*Resolución de la Secretaría de Estado de la Seguridad Social y Pensiones por la que se actualiza la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.*

La Resolución de 2 de septiembre de 2013 de esta Secretaría de Estado definió la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social, política que conviene actualizar para recoger, entre otras cuestiones, la entrada en vigor 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) (en adelante, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. De este modo, se hace ahora mención expresa en la política de seguridad a la necesaria coordinación en el desarrollo normativo, y también en su implantación, del Esquema Nacional de Seguridad (en adelante, ENS) y del RGPD.

En virtud de lo expuesto, esta Secretaría de Estado de la Seguridad Social y Pensiones resuelve:

Primero. Actualización de la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.

Se aprueba la actualización de la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social, que se incorpora como anexo a esta resolución, y que se aplicará y observará por todos los organismos adscritos y órganos y unidades, centrales y territoriales, dependientes orgánicamente de la Secretaría de Estado de la Seguridad Social y Pensiones, en todos sus sistemas de información y por todo el personal destinado en ellos, así como por el personal de otros organismos o entidades que en virtud de norma legal, acuerdo o convenio tengan acceso a los sistemas de información de la Administración de la Seguridad Social, en particular las entidades colaboradoras de la Seguridad Social.

Segundo. No incremento del gasto público.

La aplicación de esta resolución no conllevará incremento del gasto público, atendiéndose el desarrollo normativo y la estructura organizativa contemplados en la política de seguridad con los recursos humanos y materiales disponibles en la Administración de la Seguridad Social.

Tercero. Fecha de efectos.

Lo dispuesto en esta resolución surtirá efectos desde el día siguiente al de su publicación en la sede electrónica de la Secretaría de Estado de la Seguridad Social y Pensiones.

Madrid, a la fecha de la firma.

El Secretario de Estado de la Seguridad Social y Pensiones,

Seguridad Social
Firmado electrónicamente

Firmado electrónicamente por: SUAREZ CORUJO FRANCISCO DE BORJA
23.03.2026 15:10:06 CET

Francisco de Borja Suárez Corujo

ANEXO

## Política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social

*Introducción.*

La política de seguridad en la utilización de medios electrónicos identifica responsabilidades y establece principios y directrices para una protección adecuada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones.

Esta política de seguridad es el instrumento en que se apoya la Administración de la Seguridad Social para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones y debe entenderse no como un producto sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implementando la cultura de la seguridad en la Administración de la Seguridad Social.

En este sentido, la entrada en vigor del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, plantea nuevos retos, así como la necesidad de dar un nuevo enfoque al tratamiento de datos de carácter personal. De este modo, para garantizar su adecuada implantación resulta necesario intensificar la labor de coordinación con la aplicación del resto de normativas de obligatoria implantación en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas, dado que uno de los objetivos para el cumplimiento del RGPD es la implantación de las medidas técnicas previstas en el ENS. Para garantizar la coordinación en la implantación de estas normativas se deberá procurar:

- Que el cumplimiento de ambas normativas (ENS y RGPD) esté alineado, apoyándose mutuamente en la medida de lo posible, aunque en algunos casos la implantación de determinadas medidas se tenga que realizar por separado.
- Que los planes de concienciación y formación que se definan sean comunes o, por lo menos, se coordinen los contenidos comunes.
- Que las Auditorías de cumplimiento referente a ambas normas se efectúen de manera conjunta.
- Que se lleve a cabo un control común de las responsabilidades con organismos externos y proveedores.

Se deberá procurar la correspondencia de los tratamientos RGPD con los sistemas de información ENS con datos de carácter personal actualmente identificados en la organización, buscando unificar en una única declaración los atributos y características que son necesarios para cumplir tanto con el RGPD como con el ENS.

