Orden PRE / 2011, de 16 de septiembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración electrónica del Ministerio de la Presidencia.

El desarrollo de la Administración electrónica implica el tratamiento automatizado de gran cantidad de información, así como el almacenamiento de la misma, por parte de sistemas de tecnologías de la información y de las comunicaciones.

Estos sistemas se encuentran sometidos a diferentes tipos de amenazas y vulnerabilidades que pueden poner en peligro la información por ellos manejada. En el contexto de la Administración electrónica se entiende por seguridad la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

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, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Para ello, el Real Decreto 3/2010, de 8 de enero, enuncia, en sus artículos 5 a 10, los principios básicos en materia de seguridad de la información (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) y establece el marco regulatorio de la Política de Seguridad de la Información (en adelante PSI).

La PSI, según el Real Decreto 3/2010, de 8 de enero, es el documento que define lo que significa seguridad de la información en una organización determinada, rige la forma en que dicha organización gestiona y protege la información y los servicios que considera críticos y debe plasmarse en un documento, accesible y comprensible para todos los miembros de la organización.

El mismo real decreto regulador del ENS dispone que:

1. "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" (artículo 11)

2. "La política de seguridad... deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa" (artículo 12)

3. "La Política de Seguridad… se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

(Anexo 11.3 Política de Seguridad [org.1].

Además, el Real Decreto 3/2010 establece que la PSI debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

Para la elaboración de la PSI el Real Decreto 3/2010 prevé la utilización de las recomendaciones elaboradas por el Centro Criptológico Nacional (en adelante CCN) del Centro Nacional de Inteligencia (en adelante CNI), que establecen las pautas de carácter general relativas a la organización de seguridad y sus responsables, así como sobre la estructura y contenido mínimo de la PSI y que se contienen en los documentos sobre "Seguridad en las Tecnologías de la Información y las Comunicaciones" (en adelante STIC) conocidas como guías CCN-STIC 001, 201, 402, 801 y 805.

Esta orden ha sido informada por el CCN dependiente del CNI del Ministerio de Defensa.

En su virtud, dispongo:

Artículo 1. Objeto y ámbito de aplicación.

l. Constituye el objeto de la presente orden la aprobación de la política de seguridad de la información (en adelante, PSI) en el ámbito de la Administración electrónica del Ministerio de la Presidencia, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La PSI que se aprueba por esta orden se aplicará con carácter imperativo por todos los órganos superiores y directivos del Ministerio de la Presidencia, siendo de aplicación a todos sus sistemas de información y debiendo ser observada por todo el personal destinado en dichos órganos, así como por aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso a sus sistemas de información o a la información gestionada por ellos.

Artículo 2. Misión del Departamento.

Corresponde al Ministerio de la Presidencia la coordinación de los asuntos de relevancia constitucional, la preparación, desarrollo y seguimiento del programa legislativo del Gobierno, el apoyo inmediato a la Presidencia del Gobierno, la asistencia al Consejo de Ministros, a las Comisiones Delegadas del Gobierno, a la Comisión General de Secretarios de Estado y Subsecretarios y, en particular, al Gobierno en sus relaciones con las Cortes Generales.

Es misión asimismo del Ministerio de la Presidencia la coordinación de la política informativa del Gobierno, la elaboración de los criterios para su determinación y la organización de la cobertura informativa de la actividad gubernamental.

Artículo 3. Marco normativo.

1. El marco normativo en que se desarrollan las actividades del Ministerio de la Presidencia y, en particular, la prestación de sus servicios electrónicos a los ciudadanos, está integrado fundamentalmente por las siguientes normas:

a) La legislación sectorial que sea de aplicación a sus órganos superiores y directivos, así como el Real Decreto 392/2011, de 18 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia.
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 lnteroperabilidad en el ámbito de la Administración electrónica.
f) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
g) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 1511999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
h) Ley 59/2003, de 19 de diciembre, de firma electrónica.
i) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
j) Orden PRE/1010/2010, de 23 de abril, por la que se crea la Sede Electrónica del Ministerio de la Presidencia.
k) Orden PRE/1009/2010, de 23 de abril, por la que se regula el Registro Electrónico del Ministerio de la Presidencia.

Forman parte asimismo del marco normativo las restantes normas aplicables a la Administración electrónica del Departamento derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la PSI.

Artículo 4. Estructura organizativa de la PSI.

