seguridad de la Información Sectoriales.

— El Delegado de Protección de Datos.

— El órgano u órganos directivos competentes en materia de Administración Electrónica, Tecnologías de la Información y Comunicación o aquellos otros con competencias en Ciberseguridad.

— El órgano directivo competente en Función Pública.

— Titulares designados Responsables (operadores críticos) por el CNPIC en este ámbito.

— En su caso, las personas titulares de los Centros Directivos que se determine por el titular de la Consejería con competencias en materia de administración electrónica a propuesta del RPSI por razón de la temática concreta de la reunión.

Puntualmente, podrán formar parte del CPSI, en calidad de asesores, las personas que en cada caso proponga motivadamente alguno de sus miembros y previa aceptación del titular del Órgano Directivo coordinador del CPSI. Precisar, a su vez, que en función del régimen de competencias que se encuentre vigente, más de un rol de los indicados anteriormente podrían coincidir en el mismo Órgano o Centro Directivo.

Las delegaciones de asistencia de los respectivos titulares de los Centros Directivos que conforman el CPSI se realizarán a un nivel -mínimo- de Jefe de Servicio o Unidad dependientes del Órgano o Centro Directivo delegante, pudiendo realizarse esta delegación -solo- al nivel jerárquico inmediatamente inferior del delegante.

8.2.10. Operador crítico. Protección de Infraestructuras Críticas.

La Comisión Nacional de Protección de Infraestructuras Críticas es la competente para designar Operadores Críticos. Estos operadores críticos se designarán de entre los propietarios o gestores de las distintas Infraestructuras Críticas. En el caso de la Administración, se designarán de entre los Centros Directivos competentes sobre las infraestructuras críticas a un nivel mínimo de Dirección General.

Las funciones derivadas de esta designación son:

— La colaboración con la Secretaría de Estado de Seguridad y CNPIC en la protección de infraestructuras críticas en el ámbito de competencias de la Junta de Extremadura como operador de servicios esenciales.

— La elaboración de los distintos planes de seguridad y de protección derivados de las distintas infraestructuras críticas.

— La designación de los distintos Responsables y Delegados dimanantes de la normativa sectorial en esta materia.

— Trasladar a los distintos Responsables de los servicios esenciales soportados por las Infraestructuras Críticas de la ACAEx las necesidades derivadas de su protección y recabar de dichos Responsables los recursos su protección.

8.3. DIFERENCIACIÓN DE RESPONSABILIDADES.

En los sistemas de información se diferenciarán las figuras de responsable de la información, responsable del servicio, responsable de la seguridad y responsable del sistema.

De manera específica, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos, procurando la ausencia de dependencia jerárquica entre ambos roles.

Por otra parte, cuando no sea posible la ausencia de dependencia jerárquica entre los roles que asumen la responsabilidad de la seguridad de los sistemas de información y la de los sistemas, para aquellas decisiones que deba tomar el responsable de seguridad de la información que afecten a la seguridad de los sistemas cuyo responsable esté en su ámbito de dependencia jerárquica, se apoyará en informe motivado del Administrador de Seguridad.

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

El ENS, como casi cualquier normativa o estándar de seguridad, se estructura en principios, requisitos y medidas de seguridad, aportando así un enfoque de lo más general a lo más concreto en su desarrollo.

Los principios son las premisas a tener en cuenta para garantizar que una organización puede cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información y que se concretan en requisitos mínimos como especificaciones para una protección adecuada de la información y los servicios. Los anteriores descienden a un conjunto de medidas de seguridad que conducen el proceso de seguridad para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos.

