

### III. OTRAS DISPOSICIONES

## MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

- 165** *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.*

El marco normativo de la Administración electrónica que surge a partir de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, considera la seguridad como un elemento fundamental para la confianza en las relaciones entre las administraciones públicas y entre éstas y los ciudadanos, siendo uno de sus pilares el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica.

Las tendencias tecnológicas actuales hacia el acceso en movilidad, la virtualización y el paradigma de «nube», y la necesidad de tratamiento de ingentes cantidades de información, incluso procedentes de las propias redes sociales, han llevado, no sólo a las organizaciones sino también a los Gobiernos, a implicarse en la política de seguridad a los más altos niveles de decisión.

La evolución y complejidad de las amenazas y ataques a través de la red que afectan a ciudadanos, empresas y administraciones públicas ha propiciado la definición de una Estrategia de Seguridad Nacional (en adelante ESN), una de cuyas líneas de actuación es la Ciberseguridad que se ha desarrollado mediante la definición de la Estrategia de Ciberseguridad Nacional (en adelante, ECN), que tiene por objeto garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades de prevención, dirección y respuesta a los ciberataques.

La Secretaría de Estado de Presupuestos y Gastos 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. Asumen, 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, trazabilidad y conservación.

Esta responsabilidad por la seguridad de la información tuvo su primer reflejo normativo a través de la Resolución de la Secretaría de Estado de Presupuestos y Gastos, de 8 de julio de 2002, y, posteriormente, mediante la Resolución 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.

Desde un enfoque de la seguridad centrado en el control de accesos a los sistemas se evolucionó hacia una política global de seguridad a través de la Resolución de 27 de febrero de 2009, de la Secretaría de Estado de Hacienda y Presupuestos, por la que se regula la política de seguridad de los sistemas de información de la Secretaría General de Presupuestos y Gastos y de la Intervención General de la Administración del Estado.

Corresponde ahora adaptar esta política de seguridad del ámbito de la Administración presupuestaria al ENS, a la línea 3 de la ESN y a la ECN, estableciendo una estrategia y una estructura organizativa para su desarrollo que permitan adaptarse a los cambios permanentes en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esta política de seguridad del ámbito de la Administración presupuestaria debe estar asimismo inscrita en el marco establecido por la recientemente aprobada Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Hacienda y Administraciones Públicas.

La seguridad es una función transversal en las administraciones públicas, caracterizada por tratarse de un proceso integral constituido por todos los elementos humanos, técnicos, materiales y organizativos, relacionados con un sistema, como se deduce tanto del artículo cinco del ENS como de la ECN en su conjunto. Es por ello, que la seguridad debe abarcar cada etapa del ciclo de vida del sistema y sus documentos (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción), así como de los sistemas que lo soportan (análisis, diseño, desarrollo, implementación, operación, mantenimiento y obsolescencia).

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, ESN y ECN, dentro del marco de referencia establecido por la política de seguridad del Ministerio de Hacienda y Administraciones Públicas.

Asimismo esta Política de Seguridad de la Información debe ajustarse a lo establecido en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

El Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, establece en su artículo 11, apartado 1.h), que la Intervención General de la Administración del Estado es el órgano encargado de la planificación, diseño y ejecución de la política informática de la Secretaría de Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado, el soporte informático de las actividades y el asesoramiento, coordinación e instrumentación de los proyectos informáticos de sus órganos.

En su virtud, a propuesta de la Intervención General de la Administración del Estado, he tenido a bien disponer:

**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 objeto 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, trazabilidad y conservación.

Todo el patrimonio tecnológico proporcionado por el Estado a la Administración presupuestaria para el desempeño de sus funciones estará sujeto a la presente PSI.

**Segundo. Ámbito de aplicación.**

La PSI será de aplicación al personal de los centros directivos de la Administración presupuestaria y de sus organizaciones delegadas y territoriales, a sus dependencias e instalaciones, a sus sistemas de información y telecomunicaciones, y a las entidades que se relacionen con la Administración presupuestaria.