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la Administración electrónica del Ministerio de la Presidencia está compuesta por los siguientes agentes:

a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.
b) El Responsable de Seguridad.
c) El Responsable de la Información.
d) El Responsable del Servicio.

Artículo 5. El Comité para la Gestión y Coordinación de la Seguridad de la Información.

1. Se crea el Comité para la Gestión y Coordinación de la Seguridad de la Información (en adelante, el Comité), que coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI, que serán aprobadas por el titular del órgano superior competente.
b) Establecer la normativa de seguridad derivada de segundo nivel que, materializada en instrucciones o resoluciones de los titulares de los órganos correspondientes, sea de obligado cumplimiento: procedimientos de STIC, normas STIC e instrucciones técnicas STIC.
c) Acordar el procedimiento de control de accesos a la red y a las bases de datos de la Administración electrónica del Ministerio la Presidencia, así como los demás procedimientos de actuación en lo relativo al uso de los sistemas de información.
d) Fijar las condiciones para satisfacer los requisitos de seguridad de la información y de los servicios.
e) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.
f) Informar sobre el estado de las principales variables de seguridad en los sistemas de información al Comité de Seguridad de la Información de las Administraciones Públicas para la elaboración de un perfil general del estado de seguridad de las mismas.
g) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

2. El Comité estará compuesto por los siguientes miembros:

a) Presidencia: corresponderá a la persona titular de la Dirección General de Recursos Humanos, Servicios e Infraestructuras.
b) Vicepresidencia: corresponderá a la persona titular de la Subdirección General de Tecnologías y Servicios de información.
c) Vocalías: serán ocupadas por personas pertenecientes a los siguientes órganos del Departamento:

1. Gabinete del Ministro
2. Secretaría de Estado de Asuntos Constitucionales y Parlamentarios
3. Secretaría de Estado de Comunicación
4. Subsecretaría
5. Dirección General de Recursos Humanos, Servicios e Infraestructuras
6. Subdirección General de Tecnologías y Servicios de Información

Quienes ocupen los puestos de vocalía serán designados por la persona titular del órgano correspondiente entre funcionarios que ocupen puestos con categoría mínima de subdirector general o asimilado, pudiendo designar un suplente con el mismo nivel que el titular.

d) Secretaría: la persona titular de la Jefatura de Área de Seguridad y Procedimientos, de la Subdirección General de Tecnologías y Servicios de Información, que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar. Tendrá voz pero no voto.

3. El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones.

Artículo 6. El Responsable de Seguridad.

1**.** Las funciones del Responsable de Seguridad se ejercerán por el grupo técnico de seguridad de la información coordinado por la persona titular de la Subdirección General de Tecnologías y Servicios de Información y estará compuesto por los siguientes miembros:

a) Un funcionario designado por la persona titular de la Subdirección General de Tecnologías y Servicios de Información
b) Un funcionario designado por la persona titular de la Subdirección General de Gestión Económica.
c) Un funcionario designado por la persona titular de la Subdirección General de Recursos Humanos.

2. Serán funciones del responsable de seguridad, las siguientes:

a) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
c) Monitorizar el estado de seguridad del sistema de información.
d) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
e) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
f) Elaborar informes periódicos de seguridad para el Comité que incluyan los incidentes más relevantes de cada periodo.

3. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el responsable de seguridad podrá designar los responsables de seguridad delegados que considere necesarios, que tendrán dependencia funcional directa del responsable de seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Artículo 7. El Responsable de la Información.

1. El Responsable de la Información es la persona que determina los niveles de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, previa propuesta del responsable de seguridad.

2. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

3. El Anexo I identifica los responsables de la información de los sistemas de administración electrónica del Ministerio de la Presidencia y será actualizado por el Comité para la Gestión y Coordinación de la Seguridad de la Información cuando se produzcan variaciones en dichos sistemas.

Artículo 8.El Responsable del Servicio.

1. El Responsable del Servicio es la persona que determina los niveles de seguridad de los servicios dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, previa propuesta del responsable de seguridad.

2. Esta responsabilidad recaerá en la persona titular de la Subdirección General de Tecnologías y Servicios de Información, como titular de la unidad responsable del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.

3. Las funciones del responsable del servicio serán las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así como aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
c) Realizar el preceptivo proceso de análisis y gestión de riesgos del sistema.
d) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse según lo descrito en el Anexo II del mismo.
e) Establecer planes de contingencia y emergencia.
f) Suspender, previo acuerdo con los responsables de seguridad y de la información, el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad.

