Decreto 57/2012, de 23 de febrero, por el que se establece la política de seguridad de la información en la Administración de la Junta de Comunidades de Castilla-La Mancha. (*)

(DOCM 43 de 28-02-2012)

(*) Incorpora corrección de errores publicada en el DOCM 53 de 23-02-2012

La Administración de la Junta de Comunidades de Castilla-La Mancha considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por tanto, la seguridad de la información como una responsabilidad asociada a su protección frente a las amenazas que puedan afectar a su autenticidad, integridad, disponibilidad, confidencialidad o trazabilidad.

Como parte de esa responsabilidad, la Administración de la Junta de Comunidades de Castilla-La Mancha define, a través de este decreto, una política de seguridad de la información con el objetivo de dirigir y dar soporte a la gestión de la seguridad de la información mediante el establecimiento de unas directrices básicas de acuerdo a los requisitos propios de seguridad y a la regulación aplicables.

Con el uso generalizado de las nuevas tecnologías en los servicios que se prestan al ciudadano, la Administración tiene que generar la confianza suficiente para que éste utilice como canal de comunicación principal los medios electrónicos. Es por ello que se considera imprescindible elaborar una norma que defina la política de seguridad en el tratamiento de la información que se maneja para el desempeño de las competencias que tiene asignadas. No se trata, por tanto, de limitarse a regular la seguridad en el ámbito del uso de las tecnologías de la información y las comunicaciones, sino en el tratamiento global de la información.

De este modo, la política de seguridad de la información constituirá el marco bajo el que definir el conjunto de normas reguladoras, procedimientos y prácticas que determinen el modo en que los activos son gestionados, protegidos y distribuidos, manifestando así la Administración regional su apoyo y compromiso con la seguridad de los datos manejados.

Esta política de seguridad de la información está alineada con los objetivos globales de la Administración regional enmarcándose dentro del Plan de Garantías de los Servicios Sociales Básicos, abordando la seguridad de la información como un proceso integral, gestionándola de forma global, lo que proporciona un escenario controlable y de mejora continua, y diferenciándola de la gestión de los servicios prestados. De esta manera se garantizan los principios de eficacia y eficiencia que rigen sus actuaciones.

En base a todo lo anterior esta política define un marco organizativo y operacional que garantiza la confidencialidad, integridad y disponibilidad de la información que integran los servicios que la Administración presta a los ciudadanos, conforme con la normativa vigente en esta materia.

En su virtud, a propuesta del Consejero de Presidencia y Administraciones Públicas, y previa deliberación del Consejo de Gobierno en su reunión del día 23 de febrero de 2012.

Dispongo

Capítulo I
Disposiciones generales

Artículo 1. Objeto.

El presente Decreto tiene por objeto definir la política en materia de seguridad de la información de la Administración Junta de Comunidades de Castilla-La Mancha, así como el establecimiento del marco organizativo y operacional, garantizando a los ciudadanos de Castilla-La Mancha la gestión de sus datos de forma segura y conforme a la legislación vigente en esta materia.

Artículo 2. Ámbito de aplicación.

La política de seguridad de la información que se define mediante este Decreto será de aplicación en la Administración de la Junta de Comunidades de Castilla-La Mancha. A estos efectos, se entiende por Administración de la Junta de Comunidades de Castilla-La Mancha:

a) La Administración regional.
b) Los organismos autónomos adscritos a la Administración regional.
c) El resto de entidades de Derecho Público vinculadas o dependientes, cuando ejerzan potestades administrativas.

Artículo 3. Misión de la Organización.

La Junta de Comunidades de Castilla-La Mancha es la institución en la que se organiza política y jurídicamente el autogobierno de la Región. Sus competencias están recogidas en el título IV del Estatuto de Autonomía de Castilla-La Mancha.

Artículo 4. Marco normativo.

