I. Principado de Asturias

• Otras Disposiciones

CONSEJERÍA DE HACIENDA, JUSTICIA Y ASUNTOS EUROPEOS

ENTE PÚBLICO DE SERVICIOS TRIBUTARIOS DEL PRINCIPADO DE ASTURIAS

RESOLUCIÓN de 4 de noviembre de 2026, de la Presidencia del Ente Público de Servicios Tributarios del Principado de Asturias, por la que se aprueba la política de seguridad de la información y protección de datos personales del ente público de Servicios Tributarios del Principado de Asturias.

El artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que el Esquema Nacional de Seguridad (ENS) tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el sector público, mediante principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), dispone en el artículo 1.2 que éste está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

En su artículo 2 el Real Decreto 311/2022, de 3 de mayo, indica que es de aplicación a todo el sector público, en el que está incluido el Ente Público de Servicios Tributarios del Principado de Asturias (Ente Público).

El artículo 10 de la Ley del Principado de Asturias 15/2002, de 27 de diciembre, de acompañamiento a la Ley de Presupuestos Generales para 2003, creó el Ente Público, como organización administrativa responsable, en nombre y por cuenta del Principado de Asturias, de la aplicación efectiva del sistema tributario de la comunidad autónoma y de aquellos otros recursos de otras administraciones y entidades que se le atribuyan por ley o por convenio.

La implantación de las tecnologías de la información y de las comunicaciones en el Ente Público para el ejercicio de sus funciones y su continua evolución han ido facilitado el avance y la mejora de la calidad de los servicios que presta, con eficacia y eficiencia en la gestión de los mismos.

En su operativa diaria, el Ente Público depende de los sistemas de información para alcanzar sus objetivos que deben ser administrados con diligencia, adoptando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

En su artículo 12 Real Decreto 311/2022, de 3 de mayo, establece que:

"La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente. No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización."

En este contexto y por lo que se refiere a la Administración del Principado de Asturias, la Orden de 35 de marzo de 2026, de la Consejería de Presidencia, Reto Demográfico, Igualdad y Turismo, aprueba la Política de Seguridad de la Información y Protección de Datos Personales de la Administración del Principado de Asturias, que, en lo que a su alcance se refiere, dispone que "los entes que se encuentren dentro del ámbito de aplicación de esta política podrán complementarla con documentos específicos que recojan sus particularidades y requisitos adicionales en materia de seguridad, siempre que estos se ajusten al marco general establecido."

Cód. 2026-09349

Además, la protección de los datos personales regulada por el Reglamento general de protección de datos): 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 a tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) deben ser un todo integrado y coordinado, por lo que la política de seguridad en el Ente Público debe incluir la protección de los datos de carácter personal y sin que ello suponga pérdida de competencias o responsabilidad en cada ámbito (ENS y RGPD)

Mediante la presente Resolución, el Ente Público establece para sus sistemas de información propios un marco de gestión de la seguridad según lo establecido por el ENS, reconociendo como activos estratégicos la información que maneja, los servicios que presta y los sistemas TIC que soportan aquella y hacen posible estos, incluyendo el tratamiento de los datos personales de los que sean responsables los órganos del Ente Público.

En el artículo 12 del citado Real Decreto 311/2022, de 3 de mayo se establece que cada Administración Pública, órgano o entidad con personalidad jurídica propia comprendida en su ámbito de aplicación deberá contar con una política de seguridad formalmente aprobada por el órgano competente. De acuerdo con lo anterior y de conformidad con este precepto, y de acuerdo con el artículo 25 del Reglamento de organización y funcionamiento del Ente Público, aprobado por Decreto 38/2005, de 12 de mayo.

R E S U E L V O

Primero.—Aprobar la Política de Seguridad de la Información y Protección de Datos Personales del Ente Público de Servicios Tributarios del Principado de Asturias, cuyo texto se incorpora como anexo y, que será efectiva desde el día siguiente al de la publicación en el *Boletín Oficial del Principado de Asturias*.

Segundo.—Ordenar la publicación de la presente Resolución en el *Boletín Oficial del Principado de Asturias*. También se publicará en el portal de trasparencia y en la sede electrónica del Ente Público.

Oviedo, a 4 de noviembre de 2026.—El Presidente.—Cód. 2026-09349.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ENTE PÚBLICO DE SERVICIOS TRIBUTARIOS DEL PRINCIPADO DE ASTURIAS

Índice.

Siglas y acrónimos.

Glosario.