Artículo 9. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. Si este criterio no fuese suficiente, prevalecerá la decisión del Responsable de Seguridad.

Artículo 10. Gestión de riesgos.

1. 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 (artículo *6* Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 Real Decreto 3/2010, de 8 de enero), siendo el responsable del servicio el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

2. El Responsable de Seguridad es el encargado de que el análisis se realice en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento de los responsables de la información y del servicio.

3. Los responsables de la información y del servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su monitorización, sin perjuicio de la posibilidad de delegar esta tarea.

4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionadas a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el responsable de la información correspondiente, a través de un Plan de Adecuación al ENS.

5. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el CCN.

6. En particular, para realizar el análisis de riesgos se podrá utilizar herramientas homologadas por el CCN que facilitan el seguimiento de la aplicación de las medidas de seguridad seleccionadas y proporciona un valor de riesgo residual estabilizado y comparable entre diferentes sistemas de información.

Artículo 11. Desarrollo normativo.

1. El cuerpo normativo sobre seguridad de la información se desarrollará en cuatro niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: PSI. Está constituido por la presente orden y es de obligado cumplimiento.
b) Segundo nivel normativo: Normativa y recomendaciones de seguridad. Está constituido por la normativa y recomendaciones de seguridad que se definan en cada ámbito organizativo de aplicación específico (órganos superiores y directivos).
La normativa, que comprende los procedimientos STIC, las normas STIC y las Instrucciones Técnicas STIC, es de obligado cumplimiento y se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, previa aprobación del Comité, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.
c) Tercer nivel normativo: Procedimientos técnicos (Guías STIC). Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en Instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo.
La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel normativo las guías CCN-STIC.
d) Cuarto nivel normativo: Informes, registros y evidencias electrónicas. Está constituido por los informes técnicos, (documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación), registros de actividad (o alertas de seguridad, documentos de carácter técnico que recogen amenazas a y vulnerabilidades de sistemas de información y son responsabilidad del responsable de seguridad), y evidencias electrónicas (generadas 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).

2. El Comité establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

Artículo 12. Protección de datos de carácter personal.

1. Respecto a la protección de datos de carácter personal, el responsable de la información asumirá las funciones de responsable del fichero y el responsable de los servicios las del responsable del tratamiento.

2. En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 13. Formación y concienciación.

1. Con la colaboración, en su caso, del CCN, se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento, así como la difusión entre los mismos de la PSI y de su desarrollo normativo.

2. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ministerio de la Presidencia.

Artículo 14. Actualización permanente y revisiones periódicas de la PSI.

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

2. Las propuestas de las sucesivas revisiones de la PSI se elaborarán por el Comité y serán aprobadas por la Subsecretaria del Ministerio de la Presidencia, produciendo efectos a partir de su publicación en la sede electrónica del Departamento.

Disposición adicional única. No incremento del gasto público.

La aplicación de esta orden no conllevará incremento de gasto público, atendiéndose el funcionamiento del Comité con los recursos humanos y materiales de que dispone el Ministerio de la Presidencia.

Disposición final primera. Deber de colaboración en la implantación de la PSI.

Todos los órganos y unidades del departamento prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición final segunda. Publicidad de la PSI.

La presente orden se publicará en la sede electrónica del Ministerio de la Presidencia.

Disposición final tercera. Aplicabilidad.

La PSI que se aprueba por esta orden será aplicable a partir del día siguiente al de su publicación en la sede electrónica del Ministerio de la Presidencia.

Madrid, 16 de septiembre de 2011
El Ministro de la Presidencia

Ramón Jáuregui Atondo

Anexo I

Órganos responsables de la información de los sistemas de Administración Electrónica del Ministerio de la Presidencia

Agenda de Comunicación	Dirección General de Coordinación Informativa.
Acredita	Dirección General de Información Nacional.
Cortesi@	Dirección General de Relaciones con las Cortes.
Registro Electrónico	Dirección General de Recursos Humanos, Servicios e Infraestructuras.
Recursos y Peticiones	Secretaría General Técnica.
Subvenciones	Dirección General Recursos Humanos, Servicios e Infraestructuras.
Certificaciones y Cursos	Dirección General del Centro de Estudios Políticos y Constitucionales y Dirección General del Centro de Investigaciones Sociológicas, cada uno en el ámbito de sus respectivas competencias