III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA

4929 *Resolución de 18 de febrero de 2026, de la Intervención General de la Administración del Estado, por la que se regula la política de seguridad de la información de la Secretaría de Estado de Presupuestos y Gastos, la Secretaría General de Fondos Europeos y la Intervención General de la Administración del Estado.*

En un contexto en el que la tramitación electrónica de los procedimientos ha dejado de ser una excepcionalidad, la relación de las Administraciones Públicas con las personas jurídicas, entes sin personalidad y, en algunos supuestos, con las personas físicas ha de ser obligatoriamente electrónica, debiendo garantizar que se sustentan en redes y sistemas de información seguros y fiables, al objeto de trasladar confianza a las partes concernidas.

Es por ello que la Secretaría de Estado de Presupuestos y Gastos, la Secretaría General de Fondos Europeos y la Intervención General de la Administración del Estado, ámbito funcional conjunto, al que, en adelante, esta resolución se refiere como Administración presupuestaria, consideran la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por tanto, la seguridad de la información como una responsabilidad asociada a su protección frente a las amenazas que puedan afectar a su autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas regula en su artículo 13 los derechos de las personas en sus relaciones con las Administraciones Públicas, incluyendo en su apartado h) el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, al regular en su artículo 3 los principios generales que las Administraciones Públicas deben respetar en su actuación y relaciones, establece en su apartado 2 que aquellas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la presentación conjunta de servicios a los interesados.

El artículo 156.2 de la Ley 40/2015 regula el Esquema Nacional de Seguridad (en adelante, ENS) cuyo objeto es establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las Administraciones Públicas y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El ENS está regulado por el Real Decreto 311/2022, de 3 de mayo. En el punto 1 del artículo 3 establece que cuando un sistema de información trate datos personales le será de aplicación 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 o RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD).

En el punto 2 del artículo 12 del ENS establece que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

que articule la gestión continuada de la seguridad y que será aprobada por el titular del órgano superior correspondiente. La Política de Seguridad de la Información del Ministerio de Hacienda está regulada por la Orden HAC/800/2025, de 16 de julio. La Política de Seguridad regulada en esta resolución se redacta tomando en consideración el punto 3 del antedicho artículo 12 del ENS («También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos»), habiéndose asegurado su coherencia con la Política de Seguridad de la Información del Ministerio de Hacienda.

La primera política de seguridad de la Administración presupuestaria data del año 2009 y se reguló mediante la Resolución de 27 de febrero de 2009, de la Secretaría de Estado de Hacienda y Presupuestos. Su redacción se cimentó en las Resoluciones de la Secretaría de Estado de Presupuestos y Gastos, de 8 de julio de 2002 y de la Secretaría de Estado de Hacienda y Presupuestos de 24 de mayo de 2005, de acceso a las bases de datos de la Secretaría General de Presupuestos y Gastos y de la Intervención General de la Administración del Estado que sentaron las bases organizativas y técnicas para la instrumentación de la seguridad informática en la vertiente del control de accesos a las bases de datos, en el ámbito de la Administración presupuestaria. A continuación, la política de seguridad fue actualizada mediante la Resolución de 21 de diciembre de 2015, de la Secretaría de Estado de Presupuestos y Gastos, por la que se regula la política de seguridad de los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado. Y, posteriormente y en última instancia, se ha actualizado mediante la Resolución de 27 de marzo de 2024, de la Intervención General de la Administración del Estado, por la que se regula la política de Seguridad de la Información de la Secretaría de Estado de Presupuestos y Gastos, de la Secretaría General de Fondos Europeos y de la Intervención General de la Administración del Estado.

La seguridad es una función transversal en las Administraciones Públicas, habiéndose convertido en un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con un sistema. Es por ello que la seguridad debe abarcar cada etapa del ciclo de vida del sistema (análisis, diseño, desarrollo, implementación, operación, mantenimiento y obsolescencia) y sus documentos (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción).