1. Misión del Ente Público de Servicios Tributarios del Principado de Asturias.
2. Objetivos de la política de seguridad y de protección de datos personales.
3. Alcance.
4. Marco normativo.
5. Principios rectores de la política.
    5.1. Principios básicos de la seguridad de la información.
    5.2. Principios básicos de protección de datos.
6. Organización de la seguridad y la protección de datos.
    6.1. Definición de roles, funciones y responsabilidades asociados al ENS.
    6.2. Definición de roles, funciones y responsabilidades asociados a la protección de datos personales.
    6.3. Designación de roles y responsabilidades.
        6.3.1. Asociados al ENS.
        6.3.2. Asociados a la protección de datos personales.
    6.4. Comité de seguridad de la información.
    6.5. Procedimientos de designación.
    6.6. Resolución de conflictos.
    6.7. Creación de grupos de trabajo.
7. Desarrollo de la política de seguridad de la información y protección de datos.
8. Gestión de riesgos.
9. Obligaciones del personal del Ente Público.
10. Terceras partes.
11. Auditoría y control.
12. Aprobación y entrada en vigor.

Cód. 2026-09349

Siglas y acrónimos.

ENS: Esquema Nacional de Seguridad.

RGPD (Reglamento general de protección de datos): 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 a tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

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

CCN: Centro Criptológico Nacional.

AEPD: Agencia Española de Protección de Datos.

DPD: Delegado/a de Protección de Datos.

POC: Punto de contacto.

Glosario.

Los términos, palabras, expresiones y las definiciones contenidas en este documento han de ser entendidos en el siguiente sentido:

a) Gestión de riesgos: actividades coordinadas a dirigir y controlar los riesgos dentro de la organización.

b) Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

c) Sistema de Información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

d) Datos personales: toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

e) Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

1.—*Misión del Ente Público de Servicios Tributarios del Principado de Asturias.*

El Ente Público de Servicios Tributarios del Principado de Asturias (en adelante, Ente Público) es la organización administrativa responsable, en nombre y por cuenta de la Administración del Principado de Asturias, de la aplicación efectiva del sistema tributario de ésta, y de aquellos recursos del Estado u otras Administraciones y Entidades que se le atribuyan por ley o por convenio.

Corresponde al Ente Público el ejercicio de las siguientes competencias:

- La gestión, liquidación, inspección, recaudación y revisión de los tributos propios y demás ingresos de derecho público del Principado de Asturias cuya competencia tenga atribuida la Consejería competente en materia tributaria, salvo que expresamente se hubiera atribuido a otro órgano de la Administración del Principado de Asturias.
- La gestión, liquidación, inspección, recaudación y revisión de los tributos cedidos por el Estado, de acuerdo con la Ley que fije el alcance y condiciones de la cesión.
- La gestión, liquidación, inspección, recaudación y revisión de los tributos locales cuya competencia le haya sido delegada por las corporaciones locales.
- El ejercicio de la potestad sancionadora en relación con los tributos cuya aplicación corresponda al Ente Público de Servicios Tributarios del Principado de Asturias.
- Cualesquiera otras competencias que pudieran serle atribuidas.

En su operativa diaria, el Ente Público depende de los sistemas de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que el Ente Público pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para los cuales ha sido constituido, manteniendo la calidad de la información y la prestación continuada de los servicios, actuando preventivamente ante posibles amenazas, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Para defenderse de estas amenazas se deberán aplicar las medidas mínimas de seguridad exigidas por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS, así como realizar un seguimiento continuo de los niveles

Cód. 2026-09349

de prestación de servicios y las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Para el Ente Público la seguridad es una parte integral de cada etapa del ciclo de vida de los sistemas de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y sus necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales o se adquieran servicios que afecten a los sistemas de información.

Igualmente, el ejercicio de las competencias atribuidas al Ente Público implica el tratamiento continuado de datos personales en ámbitos esenciales de la actividad tributaria, incluyendo la gestión, liquidación, inspección, recaudación y revisión, así como la prestación de servicios presenciales y electrónicos a los administrados. El Ente Público debe garantizar que dichos tratamientos se realizan conforme a los principios básicos de la normativa de protección de datos que se detallan más adelante.

La protección de los datos personales constituye un elemento inseparable de la seguridad de la información. En aplicación del RGPD, de la LOPDPyGDG, y del ENS, el Ente Público adoptará las medidas técnicas y organizativas necesarias para garantizar y poder demostrar el cumplimiento de dichas obligaciones, integrando la gestión de la seguridad y la protección de datos en todos los tratamientos, sistemas y servicios que utilice.

La presente Política se desarrolla de forma coordinada con la Política de Seguridad de la Información y Protección de Datos Personales del Principado de Asturias, aplicable cuando el Ente Público hace uso de los recursos o sistemas de información gestionados por la Dirección General con competencias en el ámbito TIC del Principado de Asturias.

