MINISTERIO
DE EMPLEO
Y SEGURIDAD SOCIAL

ORDEN 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.

El Ministerio de Empleo y Seguridad Social apoya su actividad en los sistemas de información (en adelante SSII) para alcanzar sus objetivos. Estos SSII deben ser administrados con diligencia, tomando las medidas de seguridad adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar: a la autenticidad o aseguramiento de la identidad u origen, a la confidencialidad de la información que asegura que ésta no es conocida por individuos, entidades o procesos no autorizados, a la integridad o garantía de la exactitud y completitud de la información y de los métodos para su procesamiento, a la disponibilidad de la información que permite a las personas o procesos autorizados acceder a ella cuando se requiera de acuerdo a los requisitos establecidos, y a la trazabilidad o aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

El objetivo de la seguridad es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para ello se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la calidad de la información y la prestación continua de los servicios.

Normativamente ya en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se menciona el impulso al uso de medios electrónicos para el desarrollo de su actividad y el ejercicio de sus competencias y también determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones electrónicas.

Ya la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y posteriormente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre, ponen de relieve que el uso de medios electrónicos conlleva unas necesidades de seguridad especifica de estos medios traducidas en una serie de medidas concretas aplicables a cualquier sistema de información (en adelante SI) que trate datos de carácter personal.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos consagra el derecho de los ciudadanos a comunicarse electrónicamente con la Administración Pública, dando respuesta también a los compromisos comunitarios y a las iniciativas europeas puestas en marcha a partir de Consejo Europeo de Lisboa. Esta Ley manifiesta la necesidad de una adecuada protección de la información y de los servicios que permita usar los medios electrónicos con confianza.

El Esquema Nacional de Seguridad, en adelante ENS, creado por 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, persigue fundamentar la confianza en que los SSII prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Esto implica que deben aplicarse, al menos, las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. El ENS en su artículo 11 dispone que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

Una política de seguridad establece las orientaciones o directrices que rigen la actuación de una persona o entidad en relación a la seguridad de los SSII, entendiendo que SI es cualquier conjunto de elementos (físicos, lógicos, comunicación, datos, procedimientos y personal) que permiten el almacenamiento, transmisión y proceso de la información.

El Departamento debe cerciorarse de que la seguridad es una parte integral de cada etapa del ciclo de vida de cada SI, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Además debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

Esta orden ministerial crea la política de seguridad de los sistemas de información del Ministerio de Empleo y Seguridad Social, con el fin de proteger adecuadamente todos los SSII del Departamento y dar cumplimiento a lo establecido para la política de seguridad 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.

En su virtud,

Dispongo:

Artículo 1. *Objetivo y ámbito de aplicación.*

Esta Orden tiene por objeto aprobar la política de seguridad que proteja adecuadamente todos los SSII del Ministerio de Empleo y Seguridad Social y garantice que prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Los SSII deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, uso previsto y valor de la información y los servicios.

La política de Seguridad de los Sistemas de Información que se aprueba por esta orden será de obligado cumplimiento para todas las Unidades, Organismos Autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Empleo y Seguridad Social.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Empleo y Seguridad Social la propuesta y ejecución de la política del Gobierno en materia de empleo y de Seguridad Social, así como el

desarrollo de la política del Gobierno en materia de extranjería, inmigración y emigración, de acuerdo con lo establecido en el Real Decreto 343/2012, de 10 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Empleo y Seguridad Social.

Artículo 3. *Marco normativo*

El marco normativo en que se desarrollan las actividades del Ministerio de Empleo y Seguridad Social y, en particular, la prestación de sus servicios electrónicos a los ciudadanos, está integrado fundamentalmente por las siguientes disposiciones.

a) La legislación sectorial que sea de aplicación a sus órganos superiores y directivos, así como el Real Decreto 343/2012, de 10 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Empleo y Seguridad Social.
b) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
c) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
d) 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.
e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
f) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo.
g) Ley 59/2003, de 19 de diciembre, de firma electrónica.
h) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
i) 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 (hoy Ministerio de Empleo y Seguridad Social).

Artículo 4. *Responsables de los sistemas de información.*

Los órganos superiores y directivos del Departamento son los responsables de los SSII, fijan sus objetivos y dan soporte a las unidades administrativas que están a su cargo.

Artículo 5. *Dirección, gestión y coordinación de la seguridad de los sistemas de información*

Corresponde al Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante TIC) del Ministerio de Empleo y Seguridad Social, creado mediante la Orden TIN/3016/2011, de 28 de octubre, el establecimiento, gestión, coordinación y aprobación de las actuaciones en materia de seguridad de las tecnologías de la información y las comunicaciones, incluyendo dentro del ámbito de actuación del mismo a todos los SSII del Ministerio de Empleo y Seguridad Social, de manera que se gestione de forma conjunta la seguridad de dichos sistemas. Este Comité es el encargado de revisar anualmente, y en su caso, modificar, la presente política de seguridad

Cada SI tiene un responsable que garantiza que se ponen en marcha, mantienen y actualizan las medidas pertinentes en materia de seguridad de los SSII atendiendo a lo dispuesto por el Comité de Seguridad de las TIC del Ministerio de Empleo y Seguridad Social..

Artículo 6. *Deberes del responsable del sistema de información.*

El responsable de cada SI:

1. Garantizará que se gestiona el riesgo de sus SSII, definiendo para cada uno de ellos su nivel de riesgo residual aceptable, es decir, el riesgo remanente en el SI tras la implantación de las medidas de seguridad establecidas en el plan de seguridad asociado.