*I. Misión y marco regulatorio.*

A la Secretaría de Estado de la Seguridad Social y Pensiones, bajo la superior autoridad de la persona titular del Ministerio de Inclusión, Seguridad Social y Migraciones le corresponde la dirección y tutela de las entidades gestoras y servicios comunes de la Seguridad Social adscritas al departamento, el impulso y la dirección de la ordenación jurídica del sistema de la Seguridad Social, la dirección y coordinación de la gestión de los recursos financieros y gastos de la Seguridad Social, la planificación y tutela de la gestión ejercida por las entidades colaboradoras de la Seguridad Social, así como cualquier otra competencia que, legal o reglamentariamente, le esté atribuida.

El marco normativo en el que desarrolla sus actividades la Secretaría de Estado de la Seguridad Social y Pensiones está regulado esencialmente por las siguientes disposiciones, sin perjuicio de la aplicación de todo el ordenamiento jurídico en aquello que le afecte:

a) Texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.

b) Ley 27/2011, de 1 de agosto, sobre actualización, adecuación y modernización del sistema de Seguridad Social.

c) Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

d) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

e) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Adicionalmente, y debido al carácter personal y reservado de la información manejada y a la necesidad de garantizar la seguridad de los servicios prestados al ciudadano en el ámbito de la administración electrónica, la Secretaría de Estado de la Seguridad Social y Pensiones desarrolla sus actividades de acuerdo con la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

f) 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), siendo de aplicación igualmente, la normativa vigente que con relación a este ámbito sea aprobada a nivel nacional.

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

h) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

i) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

j) Orden ISM/1320/2024, de 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información.

*II. Estructura organizativa.*

La estructura organizativa de la gestión de la seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social y Pensiones está compuesta por:

- El responsable del sistema global de información.
- El Comité de Seguridad de los Sistemas de Información de la Seguridad Social.
- Los responsables de los sistemas de información.
- Los responsables de la información y/o tratamientos.
- Los responsables de los servicios electrónicos.
- El responsable de seguridad.
- El responsable de la prestación del servicio.
- El Delegado de Protección de Datos.
- El encargado del tratamiento.

II. 1. Responsable del sistema global de información.

El responsable del sistema global de información será la persona titular de la Secretaría de Estado de la Seguridad Social y Pensiones como responsable último del funcionamiento de los servicios. El sistema global de información integra todos los sistemas de información de los organismos adscritos y órganos y unidades dependientes de la Secretaría de Estado de la Seguridad Social y Pensiones de los que son responsables las personas titulares de los mismos.

El responsable del sistema global de información tiene las siguientes funciones:

1. Hacer cumplir las disposiciones establecidas en el ENS cuando el sistema de información se encuentre dentro del ámbito de aplicación del mismo y, en su caso, emitir directrices.
2. Resolver los conflictos que puedan surgir entre los distintos responsables de los sistemas de información, en el ejercicio de sus funciones, en los términos establecidos en el apartado VIII de este anexo.
3. Designar a los representantes que formarán parte del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones del Ministerio de Inclusión,

Seguridad Social y Migraciones, en nombre de la Secretaría de Estado de la Seguridad Social y Pensiones.

II. 2. El Comité de Seguridad de los Sistemas de Información de la Seguridad Social (en adelante, CSSISS) coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito de la Secretaría de Estado de la Seguridad Social y Pensiones, elaborando y aprobando las normas y procedimientos en materia de seguridad, revisando el estado global de seguridad, proponiendo la aprobación de planes estratégicos y cuantas otras funciones le sean encomendadas en su norma de creación. Dicho comité se comunicará con el Comité de Seguridad de las Tecnologías de la Información y Comunicaciones del Ministerio de Inclusión, Seguridad Social y Migraciones.

II. 3. Responsables de los sistemas de información.

Los responsables de los sistemas de información garantizan que se implantan, mantienen y actualizan, en sus respectivos ámbitos, las medidas pertinentes en materia de seguridad de los sistemas de información.

