I. COMUNIDAD DE CASTILLA Y LEÓN

A. DISPOSICIONES GENERALES

CONSEJERÍA DE HACIENDA

ORDEN HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León.

Uno de los principales compromisos de la Junta de Castilla y León es conseguir que la Administración autonómica proporcione a los ciudadanos una respuesta de calidad y con la máxima eficiencia posible, como reflejo del derecho a una buena Administración, recogido en el artículo 12 de la Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León.

Este derecho tiene su reflejo en la gestión diligente y eficaz de los sistemas de información, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, autenticidad, confidencialidad y trazabilidad de la información tratada o de los servicios prestados. Todas estas medidas deben de ser proporcionales al valor de la información y se ajustarán a la evolución de la tecnología.

Esta política se desarrollará aplicando los principios básicos y los requisitos mínimos recogidos 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. La Ley 2/2010, de 11 de marzo, de Derechos de los Ciudadanos en sus relaciones con la Administración de la Comunidad de Castilla y León y de Gestión Pública se refiere a la protección de datos y a la seguridad en los artículos 45 y 47. Por su parte, el Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León, en su artículo 5 atribuye a la consejería competente para la dirección y ejecución de actuaciones en materia de Administración electrónica, la competencia para la aprobación de la política de seguridad de los sistemas de información de la Administración de la Comunidad de Castilla y León, sin perjuicio de las especialidades del organismo pagador de los gastos financiados por el FEAGA y FEADER que también se recogen en esta orden.

Esta orden establece el compromiso de la Administración de la Comunidad de Castilla y León con la seguridad de los sistemas de la información, define los objetivos y criterios básicos para el tratamiento de la misma y determina la estructura organizativa y de gestión que velará por su cumplimiento.

En su virtud, y de conformidad con lo establecido en el citado artículo 5 y en la disposición final sexta del Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León.

DISPONGO

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. Esta orden tiene por objeto regular la política de seguridad de la información de la Administración de la Comunidad de Castilla y León, así como el establecimiento de su marco organizativo, que se ha de aplicar para la protección de los servicios y activos de información gestionados por medio de las tecnologías de la información y de las comunicaciones.

El objetivo de esta política es garantizar la protección y calidad de la información, así como la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con agilidad ante los incidentes que puedan tener lugar.

Artículo 2. Ámbito subjetivo de aplicación.

La política de seguridad de la información es de aplicación a la Administración de la Comunidad de Castilla y León.

CAPÍTULO II

Estructura organizativa para la gestión de la seguridad de la información de la Administración de la Comunidad de Castilla y León

Artículo 3. Marco organizativo para la gestión de la seguridad de la información de la Administración de la Comunidad de Castilla y León.

El marco organizativo para la gestión de la seguridad de la información en la Administración de la Comunidad de Castilla y León está constituido por:

a) La Consejería de Hacienda, a través de la Dirección General de Atención al Ciudadano, Calidad y Modernización.

b) El Comité de Seguridad de la Información.

c) Los responsables en materia de gestión de la seguridad de la información de las consejerías, de los organismos autónomos y los entes públicos de derecho privado incluidos en el ámbito de aplicación.

d) Los responsables de servicios comunes de las tecnologías de la información y de las comunicaciones.

Artículo 4. Dirección General de Atención al Ciudadano, Calidad y Modernización.

La Dirección General de Atención al Ciudadano, Calidad y Modernización es el órgano directivo central encargado de promover la aplicación efectiva, seguimiento y propuesta de modificación de la política de seguridad de la información. Además, deberá:

e) Dirigir y, en su caso, ejecutar las auditorías en esta materia.

f) Proporcionar las directrices e instrucciones oportunas que faciliten el seguimiento de la implantación de las medidas de seguridad necesarias para garantizar un nivel de protección adecuado a la criticidad de los sistemas de información.