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

### Tercero. *Definiciones.*

Con carácter general, se asumen a efectos de esta resolución las definiciones recogidas en el anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal; en el anexo IV del Real Decreto 3/2010, de 8 de enero, publicado el 29 de enero; y en el artículo 4 de la Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Hacienda y Administraciones Públicas (en adelante, PSI-MINHAP).

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

Base de datos: conjunto de datos organizados sistemáticamente con objeto de facilitar su tratamiento posterior.

Seguridad de la información: conjunto de controles cuyos objetivos son:

- a) Definir las directrices a aplicar en la protección de los sistemas de la Administración presupuestaria.
- b) Dar cumplimiento a los requisitos exigidos por la normativa nacional sobre protección de datos y de impulso de la administración electrónica.

Control: Instrumento en forma de política, praxis, procedimiento, estructura organizativa, función de software o cualquier otro elemento que permita alcanzar los objetivos de seguridad de la información en la Administración Presupuestaria.

Sistema de información: Conjunto de datos, documentación, procedimientos y tratamientos informáticos, así como bases de datos, redes de comunicaciones y sistemas de interconexión, sistemas de control de accesos, personas, y ordenadores, periféricos y terminales instalados en los Servicios centrales y Organizaciones delegadas y territoriales de la Administración presupuestaria.

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.

Servicios de informática presupuestaria: área de la Intervención General de la Administración del Estado encargada de la definición, desarrollo y ejecución de la política informática de la Administración presupuestaria.

### Cuarto. *Misión.*

El Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas establece el propósito general de la Secretaría de Estado de Presupuestos y Gastos, y sus centros directivos, y de la Intervención General de la Administración del Estado.

La Secretaría de Estado de Presupuestos y Gastos es el órgano directivo al que le corresponde dirigir y coordinar las actuaciones relativas a la planificación, programación y presupuestación del sector público estatal y de sus costes de personal; el diseño, planificación y gestión de los fondos destinados a la política económica regional y el seguimiento y gestión de la participación española en el presupuesto de la Unión Europea.

La Intervención General de la Administración del Estado, por otro lado, tiene a su cargo las funciones de control interno de la gestión económico-presupuestaria, el seguimiento y control de subvenciones y ayudas públicas, el ejercicio de las funciones de autoridad de auditoría en aquellos programas comunitarios en los que la IGAE tenga tal condición, la coordinación de las acciones encaminadas a proteger los intereses financieros de la Unión Europea contra el fraude, la dirección y la gestión de la contabilidad pública y la formación de las cuentas económicas del sector público, la relación con las haciendas territoriales a los efectos de la información contable que deben remitir para la formación de las cuentas económicas del sector público, la integración, gestión y publicación del Inventario de Entes

del Sector Público Estatal, Autonómico y Local, el asesoramiento a los órganos de gestión derivado de sus funciones de control, la gestión de la información económico-financiera derivada del ejercicio de sus funciones contables y de control, y el auxilio y colaboración con la Administración de Justicia.

La Intervención General de la Administración del Estado, por otro lado, es el órgano encargado de la planificación, diseño y ejecución de la política informática de la Secretaría Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado, el soporte informático de las actividades y el asesoramiento, coordinación e instrumentación de los proyectos informáticos de sus órganos y la seguridad de la información. Atribuyendo esta última función a la Subdirección General de Explotación de los servicios de informática presupuestaria.

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, está integrado por:

- a) La normativa sobre la estructura organizativa del ámbito de esta resolución.
- b) El marco normativo de la Administración electrónica, y en particular el Esquema Nacional de Seguridad, y de la protección de datos de carácter personal, con el desarrollo establecido en el artículo 3 sobre marco legal y regulatorio de la Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la PSI-MINHAP.
- c) La normativa específica referida a la Estrategia de Seguridad Nacional y a la Estrategia de Ciberseguridad Nacional.
- d) La normativa departamental en materia de Administración electrónica y respecto a la política de seguridad.
- e) La normativa del ámbito de la Administración presupuestaria en materia de Administración electrónica y respecto a la política de seguridad.