Se designan como responsables de sus sistemas de información a las personas titulares de todos los organismos adscritos y órganos dependientes de la Secretaría de Estado de la Seguridad Social y Pensiones.

Les corresponden las siguientes funciones:

1. Garantizar que se gestiona el riesgo de seguridad de sus sistemas de información, definiendo para cada uno de ellos su nivel de riesgo residual aceptable, es decir, el riesgo restante en el sistema de información tras la implantación de las medidas de seguridad establecidas en el plan de seguridad y que puede ser asumido por su entidad.
2. Suspender, previo acuerdo de los responsables de información y de servicios, el manejo de una determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad.
3. Adoptar las medidas necesarias para que el personal con acceso a un sistema de información conozca las normas de seguridad que debe aplicar.
4. Proponer planes de formación, información y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad y elevarlos al CSSISS para su incorporación en los planes de los organismos o unidades dependientes de la Secretaría de Estado de la Seguridad Social y Pensiones, así como establecer actuaciones disuasorias a favor de la seguridad.

II. 4. Responsables de la información y/o tratamientos.

Los responsables de la información son quienes deben determinar los requisitos de seguridad de la información tratada en la organización.

Se designan como responsables de la información a las personas titulares de las subdirecciones generales de los organismos adscritos y órganos y unidades incluidas en el ámbito de aplicación de esta resolución para la información que tratan en el ejercicio de sus competencias, sin perjuicio de que estas puedan delegar ciertas funciones en las direcciones y subdirecciones provinciales correspondientes. Es también responsable en la parte de información la persona titular de la División de Administración y Análisis Presupuestario del Instituto Social de la Marina.

Tienen las siguientes obligaciones:

1. Identificar y valorar la criticidad de la información que manejan en el ámbito de sus funciones y determinar en función de la misma, los requisitos de seguridad que es necesario cumplir para cada tipo de información.
2. Determinar el ciclo de vida de la información manejada y determinar los procedimientos de creación, tratamiento y destrucción de la misma.

Los responsables del tratamiento tienen como funciones:

- Satisfacer las solicitudes de derechos de las personas titulares de los datos (información, derecho de supresión, oposición, limitación al tratamiento, acceso, rectificación y olvido).
- Registrar la base que legitima el tratamiento.
- Comunicar previamente al Delegado de Protección de Datos los nuevos tratamientos de alto riesgo.
- Limitar los tratamientos en función del consentimiento de la persona titular del dato.
- Realizar la evaluación de impacto en la privacidad y el análisis de privacidad desde el diseño y por defecto.
- Elaborar el registro de las actividades de tratamiento de las que son responsables.
- Elaborar las cláusulas destinadas a informar a los afectados cuyos datos personales están tratando como responsables de tratamiento de los contenidos incluidos en los artículos 13 y 14 del RGPD.

II. 5. Responsable de los servicios electrónicos.

Los responsables de los servicios electrónicos son quienes deben determinar los requisitos de seguridad para los servicios prestados por la organización.

Se designan como responsables de servicios electrónicos a las personas titulares de las subdirecciones generales de los organismos adscritos y órganos y unidades incluidas en el ámbito de aplicación de esta resolución para los servicios que prestan en el ejercicio de sus competencias, sin perjuicio de que estas puedan delegar ciertas funciones en las direcciones y subdirecciones provinciales correspondientes. Es también responsable de los servicios la persona titular de la División de Administración y Análisis Presupuestario del Instituto Social de la Marina.

Tienen por función identificar los servicios que se prestan en su ámbito organizativo y determinar para cada uno de ellos los requisitos de seguridad que es necesario cumplir.

II. 6. Responsable de seguridad.

El responsable de seguridad es el encargado de determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Se designa como responsable de seguridad al director del departamento de la Gerencia Informática de la Seguridad Social que tiene atribuidas las competencias de seguridad de la información, sin perjuicio de que pueda delegar ciertas funciones.