9.1. PRINCIPIOS BÁSICOS.

La ACAEx, para la gestión de la Privacidad y Seguridad de la Información como proceso iterativo para la mejora continua y el control del nivel de riesgo seguirá los siguientes principios:

En el ámbito de la protección de datos personales:

a) Licitud, lealtad y transparencia: Los datos personales se tratarán de manera lícita, leal y transparente en relación con el interesado.

b) Legitimación en el tratamiento de datos personales: Solo se llevará a cabo el tratamiento cuando esté legitimado en la normativa aplicable.

c) Limitación de la finalidad: Serán tratados, únicamente, para el cumplimiento de fines determinados, explícitos y legítimos, y no ulteriormente de manera incompatible con dichos fines.

d) Minimización de datos: Serán adecuados, pertinentes y limitados a los fines para los que son tratados.

e) Exactitud: Serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación cuando sean inexactos impidiendo el cumplimiento de la finalidad.

f) Limitación del plazo de conservación: 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: Se garantizará 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 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) 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.

En el ámbito de la seguridad de la información:

a) 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.

b) Seguridad integral: La seguridad en la Junta de Extremadura se entiende como un proceso integral coordinado y planificado que atañe a todos los elementos humanos, materiales, técnicos, jurídicos, organizativos e infraestructuras relacionados con el sistema de información y que evita, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.

c) Gestión de riesgos: La gestión del riesgo es piedra angular del proceso de seguridad de la información de la ACAEx por permitir el mantenimiento de un entorno controlado que mantenga los riesgos en niveles aceptables. La identificación y reducción de estos niveles se realizará mediante el despliegue de un proceso fundamentado e integrado que permita la aplicación de medidas de seguridad de manera equilibrada entre la naturaleza y valoración de los activos afectados, el impacto y la probabilidad de los riesgos a los que estén expuestos y el coste y eficacia 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.

d) Prevención, detección, respuesta y conservación: La seguridad del sistema contemplará acciones relativas a todos estos aspectos y orientadas a minimizar sus vulnerabilidades, reduciendo la probabilidad de materialización de amenazas sobre el sistema o controlando el impacto que las mismas tendrían. Así, prevención, detección y respuesta - recuperación constituyen el modelo de operación de la seguridad del sistema de información; sin perjuicio de que las medidas de seguridad desplegadas sobre el sistema deban garantizar la conservación de datos e información.

e) Líneas de defensa: Los sistemas de información han de disponer de una estrategia de protección constituida por múltiples capas de seguridad que permitan la respuesta a incidentes proporcionada y siguiendo un esquema de contención, mitigación y recuperación.

f) Reevaluación periódica: La gestión de la Privacidad y Seguridad de la Información se revisará, evaluará y actualizará periódicamente para mantener su eficacia de forma

continua, con la finalidad de hacer frente a la constante evolución de los riesgos con medidas de seguridad eficaces.

g) 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, observando siempre el principio de mínimo privilegio en el acceso a la información.

h) 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.

i) Vigilancia continua: Establecer mecanismos jurídicos, técnicos y organizativos para la detección de actividades o comportamientos anómalos y su oportuna respuesta.

j) Cultura de la Privacidad y la Seguridad: La Cultura se refiere a los conocimientos, percepciones, actitudes y madurez en este ámbito de los diversos actores que intervienen en la ACAEx.

9.2. REQUISITOS MÍNIMOS.

La ACAEx establece los siguientes requisitos mínimos, que han de guiar 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 diferenciando, a su vez, roles y responsabilidades tal como se establecen en el mismo.

b) Análisis y gestión de los riesgos: La ACAEX debe gestionar sus riesgos empleando metodologías reconocidas. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá proporcionalidad entre ellas y los riesgos considerando, asimismo, el tratamiento de datos personales.