En este contexto, la presente Política de Seguridad de la Información constituye el marco normativo y organizativo orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad en el ámbito de la Administración presupuestaria, adaptados al ENS, dentro del marco de referencia establecido por la política de seguridad del Ministerio de Hacienda.

El Real Decreto 206/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda, establece en su artículo 11, apartado 1.h), que la Intervención General de la Administración del Estado es el centro directivo encargado de la planificación, diseño y ejecución de la política informática de la Secretaría de Estado de Presupuestos y Gastos, de la Secretaría General de Fondos Europeos y de la Intervención General de la Administración del Estado, el soporte informático de sus respectivas actividades y el asesoramiento, coordinación e instrumentación de los proyectos informáticos de sus órganos.

Así mismo, el antedicho real decreto en el artículo 11, apartado 5.f).1.º le atribuye a la Oficina de Informática Presupuestaria la función de la seguridad de la información.

Esta norma se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En particular, a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

En virtud de lo anterior,

Esta Intervención General de la Administración del Estado adopta la siguiente resolución:

Primero. *Objeto.*

Constituye el objeto de la presente resolución la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración presupuestaria.

El objetivo de la PSI es lograr la protección, proporcional al riesgo, de la información y documentos manejados en la Administración presupuestaria, y de los sistemas, dispositivos y elementos que la elaboran, presentan, almacenan, procesan, transportan o destruyen, mediante la preservación de las dimensiones de seguridad de la información o de los servicios, es decir, su autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.

Los activos tecnológicos asignados por la Administración presupuestaria para el desempeño de las funciones de los puestos de trabajo estarán sujetos a la presente PSI.

Segundo. *Ámbito de aplicación.*

La PSI se aplicará a todo el personal y en todas las dependencias e instalaciones de la Administración presupuestaria, y de sus organizaciones delegadas y territoriales, a sus sistemas de información y telecomunicaciones, y a las entidades con las que la Administración presupuestaria se relaciona en lo relativo a la prestación de servicios en uno u otro sentido.

La PSI será observada asimismo por aquellas personas que, aun no perteneciendo a la Administración presupuestaria, dispongan de acceso a sus sistemas de información.

Tercero. *Definiciones.*

Con carácter general, a efectos, de esta resolución, se asumen las definiciones recogidas en el artículo 6 de la Directiva (UE) 2022/2555 (NIS2) del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI2), en el artículo 4 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); y en el anexo IV del Real Decreto 311/2022 (ENS).

Adicionalmente se introducen las siguientes definiciones a efectos de esta resolución:

Servicios centrales de la Administración presupuestaria: los centros directivos que constituyen la misma.

Organizaciones delegadas y territoriales: las unidades que tengan ese carácter y que dependan de los centros directivos de la Administración presupuestaria.

Oficina de Informática Presupuestaria (en adelante, OIP): unidad de la Intervención General de la Administración del Estado encargada del desarrollo y ejecución de las actividades informáticas de la Administración presupuestaria y de la seguridad de la información.

Cuarto. *Misión.*

La misión del ámbito corporativo al que se refiere la política de seguridad regulada en esta resolución será la que corresponda a la Secretaría de Estado de Presupuestos y Gastos, a la Secretaría General de Fondos Europeos y a la Intervención General de la

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

Administración del Estado, según lo establecido en el vigente real decreto de estructura orgánica básica del Ministerio de Hacienda para estos órganos.

Quinto. *Marco normativo.*

El marco normativo en que se desarrollan las actividades de la Administración presupuestaria, y, en particular, la prestación de sus servicios electrónicos a los ciudadanos y a las Administraciones Públicas, está integrado por:

La normativa sobre la estructura organizativa del ámbito de esta resolución.

La normativa sobre el procedimiento administrativo común de las Administraciones Públicas y respecto al régimen jurídico del sector público.