Tendrá las siguientes funciones:

1. Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios establecidos por sus respectivos responsables.
2. Realizar periódicamente un proceso de análisis de los riesgos del sistema de información que permita identificar los riesgos a los que este se encuentra expuesto, y las medidas para asegurar el nivel de riesgo residual aceptable aprobado para cada sistema de información.
3. Establecer el conjunto de proyectos y actuaciones que conformarán el plan director de seguridad que permitirá implantar las medidas de seguridad propuestas y elevarlo al responsable del sistema de información.
4. Realizar el seguimiento y control del estado de la seguridad del sistema de información y verificar que las medidas de seguridad definidas son adecuadas para la protección de la información y los servicios.
5. Realizar las auditorias periódicas que se determinen en cada sistema de información, incluyendo las relativas a protección de datos, para garantizar la correcta aplicación de las medidas de seguridad y el cumplimiento de las normas y procedimientos vigentes en la organización. El informe resultante de las mismas se enviará a los responsables de los sistemas de información y al responsable de la prestación del servicio para subsanar las deficiencias encontradas.
6. Redactar, cuando sea necesario, las declaraciones de aplicabilidad de los sistemas de información respecto al ENS.

II. 7. Responsable de la prestación del servicio.

El responsable de la prestación del servicio implementará las medidas de seguridad relativas a su ámbito de competencias incluidas en el plan director de seguridad.

Se designa como responsable de la prestación del servicio al director del departamento de la Gerencia Informática de la Seguridad Social que tiene atribuidas las competencias del mantenimiento de las infraestructuras técnicas que soportan los servicios, sin perjuicio de que pueda delegar ciertas funciones.

Tendrá las siguientes funciones:

1. Implementar las medidas de seguridad que entren en su ámbito de actuación establecidas en el plan director de seguridad elaborado por el responsable de seguridad y aprobado por el responsable del sistema de información.

2. Observar el cumplimiento de las normas y procedimientos establecidos y aprobados por el CSSISS en la administración y operativa habitual de los sistemas de información.
3. Supervisar y garantizar la gestión, configuración y actualización, en su caso, de los recursos que soportan el funcionamiento correcto de los sistemas de información y de la prestación de los servicios.
4. Colaborar en las auditorias llevadas a cabo por el responsable de seguridad y aportar información completa y veraz sobre el estado de las medidas de seguridad implantadas que sean de su responsabilidad.

*II. 8. Delegado de Protección de Datos.*

Mediante Resolución de 17 de abril de 2018 esta Secretaría de Estado definió las funciones del Delegado de Protección de Datos de la Administración de la Seguridad Social (en adelante, DPD), constituyendo igualmente la Comisión de Protección de Datos. En su Instrucción Octava se hacía mención expresa a la posibilidad de que otros comités pudiesen solicitar asesoramiento al DPD en relación con las materias propias de su competencia.

En atención a lo anterior y a lo señalado en la introducción de esta política, el CSSISS y DPD colaborarán en el compartido objetivo de procurar: a) alinear las respectivas normativas de cumplimiento, así como la definición e implantación de medidas de seguridad, b) realizar auditorías de cumplimiento comunes, c) el diseño y ejecución de planes de formación conjuntos, y d) otras materias relacionadas. En caso de conflicto, prevalecerá la postura del DPD en materia de tratamientos de datos personales.

*II. 9. Encargado del tratamiento.*

La Gerencia de Informática de la Seguridad Social actúa como encargada de los tratamientos de datos personales que lleven a cabo las entidades, órganos y organismos que integran la Administración de la Seguridad Social, necesarios para el ejercicio de las competencias que tienen atribuidas.

Estas obligaciones se recogen en el siguiente encargo de tratamiento:

PRIMERO. - El tratamiento por parte de la Gerencia de Informática de la Seguridad Social consistirá en la recogida, estructuración, conservación, consulta, difusión, cotejo, supresión, conservación, registro, modificación, extracción, comunicación por transmisión, interconexión, limitación, destrucción y comunicación de los datos personales.