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

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

e) Profesionalidad: El personal de las entidades incluidas en el alcance de este documento tendrá la formación y/o información necesaria para el desarrollo de su puesto

de trabajo en condiciones de seguridad. A su vez, el personal que desarrolle funciones en el ámbito de la Privacidad y Seguridad de la Información dispondrá de la capacitación adecuada para la ejecución de las tareas encomendadas, siendo exigible esta capacitación para el personal de terceros que presten sus servicios en este ámbito.

f) Autorización y control de los accesos: El acceso a los sistemas de información estará controlado y limitado. Cada usuario, proceso, dispositivo, aplicación y otros sistemas que accedan a la información de los sistemas de la ACAEx estará identificado y debidamente autorizado para el acceso exclusivo a las funciones permitidas.

g) Protección de las instalaciones: Las instalaciones de la ACAEx contarán con medidas de seguridad física adecuadas a la información que tratan y servicios que prestan. Las infraestructuras críticas contarán con los instrumentos de protección específicos conforme a esta tipología.

h) Adquisición de productos y contratación de servicios: En la adquisición de productos y contratación de servicios de seguridad, se atenderá, de manera proporcionada, a la categoría y el nivel de seguridad determinados para los sistemas de información afectados, exigiendo en consecuencia la certificación de conformidad con el ENS, así como otras certificaciones internacionales, 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. Serán objeto de especial estudio las necesidades de las soluciones de ciberseguridad, la interconexión entre plataformas de entidades externas y la prestación de servicios en la nube.

i) Seguridad por defecto y mínimo privilegio: Los sistemas de información deben diseñarse y configurarse de forma que proporcionen la funcionalidad e información mínimas requeridas, incluidas aquellas funciones relacionadas con la operación, administración y registro de actividad, asegurando su disponibilidad, pero también que una utilización insegura requiera de un acto consciente por parte del usuario.

j) Integridad y actualización del sistema: El estado de seguridad de los sistemas de información se mantendrá actualizado conforme con las especificaciones de los fabricantes, vulnerabilidades y las actualizaciones que les afecten, de forma que dicho estado sirva como entrada a las actividades de gestión de riesgos. La actualización del sistema que afecte al estado de seguridad se ejecutará conforme al proceso de autorización aprobado en la ACAEx.

k) 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 entor-

nos 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 estos.

l) Interconexión de sistemas: Se protegerán las comunicaciones entre sistemas de información y con sistemas externos, en particular, los puntos de interconexión entre las redes que soporten dichas comunicaciones y especialmente aquellas que se realicen a través de redes públicas.

m) 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.

n) 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.

o) Continuidad de la actividad: La continuidad de las operaciones se basará en la formalización y prueba de los procesos técnicos que la soportan, como los de copia de seguridad de los sistemas.

p) Mejora continua del proceso de seguridad: La gestión de Privacidad y Seguridad de la Información estará sometida a un ciclo de mejora continua y coherente con el principio de reevaluación periódica.

10. SISTEMA DE GESTIÓN DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

La ACAEx considera fundamental la gestión de la privacidad y seguridad de la información, por lo que se plantea como objetivo disponer de un sistema de gestión que incluya la planificación, organización, control de recursos de privacidad y seguridad de la información con mejora continua, actualización y aprobación periódica.

10.1. PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

El proceso de protección de datos personales en la ACAEx se regirá por las siguientes directrices que conducen el cumplimiento de los principios de protección de datos.

10.1.1. Responsabilidad proactiva y modelo de gobierno.

El responsable del tratamiento deberá garantizar el cumplimiento de la normativa de protección de datos personales y tener la capacidad de demostrarlo o evidenciarlo.

Para cumplir con la responsabilidad proactiva en ACAEx resultará necesaria la concienciación y formación del personal que realice tratamiento de datos personales, de manera que conozcan sus obligaciones y responsabilidades asociadas y colaboren en el proceso de recopilación y almacenamiento de evidencias de cumplimiento, así como la articulación del proceso de cumplimiento de la normativa de protección de datos coherente con la presente política.

a) Detección de la necesidad.

La realización del tratamiento de datos personales estará precedida por un necesario análisis de necesidad, idoneidad y proporcionalidad, cuya conclusión debe ser que el tratamiento resulta imprescindible para cumplir con las funciones del Responsable del Tratamiento.

b) Identificación de actividades de tratamiento y evaluación objetiva del riesgo.