El análisis y la gestión del riesgo de cada uno de los SSII deberá actualizarse al menos cada dos años o bien cuando el SI cambie substancialmente.

2. Si un SI maneja ficheros de datos de carácter personal tal y como se definen en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, deberá además hacer cumplir para dicho SI lo dispuesto en la mencionada ley orgánica y su normativa de desarrollo. Se considera responsable de los ficheros de datos de carácter personal tratados por el SI al responsable del sistema de información.

3. Si el SI se encuentra dentro del ámbito de aplicación 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, deberá además hacer cumplir lo dispuesto en el mencionado Real Decreto.

4. Atendiendo a lo establecido en el artículo 10 del Real Decreto 3/2010, de 8 de enero, que regula el ENS, designará los siguientes responsables: responsable de la información, responsable del servicio, responsable de seguridad y responsable de la prestación de los servicios. El responsable de la información y el responsable del servicio pueden estar unificados, pero el responsable de seguridad y el responsable de la prestación de los servicios nunca se pueden unificar.

5. Resolverá los conflictos que puedan surgir entre los distintos responsables en el ejercicio de sus funciones.

6. Adoptará las medidas necesarias para que el personal con acceso a un SI conozca las normas de seguridad que debe aplicar.

7. Establecerá con carácter anual un programa de concienciación y formación en materia de seguridad para todo su personal. Será obligatoria esta formación antes de ejercer un nuevo trabajo o cuando se produzcan cambios substanciales en el mismo

Artículo 7. *Responsable de información*

El Responsable de información determinará los requisitos de seguridad de la información tratada.

Deberá generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

Artículo 8. *Responsable del servicio.*

El Responsable de servicios determinará los requisitos de seguridad de los servicios prestados.

Deberá generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

Artículo 9. *Responsable de seguridad.*

El responsable de seguridad determinará las medidas necesarias para satisfacer los requisitos de seguridad de la información y de los servicios que permitan asegurar el nivel de riesgo residual aceptable aprobado para el SI. Estas medidas se materializarán en un conjunto de normas y proyectos que conformarán el Plan de Seguridad.

Realizará periódicamente auditorías del SI que garanticen la correcta aplicación de las normas y medidas del plan de seguridad. Como resultado de estas auditorías se obtendrá un informe que deberá ser remitido al responsable del sistema de información y al responsable de la prestación del servicio, debiendo subsanarse las deficiencias que pudieran haberse encontrado.

Redactará las Declaraciones de Aplicabilidad pertinentes del Sistema de Información.

Deberá generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

Artículo 10. *Responsable* de la prestación de los servicios.

El Responsable de la prestación de los servicios implementará las normas y proyectos incluidos en el Plan de Seguridad, en relación a su ámbito de competencias.

Deberá generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

Artículo 11. Normativa de seguridad

La normativa de seguridad se estructura en cuatro niveles, siendo de obligatoria aplicación los tres primeros, de la siguiente manera:

1. Primer nivel: La política de seguridad.
2. Segundo nivel: Las normas de seguridad. Conjunto de documentos que sirven para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito. Deberán:

a) Centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Las normas ayudan a tomar la decisión correcta en caso de duda.

b) Describir lo que se considera uso correcto, así como lo que se considera uso incorrecto.

c) Cada norma debe indicar la forma de localizar los procedimientos de seguridad que se han desarrollado en la materia tratada.

d) Ser concisas, motivadas, descriptivas y definir puntos de contacto para su interpretación correcta.

e) Cómo actuar ante situaciones anómalas y no previstas.

f) Describir la responsabilidad del personal con respecto al cumplimiento o violación de cada norma: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3. Tercer nivel: Los procedimientos de seguridad. Conjunto de documentos que describen explícitamente y paso a paso cómo realizar una cierta actividad. Cada procedimiento debe detallar:

a) En qué condiciones debe aplicarse.

b) Quiénes son los que deben llevarlo a cabo.

c) Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada.

d) Cómo se miden sus resultados.

e) Cómo se reportan posibles mejoras y deficiencias en los procedimientos.

4. Cuarto nivel: documentación de buenas prácticas, recomendaciones, etc.

Artículo 12. *Responsabilidad del personal.*

Todo el personal de los diferentes órganos deberá conocer y aplicar, en su ámbito de actuación, las normas de seguridad del SI al que tenga acceso. Estas normas les serán proporcionadas por el responsable del sistema de información.

Artículo 13. *Relación con otras Administraciones Públicas*

Cuando el Departamento preste servicios o ceda información a otras Administraciones Públicas, se les hará participes 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.

Cuando algún aspecto de la política de seguridad o de las normas de seguridad no pueda ser satisfecho por la otra Administración Pública, se requerirá la aprobación previa del responsable del sistema de información al que pertenezcan los servicios prestados o la información cedida, previo informe del responsable de seguridad del sistema de información que precise los riesgos en que se incurre.

Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Disposición adicional única. *Plazo de aplicación.*

Esta política de seguridad deberá estar aplicada completamente en el plazo de dos años a partir de su fecha de entrada en vigor.

Disposición final única. *Entrada en vigor*

La presente Orden entrará en vigor el día siguiente al de su publicación en la sede electrónica del Ministerio de Empleo y Seguridad Social.

Madrid, a 30 de julio de 2012

LA MINISTRA DE EMPLEO Y SEGURIDAD SOCIAL

Fátima Báñez García