El marco normativo en que se desarrollan las actividades de la Administración de la Junta de Comunidades de Castilla-La Mancha, y, en particular, la prestación de sus servicios electrónicos a los ciudadanos, está integrado por las siguientes normas:

a) Decreto 10/2012, de 25 de enero, por el que se establece la estructura de la Administración Regional.
b) Decreto 123/2011, de 7 de julio, por el que se establece la estructura orgánica y competencias de la Consejería de Sanidad y Asuntos Sociales.
c) Decreto 124/2011, de 7 de julio, por el que se establece la estructura orgánica, organización de funciones y competencias de la Consejería de Educación, Cultura y Deportes.
d) Decreto 125/2011, de 7 de julio, por el que se establecen la estructura orgánica y las competencias de los distintos órganos de la Consejería de Fomento.
e) Decreto 126/2011, de 07/07/2011 por el que se establece la estructura orgánica y las competencias de la Consejería de Agricultura.
f) Decreto 14/2012, de 26 de enero, por el que se modifica el Decreto 279/2011, de 22 de septiembre, por el que se establece la estructura orgánica y se fijan las competencias de los órganos integrados en la Presidencia de la Junta de Comunidades de Castilla-La Mancha.
g) Decreto 15/2012, de 26 de enero, por el que se establece la estructura orgánica y competencias de la Consejería de Hacienda
h) Decreto 16/2012, de 26 de enero, por el que se establece la estructura orgánica y se fijan las competencias de los órganos integrados en la Consejería de Empleo y Economía
i) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
j) 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.
k) 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.
l) 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.
m) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
n) 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.
o) Ley 59/2003, de 19 de diciembre, de firma electrónica.
p) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
q) Decreto 12/2010, de 16 de marzo, por el que se regula la utilización de medios electrónicos en la actividad de la Administración de la Junta de Comunidades de Castilla-La Mancha.

r) Decreto 104/2008, de 22 de julio, de protección de datos de carácter personal en la Junta de Comunidades de Castilla-La Mancha.

Capítulo II
Organización de la seguridad de la información

Artículo 5. Estructura organizativa.

La estructura organizativa de la gestión de la seguridad de la información en la administración de la Junta de Comunidades de Castilla-La Mancha está compuesta por los siguientes agentes:

a) El Comité de Seguridad de la Información.
b) El Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones.
c) El Responsable de la Información.
d) El Responsable del Servicio.
e) El Responsable de Seguridad.
f) El Responsable del Sistema.
g) El Responsable de servicios comunes de las Tecnologías de la Información y las Comunicaciones.

Artículo 6. El Comité de Seguridad de la Información

1. Se crea el Comité de Seguridad de la Información en el seno de la Comisión de la Administración Electrónica y Simplificación de Trámites Administrativos creada por el Decreto 12/2010, de 16/03/2010, por el que se regula la utilización de medios electrónicos en la actividad de la Administración de la Junta de Comunidades de Castilla-La Mancha.

2. El Comité estará formado por las personas miembros de la Comisión de la Administración Electrónica y Simplificación de Trámites Administrativos, elegidas en el seno de la misma.

3. Serán funciones propias del Comité:

a) Velar por el cumplimiento y difusión de la política de seguridad de la información.
b) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad de tecnologías de la información y comunicaciones.
c) Fijar las condiciones para satisfacer los requisitos de seguridad de la información.
d) La aprobación y seguimiento de las normativas en materia de seguridad que serán de obligado cumplimiento.
e) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos de seguridad necesarios.
f) El control de las actuaciones del Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones en lo que a la seguridad de la información se refiere y atribuir o delegar en el mismo las competencias que estime oportuno.
g) Promover la formación y concienciación en materia de seguridad de la información.

4. A las reuniones del Comité de Seguridad de la Información podrá asistir personal técnico si la Presidencia lo considerase oportuno a petición de cualquier miembro del Comité.

Artículo 7. El Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones.

1. Se crea el Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones como órgano colegiado adscrito a la Dirección General competente en materia de seguridad de la información.

2. El Comité estará formado por:

a) La persona titular de la Dirección General competente en materia de seguridad de la información, que lo presidirá
b) Una persona de la Dirección General competente en materia de seguridad de la información, que actuará como secretario, con voz y voto
c) El responsable de seguridad
d) Los responsables de sistemas
e) Si los hubiese, los responsables de la gestión de la seguridad a que se refiere el artículo 10.3
3. El Comité tendrá asignadas las siguientes funciones:

a) Asesorar al Comité de Seguridad de la Información en todo lo que solicite e informarle sobre el estado de la seguridad de cada una de sus unidades.
b) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la política de seguridad de la información y su normativa de desarrollo.
c) Impulsar la elaboración de directrices en materia de seguridad de la información.
d) Crear y determinar la composición, objetivos y funcionamiento de grupos de trabajo así como el ámbito de actuación y el periodo de vigencia de los mismos, dando cuenta de ello al Comité de Seguridad de la Información.