La normativa de estabilidad presupuestaria y sostenibilidad financiera, presupuestaria, de costes de personal, contable, de contratación del sector público, de subvenciones, y de control de la actividad económico-presupuestaria del sector público estatal, incluida la normativa comunitaria al respecto.

El marco normativo de la Administración electrónica, en particular el ENS y el Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad.

La normativa de la protección de datos personales y de garantía de los derechos digitales.

La normativa de protección de las infraestructuras críticas.

La normativa departamental en materia de Administración electrónica y respecto a la política de seguridad.

La normativa del ámbito de la Administración presupuestaria en materia de Administración electrónica y respecto a la política de seguridad.

Sexto. *Principios de la seguridad de la información.*

La política de seguridad de la información de la Administración presupuestaria asume los principios básicos y particulares que se establecen en la Orden HAC/800/2025, de 16 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda (en adelante, PSI-MINHAC). Se refuerza la seguridad desde el diseño y por defecto, en línea con el RGPD.

Séptimo. *Estructura organizativa para la administración de la seguridad de la información.*

En concordancia con la PSI-MINHAC, el ENS, y las Guías CCN–STIC elaboradas por el Centro Criptológico Nacional que desarrollan el ENS, se identifican tres grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, de la cual se encargan los responsables de la información y del servicio, que a efectos de esta resolución se denominarán responsables de sistemas de información; la operación del sistema de información, encomendada al responsable del sistema, que en esta resolución se asigna al titular de la Dirección de la OIP; y la función supervisora de la seguridad, encargada a la persona que ejerza el rol de responsable de seguridad de la información.

De conformidad con el artículo 11 de la PSI-MINHAC el Delegado de Protección de Datos es único para todo el Departamento, sin perjuicio de la existencia de Delegados de Protección de Datos en los organismos públicos adscritos al Departamento y del nombramiento de coordinadores en todos los órganos superiores del Departamento y en la Intervención General de la Administración del Estado; la función de coordinación recae sobre quién tenga el rol de responsable de seguridad de la información. La Orden HAC/800/2025 amplía las funciones del Delegado de Protección de Datos de asesoramiento, supervisión y coordinación, incluyendo participación activa en la gestión de brechas de seguridad y en la definición de medidas de seguridad que impliquen tratamiento de datos personales.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

La gestión de la seguridad en la Administración presupuestaria requiere, además de la implicación activa de todas las personas que utilizan los sistemas de información, la existencia de un marco organizativo orientado a dicha gestión en el que desempeñarán un papel primordial las siguientes entidades y agentes:

Comité de coordinación de la seguridad de la información.

Responsable de seguridad de la información que asume las funciones de ese rol en los términos establecidos por el RGPD, el ENS y la PSI-MINHAC.

Responsables de seguridad en los centros directivos, organizaciones delegadas o territoriales de la Administración presupuestaria que, a efectos de esta resolución, se denominarán responsables de centro.

Responsables de seguridad de los sistemas de información de los centros directivos, organizaciones delegadas o territoriales de la Administración presupuestaria que, a efectos de esta resolución, se denominarán responsables de sistemas de información.

Dirección y Divisiones de la OIP, a través de las que la OIP ejercerá las funciones asignadas al responsable del sistema y al encargado de tratamiento por el ENS y sus guías de desarrollo, en el primer caso, y por el RGPD en el segundo.

Para la gestión adecuada de la seguridad de la información en el ámbito de la Administración presupuestaria, en la estructura organizativa también se contemplan los agentes que se indican a continuación:

Administradores de seguridad de los accesos a las redes departamentales de cada uno de los centros directivos, organizaciones delegadas o territoriales de la Administración presupuestaria que, a efecto de esta resolución, se denominarán administradores de centro.

Administradores de seguridad de los accesos a las bases de datos de la red de la Administración presupuestaria que, a efectos de esta resolución, se denominarán administradores de sistemas de información.