Se trata de un marco normativo complejo y en permanente evolución para adaptarse a un escenario en continuo proceso de cambio.

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

La PSI de la Administración presupuestaria asume los principios básicos y particulares así como las responsabilidades específicas que se indican en el artículo 5 de la Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la PSI-MINHAP.

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

En concordancia con la PSI-MINHAP, el ENS, y las Guías CCN-STIC elaboradas por el Centro Criptológico Nacional que desarrollan el Esquema Nacional de Seguridad, 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 Centro); la operación del sistema de información (encomendada al Responsable del Sistema, que en esta resolución se asigna al Coordinador de los SIP) y la función supervisora (encargada al Responsable de Seguridad de la Información).

La gestión de la seguridad en la Administración presupuestaria requiere, además de la implicación activa de todos los usuarios de los sistemas de información, la existencia de un marco organizativo orientado a dicha gestión en el que desempeñarán un papel primordial los siguientes agentes:

- a) Comité de Coordinación de la Seguridad de la Información.
- b) Coordinador de los Servicios de Informática Presupuestaria (SIP).

c) Responsable de Seguridad de la Información que asume las funciones de ese rol en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre, el ENS y la PSI-MINHAP.

d) 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.

e) Responsables de Seguridad de los Ficheros de los centros directivos, organizaciones delegadas o territoriales de la Administración presupuestaria que, a efectos de esta resolución, se denominarán Responsables de Fichero.

f) Subdirecciones Generales de los SIP.

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:

g) 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 efectos de esta resolución, se denominarán Administradores de Red.

h) Administradores de Seguridad de los Accesos a los Sistemas de Información y Bases de Datos de la red de la Administración presupuestaria que, a efectos de esta resolución, se denominarán Administradores de Sistemas de Información.

En el contexto de esta resolución, las figuras de Administrador de Red y de Sistemas de Información tienen un carácter organizativo, de acuerdo con las funciones encomendadas en apartados undécimo y duodécimo, y no un significado técnico.

En el caso específico de determinada información, y para el acceso desde el ámbito externo a la Administración presupuestaria, el responsable de la misma podrá requerir la identificación por parte del titular de cada órgano que desee acceder, de un único responsable al que se le exigirán obligaciones de seguridad para el señalamiento y control de los usuarios de su ámbito.

#### 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:

a) El Interventor General de la Administración del Estado y los directores generales de los centros directivos de la Secretaría de Estado de Presupuestos y Gastos, que actuarán rotatoriamente, cada seis meses, como presidente del Comité. El titular del centro directivo podrá delegar esta función, para cada reunión que le corresponda presidir, en el Director o Subdirector General que designe.

b) El Coordinador de los SIP, que actuará como vicepresidente del Comité.

c) El Subdirector General de Explotación de los SIP.

d) El Responsable de Seguridad de la Información que actuará como secretario del Comité.

e) Los Responsables de Centro, previstos en el apartado décimo, designados por el titular de cada uno de los centros directivos de la Administración presupuestaria.

f) Tres Interventores Delegados en representación del conjunto de las Intervenciones delegadas en Ministerios, Agencias y Organismos públicos, Intervenciones regionales y territoriales, designados por el Interventor General de la Administración del Estado.

Además, el Comité podrá convocar a representantes de unidades organizativas 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 establecer 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 del Estado, que emanen de la Comisión de Estrategia TIC, o del Departamento, que emanen de la Comisión Ministerial de Administración digital, dirigidas a garantizar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y conservación 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 tenga 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 los SIP.

En los apartados noveno, décimo, undécimo y duodécimo de esta resolución se recogen las funciones de seguridad específicas al ámbito de la Administración presupuestaria asignadas al Responsable de Seguridad de la Información, al Responsable de Centro y a los Administradores de Red y de Sistemas de Información.