Una vez detectada la necesidad de uso de datos personales en el marco de algún procedimiento, gestión o servicio administrativo, dicha actividad será determinada y caracterizada con precisión. Este proceso de caracterización será conducido por los principios de la protección de datos personales.

c) Registro de Actividades de Tratamiento.

La ACAEx mantendrá actualizado el registro de las actividades de tratamiento de datos personales que incluirá toda la información requerida normativamente y que podrá consultarse en el Punto de Acceso General de la ACAEx.

d) Información del tratamiento.

La información a los interesados sobre el tratamiento de datos personales es esencial para la ACAEx, como lo es para el cumplimiento del principio de transparencia y para acreditar el cumplimiento del resto de principios de la protección de datos personales. Se cumplirá con el deber de información facilitando el acceso a la misma de forma fácil e intuitiva, salvo aquellos casos que la información al interesado esté excepcionada en la normativa reguladora.

e) Ejercicio de derechos.

La ACAEx mantendrá canales habilitados para el ejercicio de los derechos de las personas interesadas, así como para proporcionar la información que proceda de manera concisa, transparente, inteligible y de fácil acceso en los plazos previstos a tal efecto, informando del resto de canales habilitados, así como la posibilidad de acudir a la tutela de la Autoridad de Control.

f) Transferencias internacionales.

Solo podrán realizarse transferencias internacionales a terceros países en que se cumplan determinadas garantías reguladas normativamente. La ACAEX, consciente de la actual deslocalización de los datos electrónicos, velará por que el tratamiento de los datos personales en su ámbito de responsabilidad se produzca cumpliendo con estas garantías.

10.1.2. Privacidad desde el Diseño y por Defecto.

a) Gestión de riesgos.

El principio de privacidad desde el diseño y por defecto obliga a considerar la protección de datos desde la concepción y diseño de los procesos y procedimientos. La ACAEx seguirá un proceso formal de análisis de riesgos y, en su caso, de evaluación de impacto de los tratamientos de datos personales de forma previa a su realización.

De manera periódica o cuando existan cambios sustanciales en las actividades, revisará los análisis de riesgos realizados, y en su caso, evaluaciones de impacto en protección de datos, con el objetivo de identificar nuevos riesgos y gestionar los riesgos existentes minimizándolos hasta los niveles que puedan considerarse aceptables.

El proceso expuesto conlleva un análisis de riesgos para los derechos y libertades de las personas objeto del tratamiento de datos, así como el análisis de los riesgos tecnológicos sobre los sistemas de información que soporten dichas actividades.

Los Responsables de la Información y 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.

b) Medidas de seguridad.

La ACAEx determinará e implementará las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en privacidad sobre las actividades de tratamiento. En este sentido, se incluirán entre otras en función del grado de control necesario para el tratamiento específico:

i. Mínimo privilegio en el acceso a datos personales, garantizando el acceso a aquella información imprescindible para el puesto de trabajo concreto.

ii. La pseudonimización y el cifrado de los datos personales;

iii. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de manera continua en los sistemas y servicios de tratamiento;

iv. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

v. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

c) Gestión de brechas de seguridad de los datos personales.

La ACAEX habilitará mecanismos que posibiliten la detección temprana de aquellas situaciones que puedan suponer una brecha de seguridad en la gestión de los datos personales y establecerá los procedimientos para su investigación y análisis, identificación y adopción de medidas de contención y mitigación de riesgos, así como eliminación de causas y/o resolución de problemas causantes.

La ACAEx prestará especial atención y no retrasará el proceso de toma de decisión en relación con la notificación a la Autoridad de Control y / o comunicación a los interesados del incidente sufrido, adoptando las medidas necesarias que garanticen la notificación a la Autoridad de Control y comunicación a las personas interesadas, según corresponda, de las violaciones y/o incidentes de seguridad de los datos personales que pudieran producirse siguiendo los procedimientos establecidos por la Autoridad de Control.