4. A las reuniones del Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones podrá asistir personal técnico si la Presidencia lo considerase oportuno, a petición de cualquier miembro del comité.

5. El Comité Técnico de Seguridad de las Tecnologías de la Información y las Comunicaciones se reunirá, previa convocatoria de la presidencia, siempre que sea necesario para el cumplimiento de sus funciones, o cuando aquella lo considere conveniente por iniciativa propia o a petición de alguno de sus miembros.

Artículo 8. El Responsable de la Información.

1. El responsable de la información tiene la responsabilidad última del uso que se haga de una cierta información y de su protección y se corresponderá con el titular del órgano de la Administración con competencia suficiente para decidir sobre la finalidad, contenido y uso de dicha información.

2. 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 en el ámbito de la Administración Electrónica, tiene la potestad de establecer sus requisitos en materia de seguridad.

Artículo 9. El Responsable del Servicio.

1. El responsable del servicio tiene la responsabilidad última de la prestación de un cierto servicio y de su protección y se corresponderá con el titular del órgano de la Administración con competencia suficiente para decidir sobre la finalidad y prestación de dicho servicio.

2. 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 en el ámbito de la Administración Electrónica, tiene la potestad de establecer sus requisitos en materia de seguridad.

3. El responsable de la información y el responsable del servicio coincidirán cuando la prestación del servicio dependa de la unidad que es responsable de la información o cuando el servicio no maneje información de diferentes procedencias.

Artículo 10. El Responsable de Seguridad.

1. El responsable de seguridad tendrá las siguientes atribuciones:

a) Elaborar las propuestas de modificación y actualización de la política de seguridad de la información en la Junta de Comunidades de Castilla-La Mancha.
b) Coordinar el proceso de gestión de la seguridad.
c) Desarrollar la política de seguridad de la información mediante planes y normativas.
d) La supervisión del cumplimiento de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de la información.
e) Promover las actividades de concienciación y formación en materia de seguridad siguiendo las directrices marcadas por el Comité de Seguridad de la Información.
f) Proponer para su aprobación y seguimiento en el Comité de Seguridad de la Información, los planes estratégicos, planes directores y líneas de actuación en materia de seguridad de la información.
g) Proponer para su aprobación y seguimiento en el Comité de Seguridad de la Información, las políticas de auditoría para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

2. El responsable de seguridad se corresponderá con el titular del servicio responsable de la seguridad de la información.
3. Sin perjuicio de las atribuciones del responsable de seguridad, en cada una de las entidades incluidas en el ámbito de aplicación del presente Decreto podrá designarse un responsable de la gestión de la seguridad en dichas entidades.

Artículo 11. El Responsable del Sistema.

1. El responsable del sistema se corresponderá con el responsable del área informática de cada unidad y tendrá encomendadas, entre otras, las siguientes funciones:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.
d) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

2. Dentro del marco establecido 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, tiene la facultad para determinar la categoría de los sistemas.

Artículo 12. El Responsable de servicios comunes de las Tecnologías de la Información y las Comunicaciones.

Dependiente de la Dirección General competente en materia de servicios e infraestructuras comunes de las tecnologías de la información y las comunicaciones, tiene encomendadas, entre otras, las siguientes funciones:

a) Gestionar y mantener los servicios e infraestructuras comunes a todos los sistemas de información de la Administración regional.
b) Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.
c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Capítulo III

Gestión de la seguridad de la información

Artículo 13. Desarrollo normativo de la seguridad.

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

a) Primer nivel normativo: política de seguridad de la información. Está constituido por el presente Decreto y es de obligado cumplimiento.
b) Segundo nivel normativo: normativa de seguridad de la información. Está constituido por el conjunto de normas que desarrollan la política de seguridad y que regulan qué se puede hacer y qué no, en relación a un cierto tema, desde el punto de vista de la seguridad sin entrar en detalles de implementación ni tecnológicos. Los documentos relativos a este segundo nivel normativo los propone el responsable de seguridad y los aprueba el Comité de Seguridad de la Información.
c) Tercer nivel normativo: procedimientos técnicos. Está constituido por el conjunto de procedimientos técnicos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos en ella establecidos.