Las funciones y obligaciones reguladas en el Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y por el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD, debido a su extensión se recogerán detalladamente en el procedimiento de desarrollo de la presente resolución «Funciones y obligaciones del personal de la Administración Presupuestaria en relación con la seguridad de los sistemas de información».

En el anexo I de esta resolución se indica cómo se han distribuido las obligaciones y funciones de seguridad teniendo en cuenta el marco organizativo de la Administración presupuestaria, en general, y de seguridad, en particular.

*Noveno. Responsable de Seguridad de la Información.*

El Responsable de Seguridad de la Información aplicará las medidas de seguridad a los sistemas de información de la Administración presupuestaria de acuerdo con las directrices establecidas por el Comité. Será designado por el Comité a propuesta del Coordinador de los SIP.

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 los SIP bajo la iniciativa y coordinación del 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 Red y de Sistemas de Información y, en general, las difundirá a todo el ámbito de aplicación.

*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 en materia de seguridad de la información las funciones y obligaciones que el ENS asigna 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 un Administrador único de red y a los suplentes que considere precisos. No obstante, en el caso de los centros directivos, la designación del Administrador de Red podrá efectuarse, si la estructura así lo aconseja, a nivel de Subdirección General o de ubicaciones administrativas diferentes.

d) Designará a los Administradores de Sistemas de Información de su ámbito de competencia.

e) Autorizará el acceso de usuarios a la red departamental y a los sistemas de información de su centro. Asimismo, comunicará la anulación de los accesos permitidos a la red departamental y a las bases de datos de su propio centro.

Quien ostente la función de autorización de accesos a la información actuará así mismo como Responsable de Fichero en los términos del Real Decreto 1720/2007, de 21 de diciembre, o designará a dicho Responsable.

f) Solicitará el 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) Solicitará el 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 d), e), f) y g) podrán ser desempeñadas por los 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 Subdirectores 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.

El Responsable de Centro actuará como Responsable de Fichero en los términos del real decreto 1720/2007, de 21 de diciembre, o designará a dicho Responsable, el cuál se encargará de la finalidad, contenido y uso del tratamiento.

#### Undécimo. *Administrador de Red.*

Cada Administrador de Red será el responsable de la aplicación, en su ámbito de actuación, de la presente resolución y de sus normas de desarrollo, bajo la dependencia del Responsable de Centro que lo designara. Para esta misión el Administrador de Red actuará de acuerdo con las instrucciones, procedimientos y herramientas de carácter técnico que establezcan los SIP.

Las funciones y obligaciones del Administrador de Red en materia de seguridad serán:

a) Instrumentar las solicitudes de acceso a la red de los nuevos usuarios autorizados.  
b) Realizar el mantenimiento y actualización del inventario de usuarios con acceso permitido a la red departamental.

c) Obtener periódicamente y, al menos una vez al año, a través de los medios puestos a su disposición por los SIP, estadística de accesos realizados por los usuarios de la red departamental a los sistemas de información.

d) Mantener y custodiar la información necesaria sobre la autorización y denegación del acceso de cada uno de los usuarios a la red, como mínimo, el puesto de trabajo, el responsable de la autorización y anulación de los accesos, la fecha de autorización o denegación, al menos durante 2 años.

e) Informar de los incidentes relativos a la seguridad de la información, según los procedimientos establecidos para tal fin.

Duodécimo. *Administrador del Sistema de Información.*

Cada base de datos, correspondiente a un sistema de información o aplicación informática, tendrá asignado un Administrador de Sistemas de Información cuya designación corresponderá a:

a) En caso de sistemas de información centrales, al Responsable de Centro del centro directivo al que competa la responsabilidad de realizar la función asociada al sistema de información o aplicación informática. No obstante, si el Responsable de Centro ha nombrado Responsable de la Información, será el Responsable de la Información el que nombre al Administrador de la misma.

Cuando el contenido de la base de datos central sea el resultado de una gestión descentralizada, el Responsable del Servicio competente, o el Responsable de la Información nombrado por él, podrá designar Responsable Delegado de Autorización de Accesos, por cada unidad u oficina de gestión que participe. Estos Responsables Delegados designarán al correspondiente Administrador de Sistemas de Información.