2.—*Objetivos de la política de seguridad y de protección de datos personales.*

2.1.—Objetivos en el ámbito de la seguridad.

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar al personal del Ente Público respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmitida a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

2.2.—Objetivos en el ámbito de protección de datos personales.

- Establecer los principios, criterios de actuación, responsabilidades y mecanismos organizativos aplicables al tratamiento de datos personales realizado por Ente Público.
- Garantizar la licitud y el cumplimiento de los principios de protección de datos en todos los tratamientos realizados por el Ente Público.
- Garantizar la protección de los derechos y libertades de las personas físicas cuyos datos sean tratados por el Ente Público.
- Aplicar medidas técnicas y organizativas apropiadas conforme al riesgo y al principio de responsabilidad proactiva.
- Integrar la protección de datos desde el diseño y por defecto en los procesos, servicios y sistemas de información.
- Asegurar la supervisión, revisión y mejora continua del modelo de cumplimiento en materia de protección de datos.

Cód. 2026-09349

3.—*Alcance.*

La presente Política se aplicará a todos los sistemas de información del Ente Público, así como a todos los tratamientos de datos personales de los que sea responsable en el ejercicio de sus competencias, con independencia de que dichos tratamientos se realicen por medios electrónicos, en soporte papel o mediante cualquier otro soporte. Se aplica a todas las personas que, con independencia de la naturaleza de su relación jurídica con el Ente Público, tengan acceso autorizado a sus sistemas de información o a información tratada por éste, incluidos, los empleados públicos, las empresas contratistas y cualquier otra persona usuaria autorizada.

La presente Política complementa la Política de Seguridad de la Información y Protección de Datos Personales del Principado de Asturias y desarrolla sus previsiones en aquellas materias que requieren adaptación a la organización, funciones tributarias, sistemas de información y actividades de tratamiento propias del Ente Público.

4.—*Marco normativo.*

El marco normativo, en materia de seguridad de la información y protección de datos personales, en que se desarrollan las actividades del Ente Público y, en particular la prestación de sus servicios, se encuentra recogido en una norma de seguridad específica al efecto, dentro del primer nivel normativo que desarrolla esta Política, bajo la denominación "Cumplimiento Normativo". Esta norma estará disponible y permanentemente actualizada en el repositorio del Ente Público donde se ubique el conjunto del cuerpo normativo de seguridad.

5.—*Principios rectores de la política.*

5.1.—Principios básicos de la seguridad de la información.

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

- Alcance estratégico.

  La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles del Ente Público y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.

- Seguridad integral.

  La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de la seguridad basada en el riesgo.

  La gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

- Prevención, detección, respuesta y conservación.

  Implementando acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando éstas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- Existencia de líneas de defensa.

  La estrategia de seguridad del Ente Público se diseña e implementa en capas de seguridad.

- Vigilancia continua y reevaluación periódica.

  El Ente Público establece medios para detectar y responder a actividades o comportamientos anómalos. Además de otros que permitan una evaluación continuada del estado de seguridad de los activos, existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

- Seguridad por defecto y desde el diseño.

  Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

- Diferenciación de responsabilidades.

  En aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

5.2.—Principios básicos de protección de datos.

El Ente Público debe garantizar que los tratamientos de datos personales se realicen conforme a los siguientes principios establecidos en el Capítulo II del RGPD y en el Título II de la LOPDPyGDG:

- Licitud, lealtad y transparencia.

Cód. 2026-09349

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

- Legitimación.

  Sólo 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.

- Limitación de la finalidad.

  Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

- Minimización de datos.

  Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que sean tratados.

- Exactitud.

  Los datos personales serán exactos y, en su caso, 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.

- Limitación del plazo de conservación.

  Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que pudieran derivarse de su tratamiento. Los datos podrán conservarse durante períodos más largos cuando sean tratados exclusivamente con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, de acuerdo con lo establecido en el RGPD.

- Integridad y confidencialidad.

  Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

- Responsabilidad proactiva.

  El Ente público aplicará las medidas técnicas y organizativas adecuadas a fin de garantizar y poder demostrar que el tratamiento de los datos se hace conforme con la normativa vigente en materia de protección de datos.

- Atención efectiva de los derechos de las personas interesadas.

  Se adoptarán medidas en el Ente Público que garanticen el ejercicio y la atención de los derechos de protección de datos de forma eficaz y dentro de los plazos legales.

- Proporcionalidad.

  Se establecerán medidas de protección, detección y recuperación de forma que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

- Protección de datos desde el diseño y por defecto.

  La protección de datos debe incorporarse desde la concepción de los procedimientos, servicios o sistemas, garantizando que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines para los que se recabaron.