Las funciones y obligaciones reguladas en el Real decreto 311/2022, el RGPD y la Ley Orgánica 3/2018, debido a su extensión, así como las de Administrador de centro y de sistemas de información se recogen detalladamente en una política de desarrollo de la presente resolución.

Octavo. *Comité de coordinación de la seguridad de la información.*

El comité de coordinación de la seguridad de la información (en adelante, Comité) es un órgano colegiado de carácter horizontal en materia de seguridad de la información para el ámbito de la Administración presupuestaria. Estará formado por:

Las personas titulares de la Intervención General de la Administración del Estado, de la Secretaría General de Fondos Europeos y de las Direcciones Generales de Presupuestos y de Costes de Personal que ocuparán rotatoriamente, cada seis meses, la presidencia del Comité. Para cada reunión se podrá delegar esta función en una persona del centro al que le corresponda la presidencia.

La persona titular de la Dirección de la OIP, como vicepresidente del Comité.

La persona titular de la División de Explotación de la OIP.

La persona responsable de la seguridad de la información, como secretario del Comité.

Los responsables de centros, previstos en el apartado décimo, designados por la persona titular de cada uno de los centros directivos de la Administración presupuestaria.

Tres interventores delegados en representación del conjunto de las Intervenciones delegadas en Ministerios, Agencias y Organismos públicos, Intervenciones regionales y territoriales, designados por la persona titular de la Intervención General de la Administración del Estado.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

Además, el Comité podrá convocar a representantes de unidades organizativas internas o externas que accedan a sistemas de información de la Administración presupuestaria.

A este Comité, que se reunirá al menos dos veces al año, le corresponde aprobar las directrices, normas y actuaciones de orden organizativo que sean precisas en desarrollo de lo dispuesto en esta resolución, ajustadas a las directrices y criterios generales en el ámbito de la Administración General del Estado, que emanen de la Comisión de Estrategia TIC y del Comité de Dirección TIC de la Administración General del Estado, o del Departamento, a través de la Comisión Ministerial de Administración digital, dirigidas a garantizar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información en la red de la Administración presupuestaria, todo ello sin perjuicio del ejercicio de las competencias decisorias por los órganos superiores o directivos del Departamento que las tengan atribuidas.

En particular, el procedimiento de control de accesos a la red y a los sistemas de información de la Administración presupuestaria será aprobado por el Comité a propuesta de la OIP.

Noveno. *Responsable de seguridad de la información.*

La persona designada como responsable de seguridad de la información velará por la aplicación de las medidas de seguridad a los sistemas de información de la Administración presupuestaria de acuerdo con las directrices establecidas por el Comité. Será designada por el Comité a propuesta de la persona titular de la Dirección de la OIP, y llevará a cabo las funciones asociadas a la secretaría del Comité.

Son funciones asociadas al/la responsable de seguridad de la información:

a) Impulsar y velar por el cumplimiento y difusión de la política de seguridad y de su cuerpo normativo.

b) Elaborar la normativa técnica de seguridad de tercer nivel.

c) Promover las actividades de concienciación y formación en materia de seguridad para todo el personal afectado por la política de seguridad.

d) Aprobar la Declaración de Aplicabilidad elaborada en los términos establecidos por el ENS.

e) Asesorar, en colaboración con el Responsable del sistema, a los Responsables de seguridad de los centros directivos, en la realización de los preceptivos análisis de riesgos.

f) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, analizar los informes resultantes con objeto de asignar a los agentes concernidos la subsanación de las no conformidades, recomendaciones u observaciones identificadas.

g) Cualesquiera otras funciones que la PSI-MINHAC asigne a los responsables de seguridad.