Entre los mecanismos a habilitar para la gestión eficiente de incidentes y brechas de datos personales estarán aquellos que propicien la detección temprana y proactiva de vulnerabilidades, así como los procedimientos de respuesta ágiles y efectivos que garanticen la investigación de la brecha, la adopción de medidas para mitigar los riesgos o consecuencias adversas derivadas de la misma y la toma de decisión en relación con la notificación a la Autoridad de Control y / o comunicación a los interesados del incidente sufrido.

10.1.3. Relaciones con terceros en el ámbito de la privacidad.

La ACAEX, en el ámbito de la colaboración con distintas entidades públicas o privadas velará porque el tratamiento de datos personales se produzca de cumplimiento con los

principios y garantías previstos en la normativa aplicable y, especialmente, bajo la premisa de mínimo privilegio.

Los citados accesos estarán precedidos del análisis del supuesto concreto que determine la responsabilidad o corresponsabilidad de cada uno de los intervinientes en el proceso, la existencia de acuerdos que regularicen el tratamiento ajustados al modelo de colaboración concreto, las características y finalidades de los tratamientos y las medidas de seguridad apropiadas.

El acceso a datos por cuenta de terceros se llevará a cabo, fundamentalmente, mediante encargo de tratamiento, acuerdo de cesión o de corresponsabilidad en el tratamiento, según corresponda, estando habilitada la Administración para articular los procedimientos técnicos necesarios para supervisar el cumplimiento de las previsiones concretas.

10.2. SEGURIDAD DE LA INFORMACIÓN.

10.2.1. Gobernanza.

ACAEx ha implantado un sistema orientado al riesgo, mediante el cual se dirigen y controlan las actividades de seguridad de la información para cumplir con los objetivos establecidos frente a las amenazas a las que están expuestos los procesos de esta Administración y los activos de información que los soportan.

A su vez, el gobierno de la seguridad de la información está soportado en la distribución orgánica de funciones descrita en esta Política y que asegura la segregación de funciones y la independencia de los roles de ACAEx en la definición, la implementación y la supervisión del cumplimiento de las medidas de control derivadas de los riesgos observados y el nivel de riesgo aceptable determinado por esta Administración.

10.2.2. Gestión del riesgo.

Las medidas de seguridad son definidas mediante un enfoque sistemático basado en la gestión del riesgo, contemplando los principios básicos descritos en esta política. En este sentido, ACAEx tiene en consideración los distintos requisitos derivados de la normativa de seguridad de la información aplicable, así como las mejores prácticas en la materia.

Esta gestión del riesgo se aborda desde el diseño (nuevos requisitos aplicables a las necesidades de negocio y del contexto de la ACAEx) y por defecto (medidas de control base orientadas a la criticidad inherente de los procesos y activos de información que los soportan) y se lleva a cabo mediante un proceso sistemático que recoge:

a) Identificación y protección, correspondientes a la planificación y provisión de recursos para lograr los objetivos que emanan del gobierno de la seguridad de la información.

b) Detección, respuesta y recuperación, soportadas en las actividades de gestión de seguridad de la información, con la finalidad de mantener en el nivel de riesgo determinado los activos de la información afectados.

c) Control y mejora, mediante las actividades de control del gobierno de la seguridad de la información.

10.3. CUMPLIMIENTO.

ACAEx establece la responsabilidad proactiva y mejora continua en el gobierno de la seguridad de la información, en la gestión de riesgo, así como en el mismo cumplimiento interno.

Para ello ACAEx define revisiones planificadas para evaluar la gestión de riesgos de la seguridad de la información, contemplando:

a) Reevaluar y actualizar periódicamente los riesgos a los que la Administración está expuesta.

b) Evaluar la eficacia de las medidas implantadas para la gestión de dichos riesgos.