SEGUNDO. - Para el cumplimiento de las funciones que corresponden a la Gerencia de Informática de la Seguridad Social como encargada del tratamiento, las entidades, órganos y organismos que integran la Administración de la Seguridad Social pondrán a su disposición la información que consta en las bases de datos corporativas del sistema.

TERCERO. - La Gerencia de Informática de la Seguridad Social actuará como encargada del tratamiento durante el tiempo necesario para cumplir las finalidades para las que fueron recabados los datos personales, así como otras finalidades compatibles y dirimir las posibles responsabilidades que pudieran derivar de dicho tratamiento.

CUARTO. - En su actividad como encargada del tratamiento, la Gerencia de Informática de la Seguridad Social:

- Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o a una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de una norma con rango de ley; en tal caso, informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal derecho o norma lo prohíba por razones importantes de interés público;

- Garantizará que las personas autorizadas para tratar datos personales estén sujetas a una obligación legal de confidencialidad o, en su caso, se hayan comprometido a respetar la confidencialidad.

- Tomará todas las medidas de seguridad necesarias para garantizar un nivel de seguridad adecuado al riesgo.

- No recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. Cuando recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, impondrá a este otro encargado, mediante contrato u otro acto jurídico, las mismas obligaciones de protección de datos, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Si ese otro encargado incumple sus obligaciones de protección de datos, la Gerencia de Informática de la Seguridad Social seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

- Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

- Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD.

- Siguiendo las indicaciones del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento.

- Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones en materia de protección de datos personales, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

QUINTO. - A las entidades, órganos y organismos que integran la Administración de la Seguridad Social, como responsables del tratamiento, les corresponde:

- Entregar a la Gerencia de Informática de la Seguridad Social como encargada del tratamiento, la información que consta en las bases de datos de la Administración de la Seguridad Social.

- Realizar, en su caso, la evaluación de impacto en la protección de datos personales de las operaciones de tratamiento a realizar por la Gerencia de Informática de la Seguridad Social.

- Realizar las consultas previas que correspondan.

- Velar de forma previa y durante el tratamiento por el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por parte de la Gerencia de Informática de la Seguridad Social.

- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO. – El objeto, la duración, la naturaleza y la finalidad del tratamiento, así como el tipo de los datos personales y las categorías de interesados, quedan debidamente definidos en los Registros de Actividades de Tratamiento de los organismos adscritos y órganos y unidades dependientes de la Secretaría de Estado de la Seguridad Social y Pensiones.

*III. Gestión de los riesgos.*

Se realizará de forma continua un proceso de análisis de riesgos sobre los sistemas de información, conforme a los principios de gestión de la “seguridad basada en los riesgos” y “reevaluación periódica” establecidos en el ENS.

El responsable de seguridad será el encargado de realizar el análisis de riesgos del sistema de información, garantizando que el mismo se realiza de forma correcta y completa y comunicando los resultados a los responsables del sistema de información.

El responsable del sistema de información es el propietario de los riesgos sobre dicho sistema de información, siendo responsable de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

*IV. Dimensiones de seguridad.*

Las medidas necesarias para garantizar la seguridad de los sistemas y activos de información de la Seguridad Social y la correcta gestión de riesgos deben garantizar el cumplimiento de las dimensiones de seguridad definidas en el anexo I del Real Decreto 311/2022, de 3 de mayo. Estas dimensiones son las siguientes:

- Confidencialidad: Se refiere a la garantía de que la información no se divulga a personas o sistemas no autorizados.
- Integridad: Asegura que la información no ha sido alterada o modificada de forma no autorizada.

