Resolución de 21 de junio de 2019, de la Secretaría de Estado de la Seguridad Social, 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 General de Protección de Datos RGPD) y de la Ley 3/2018, 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 y del RGPD.

En virtud de lo expuesto, esta Secretaria de Estado de la Seguridad Social resuelve:

Primero. Actualización de la política de seguridad en la utilización de medios electrónicos en 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 Secretaria de Estado de la Seguridad Social, 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 a la estructura organizativa contemplada 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.

Madrid, 21 de junio de 2019

El Secretario de Estado de la Seguridad Social,

Seguridad Social
Firmado electrónicamente

Firmado electrónicamente por: OCTAVIO JOSE GRANADO MARTINEZ

Octavio José Granado Martínez.

SEÑOR GERENTE DE INFORMÁTICA DE LA SEGURIDAD SOCIAL

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 (TIC).

Esta política de seguridad es el instrumento en que se apoya la Administración de 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 Reglamento Europeo de Protección de Datos (en adelante RGPD) y de la Ley 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, 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 (en adelante ENS), 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 Secretaria de Estado de la Seguridad Social, bajo la superior autoridad de la persona titular del Ministerio de Trabajo, Migraciones y Seguridad Social 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 Secretaria de Estado de la Seguridad Social, y sin perjuicio de la aplicación de todo el ordenamiento jurídico en aquello que le afecte, está regulado esencialmente por las siguientes disposiciones:

a) Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.
b) Ley 40/2007 de 4 de diciembre, de medidas en materia de Seguridad Social.
c) Ley 27/2011, de 1 de agosto, sobre actualización, adecuación y modernización del Sistema de la Seguridad Social.

d) Real Decreto 903/2018, de 20 de julio, por el que se desarrolla la estructura orgánica del Ministerio de Trabajo, Migraciones y Seguridad Social.
e) Orden TMS/722/2018, de 5 de julio, por la que se delegan y se aprueban delegaciones del ejercicio de competencias en determinados órganos administrativos del Ministerio de Trabajo, Migraciones y Seguridad Social y sus organismos públicos.

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

a) 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 en relación a este ámbito sea aprobada a nivel nacional.
b) Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
c) Ley 59/2003, de 19 de diciembre, de firma electrónica.
d) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
e) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
f) 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.
g) Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
h) Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social para la realización de trámites y actuaciones por medios electrónicos.
i) Orden TIN 1459/2010, de 28 de mayo, por la que se crea la Sede Electrónica de la Secretaría de Estado de la Seguridad Social.
j) Orden ESS/1222/2015, de 22 de junio, por la que se regula el tablón de anuncios de la Seguridad Social.
k) Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.
l) Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la política de seguridad de los sistemas de información del Ministerio de Empleo y Seguridad Social.
m) Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social.
n) Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social.
o) Orden ESS/485/2013, de 26 de marzo, por la que se regulan las notificaciones y comunicaciones por medios electrónicos en el ámbito de la Seguridad Social.

II Estructura organizativa.

La estructura organizativa de la gestión de la seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social 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 el titular de la Secretaría de Estado de la Seguridad Social 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 de los que son responsables los titulares de los mismos.

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

1. Hacer cumplir las disposiciones establecidas en el Esquema Nacional de Seguridad 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 VII 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 Trabajo, Migraciones y Seguridad Social, en nombre de la Secretaría de Estado de la Seguridad Social.

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, 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 Trabajo, Migraciones y Seguridad Social.

II. 3. Responsables de los sistemas de información.

Los responsables de los sistemas de información garantizan que se ponen en marcha, 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 los titulares de todos los organismos adscritos y órganos dependientes de la Secretaría de Estado de la Seguridad Social.

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 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, 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 los 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 el 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 los derechos de los titulares de los datos.
- Registrar la condición que legitima el tratamiento.
- Atender los derechos de información, ARCO, olvido y portabilidad.
- Comunicar previamente al Delegado de Protección de Datos los nuevos tratamientos de alto riesgo.
- Limitar los tratamientos en función del consentimiento del titular del dato.
- Realizar la evaluación de impacto en la privacidad.

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 los 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 éstas puedan delegar ciertas funciones en las direcciones y subdirecciones provinciales correspondientes. Es también responsable de los servicios el 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 éste 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 Esquema Nacional de Seguridad.

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, 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, etc. En caso de conflicto, prevalecerá la postura del DPD en materia de tratamientos de datos personales.

II. 9. Encargado del tratamiento.

El encargado del tratamiento es quién, con el previo consentimiento del titular, realiza el tratamiento de los datos de carácter personal y aplica controles de seguridad en los mismos.

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 Esquema Nacional de Seguridad.

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. Normativa de seguridad.

La presente 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 esta normativa se estructura en los siguientes niveles:

1. La política de seguridad. Establece la estrategia general de seguridad y se define en el presente 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 determinada 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.

V. Responsabilidad del personal.

Todo el personal que forme parte de la Secretaria de Estado de la Seguridad Social 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.

VI. Relación con otras administraciones públicas.

Cuando la Secretaría de Estado de la Seguridad Social 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.

VII. Resolución de conflictos.

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

VIII. Formación y concienciación.

La Secretaría de Estado de la Seguridad Social desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de la presente 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 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.

IX. 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 Comité de Seguridad de los Sistemas de Información de la Seguridad Social 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.