

CONSEJERÍA DE PRESIDENCIA Y JUSTICIA

CVE-2016-6833 *Orden PRE/49/2016, de 22 de julio, por la que regula la estructura de gestión de seguridad de la información y de la continuidad de los servicios del Organismo Pagador.*

El Reglamento (UE) número 1306/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013 sobre la financiación, gestión y seguimiento de la Política Agrícola Común, desarrollado y complementado por el Reglamento de ejecución (UE) número 908/2014 de la Comisión de 6 de agosto de 2014, por el que se establecen disposiciones de aplicación del Reglamento (UE) número 1306/2013 del Parlamento Europeo y del Consejo en relación con los organismos pagadores y otros organismos, la gestión financiera, la liquidación de cuentas, las normas relativas a los controles, las garantías y la transparencia, y por el Reglamento Delegado (UE) nº 907/2014 de la Comisión, de 11 de marzo de 2014, que completa el Reglamento (UE) nº 1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, fijan el procedimiento y los criterios de autorización de los Organismos Pagadores, así como la regulación del mantenimiento de dicha autorización.

En el punto 3.B) del anexo I de éste último, se especifica como criterio de autorización la seguridad de los sistemas de información que debe estar basada en los criterios fijados en una de las siguientes normas: a) Organización internacional de normalización 27002: Código de prácticas para la gestión de la seguridad de la información (ISO); b) Manual de protección informática de base (BSI) o c) Asociación para la auditoría y el control de los sistemas de información: Objetivos de control para la información y tecnologías afines (COBIT).

El punto 2 del artículo 9 del Decreto 137/2006, de 28 de diciembre, por el que se adapta la organización y funcionamiento del Organismo Pagador de los gastos financiados por el FEAGA y el FEADER en la Comunidad Autónoma de Cantabria, dicta que la seguridad de los sistemas de información del Organismo Pagador de Cantabria se basará en la norma UNE-ISO/IEC 17779. Dicha norma se ha convertido en la actualidad en la ISO 27002.

La Resolución de la Dirección del Organismo Pagador de la Consejería de Ganadería, Agricultura y Pesca, de 28 de abril de 2006, por la que se crean los Comités de Dirección y de Seguridad del Organismo Pagador de Cantabria, considerando lo indicado en los apartados 4.1.1 y 4.1.2 de la norma ISO citada, y con objeto de garantizar la dirección y el seguimiento adecuado de la seguridad de los sistemas de información (SSII) del Organismo Pagador, crea un Comité de Seguridad de los SSII y un Comité de Dirección de la seguridad de la información. La composición de estos Comités queda posteriormente modificada por la Resolución de la Dirección del Organismo Pagador de la Consejería de Ganadería, Pesca y Desarrollo Rural, de 1 de octubre de 2012.

El Comité de Dirección de la seguridad de la información decidió en su reunión de 5 de noviembre de 2014, modificar los Comités de Dirección y de Seguridad del Organismo Pagador convirtiéndolos en Comisiones y modificando sus nombres y su composición.

Recientemente se ha publicado Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria y en su artículo 21, se regula la creación de los Comités o Comisiones para el estudio, informe y propuesta sobre seguridad de la información en materias sectoriales concretas.

A la vista de lo expuesto, es conveniente adaptar la estructura de gestión de la seguridad de la información del Organismo Pagador al referido Decreto, sustituyendo las dos Comisiones previamente existentes por dos nuevas Comisiones y creando la figura del Responsable Sectorial de la Seguridad de la Información del Organismo Pagador.

Por lo expuesto, de conformidad a lo dispuesto en el artículo 21 del Decreto 31/2015, procede aprobar la presente orden de creación de la Comisión Sectorial de Dirección de la Seguridad de la Información del Organismo Pagador, Comisión Sectorial de Seguimiento de la

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

Seguridad de la Información del Organismo Pagador y la figura de Responsable Sectorial de la Seguridad de la Información del Organismo Pagador.

DISPONGO

Artículo 1. Objeto.

El objeto de esta orden lo constituye la aprobación y regulación de la estructura de gestión de la seguridad de la información del Organismo Pagador de conformidad con el Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, creando la Comisión Sectorial de Dirección de la Seguridad del Organismo Pagador, la Comisión Sectorial de Seguimiento de la Seguridad del Organismo Pagador y la función de Responsable Sectorial de Seguridad de la Información del Organismo Pagador.