g) Constituirse como interlocutor con el Centro Criptológico Nacional y otros centros nacionales e internacionales de referencia en la utilización de servicios de respuesta a incidentes de seguridad de especial gravedad.

h) Proponer y extender las actuaciones de los diferentes responsables de seguridad, bajo el criterio de garantizar la seguridad de las infraestructuras tecnológicas compartidas.

i) Proponer las actuaciones de formación y concienciación previstas en el artículo 16 de esta orden.

j) Publicar en la sede electrónica, *https://www.tramitacastillayleon.jcyl.es* las declaraciones de conformidad de los sistemas de información remitidas por las consejerías, los organismos autónomos y los entes públicos de derecho privado dependientes de la Administración de la Comunidad Autónoma.

k) Las demás competencias otorgadas en esta materia por la legislación vigente.

Artículo 5. Comité de Seguridad de la Información.

1. El Comité de Seguridad de la Información es el órgano colegiado de seguimiento en esta materia en el ámbito de la Administración de la Comunidad de Castilla y León. Está adscrito a la Consejería de Hacienda y estará formado por:

a) El titular de la Viceconsejería de Función Pública y Modernización que actuará como presidente.

b) El titular de la Dirección General de Atención al Ciudadano, Calidad y Modernización que actuará como ponente.

c) Los titulares de las Secretarías Generales de las consejerías u órgano equivalente de los organismos autónomos y entes públicos de derecho privado o personas en quien deleguen.

d) Un funcionario de la Dirección General de Atención al Ciudadano, Calidad y Modernización, elegido por el presidente, que actuará como secretario, con voz pero sin voto.

2. Serán funciones del Comité de Seguridad de la Información:

a) Informar las propuestas de revisión de la política de seguridad así como ser informado de su seguimiento.

b) Recibir información o proponer, en su caso, la revisión de las actuaciones conjuntas en relación a la seguridad de la información.

c) Impulsar el cumplimiento de la política de seguridad y su desarrollo normativo.

d) Resolver los conflictos entre los diferentes responsables que componen la estructura organizativa para la gestión de la seguridad de la información de la Administración de la Comunidad de Castilla y León en el supuesto previsto en el artículo 12.1 de esta orden.

3. Su funcionamiento se regirá por lo dispuesto en el Capítulo IV del Título V de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León y por la legislación básica estatal.

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

5. Este Comité se reunirá al menos un vez al semestre.

Artículo 6. Estructura organizativa para la gestión de la seguridad de la información dependiente de cada consejería, organismo autónomo o ente público de derecho privado.

1. Las consejerías, organismos autónomos y los entes públicos de derecho privado incluidos en el ámbito de aplicación de esta orden, realizarán un seguimiento continuado de los niveles de prestación de servicio, calidad y seguridad de la información, analizando vulnerabilidades y preparando una respuesta efectiva a los incidentes de seguridad dependiendo del ámbito que les compete, a tal efecto, existirán:

a) Uno o varios responsables de la información y del fichero, según proceda.

b) Uno o varios responsables del servicio y tratamiento, según proceda.

c) Un responsable de seguridad.

d) Un responsable de los sistemas.

2. Un única persona podrá desempeñar las funciones de responsable del servicio y tratamiento y de responsable de la información y del fichero, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad cuando:

a) Los servicios prestados contengan datos de carácter personal.

b) La prestación del servicio dependa de la misma unidad u órgano administrativo que es responsable de la información.

c) La información utilizada para la prestación del servicio proceda de la misma unidad u órgano administrativo que lo presta.

3. Los responsables de seguridad previstos en el Esquema Nacional de Seguridad, y en la Ley Orgánica 15/1999, de 13 de diciembre, podrán coincidir en única figura.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, podrán designarse los responsables de seguridad delegados que se consideren necesarios. Así mismo, por idénticas razones

se podrán designar los responsables de sistemas delegados que consideren para la realización de las actividades relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema.