- Autenticidad: Se refiere a la verificación de la identidad de las entidades (usuarios, sistemas, etc.) que acceden a la información o sistema.
- Trazabilidad: Permite rastrear las acciones realizadas sobre los sistemas y la información, identificando quién las realizó y cuándo.
- Disponibilidad: Implica que la información y los sistemas estén accesibles y utilizables por las personas autorizadas cuando sea necesario.

*V. Normativa de seguridad.*

Esta política de seguridad debe ser desarrollada en diferentes normativas de seguridad que detallen y concreten los requisitos de seguridad de la información y los servicios, las tareas necesarias para garantizar su cumplimiento y las responsabilidades de todo el personal implicado en las mismas.

En la Secretaría de Estado de la Seguridad Social y Pensiones esta normativa se estructura en los siguientes niveles:

1. La política de seguridad. Establece la estrategia general de seguridad y se define en este documento.
2. Las normas de seguridad. Conjunto de documentos que determinan los objetivos de seguridad y directrices generales en cada ámbito concreto y establecen las responsabilidades del personal implicado. Deben ser globales, concisas y definir puntos de contacto para su interpretación correcta.
3. Los procedimientos de seguridad. Conjunto de documentos que describen explícitamente y paso a paso cómo realizar determinadas tareas para cumplir lo estipulado en las normas de seguridad. Cada procedimiento debe detallar al menos en qué condiciones debe aplicarse, quienes deben llevarla a cabo y qué hacer en cada momento.
4. Las guías de seguridad. Documentación que propone recomendaciones de actuación para mejorar, entre otras, la eficacia y eficiencia de los procedimientos de seguridad, información adicional de apoyo y buenas prácticas.

La política y las normas de seguridad serán aprobadas por el CSSISS y serán de obligado cumplimiento en toda la organización. Los procedimientos de seguridad son de obligado cumplimiento, pero no requieren aprobación del CSSISS y serán de aplicación en su ámbito correspondiente.

Las guías de seguridad no se consideran de obligado cumplimiento y no requieren aprobación del CSSISS. Estas últimas se proporcionarán a título meramente informativo.

*VI. Responsabilidad del personal.*

Todo el personal que forme parte de la Secretaría de Estado de la Seguridad Social y Pensiones o que colabore con ella en el ejercicio de sus funciones, deberá conocer y aplicar en su ámbito de actuación esta política de seguridad, así como las normas y procedimientos de seguridad del sistema de información al que tenga acceso. Estas normas y procedimientos les serán proporcionadas por el responsable del sistema de información.

*VII. Relación con otras administraciones públicas.*

Cuando la Secretaría de Estado de la Seguridad Social y Pensiones preste servicios o ceda información a otras administraciones públicas, les hará partícipes de esta política de seguridad y de las normas de seguridad que apliquen. Las administraciones públicas receptoras quedarán sujetas a las obligaciones establecidas en ellas, debiendo desarrollar sus propios procedimientos para satisfacerlas.

*VIII. Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, este será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del responsable global del sistema de información.

*IX. Formación, información y concienciación.*

La Secretaría de Estado de la Seguridad Social y Pensiones desarrollará actividades específicas orientadas a la formación, información y concienciación de su personal en materia de seguridad de la información, así como a la difusión de esta política de seguridad y su desarrollo normativo, en particular entre el personal de nueva incorporación. A estos efectos, los planes de formación de la Secretaría de Estado incluirán actividades formativas específicas sobre esta materia.

La Secretaría de Estado de la Seguridad Social y Pensiones promoverá una cultura de seguridad de la información alineada con la política de seguridad entre aquellas organizaciones y usuarios externos que tengan acceso por acuerdo o convenio a los sistemas de información de la Seguridad Social.

*X. Actualización y revisión periódica.*

La política de seguridad deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de la administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

Las propuestas de revisión de la política de seguridad se elaborarán por el CSSISS que, con tal objetivo, revisará regularmente la oportunidad, idoneidad, completitud y precisión de lo establecido en la política de seguridad en la utilización de medios electrónicos.