Para asegurar el cumplimiento efectivo de los principios anteriores el Ente Público adoptará, entre otras, las siguientes directrices:

- Mantener actualizado el Registro de Actividades de Tratamiento.
- Garantizar una información clara, accesible y transparente a las personas interesadas.
- Implantar procedimientos internos para el ejercicio de derechos.
- Aplicar medidas técnicas y organizativas apropiadas al riesgo.
- Establecer mecanismos para la detección y la gestión de incidentes y brechas de seguridad.
- Exigir garantías adecuadas en la contratación con terceros.
- Coordinar la protección de datos con la seguridad de la información.
- Establecer las medidas necesarias para la Protección de datos por defecto y desde el diseño.
- Implantar mecanismos de control, revisión y mejora continua.

Cód. 2026-09349

6.—*Organización de la seguridad y la protección de datos.*

El Ente Público, teniendo en cuenta los artículos 11, 12 y 13 del Real Decreto 311/2022, de 3 de mayo, por el que regula el ENS, así como las obligaciones establecidas en el RGPD y en la LOPDPyGDG, establece las siguientes acciones para organizar la seguridad de la información y la protección de los datos personales:

i. Designa roles en el ámbito de la seguridad: Responsables de Servicios y de la Información, Responsable de la Seguridad, Responsable del Sistema y DPD.

ii. Constituye un órgano consultivo y estratégico para la toma de decisiones en materia de seguridad de la información. Este órgano se denomina Comité de Seguridad de la información.

iii. Establece una estructura organizativa de protección de datos que determine las funciones, responsabilidades y mecanismos de supervisión aplicables a los tratamientos de datos personales realizados por el Ente Público.

6.1.—Definición de roles, funciones y responsabilidades asociados al ENS.

6.1.1.—Responsables de los Servicios y de la Información:

- Establecer los requisitos de seguridad aplicables a la información (niveles de seguridad de la información) y a los servicios (niveles de seguridad de los servicios), dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que regula el ENS, pudiendo recabar una propuesta al Responsable de la Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Decidir respecto a los derechos de acceso a la información y los servicios.
- Poner en comunicación del Responsable de la Seguridad cualquier variación respecto a la información y los servicios de los que es responsable, especialmente la incorporación de nuevos servicios o información a su cargo. El Responsable de la Seguridad dará traslado de dichos cambios al comité de seguridad.
- Ser responsable último del uso que se haga de los servicios e información dependientes de su ámbito funcional de competencia y por tanto de su protección.

6.1.2.—Responsable de la Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias y elaborar documentación del sistema.
- Aprobar la declaración de aplicabilidad a partir de las medidas de seguridad requeridas conforme al anexo II del Real Decreto 311/2022, de 3 de mayo, por el que regula el ENS.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad de la Información la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del catálogo normativo (y no son competencia del Comité de Seguridad) y poner en conocimiento del Comité de Seguridad de las modificaciones que se hayan realizado a lo largo del período en curso.
- Participar en la elaboración, en el marco del Comité de Seguridad, de la Política de Seguridad de la Información y Protección de Datos Personales, para su aprobación por el órgano competente.

6.1.3.—Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la tipología y la gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable de la Seguridad y/o Comité de seguridad.

Cód. 2026-09349

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Coordinar tareas de la administración de la seguridad del sistema:
  - — La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
  - — La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
  - — Aprobar los cambios en la configuración vigente del sistema de información.
  - — Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
  - — Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
  - — Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - — Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
  - — Informar al responsable de la seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
  - — Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.2.—Definición de roles, funciones y responsabilidades asociados a la protección de datos personales.

La organización interna del Ente Público en materia de protección de datos respetará el principio de diferenciación de responsabilidades y la necesaria coordinación con los roles y funciones definidos en materia de seguridad de la información.

En todo caso, deberá garantizarse la adecuada delimitación de funciones entre quienes determinen los fines y medios del tratamiento, quienes supervisen su cumplimiento y quienes participen en la gestión técnica de los sistemas.