Cuando se trate de productos o aplicaciones informáticas de utilización general en todo el entorno de la Administración presupuestaria, cuya responsabilidad no esté asignada a un centro directivo concreto, el Administrador de Sistemas de Información será designado por el Coordinador de los SIP.

b) En el caso de sistemas de información departamentales, al Responsable del centro directivo u organización delegada o territorial en la que residan.

c) En el caso de sistemas de información externos, al Coordinador de los SIP.

El Administrador de Sistemas de Información será el responsable de la aplicación de la presente resolución y de las instrucciones y procedimientos que, en esta materia, se desarrollen, en lo que afecta al sistema de información, bajo la dependencia del Responsable de Centro o de Información que lo designara. Para esta misión el Administrador de Sistemas de Información actuará de acuerdo con las instrucciones, procedimientos y herramientas de carácter técnico que establezcan los SIP. Serán funciones y obligaciones del Administrador de Sistemas de Información las siguientes:

a) Instrumentar y gestionar las altas, bajas y el mantenimiento de autorizaciones de acceso a los usuarios de los sistemas de información y, en su caso, de las funciones permitidas (por ejemplo, asignación de perfiles de acceso).

b) Instrumentar y gestionar el acceso de los usuarios externos a los sistemas de información de la red de Informática presupuestaria, previa comunicación a la Unidad de los SIP designada a tal efecto, cuando proceda.

c) Mantener y custodiar la información necesaria sobre la autorización o denegación del acceso de los usuarios a los sistemas de información, al menos durante 2 años.

d) Obtener periódicamente, mediante los medios puestos a su disposición por los SIP, estadística de los accesos realizados por los usuarios a los sistemas de información centrales y departamentales administrados por él.

Además, cuando el sistema de información trate datos de carácter personal, a los que resulten de aplicación las medidas de seguridad de nivel alto del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el Administrador de Sistemas de Información, central o departamental, obtendrá un informe mensual de los accesos y operaciones realizadas por los usuarios del sistema, identificando, como mínimo, el usuario, fecha y hora en que se realizó el acceso, el sistema accedido, el tipo de acceso y si ha sido autorizado o denegado.

e) Informar de los incidentes relativos a la seguridad de la información según los procedimientos establecidos para tal fin.

Decimotercero. *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.

Decimocuarto. *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 requerimientos mínimos establecidos por el ENS, la ESN y la ECN.

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 representen un equilibrio, de acuerdo con la naturaleza de la información y los tratamientos, entre los riesgos a los que estén expuestos y el coste de 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.

Para la armonización de los análisis de riesgos se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

El Responsable de Seguridad de la Información será el encargado de que el análisis se realice en tiempo y forma, así como de identificar carencias y debilidades y de ponerlas en conocimiento del Comité. El Comité adoptará las decisiones adecuadas de forma que los Responsables de Centro, independientemente del centro directivo al que pertenezcan, puedan aplicarlas.

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

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 cuáles deberán ser proporcionadas a los riesgos y estar justificadas. Con carácter bienal el Comité de coordinación de la seguridad de la información revisará y aprobará, en su caso, el análisis de riesgos presentado por el Responsable de Seguridad de la Información.

Decimoquinto. *Responsabilidades 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 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 del usuario 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.

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.

Es por ello que 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.

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

Se prestará la máxima atención a la concienciación de las personas que intervienen en la seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad. Es por ello que la presente resolución y sus normas de desarrollo estarán accesibles para todo el personal que acceda a sistemas y recursos de la Administración presupuestaria.

La formación del personal de los SIP será responsabilidad del Coordinador y de los Subdirectores Generales de los SIP. La formación del personal de los centros directivos, organizaciones delegadas o territoriales de la Administración presupuestaria corresponderá a los Administradores de Centro. La concienciación en materia de seguridad en el ámbito de la Administración presupuestaria corresponderá al Comité de Coordinación de la Seguridad de la Información.