5. De acuerdo con el principio de función diferenciada, previsto en los artículos 4 f) y 10 del Esquema Nacional de Seguridad, el responsable de seguridad nunca podrá coincidir con el responsable del sistema, ni depender funcionalmente de éste.

Artículo 7. Responsable de la información y del fichero.

El responsable de la información y del fichero es el titular del centro directivo, o persona en quien delegue, con competencia para decidir sobre la finalidad, contenido y uso de dicha información y fichero, a cuyo efecto determinará los requisitos en materia de seguridad de la información que se maneja.

Asimismo, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, establecerá los niveles de seguridad requeridos para la información, efectuando para ello las valoraciones del impacto que tendría un incidente que afectara a dicha información.

Artículo 8. Responsable del servicio y tratamiento.

1. El responsable del servicio es la persona que tiene la competencia de establecer de manera funcional los requisitos de seguridad de los servicios prestados.

2. El responsable del servicio junto con el responsable de la Información serán los encargados de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control.

Artículo 9. Responsable de seguridad.

1. El responsable de seguridad es la persona designada por el titular de la Secretaría General u órgano equivalente en cada organismo o ente que adoptará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios afectados por los sistemas de información gestionados por esa consejería, organismo o entidad.

2. Serán funciones de cada responsable de seguridad, dentro de su ámbito de actuación, las siguientes:

a) Mantener y gestionar la seguridad de la información y de los servicios prestados, en su ámbito de responsabilidad y desarrollar la política de seguridad de la información mediante planes, procedimientos e instrucciones técnicas de seguridad, coordinando el proceso de gestión de la seguridad.

b) Mantener actualizada y disponible dicha documentación y promover las actividades de concienciación y formación en materia de seguridad, siguiendo las directrices marcadas por el Comité de Seguridad.

c) Elaborar informes periódicos de seguridad, conforme a la normativa vigente, para el Comité de Seguridad que incluyan los incidentes más relevantes de cada período, así como cualquier otra documentación de apoyo que el Comité necesite recabar dentro del ámbito de actuación del responsable de seguridad.

d) Supervisar el cumplimiento de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de la información.

e) Promover y proponer auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los responsables del servicio o tratamiento y a los responsables de la información y del fichero para que adopten las medidas correctoras adecuadas.

f) Realizar la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad, y en particular, asesorar, en colaboración con el responsable del sistema, a los responsables de la información y a los responsables del servicio en la realización de los preceptivos análisis de riesgos, y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité de Seguridad de la Información.

g) Ser interlocutor entre su consejería, organismo o ente y la Dirección General de Atención al Ciudadano, Calidad y Modernización para las actuaciones conjuntas en materia de seguridad.

h) Las demás atribuidas por la normativa vigente y, en concreto, las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 10. Responsable de los sistemas.

1. El responsable de los sistemas será el encargado de la supervisión del desarrollo, integración, modificación, operación, mantenimiento y verificación del correcto funcionamiento de los sistemas de información, de acuerdo con los criterios corporativos establecidos.

2. El responsable de los sistemas será el titular de la jefatura del Servicio de Informática o persona de análoga funciones de cada consejería, organismo o entes públicos de derecho privado y, en su caso, quien se determine expresamente en la respectiva estructura orgánica.

3. Sus funciones serán:

a) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del Esquema Nacional de Seguridad y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del citado texto legal.

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) Implantar las medidas seguridad que requieren los servicios durante todo su ciclo de vida, siguiendo las indicaciones del responsable de seguridad. Para ello, deberán aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema y asesorar a los responsables de la información y a los responsables del servicio en la realización de los análisis de riesgos.

d) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo

acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

Artículo 11. Los responsables de servicios comunes de las tecnologías de la información y las comunicaciones.

1. Serán responsables de los servicios comunes de las tecnologías de la información y las comunicaciones los titulares de las unidades administrativas competentes de la Dirección General de Atención al Ciudadano, Calidad y Modernización, según establezca la orden de estructura orgánica.