6.2.1.—Responsable del tratamiento:

- Determinar los fines y medios esenciales del tratamiento, bien por decisión directa o porque así le viene impuesto por una norma con rango legal.
- Mantener y actualizar el registro de actividades de tratamiento de datos personales dentro de su ámbito de actuación y comunicarlo al DPD.
- Publicar el inventario de actividades de tratamiento en el Portal de Transparencia, conforme a lo establecido en el artículo 6 bis de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Atender las solicitudes relativas al ejercicio de los derechos en materia de protección de datos, garantizando la correcta gestión y resolución de las mismas en los plazos establecidos.
- Aplicar medidas de protección de datos desde el diseño y por defecto, asegurando que los tratamientos de datos personales respeten la privacidad desde su concepción y a lo largo de todo su ciclo de vida.
- Aprobar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas, basándose en un análisis de riesgos previo que permita identificar y mitigar los posibles impactos sobre los derechos y libertades de las personas.
- Cumplir con el deber de información en la recogida de los datos personales, de acuerdo con el principio de transparencia.
- Garantizar el cumplimiento del deber de confidencialidad, adoptando las medidas necesarias para asegurar que los datos personales no sean divulgados o sean accesibles a personas no autorizadas.
- Realizar evaluaciones de impacto relativas a la protección de datos, cuando el tratamiento implique un alto riesgo para los derechos y libertades de las personas, con el asesoramiento del DPD y los Responsables de Seguridad y Sistemas.
- Notificar las brechas de seguridad de datos personales a la AEPD cuando las brechas puedan entrañar un riesgo para los derechos y libertades de las personas y a las personas afectadas, cuando el riesgo derivado de la brecha sea alto.
- Seleccionar encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con la normativa en materia de protección de datos y garantice la protección de los derechos de los interesados.
- Cumplir con las garantías, excepciones y requisitos establecidos en la normativa en materia de protección de datos en relación con las transferencias internacionales de datos.
- Bloquear los datos cuando proceda a su rectificación o supresión.

Cód. 2026-09349

- Consultar a la AEPD antes de proceder a realizar un tratamiento, cuando la evaluación de impacto relativa a la protección de datos determine que el tratamiento entraña un alto riesgo para los derechos y libertades de las personas y no sea capaz de mitigarlo adecuadamente.

Cuando dos o más responsables de tratamiento determinen conjuntamente los fines y los medios del tratamiento, serán considerados corresponsables del tratamiento. En estos casos, los corresponsables deben determinar de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, en particular, en cuanto al ejercicio de los derechos de los interesados y a sus respectivas obligaciones de suministro de información. En todo caso, deberá establecerse un punto de contacto para los interesados, sin perjuicio de que estos puedan ejercer sus derechos ante cualquiera de los corresponsables.

6.2.2.—Delegado de protección de datos:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados públicos que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la legislación sobre protección de datos aplicable.
- Supervisar el cumplimiento de la legislación sobre protección de datos aplicable y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Prestar la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.
- Planificar, coordinar, dirigir y controlar las actividades de tratamiento llevadas a cabo por el Ente Público.
- Resolver las reclamaciones presentadas por las personas interesadas en relación con los tratamientos de datos personales llevados a cabo por el Ente Público.

El DPD ejercerá sus funciones con independencia y contará con el apoyo, los recursos y los medios necesarios para su adecuado desempeño.

Los empleados públicos y terceros que presten servicios para el Ente Público tienen el deber de colaborar con el DPD, facilitándole la información y el acceso a los sistemas, instalaciones, documentación, procesos y demás recursos que resulten necesarios para el ejercicio de sus funciones.

6.2.3.—Encargado del tratamiento:

- Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
- Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes.
- Aplicar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, disponibilidad e integridad de los datos personales a los que tenga acceso.
- Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos en materia de protección de datos personales, o tramitar, por su cuenta, las solicitudes, si así está establecido en el contrato o acto jurídico que les vincule.
- Notificar al responsable del tratamiento, sin dilación indebida, las brechas de seguridad de los datos personales a su cargo de las que tenga conocimiento.
- Apoyar al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.
- Informar al responsable del tratamiento de cualquier cambio previsto en la incorporación o sustitución de otros encargados.
- Suprimir o devolver, a elección del responsable de tratamiento, todos los datos personales una vez finalice la prestación de los servicios de tratamiento.
- Designar un DPD, cuando proceda, y comunicarlo al responsable de tratamiento.
- Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- Cualquier otra que le atribuya la normativa en materia de protección de datos.

Cód. 2026-09349

6.3.—Designación de roles y responsabilidades.

Corresponderá a la Presidencia del Ente Público aprobar la presente Política y sus revisiones y formalizar, cuando proceda, los contratos o actos jurídicos de encargo de tratamiento de datos personales.

Corresponderá a la Dirección General del Ente Público, sin perjuicio de las competencias de otros órganos, dirigir e impulsar la aplicación efectiva de la presente Política, coordinar su desarrollo interno, promover la aprobación de procedimientos y elevar, cuando proceda, las propuestas que resulten necesarias para su revisión y actualización.