Las medidas identificadas en los análisis realizados estarán orientadas a gestionar riesgos sobre los procesos y activos de información y estarán alineadas con la legislación y regulación aplicable, así como con otros requisitos de aplicación que se identifiquen. Por otra parte, los incumplimientos sobre las medidas implantadas formarán parte de las acciones de mejora a recoger en el plan de mejora de la seguridad, sin perjuicio de las acciones de carácter inmediato que deban llevarse a cabo para la contención y/o mitigación del riesgo derivado de un incumplimiento, así como para la identificación de responsabilidades.

10.4. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS.

La ACAEx establece la gestión de la seguridad como un proceso corporativo global y consecuencia del desarrollo del marco establecido en la presente PPSI de la organización. Dada la existencia de Infraestructuras Críticas en el ámbito de aplicación de esta Política y atendiendo al carácter global de la misma, se procede a regular este ámbito de la siguiente manera:

10.4.1. Carácter integral de la seguridad.

En el ámbito de la Protección de las Infraestructuras Críticas, la PPSI constituye también el marco de referencia para la Política General de Seguridad del Operador que se identifica en el Plan de Seguridad del Operador (PSO) de la ACAEx, siendo este el instrumento de planificación del Sistema de Protección de Infraestructuras Criticas.

Por tanto, la ACAEx hará referencia, en el PSO, a esta PPSI como base de la seguridad integral del conjunto de instalaciones o sistemas de propiedad o gestión de la ACAEx que tienen la consideración de infraestructuras críticas, por ser necesarios para garantizar a la Ciudadanía el acceso a los servicios prestados como Operador de Servicios Esenciales, así como a los procesos de continuidad que permiten la resiliencia de los servicios de la ACAEx.

En línea con lo anterior, los aspectos y ámbitos de protección que desarrolla la PPSI y que tienen un mayor impacto en la Protección de Infraestructuras Críticas y que así deberán considerarse en el PSO, serán:

— La Organización para la seguridad de la información.

— La protección de instalaciones, comunicaciones e infraestructuras.

— Gestión de incidentes de seguridad.

— La continuidad de los servicios.

— La explotación y monitorización de los sistemas y servicios.

10.4.2. Roles y responsabilidades en materia de PIC.

Los operadores de infraestructuras críticas de la Junta de Extremadura estarán representados en el CPSI. Así mismo, de las decisiones que deban adoptarse en este ámbito se informará al CPSI.

Los roles más relevantes, sin perjuicio de otros que deban identificarse más adelante o deban dar soporte a los mismos en la toma de decisiones o ejecución de acciones, son:

— Operador de Infraestructuras Críticas – El Centro Directivo designado por el CNPIC como Operador Crítico de la Infraestructura responsabilidad de la ACAEx que alberga los sistemas de información que soportan la prestación de servicios esenciales a la Ciudadanía.

— Operador de Servicios Esenciales. El Centro Directivo designado por el CNPIC como Operador de Servicios Esenciales.

— RSI – la Unidad administrativa con competencias en Seguridad de la Información dependiente del Responsable de Privacidad y Seguridad de la Información.

— RSE – la Unidad administrativa con competencias en materia de soporte a las infraestructuras designadas como críticas.

10.4.3. Marco de gobierno de PIC y cultura de seguridad.

Con el objetivo de disponer de los recursos adecuados para la gestión integral de la Seguridad, así como definir las responsabilidades necesarias en cuanto a la definición, implantación y seguimiento de políticas, procedimientos, controles y medidas de seguridad en la organización, la ACAEx detallará y mantendrá actualizada, en los instrumentos de planificación de la seguridad del operador crítico, la estructura organizativa que comprenderá, tanto la seguridad física como la ciberseguridad.

A su vez, con el objetivo de mantener una cultura de seguridad permanente, la ACAEx prestará especial atención a la preparación de recursos formativos para el personal con responsabilidades específicas en la materia y de concienciación para todo el personal en general.