2. Tendrán encomendados, entre otras las siguientes funciones:

a) Gestionar y mantener los servicios e infraestructuras comunes a todos los sistemas de la Administración Autonómica.

b) Implantar y hacer efectivas las medidas de seguridad que afecten a los servicios e infraestructuras de los que sean responsables, así como de su integración en el marco general de seguridad.

Artículo 12. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa para la gestión de la seguridad de la información, éste será resuelto por su superior jerárquico común. Si no existiera, deberá resolver el Comité de Seguridad de la Información.

2. En caso de conflictos entre los responsables que componen la estructura organizativa de la política de seguridad de la información, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

CAPÍTULO III

Gestión de la seguridad de los sistemas de información

Artículo 13. Obligaciones del personal.

1. Todo el personal con acceso a los sistemas de información de la Administración Autonómica deberá conocer y aplicar, en su ámbito de actuación, la política de seguridad, así como las normas, instrucciones y procedimientos que en materia de seguridad de la información se establezcan.

A tal efecto, la política de seguridad será comunicada a todos los usuarios de los sistemas de información de la Administración Autonómica incluidos en el ámbito de aplicación de esta orden, de manera pertinente, accesible y comprensible.

2. La Consejería de Hacienda, a través de la Dirección General de Atención al Ciudadano, Calidad y Modernización, deberá establecer los procedimientos de control que garanticen el cumplimiento efectivo de esta política que serán efectuados por las consejerías, los organismos autónomos y los entes públicos de derecho privado.

3. El incumplimiento manifiesto de esta política podrá dar lugar a la exigencia de las responsabilidades correspondientes.

Artículo 14. Gestión de Riesgos.

1. La selección de las medidas de seguridad a aplicar a los sistemas de información, deberá ser proporcional a los riesgos. Dichas medidas de seguridad deben estar justificadas, tanto en costes económicos como operativos.

2. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y en todas las fases de su ciclo de vida, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica a que se refiere el Esquema Nacional de Seguridad. El responsable de seguridad realizará una revisión de los estados del riesgo, al menos, una vez al año.

La reducción de los niveles de riesgo se realizará mediante la aplicación de controles eficaces con carácter previo, durante el incidente de seguridad o con posterioridad al mismo.

3. Los responsables de informaciones y servicios afectados por el Esquema Nacional de Seguridad y regulados en los artículos 7 y 8 de esta orden respectivamente, deben valorar los riesgos de acuerdo a su importancia. También son responsables de la realización del seguimiento y control de las medidas de seguridad seleccionadas para su prevención.

Artículo 15. Procesos de implantación de sistemas de información.

De acuerdo con lo dispuesto en el Esquema Nacional de Seguridad, la Dirección General de Atención al Ciudadano, Calidad y Modernización habilitará procesos específicos para implantar los sistemas de información y cualquiera de sus elementos, teniendo en cuenta:

a) La existencia de las plataformas corporativas de la Administración de la Comunidad de Castilla y León.

b) Los riesgos existentes, tanto en el sistema de información, componente o servicio a asegurar, como en los interconectados.

c) La proporcionalidad de las actuaciones, y la asunción de riesgos cuando así se determine de forma expresa.

Artículo 16. Formación y concienciación.

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos informándoles de sus deberes y obligaciones en cuanto al tratamiento seguro de la información.

2. Se fomentará la formación específica en materia de seguridad de las tecnologías de la información y el conocimiento de todas aquellas personas que gestionan y administran sistemas de información y de telecomunicaciones.

3. Todas las actuaciones descritas en los apartados 1 y 2 de este artículo, se realizarán conforme a las disponibilidades presupuestarias y los criterios de formación que determine

la Escuela de Administración Pública de Castilla y León, incluyéndose, en su caso, dentro de los planes de formación de la Administración de la Comunidad de Castilla y León.

Artículo 17. Tratamiento de incumplimientos e incidentes de seguridad.