Las personas titulares de las Áreas en cuyo ámbito se desarrollen tratamientos de datos personales actuarán como responsables funcionales a efectos de identificación de tratamientos, detección de riesgos, actualización del Registro de Actividades de Tratamiento, comunicación al DPD de las incidencias detectadas o propuestas en la mejora de la gestión de la protección de datos personales y, en general, en el cumplimiento de la presente Política. Colaborarán con la Dirección General, el DPD y el Responsable de la Seguridad.

El Ente Público actuará como responsable del tratamiento respecto de los tratamientos de datos personales que realice en el ejercicio de sus competencias, sin perjuicio de la distribución interna de funciones entre sus órganos, áreas y unidades.

El Ente Público actuará como encargado del tratamiento respecto de los tratamientos de datos personales de otras Administraciones Públicas o entidades públicas que realice en cumplimiento de un encargo, convenio, u otro acuerdo jurídico sin perjuicio de la distribución interna de funciones entre sus órganos, áreas y unidades.

Los siguientes roles serán desempeñados por quienes ocupen los puestos que se indican a continuación:

6.3.1.—Asociados al ENS:

- Responsable del Sistema: Jefatura del Departamento de infraestructuras del Área de Tecnología de la Información.
- Responsable de la Seguridad: Jefatura del Área de Tecnología de la Información.
- Responsables de los Servicios y de la Información: Jefaturas de Área de Gestión Tributaria, Recaudación y Servicios al Administrado.

6.3.2.—Asociados a la Protección de Datos personales:

- Responsable del tratamiento: la persona titular de la Consejería competente en materia tributaria, en su condición de Presidente del Ente Público.
- Encargados del tratamiento: serán designados por el responsable del tratamiento cuando sea necesario que un tercero trate datos personales en su nombre. Si el encargo se deriva de un negocio jurídico suscrito por el Director General del Ente Público, en uso de sus competencias propias o delegadas, podrá ser designado por este último.
- DPD; quien ocupe la Jefatura del Área de Servicios al Administrado.

6.4.—Comité de Seguridad de la Información.

En el Ente Público, se creará el Comité de Seguridad de la Información, que estará compuesto por los siguientes miembros:

- Presidencia: Quien ocupe la Dirección General del Ente Público.
- Secretaría: Quien desempeñe la Jefatura del Área de Servicios Generales.
- Vocales.
  - — Responsables de los Servicios y de la Información.
  - — Responsable de la Seguridad.
  - — Responsable del Sistema.
  - — DPD.

Estos miembros se clasificarán en permanentes o no permanentes atiendo a la obligatoriedad de la participación del Comité de Seguridad de la Información:

- Miembros permanentes:
  - Presidencia.
  - Secretaría.
  - Responsable del Sistema.
  - Responsable de la Seguridad.
- Miembros no permanentes:
  - Responsables de los Servicios y de la Información.
  - El DPD.
  - Personal del Ente Público, especialistas externos de los sectores público o privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Cód. 2026-09349

Los Responsables de los Servicios y de la Información serán convocados por la Presidencia en función de los asuntos a tratar.

Cuando en las reuniones del Comité de Seguridad de la Información estén convocados vocales que no sean permanentes, por lo que respecta a las Áreas del Ente Público, cada una tendrá un voto, independientemente del número de asistentes de las mismas a la reunión.

Tanto el DPD, como el Secretario/a y los especialistas externos de los sectores público o privado que pudieran asistir lo harán sin tener derecho a voto.

6.4.1.—Atribuciones del Comité de Seguridad de la Información:

- Atender los asuntos planteados por la Dirección General y las diferentes Áreas.
- Informar regularmente del estado de la seguridad de la información a la Dirección General.
- Promover la mejora continua del sistema de gestión de la seguridad de la Información.
- Elaborar la estrategia de evolución en lo que respecta a la seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar la documentación de seguridad de la información.
- Estar permanentemente informado de la normativa que regula la certificación de conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de entidades de certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos mecanismos o acuerdos de reconocimiento mutuo de certificados.
- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del comité, a las que su presidente deberá dar cumplida respuesta.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la política de seguridad de la información.
- Aprobar el plan de adecuación para la implantación del ENS.

6.4.2.—Periodicidad de las reuniones:

- El Comité de Seguridad de la Información se reunirá, con carácter ordinario, previa convocatoria de la Presidencia, al menos, una vez al año.
- El Comité de Seguridad de la Información podrá reunirse con carácter extraordinario, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, a iniciativa de la Presidencia o a petición, al menos, de dos tercios de sus miembros permanentes.
- El Comité de Seguridad de la Información quedará válidamente constituido cuando asistan quienes ocupen la Presidencia y la Secretaría y se encuentren presentes, al menos, la mitad de los vocales permanentes.
- Los acuerdos se adoptarán por mayoría de votos. En caso de empate, el voto del Presidente será de calidad.