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

La PSI regulada en esta resolución será desarrollada y complementada, constituyendo lo que se denominará en adelante normativa de seguridad 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:

1. Primer nivel normativo constituido por la PSI del departamento ministerial al que pertenece la Administración presupuestaria.
2. 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.
3. Tercer nivel normativo formado por los procedimientos, guías e instrucciones técnicas orientadas a la aplicación e instrumentación de las medidas de seguridad en el desarrollo, mantenimiento y explotación de los sistemas de información.

La aprobación de estos procedimientos técnicos corresponderá a los SIP.

4. Cuarto nivel normativo constituido por los informes que recojan las conclusiones, observaciones y recomendaciones de una auditoría, estudio o evaluación de seguridad; 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 partícipe de la PSI, estableciendo canales para el reporte y coordinación de los respectivos Comités de seguridad y, en su caso, 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, se 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.*

Los órganos directivos de la Administración presupuestaria se comprometen a proteger la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y conservación 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.

Disposición adicional. *Desarrollo para su aplicación.*

Se faculta a la Intervención General de la Administración del Estado para resolver cuantas consultas de índole específica puedan plantearse en la aplicación de la presente Resolución, así como para dictar normas internas para su aplicación a propuesta del Comité de coordinación de la seguridad de la información.

Disposición transitoria.

Mientras el Comité de coordinación de la seguridad de la información no apruebe el nuevo procedimiento de control de accesos a la red y a los sistemas de información de la Administración presupuestaria, la tramitación de las solicitudes de acceso se efectuará de acuerdo con lo dispuesto en la Resolución de 27 de febrero de 2009, de la Secretaría de Estado de Hacienda y Presupuestos, por la que regula la política de seguridad de los sistemas de información de la Secretaría General de Presupuestos y Gastos y de la Intervención General del Estado.

Disposición derogatoria.

Sin perjuicio de lo dispuesto en el apartado anterior, queda derogada la Resolución de 27 de febrero de 2009, de la Secretaría de Estado de Hacienda y Presupuestos, por la

que se regula la política de seguridad de los sistemas de información de la Secretaría General de Presupuestos y Gastos y de la Intervención General de la Administración del Estado.

Disposición final. *Entrada en vigor.*

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

Madrid, 21 de diciembre de 2015.–La Secretaria de Estado de Presupuestos y Gastos, Marta Fernández Currás.

### ANEXO I

#### Asignación de las funciones y obligaciones en materia de seguridad de la información en la Administración presupuestaria

Resolución de 21 de diciembre 2015	RD 1720/2007, de 21 de diciembre	RD 3/2010, Guías CCN-STIC 801 y 802	Orden HAP/1953/201, de 15 de octubre
Comité de Coordinación de la Seguridad de la Información.	–	Comité de la Seguridad de la Información.	–
El Interventor General de la Administración del Estado y los directores generales de los centros directivos de la Secretaría de Estado de Presupuestos y Gastos, que actuarán rotatoriamente, cada seis meses, como presidente del Comité.	–	–	–
Coordinador de los SIP que actuará como Vicepresidente del Comité, y Subdirecciones IP.	–	Responsable del Sistema.	Responsable del Sistema.
Responsable de Seguridad de la Información.	Responsable de Seguridad	Responsable de Seguridad.	Responsable de Seguridad.
Responsable de Centro/Responsable de Fichero.	Responsable del Fichero	Responsable de la Información.	Responsable de la Información.
Responsable de Centro/Responsable de Fichero.	–	Responsable del Servicio.	Responsable del Servicio.
Subdirecciones Generales de Aplicaciones de Contabilidad y Control, Presupuestos y Fondos Comunitarios, Costes de Personal Activo y Pasivo, Subdirección General de Explotación. Subdirectores, Adjuntos, Jefes de Área y Jefes de Proyecto de dichas Subdirecciones.	–	Administrador de Seguridad del Sistema.	–
Usuarios.	–	–	–