RESOLUCIÓN DE 8 DE JULIO DE 2014, de la Presidencia del CSIC, por la que se aprueba la política de seguridad de la información de la Agencia Estatal Consejo Superior de Investigaciones Científicas.

Todos los órganos superiores de las Administraciones Públicas deben disponer formalmente de su política de seguridad de la información, que habrá de ser aprobada por su titular. Esta obligación, que la Agencia Estatal Consejo Superior de Investigaciones Científicas (en adelante, CSIC) debía haber tenido cumplida desde el 30 enero de 2011, viene determinada por el Real Decreto 3/2010, de 8 de enero, por el que se desarrolla la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los Servicios Públicos, por lo que la Institución no puede demorar más la aprobación de su política de seguridad de la información.

La Ley 11/2007, de 22 de junio, consagra el derecho de los ciudadanos a comunicarse con las Administraciones Públicas por medios telemáticos, lo que entraña la correlativa obligación para las Administraciones de crear las condiciones de confianza en el uso de dichos medios, estableciendo las medidas que garanticen la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

El artículo 42.2 de la Ley 11/2007, de 22 de junio, crea el Esquema Nacional de Seguridad (ENS), con el objeto de establecer los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

En cumplimiento de esta Ley, el Real Decreto 3/2010, de 8 de enero, reguló el ENS con el fin de crear las condiciones de confianza que garanticen la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos; así como aquellas en las que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con las correspondientes especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

El Real Decreto 3/2010, de 8 de enero, enuncia los principios básicos (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) que las organizaciones administrativas han de considerar en la elaboración de la Política de Seguridad, desarrollos normativos que de ella derivan y, en general, en la toma de decisiones en materia de seguridad de la información. Establece asimismo el marco regulatorio de la Política de Seguridad de la Información (PSI) que cada organización deberá definir y plasmar en un documento accesible y comprensible para todos sus miembros, que plasmará lo que supone la seguridad de la información en la organización y regirá la forma en que ésta gestiona y protege la información y los servicios que considera críticos.

El Real Decreto 3/2010, de 8 de enero, establece 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, tal y como ya se ha señalado anteriormente.

La seguridad deberá comprometer a todos los miembros de la organización. Para el proceso de su implantación es necesario que la política de seguridad identifique unos claros responsables que velen por su cumplimiento y que su conocimiento llegue a todos los miembros de la organización administrativa.

El contenido mínimo de la PSI debe precisar de forma clara la misión u objetivos de la organización, el marco normativo, la organización de la seguridad, con la definición de los comités y roles unipersonales e identificación de funciones, responsabilidades, mecanismos de coordinación y procedimientos de designación de personas, así como los mecanismos de concienciación y formación y el plan de actuación para la gestión de riesgos.

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 el 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.

En la elaboración de la PSI son una referencia las guías CCN-STIC, principalmente CCN-STIC 001, 201, 402, 801 y 805 elaboradas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), que establecen las pautas de carácter general relativas a la organización de seguridad y sus responsables, así como las relativas a la estructura y contenido mínimo de la PSI.

En consecuencia, de conformidad con los artículos 10.1 y 11.2 del Estatuto de la Agencia Estatal CSIC aprobado por Real Decreto 1730/2007, de 21 de diciembre, dispongo:

PRIMERO.- APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA ESTATAL CSIC.

Se aprueba la Política de Seguridad de la Información de la Agencia Estatal CSIC que se incorpora como Anexo de esta Resolución y que se seguirá por todos sus órganos y unidades y se aplicará a todos los datos, informaciones, sistemas de información y servicios electrónicos utilizados; debiendo ser cumplida por todo el personal destinado en dichos órganos y unidades, así como por el de otros organismos, empresas o entidades que en virtud de norma legal, acuerdo, contrato o convenio tenga acceso a los sistemas de información de esta Agencia Estatal.

DISPOSICIÓN ADICIONAL ÚNICA.- DESARROLLO NORMATIVO.