6.5.—Procedimientos de designación.

Los miembros del Comité de Seguridad de la Información, podrán ser suplidos o sustituidos por el Director General del Ente Público, en caso de vacante, ausencia, enfermedad, razones operativas o por reasignación de tareas.

Los roles de seguridad también podrán ser suplidos o sustituidos en los mismos supuestos.

6.6.—Resolución de conflictos.

En caso de contradicción entre la normativa de seguridad de la información y la de protección de datos de carácter personal prevalecerá ésta última por constituir un objeto protegido de mayor rango.

La resolución del conflicto corresponderá, en última instancia, en caso de no resolución de acuerdo con la jerarquía de la normativa, a la Dirección General, asistida por el Responsable de la Seguridad del Ente Público y por el DPD.

6.7.—Creación de grupos de trabajo.

El Director General del Ente Público, a propuesta del Responsable de la Seguridad de la Información del Ente Público o del DPD, dentro de su respectivo ámbito, podrá crear grupos de trabajo específicos para el estudio o análisis de actuaciones concretas del Ente Público y/o para la mejora del cumplimiento de los principios recogidos en la presente Política.

Cód. 2026-09349

Los grupos de trabajo podrán contar con la asistencia de personas externas al Ente Público en función de los temas a tratar.

7.—*Desarrollo de la política de seguridad de la información y protección de datos.*

La presente Política de Seguridad de la Información y Protección de Datos será complementada por medio de un cuerpo normativo de seguridad que se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento.

Se establecen los siguientes niveles:

- Primer nivel normativo: constituido por la presente Política de Seguridad de la Información y Protección de Datos, y las directrices generales de seguridad.
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de las directrices generales, que establecen los requisitos que deben ser alcanzados para satisfacer y cumplir los objetivos de seguridad establecidos en la Política de seguridad.
- Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información y Protección de Datos, determinan las acciones o tareas a realizar en el desempeño de un proceso.

La normativa de seguridad de la información y de protección de datos estará a disposición de todo el personal del Ente Público y demás usuarios que deban conocerla y aplicarla, en particular, aquellas personas que utilicen, operen o administren los sistemas de información y comunicaciones. Para ello se habilitarán los correspondientes repositorios de documentación.

El Director General del Ente Público, con el asesoramiento del DPD y, en su caso, la coordinación con los responsables funcionales y de seguridad, impulsará la aprobación de los procedimientos, guías e instrucciones necesarios para el desarrollo de esta Política, incluyendo al menos, en lo relativo a protección de datos:

a) Procedimiento de gestión integrada de incidentes.

b) Procedimiento de ejercicio de derechos.

c) Procedimiento de alta, modificación y supresión de actividades de tratamiento.

d) Procedimiento de análisis de riesgos y, en su caso, evaluaciones de impacto.

e) Modelos de contratación con encargados y prestadores de servicios.

8.—*Gestión de riesgos.*

8.1.—Gestión de riesgos de seguridad.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios en la información manejada.
- Cuando se produzcan cambios en los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8.2.—Gestión de riesgos de protección de datos personales.

Deberán someterse a revisión previa de cumplimiento de la normativa de protección de datos, con el asesoramiento del DPD, y, en su caso, del grupo de trabajo que se cree de conformidad con el apartado 6.7 de la presente Política, los cambios de relevancia que afecten al tratamiento de datos, especialmente en caso de nuevos procedimientos, nuevas aplicaciones tributarias, nuevos formularios y cambios en la sede electrónica. En estos casos, el Ente Público realizará un análisis de riesgos que permita identificar, evaluar y gestionar los riesgos para los derechos y libertades de las personas físicas.

Dicho análisis se revisará periódicamente y, en todo caso, al menos una vez al año, así como cuando varíe la información tratada, los servicios prestados, se produzca un incidente grave, se detecten vulnerabilidades graves o cambien las conclusiones de análisis anteriores.

Cuando del análisis resulte probable que el tratamiento entrañe un alto riesgo, se realizará una evaluación de impacto relativa a la protección de datos, con participación o asesoramiento del DPD y coordinación con el Responsable de la Seguridad.

Cód. 2026-09349

La gestión de riesgos en materia de protección de datos se desarrollará de forma documentada, coordinada, continua y asegurando la integración entre los requerimientos del RGPD y el ENS.

9.—*Obligaciones del personal del Ente Público.*

Todos los empleados públicos del Ente Público tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y de Protección de Datos Personales y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad del Ente Público, a través del Comité de Seguridad de la Información y del Área de Asuntos Generales, disponer de los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los empleados públicos del Ente Público, en particular, a los de nueva incorporación.