El diseño, construcción, implantación y mantenimiento de las políticas, directrices, normativa, procedimientos, guías, instrucciones y herramientas que, en aplicación de lo dispuesto en esta resolución y en sus normas de desarrollo, se implementen para la administración de la seguridad de los sistemas de información corresponderá a la OIP bajo la iniciativa y coordinación de la persona responsable de seguridad de la información, que las pondrá en conocimiento de los responsables de centro de los centros directivos u organizaciones delegadas o territoriales de la Administración presupuestaria, de los administradores de centro y de sistemas de información y, en general, las difundirá a todo el ámbito de aplicación.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

Décimo. *Responsable de centro.*

A efectos de esta resolución se considera responsable de centro a la persona que designe el titular del centro directivo o al titular de la organización delegada o territorial de la Administración presupuestaria.

El responsable de centro asumirá las funciones y obligaciones que se indican a continuación:

a) Adoptará las medidas necesarias para el cumplimiento, en su ámbito de competencia, de las normas, instrucciones y procedimientos que, en aplicación de lo establecido en esta resolución, se desarrollen para la administración de la seguridad y la gestión de accesos a la red de la Administración presupuestaria.

b) Adoptará las medidas necesarias para que el personal de su ámbito de competencia conozca las normas y procedimientos de seguridad que afecten al desarrollo de sus funciones.

c) En el caso de los centros directivos, el Responsable de centro designará a los responsables de sistemas de información relativos al ámbito competencial del centro directivo.

d) Designará a un administrador único de centro y a los suplentes que considere precisos. En el caso de los centros directivos, la designación del administrador de centro podrá efectuarse, si la estructura así lo aconseja, a nivel de subdirección general o de ubicaciones administrativas diferentes.

e) Autorizará el acceso de usuarios a la red departamental. Asimismo, comunicará la anulación de los accesos permitidos a la red departamental de su centro.

f) Autorizará la solicitud de acceso de su personal a los sistemas de información de la Administración presupuestaria, distintos de aquellos de su centro, que se requiera para el ejercicio de las funciones encomendadas.

g) Autorizará la solicitud de acceso de su personal a sistemas de información externos al ámbito de la Administración presupuestaria, cuando se requiera para el ejercicio de las funciones encomendadas.

En los centros directivos, las funciones e), f) y g) podrán ser desempeñadas por las personas que ejerzan de jefes de división, subdirectores generales, asimilados o adjuntos, respecto a las redes, bases de datos y ámbito de personal de su respectiva competencia. Para tales funciones, y a los efectos de esta resolución, dichos jefes de división o subdirectores generales serán considerados como responsables de centro.

El acceso a la red de la Administración presupuestaria podrá ser autorizado por los responsables de recursos humanos de los centros directivos en la toma de posesión de nuevo personal. Se procederá de la misma forma cuando una persona deje de prestar servicio en un centro directivo o en alguna de sus oficinas delegadas o territoriales.

Undécimo. *Responsable de sistemas de información.*

El responsable de sistemas de información asumirá en materia de seguridad de la información las funciones y obligaciones que el ENS y la PSI-MINHAC asignan a los responsables de la información y del servicio, y en el ámbito de la Administración presupuestaria las funciones y obligaciones que se indican a continuación:

a) Adoptará las medidas necesarias para el cumplimiento, en su ámbito de competencia, de las normas, instrucciones y procedimientos que, en aplicación de lo establecido en esta resolución, se desarrollen para la administración de la seguridad de los sistemas de información de la Administración presupuestaria.

b) Adoptará las medidas necesarias para que el personal de su ámbito de competencia conozca las normas y procedimientos de seguridad que afecten al desarrollo de sus funciones.

c) Designará a los administradores de sistemas de información de su ámbito de competencia.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

d) Autorizará el acceso de usuarios a los sistemas de información de su responsabilidad. Asimismo, comunicará la anulación de los accesos permitidos a dichos sistemas.

Quien ostente la función de autorización de accesos a la información actuará así mismo como Responsable de tratamiento en los términos del RGPD o designará a dicho responsable.