Se autoriza al titular de la Secretaría General para que dicte cuantas Instrucciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Norma.

DISPOSICIÓN DEROGATORIA ÚNICA.-

Quedan derogadas cuantas normas de igual o inferior rango se opongan a la presente Resolución.

DISPOSICIÓN FINAL ÚNICA.- ENTRADA EN VIGOR.

Esta Resolución entrará en vigor el día siguiente al de su firma.

ANEXO

Política de seguridad de la información de la Agencia Estatal CSIC

1. Objetivo, alcance y principios estratégicos

1.1 La Política de Seguridad de la Información (PSI) tiene como objetivo establecer el marco organizativo, así como los principios básicos y requisitos mínimos en el ámbito de la Administración Electrónica del CSIC.

1.2 Será de aplicación a todos los órganos y unidades del CSIC; a los datos, informaciones y servicios electrónicos utilizados, debiendo ser cumplida por el personal del CSIC y por cualquier otra persona física o jurídica con acceso a dichos datos, informaciones o servicios.

1.3 La Política de Seguridad de la Información es el instrumento en que se apoya la Agencia Estatal CSIC (en adelante, CSIC) para alcanzar sus objetivos, utilizando y gestionando de forma segura los datos, las informaciones y los servicios desarrollados mediante las tecnologías de la información y de las comunicaciones. Esta Política y resto de las normas que de ella se deriven deben velar por la observancia de los siguientes principios estratégicos:

a) Concebir la seguridad como un proceso integral, que comprende los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones; entendiéndose no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado.
b) Considerar la información y los sistemas que la soportan como activos estratégicos del CSIC y habilitar los medios para alcanzar los niveles de protección que garanticen su seguridad.
c) Implantar la cultura de la seguridad en la organización, concienciando sobre la crucial importancia de establecer y cumplir la política de seguridad de la información y normas que de ella se deriven.
d) Abordar y primar los aspectos de prevención, detección y corrección en materia de seguridad de la información para impedir o minimizar la materialización de las amenazas; así como disponer de una estrategia de protección que permita la reacción frente a incidentes.
e) Adoptar la Política de Seguridad de la Información del CSIC como la principal herramienta de garantía de seguridad de la información en la institución, promoviendo y asegurando su cumplimiento por parte de todos sus empleados y colaboradores.

2. Misión y marco normativo del CSIC

2.1 De acuerdo con su Estatuto, aprobado por Real Decreto 1730/2007, de 21 de diciembre, el objeto del CSIC es el fomento, la coordinación, el desarrollo y la difusión de la investigación científica y tecnológica de carácter multidisciplinar, con el fin de contribuir al avance del conocimiento y al desarrollo económico, social y cultural, así como a la formación de personal y al asesoramiento a entidades públicas y privadas en estas materias.

2.2 El marco normativo en que la Agencia desarrolla sus actividades viene dado, esencialmente, por la Ley 28/2006, de 18 de julio, de Agencias Estatales para la mejora de los servicios públicos, dada su condición de Agencia Estatal, por su Estatuto aprobado por Real Decreto 1730/2007, de 21 de diciembre; por la Ley 14/2011, de 1 de junio, de la ciencia, la tecnología y la innovación, en su condición de agencia pública de investigación; y, en general, por cualquier otra norma que pueda resultarle de aplicación en su condición de institución del sector público, y en particular, dado el objeto de esta Resolución por:

a) Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
b) Ley 59/2003, de 19 de diciembre, de firma electrónica.
c) 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) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
g) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.
h) 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.