10.4.4. Servicios esenciales soportados por la infraestructura crítica.

Será responsabilidad del operador crítico designado mantener inventariados, de manera precisa y actualizada, los servicios esenciales que se prestan y los sistemas e infraestructura que les dan soporte. Cuando difieran las figuras de Operador Crítico y Operador Esencial, deberán colaborar para la catalogación e inventario de los citados servicios esenciales.

11. EVALUACIÓN DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

De manera periódica y conforme al perfil de cumplimiento de los activos involucrados se llevará a cabo una evaluación del cumplimiento de las medidas establecidas por la ACAEx para la gestión de privacidad y seguridad de la información.

Para la realización de la evaluación se seguirá un proceso sistemático y documentado cuyos resultados formarán parte del proceso de revisión y mejora de la privacidad y seguridad.

El responsable del proceso de evaluación será el Responsables de Privacidad y Seguridad de la Información. En dicho proceso deberán participar activamente los Responsables de privacidad y seguridad sectoriales, Responsables de Tratamiento y Delegados de Protec-

ción de Datos, estando obligados a aportar, al RPSI, los recursos que resulten necesarios para su realización.

12. ORGANISMO PAGADOR DE EXTREMADURA.

El Organismo Pagador de los Fondos Europeos Agrícolas de Garantía (FEAGA) y de Desarrollo Rural (FEADER), en base a sus obligaciones legales y normativas derivadas de la gestión de los citados fondos y de manera transitoria, podrá mantener una estructura organizativa específica y complementaria a la del RPSI de la Junta de Extremadura, para la gestión de la Privacidad y Seguridad de la Información en lo referente a sus competencias como Organismo Pagador.

La citada estructura, la normativa y las actuaciones que puedan desarrollarse en el ámbito de la privacidad y seguridad de la información del Organismo Pagador deberán ser coherentes con las de la ACAEx, en general, y con esta PPSI, para lo cual Organismo Pagador informará de las distintas planificaciones y resultados en este ámbito, atendiendo a las recomendaciones que se emitan por RPSI y CPSI.

Al objeto de que el RPSI de la ACAEx pueda desarrollar sus competencias en esta materia, Organismo Pagador facilitará, al personal designado por este o dependiente del mismo, el acceso a los recursos de información, documentales y de cualquier otra índole que resulten necesarios para el Gobierno de la Privacidad y Seguridad de la Información en la ACAEx.

A su vez, Organismo Pagador presentará al RPSI, sin dilación, los resultados de las evaluaciones en privacidad y seguridad de la información -internas y externas- que se lleven a cabo y con periodicidad anual, dentro del primer trimestre de cada año, un informe de su estado de la Seguridad de la Información.

13. RELACIÓN CON TERCERAS PARTES.

Cuando un tercero lleve a cabo un suministro, preste un servicio, utilice o se le cedan activos de información de la ACAEx, deberá cumplir con esta PPSI, así como con el desarrollo de la misma en lo que respecta al ámbito de la colaboración.

Los contratos, encargos o convenios que se suscriban con terceros deben incluir la obligación de cumplir esta Política, el sistema de verificación de su cumplimiento y la designación de una persona o punto de contacto para la seguridad de la información tratada o el servicio prestado que canalice y supervise el cumplimiento de los requisitos de aplicación y la gestión de incidentes de privacidad y seguridad de la información para el ámbito de la colaboración que realice.

Las obligaciones en materia de privacidad y seguridad de la información de los terceros que colaboren con la ACAEx se extenderán a aquellos otros -subcontratistas, proveedores y/o colaboradores- que participen en la cadena de provisión necesaria para la prestación del servicio o suministro.

Las personas de la ACAEx responsables de los contratos, encargos o convenios, suscritos con terceras partes serán responsables de la verificación, a lo largo de la vida de dichos instrumentos, de los requisitos de privacidad y seguridad establecidos en estos.

• • •