En los centros directivos, las precitadas funciones podrán ser desempeñadas por las personas que ejerzan de jefes de división, subdirectores generales, asimilados o adjuntos.

Duodécimo. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos y, en su defecto, prevalecerá la decisión adoptada colegiadamente por el Comité.

Decimotercero. *Gestión de riesgos.*

El análisis y gestión de riesgos será parte esencial del proceso de seguridad, siendo la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos por el ENS.

Cuando el análisis de riesgos se realice sobre sistemas de información que traten datos personales, se tendrán en cuenta los riesgos que puedan afectar a los derechos y libertades de las personas físicas.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de la información y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y se someterá a una reevaluación periódica.

El proceso de gestión de riesgos comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionadas a los riesgos y estar justificadas; y deberá revisarse y aprobarse cada año por el Comité, a través de un plan de adecuación al ENS. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Decimocuarto. *Obligaciones del personal. Formación y concienciación.*

Los datos e informaciones de la Administración presupuestaria, cualquiera que sea su soporte, serán de uso exclusivamente reservado para el cumplimiento de los fines que le atribuye el ordenamiento jurídico.

Las autoridades, empleados públicos y demás personal al que resulte de aplicación esta resolución y que por razón de su cargo o función tuviesen conocimiento de los datos o informaciones a que se refiere el párrafo anterior, están obligados a guardar sigilo riguroso y observar estricto secreto respecto de los mismos.

El personal autorizado sólo deberá acceder a aquellos datos e información que deba conocer por razones del servicio, debiendo abstenerse de hacerlo por cualquier otra motivación.

Cada persona, debidamente autorizada, adquiere el compromiso de utilización de los datos e información con los fines exclusivos de gestión para los que ha sido autorizado. Asimismo, será responsable de todos los accesos que se realicen mediante el uso de sus credenciales de identificación lógica de usuario. A tal fin deberá mantener la custodia

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

y secreto de las credenciales, así como vigilar posibles usos ajenos, denunciando cualquier trasgresión.

En ningún caso deberá facilitar las credenciales a otra persona, ni deberá acceder a la información utilizando credenciales ajenas, incluso disponiendo del consentimiento de la persona titular.

El acceso a los datos e información de la Administración presupuestaria por una persona no autorizada, la realización de transacciones digitales que no estén relacionadas con un objetivo concreto de gestión, la asignación de perfiles de utilización a otras personas para el uso de transacciones no necesarias para la gestión que tengan encomendada, o la revelación o falta de diligencia en la custodia y secreto de sus credenciales darán lugar a la exigencia de las responsabilidades administrativas o de otra naturaleza en que se hubiese podido incurrir.

En el supuesto en que las actuaciones señaladas en el párrafo anterior hubiesen sido cometidas por un empleado público, las mismas podrán dar lugar a la incoación del oportuno expediente disciplinario a tenor de lo previsto en los artículos 6, 7 y 8 del Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado, aprobado por el Real Decreto 33/1986, de 10 de enero y en el título VII del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

De igual modo, las conductas señaladas en los párrafos anteriores darán lugar a la supresión de las autorizaciones previamente concedidas por quien las hubiera otorgado en su momento.

Todos los miembros de la Administración presupuestaria tienen la obligación de conocer y cumplir esta PSI y la normativa de seguridad que la desarrolle y, en consecuencia, todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

La Administración Presupuestaria desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, en la medida en que la necesiten para realizar su trabajo. La responsabilidad derivada del acceso y uso de los sistemas de información conlleva la correspondiente responsabilidad de la organización y de las personas en su formación. Todos los órganos y unidades de la Administración presupuestaria prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta resolución.

Decimoquinto. *Actualización permanente y revisiones periódicas de la PSI.*

La PSI definida en esta resolución deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad digital, así como a los estándares internacionales de seguridad.

Las propuestas de las sucesivas revisiones de la PSI serán aprobadas por el Comité.