3. Desarrollo normativo de la Política de Seguridad de la Información

3.1 El Cuerpo Normativo de Seguridad de la Información del CSIC estará integrado por un conjunto de normas, instrucciones, circulares, guías y procedimientos que definirán los mecanismos para garantizar el cumplimiento de la Política de la Seguridad de la Información del CSIC, y que se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel normativo: Política de Seguridad. Está constituido por la Política de Seguridad de la Información recogida en el presente documento y aprobada por Resolución de la Presidencia de la Agencia Estatal CSIC.

b) Segundo nivel normativo: Normas de Seguridad. Desarrolla la Política de Seguridad de la Información mediante normas, instrucciones o circulares específicas que abarcan un área o aspecto determinado de la seguridad de la información y que serán de aplicación en toda la organización, siendo responsable de su aprobación el Comité Corporativo de Seguridad de la Información.

c) Tercer nivel normativo: Procedimientos de Seguridad. Este nivel normativo responde habitualmente al desarrollo del segundo nivel y está constituido por los procedimientos o guías que detallan instrucciones de carácter técnico o procedimental que se deben observar en la realización de tareas o actividades relacionadas con la seguridad y con la protección de

información y servicios. Incluyen aspectos de configuración, implantación y tecnológicos relativos a la seguridad, desarrollo, mantenimiento y explotación de servicios o sistemas de información.

Quedan incluidas en este nivel las Guías del Centro Criptológico Nacional sobre Seguridad de las Tecnologías la Información y la Comunicación (CCN-STIC).

La aprobación de estos procedimientos técnicos corresponde al Responsable de Seguridad.

3.2. Todos los documentos que constituyen el Cuerpo Normativo de Seguridad de la Información del CSIC deben respetar las políticas de las instituciones con las que el CSIC mantenga una relación contractual (entorno de las comunicaciones telemáticas, RedIRIS, redes autonómicas de investigación donde están conectados los diferentes centros e institutos del CSIC, etc.).

3.3 Todas las normas relacionadas con la Política de la Seguridad de la Información, y cualquiera de sus modificaciones deberá aprobarse por el órgano correspondiente antes de su publicación en el BO CSIC y de su distribución; debiendo estar disponibles para todo el personal de la institución.

4. Organización de la seguridad.

4.1 La responsabilidad en materia de Seguridad de la Información recae sobre toda la Organización. Por tanto, cualquier persona que utilice o acceda a información del CSIC es responsable de su protección.

4.2 Se crea una estructura organizativa de gestión de la seguridad de la información con dos niveles:

a) Comités de seguridad de la información,
b) Agentes responsables.

4.3 Los Comités de seguridad de la información serán:

a) El Comité Corporativo de Seguridad de la Información
b) El Grupo Técnico de Seguridad de la Información
c) Los Grupos de Trabajo de Seguridad de la Información

El Comité Corporativo de Seguridad es el órgano decisorio encargado de mantener actualizada y adaptada la Política de Seguridad de la Información en el CSIC para lo que se encargará del análisis y evaluación de los riesgos, de establecer y mantener actualizados los criterios y directrices generales sobre seguridad de la información y de acordar y hacer operativas medidas para mejorar y reforzar los sistemas de seguridad y control.

4.4 Los agentes responsables serán los encargados de la implantación, ejecución, seguimiento y control de las normas aprobadas en materia de seguridad de la información, y actuarán de acuerdo a los siguientes niveles:

a) Nivel de supervisión: Responsable de la Seguridad.

b) Nivel de especificación: Responsable de la Información y Responsable del Servicio.
c) Nivel de gestión y operativo: Responsable del Sistema y Administrador de Seguridad del Sistema.

La Secretaría General determinará la composición, funcionamiento y funciones de la organización de la seguridad en la institución en la Instrucción de desarrollo de dicha estructura organizativa de la seguridad.

5. Resolución de conflictos

5.1 En caso de conflicto entre los diferentes responsables que componen la estructura organizativa, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité Corporativo de Seguridad de la Información.

5.2 En la resolución de las controversias que se pudieran producir prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

6. Gestión de riesgos

6.1 La gestión de riesgos sobre los sistemas de información deberá realizarse de manera continua; contemplando un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos y que proponga tratamientos adecuados.

1.2 El análisis de riesgos se realizará con la siguiente periodicidad:

a) Al menos una vez cada dos años.
b) Cuando cambie la naturaleza de la información manejada.
c) Cuando cambien los servicios prestados.
d) Cuando ocurra un incidente grave de seguridad.
e) Cuando se reporten vulnerabilidades graves.