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.

Aparte de los documentos citados, la documentación de seguridad podrá contar, con otros documentos como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.
2. El Comité de Seguridad de la Información 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 política de seguridad de la información.

Artículo 14. Protección de datos de carácter personal.

1. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

2. En lo que se refiere a los ficheros con datos de carácter personal, estarán referenciados en el correspondiente documento de seguridad donde se hará constar tanto los ficheros afectados como los responsables correspondientes.

Artículo 15. Gestión de riesgos.

1. La gestión de riesgos es parte esencial del proceso de seguridad y ha de realizase de manera continua sobre los sistemas de información con el objetivo de mantener los entornos controlados minimizando los riesgos hasta niveles aceptables.

2. La gestión de riesgos será preceptiva para los sistemas de información incluidos dentro del marco establecido 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.

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 seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea. Para ello podrán contar en el proceso con la participación y asesoramiento del responsable de seguridad y del responsable del sistema.

4. Para la realización del análisis de riesgos se podrán utilizar las herramientas establecidas para este fin por el servicio responsable de seguridad, que facilitan el seguimiento de la aplicación de las medidas de seguridad seleccionadas y proporcionan un valor de riesgos residual estabilizado y comparable entre diferentes sistemas de información.

Artículo 16. Resolución de conflictos.

En caso de surgir conflictos entre los distintos responsables, esté debe ser resuelto por el superior jerárquico de los mismos si existe, si no existiera debe resolver el Responsable de Seguridad.

Artículo 17. Obligaciones del personal

1. Todo el personal con responsabilidad en el uso, operación o administración de sistemas de tecnologías de la información y las comunicaciones recibirá formación para el manejo seguro de los sistemas. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos, así como la difusión entre los mismos de la política de seguridad de la información y de su desarrollo normativo.

2. Este personal tiene la obligación de cumplir la política de seguridad de la información y la normativa de seguridad derivada. Su incumplimiento podrá ser sancionado de conformidad con la normativa disciplinaria correspondiente.

Disposición adicional primera. Adecuación de las relaciones de puesto de trabajo.

Las relaciones de puestos de trabajo de la Junta de Comunidades de Castilla-La Mancha se adecuarán para dar soporte a la estructura organizativa necesaria para el cumplimiento del presente Decreto.

Disposición adicional segunda. No incremento del gasto público.

La aplicación de este Decreto no conllevará incremento de gasto público, atendiéndose al funcionamiento de los Comités con los recursos humanos y materiales disponibles.

Disposición final primera. Modificación del Decreto 12/2010, de 16 de marzo, por el que se regula la utilización de medios electrónicos en la actividad de la Administración de la Junta de Comunidades de Castilla-La Mancha.
Se modifica el apartado 1 del artículo 44 del Decreto 12/2010, de 16 de marzo, por el que se regula la utilización de medios electrónicos en la actividad de la Administración de la Junta de Comunidades de Castilla-La Mancha, que queda con la siguiente redacción:

“1. Se crea, bajo la dependencia de la Presidencia de la Junta de Comunidades, la Comisión de la Administración Electrónica y Simplificación de Trámites Administrativos, con funciones de coordinación, dirección y control de las actuaciones de la Administración regional en materia de optimización de los procedimientos administrativos e introducción de la gestión administrativa electrónica. Son miembros de esta Comisión las personas titulares de las Secretarías Generales de las Consejerías, de la Intervención General y de las Direcciones Generales competentes en materia de seguridad de la información, administración electrónica y sociedad de la información.”

Disposición final segunda. Habilitación de desarrollo.

Se faculta a las personas titulares de las Consejerías competentes en materia de seguridad de la información y servicios e infraestructuras comunes de las tecnologías de la información y las comunicaciones para el desarrollo de lo dispuesto en el presente Decreto.

Disposición final tercera. Entrada en vigor.

Este Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de Castilla-La Mancha.