La Dirección General de Atención al Ciudadano, Calidad y Modernización desarrollará planes y líneas de trabajo específicos orientados a tratar incumplimientos e incidentes relacionados con la seguridad de los sistemas de información.

Artículo 18. Conformidad y auditoría.

1. Periódicamente, se revisará el grado de eficacia de los controles de seguridad implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración de la Comunidad de Castilla y León.

2. Las consejerías, los organismos autónomos y los entes públicos de derecho privado, incluidos en el ámbito de aplicación de esta orden, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento de esta política de seguridad, de acuerdo con lo establecido en Esquema Nacional de Seguridad y en la legislación en materia de protección de datos de carácter personal.

3. Se podrán celebrar simultáneamente las auditorías de seguridad recogidas en la Ley Orgánica 15/1999, de 13 de diciembre, y las enmarcadas dentro del Esquema Nacional de Seguridad, así como cualquier otra auditoría relacionada con la seguridad de la información.

4. Los informes resultantes de las auditorías se remitirán a la Consejería de Hacienda sin perjuicio de que se remitan a los órganos correspondientes de los centros directivos u órgano equivalente, para que se puedan adoptar medidas coordinadas garantizando los principios de eficacia y eficiencia que rigen en toda Administración.

Artículo 19. Revisión de la Política de Seguridad.

La Consejería de Hacienda, promoverá y aprobará la revisión periódica de esta política con motivo de cambios sustanciales en la normativa vigente o en los sistemas de comunicación. En dicha revisión se deberán evaluar los siguientes aspectos:

a) La eficacia de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados.

b) El coste e impacto de los controles en la eficiencia del desarrollo de las actividades de la Administración.

c) Los efectos de los cambios en la tecnología.

DISPOSICIONES ADICIONALES

Primera.– Asistencias.

Los miembros del Comité de Seguridad de la Información no percibirán indemnización alguna por la asistencia a sus sesiones.

Segunda.– Archivos y Patrimonio Documental.

Para todo lo referido a la información contenida en los archivos, así como a los documentos incluidos en el Patrimonio Documental de Castilla y León, será de aplicación lo dispuesto por la Ley 6/1991, de 19 de abril, de Archivos y del Patrimonio Documental de Castilla y León y su desarrollo normativo.

DISPOSICIÓN DEROGATORIA

Derogación normativa

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta orden y en concreto la Orden FOM/948/2007, de 17 de mayo, por la que se crea el Comité Técnico de Seguridad de los Sistemas de Información.

DISPOSICIONES FINALES

Primera.– Política de Seguridad del Organismo Pagador de Castilla y León.

1. La Consejería de Agricultura y Ganadería como Organismo Pagador en la Comunidad de Castilla y León designado por el Decreto 86/2006, de 7 de diciembre, dispondrá de una organización de la seguridad de los sistemas de información y una política de seguridad de la información propias, pero imbricadas y coordinadas en todo momento con la política de seguridad de la información de la Administración de la Comunidad de Castilla y León, en aplicación de las disposiciones comunitarias que afectan al Organismo Pagador en lo que se refiere a la autorización de los organismos pagadores y otros órganos y la liquidación de cuentas del FEAGA y del FEADER.

2. El desarrollo y las modificaciones posteriores en materia de política de seguridad que afecten al Organismo Pagador serán realizadas por el Director de este organismo, conforme a las competencias que le confiere la normativa citada anteriormente. No obstante, esta política de seguridad de la información y sus modificaciones serán previamente comunicadas por el Organismo Pagador a la Consejería de Hacienda que emitirá informe previo.

Segunda.– Entrada en vigor.

Esta orden entrará en vigor al mes de su publicación en el «Boletín Oficial de Castilla y León».

Valladolid, 30 de septiembre de 2014.

La Consejera de Hacienda,
Fdo.: María del Pilar del Olmo Moro

CV: BOCYL-D-17102014-2