El DPD asesorará y supervisará, en el ámbito de sus funciones, la adecuación de las actuaciones de sensibilización y formación en el ámbito de esta Política.

Las personas con responsabilidad en el uso, operación o administración de sistemas informáticos recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Todo el personal deberá utilizar los datos personales exclusivamente para finalidades autorizadas y colaborar en la mejora continua de las medidas de protección de datos y seguridad de la información.

Quienes participen en el tratamiento de datos personales estarán sujetos al deber de secreto y confidencialidad, incluso después de finalizar su relación con el Ente Público.

10.—*Terceras partes.*

Actuaciones por cuenta de terceros.

Cuando el Ente Público preste servicios a otras entidades o maneje información de terceros, se les hará partícipes de esta Política de Seguridad de la Información y de Protección de Datos Personales, y se establecerán canales para reporte y coordinación de los respectivos comités de seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de la Seguridad (o persona en quien delegue) será el POC.

Cuando el Ente Público trate datos personales por cuenta de otras Administraciones o entidades en virtud de una atribución legal, convenio, encomienda o encargo, respetará las instrucciones documentadas del responsable, aplicará las medidas técnicas y organizativas apropiadas y mantendrá una actitud proactiva de colaboración en la atención de derechos, en la gestión de incidentes y en el cumplimiento de las demás obligaciones derivadas del correspondiente encargo.

Utilización de servicios de terceros.

Cuando el Ente Público utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la normativa de seguridad y de protección de datos que ataña a dichos servicios o información. Si los servicios de terceros implican acceso o tratamiento de datos personales por cuenta del Ente Público, deberá formalizarse el correspondiente contrato o acto jurídico de encargo del tratamiento con el contenido mínimo exigido por el artículo 28 del RGPD.

En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS y se exigirán, en su caso, garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento de datos sea conforme con la normativa en materia de protección de datos y garantice la protección de los derechos de los interesados.

En la adquisición de derechos de uso de activos en la nube se tendrá en cuenta los requisitos establecidos en las medidas de seguridad del anexo II y las Guías de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en la citada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que el Ente Público pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte.

Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales, por el DPD. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de esta Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los Responsables de los Servicios y de la Información afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al Director General del Ente Público que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cód. 2026-09349

Coordinación con otras Administraciones y entidades.

El Ente Público establecerá los mecanismos de coordinación necesarios con otras Administraciones Públicas y entidades con las que intercambie información o desarrolle actuaciones conjuntas que impliquen tratamiento de datos personales.

Cuando proceda, se formalizarán los instrumentos jurídicos previstos por la normativa de protección de datos para regular las responsabilidades de las partes.

Sistemas de Inteligencia Artificial.

Cuando la entidad adquiera, desarrolle o implante un sistema de inteligencia artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de los Servicios y de la Información afectado y, cuando sea necesario, al del Sistema, debiendo también el DPD emitir su parecer cuando implique tratamiento de datos personales o pueda afectar a los derechos y libertades de las personas. Deberá valorarse la necesidad de un análisis de riesgos específico y, en su caso, de una evaluación de impacto.

11.—*Auditoría y control.*

El Ente Público realizará revisiones y controles periódicos sobre la eficacia de las medidas técnicas y organizativas implantadas en aplicación de esta Política.

Se promoverán auditorías específicas cuando se produzcan modificaciones sustanciales, incidentes relevantes o cambios normativos que lo hagan necesario.

12.—*Aprobación y entrada en vigor.*

Esta Política será efectiva desde el día siguiente al de su publicación en el *Boletín Oficial del Principado de Asturias*. También se publicará en el portal de transparencia y en la sede electrónica del Ente Público y deberá ser difundida a todas las partes afectadas y estar disponible en la intranet para todos los empleados público del Ente Público.

Será revisada, como mínimo, anualmente, y siempre que se produzcan cambios normativos, organizativos, funcionales o tecnológicos significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia y que sigue cumpliendo con los requisitos del marco normativo vigente.

La revisión será realizada por el Comité de Seguridad de la Información con carácter general y de forma específica, respecto a la protección de datos personales, por un grupo de trabajo constituido al efecto, de conformidad con la previsión del apartado 6.7 de la presente Política, coordinado por el DPD y cuya composición será determinada por el Director General oído el DPD. Deberá figurar en todo caso un representante de alguna de las Áreas funcionales. El DPD formulará las recomendaciones y observaciones que estime oportunas en el ejercicio de las funciones que le atribuye la normativa vigente.

Los cambios sobre la Política de Seguridad de la Información y Protección de Datos deberán ser aprobados por el Presidente del Ente Público, de acuerdo con lo establecido en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS.

Cód. 2026-09349