6.3 Para realizar el análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el conjunto de las Administraciones Públicas y en especial, las guías elaboradas por el Centro Criptológico Nacional.

7. Obligaciones del personal

7.1 Todos los miembros del CSIC tienen la obligación de conocer y cumplir las directrices de la Política de Seguridad de la Información, así como el conjunto de normas, instrucciones, circulares, procedimientos y guías que integren el Cuerpo Normativo de Seguridad. Con el fin de promover su difusión y facilitar su conocimiento se diseñará un programa de formación, concienciación y comunicación para todo el personal, que desarrollará los distintos aspectos que incumben a la seguridad de la información.

7.2 Todo el personal que se incorpore a la Agencia Estatal CSIC o vaya a tener acceso a alguno de sus sistemas de información o a la información deberá ser informado y deberá cumplir la Política de Seguridad de la Información y la normativa de seguridad derivada.

7.3 El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa de seguridad derivada podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades contractuales y legales correspondientes.

8. Terceras partes

8.1 Cuando el CSIC preste servicios o maneje información de otros organismos, les hará partícipes de su Política de Seguridad de la Información. Se establecerán asimismo canales para facilitar la comunicación y coordinación de los respectivos Comités de Seguridad de la Información y se habilitarán procedimientos de actuación ante incidentes de seguridad.

8.2 Cuando el CSIC utilice servicios de terceros o ceda información a terceros, se les hará partícipes de la Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Estas terceras partes quedarán sujetas a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal implicado está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

8.3 Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se precisará la aprobación expresa de los responsables de la información y de los servicios afectados antes de realizar cualquier tipo de actuación.

9. Datos de carácter personal

9.1 Los datos de carácter personal que sean objeto de tratamiento en el ejercicio de las funciones que el CSIC tiene encomendadas deberán protegerse mediante la implantación de las medidas de seguridad correspondientes.

9.2 El Documento de Seguridad a que hace referencia la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que desarrolla el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de dicha Ley, recoge en el caso del CSIC la lista de ficheros afectados, relaciona los responsables correspondientes y establece las medidas de índole técnico y organizativo implantadas para garantizar la seguridad en los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos de carácter personal. El Documento de Seguridad estará disponible en el apartado destinado a este fin en la opción "Servicios TIC" de la Intranet General del CSIC.

9.3 Los ficheros que contengan datos de carácter personal se encontrarán inscritos en la Agencia Española de Protección de Datos (www.agpd.es) de acuerdo con lo dispuesto en la normativa vigente

10. Formación y concienciación

10.1 Con la colaboración, en su caso, del CCN, se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que preste servicios en el CSIC, así como a la difusión entre ellos de la Política de Seguridad de la Información y de su desarrollo normativo.

10.2 A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los planes de formación del CSIC.

10.3 El CSIC promoverá una cultura de la seguridad de la información alineada con la Política de Seguridad de la Información entre aquellas instituciones y usuarios externos que tengan acceso por acuerdo o convenio a los sistemas de información de la Agencia.

11. Actualización y revisión periódica

11.1 La Política de Seguridad de la Información 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.

11.2 El Comité Corporativo de Seguridad de la Información revisará la Política de Seguridad y su oportunidad, idoneidad, completitud y precisión, al menos una vez al año. Asimismo, en caso de considerarlo conveniente, elaborará propuestas de revisión, y, si su contenido es técnico, podrán ser aprobadas por la Secretaría General, produciendo efectos a partir del día siguiente de su publicación en el BO CSIC.

Madrid, a 8 de julio de 2014

El Presidente

Emilio Lora Tamayo D'Ocón

Sres/as Vicepresidentes, Sres/as Vicepresidentes Adjuntos, Sres/as Secretarios Generales Adjuntos, Sres/as Directores de Centros e Institutos, Sres/as Gerentes.

INDICE