Decimosexto. *Desarrollo de la política de seguridad de la información.*

La PSI regulada en esta resolución será desarrollada y complementada para poder afrontar aspectos específicos, constituyendo lo que se denominará en adelante normativa de seguridad de la información de la Administración presupuestaria.

La normativa de seguridad de la información se desarrollará en cuatro niveles, estableciendo un orden jerárquico y de dependencia entre ellos, y deberá estar a disposición de todos los miembros de la organización que necesiten conocerla. Dichos niveles de desarrollo normativo son los siguientes:

Primer nivel normativo constituido por la PSI-MINHAC del departamento ministerial al que pertenece la Administración presupuestaria y las directrices generales de seguridad aplicables a los órganos superiores o directivos del departamento ministerial.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

Segundo nivel normativo constituido por la PSI de la Administración presupuestaria, además de la normativa y recomendaciones de seguridad que se definan en este ámbito organizativo.

Tercer nivel normativo formado por los procedimientos, guías e instrucciones técnicas que determinan acciones o tareas a realizar para garantizar la seguridad de la información a lo largo del ciclo de vida de los sistemas de información de la Administración presupuestaria.

La aprobación de estos procedimientos técnicos corresponderá a la OIP.

Adicionalmente se tendrán en cuenta los informes que recojan las conclusiones, observaciones y recomendaciones de una auditoría, de un estudio o de una evaluación; registros de actividad o alertas de seguridad que informen de amenazas y vulnerabilidades que afecten a los sistemas de información, y las evidencias electrónicas que se generan durante todas las fases del ciclo de vida de los sistemas de información y en sus distintos procesos, pudiendo abarcar uno o más sistemas en función del aspecto tratado.

Decimoséptimo. *Terceras partes.*

En los casos en que la Administración presupuestaria preste servicios o gestione información de otros organismos, se les hará partícipes de la PSI, y se establecerán canales para el reporte y coordinación de los respectivos comités de seguridad, así como procedimientos de actuación para la reacción ante los ciberincidentes de seguridad.

En los casos en que la Administración presupuestaria utilice servicios de terceros o les ceda información, les hará partícipes de esta PSI y de la normativa de seguridad que afecte a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para cumplirla. Además, se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de la tercera parte esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de la política no pueda ser abordado por una tercera parte según se establece en los párrafos anteriores, se requerirá un informe del responsable de seguridad de la información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Decimoctavo. *Compromiso de la Dirección.*

1. Los órganos directivos de la Administración presupuestaria se comprometen a proteger la disponibilidad, integridad, confidencialidad y autenticidad de la información utilizada en la organización, así como sus canales de transmisión y/o comunicación, implantando para ello las medidas organizativas y técnicas necesarias y estableciendo responsabilidades sobre el acceso y utilización de la información.

2. Se debe prestar la máxima atención a la concienciación de las personas que intervienen en la seguridad y a sus responsables jerárquicos para evitar fuentes de riesgo para la seguridad. Es por ello que la presente resolución y sus normas de desarrollo estarán accesibles y tratarán de ser comprensibles para todas las personas pertenecientes o no a la Administración presupuestaria.

Decimonoveno. *Derogación.*

A la entrada en vigor de la presente resolución quedará derogada la Resolución de 27 de marzo de 2024, de la Intervención General de la Administración del Estado, por la que se regula la política de seguridad de la información de la Secretaría de Estado de Presupuestos y Gastos, de la Secretaría General de Fondos Europeos y de la Intervención General de la Administración del Estado., así como todos aquellos

cve: BOE-A-2026-4929
Verificable en https://www.boe.es

procedimientos e instrucciones de rango inferior que contradigan o se opongan a lo dispuesto en la presente resolución.

Vigésimo. *Entrada en vigor.*

La presente resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 18 de febrero de 2026.–El Interventor General de la Administración del Estado, Pablo Arellano Pardo.

cve: BOE-A-2026-4929
Verificable en https://www.boe.es