Artículo 2. Comisión Sectorial de Dirección de la Seguridad de la Información del Organismo Pagador.

1. Se crea la Comisión Sectorial de Dirección de la Seguridad de la Información del Organismo Pagador (en adelante Comisión SDSIOP) cuyo fin es la dirección de la seguridad de la información del Organismo Pagador, coordinando la implantación de medidas de seguridad, supervisando su efectividad y estableciendo controles para garantizar el cumplimiento de la legislación en la materia.

2. La Comisión SDSIOP tiene las siguientes funciones:

a) Asegurar el compromiso de la Dirección del Organismo Pagador con una efectiva gestión de la seguridad de la información y con su mejora continua.

b) Establecer las funciones y responsabilidades específicas de seguridad de la información en el Organismo Pagador de Cantabria.

c) Aprobar planes de mejora de la seguridad de la información, impulsando la implantación de medidas de seguridad y la adaptación de procedimientos internos de actuación atendiendo al resultado de los análisis de riesgos, informes sobre incidentes de seguridad y auditorías.

d) Supervisar el cumplimiento de los planes de mejora de la seguridad y las actividades de implantación de medidas de seguridad.

e) Aprobar planes de continuidad de los servicios prestados por el Organismo Pagador de Cantabria y proponer cambios en la política de continuidad a la Dirección del Organismo Pagador de Cantabria.

f) Aprobar los análisis de riesgos y, en su caso, aceptar el riesgo residual.

g) Revisar los informes sobre incidencias de seguridad y encargar el estudio de medidas o iniciativas específicas.

h) Discutir y aprobar, en su caso, las propuestas que, relacionadas con la seguridad de la información, le eleve la Comisión de Seguimiento de la Seguridad de la Información del Organismo Pagador.

i) Elevar a la Comisión General de la Seguridad de la Información, creada en el artículo 6 de decreto 31/ 2015, las necesidades del Organismo Pagador de Cantabria que requieran actuaciones globales en el ámbito de aplicación definido en el artículo 1 del citado decreto.

j) Solucionar los conflictos que puedan surgir en la interpretación y cumplimiento del Acuerdo de Servicio entre la Dirección del Organismo Pagador y la Dirección General de Organización y Tecnología en materia de apoyo y soporte informático.

k) Ratificar el Plan de Necesidades Informáticas Anuales al que se hace referencia en el Acuerdo de Prestación de Servicios que establece la relación entre la Dirección General de Organización y Tecnología y el Organismo Pagador de Cantabria en lo relativo a la prestación de servicios informáticos.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

Artículo 3. Comisión Sectorial de Seguimiento de la Seguridad de la Información del Organismo Pagador.

1. Se crea la Comisión Sectorial de Seguimiento de la Seguridad de la Información del Organismo Pagador (en adelante Comisión SSSIOP) cuyo fin es la gestión de la seguridad de la información del Organismo Pagador, desarrollando las instrucciones que reciba de la Comisión SDSIOP.

2. La Comisión SSSIOP tiene las siguientes funciones:

a) Promover la seguridad de la información en el Organismo Pagador y proponer la implantación de las medidas de seguridad que sean necesarias.

b) Proponer planes de mejora de la seguridad de la información, impulsando la implantación de medidas de seguridad y la adaptación de procedimientos internos de actuación atendiendo al resultado de los análisis de riesgos, informes sobre incidentes de seguridad y auditorías.

c) Coordinar la gestión de la continuidad de la actividad del Organismo, proponiendo la aprobación de los planes estratégicos que procedan.

d) Realizar el seguimiento de las incidencias que afecten a la seguridad de la información.

e) Proponer la realización de auditorías, supervisar los resultados de las mismas e impulsar la realización de acciones correctivas.

f) Supervisar y controlar los cambios significativos que afecten a los sistemas de información y asegurar las medidas oportunas para salvaguardar su seguridad.

g) Velar por la existencia de un inventario de activos y servicios actualizado en materia de seguridad de la información.

h) Establecer recomendaciones a la Comisión de Dirección y aplicar las medidas correctoras decididas en la Comisión de Dirección.

i) Supervisar los trabajos desarrollados en cumplimiento del Acuerdo de Prestación de Servicios, y en particular los recogidos en el Plan de Necesidades Informática Anuales, a fin de que se realicen de conformidad con lo estipulado.

Artículo 4. Responsable Sectorial de Seguridad de la Información del Organismo Pagador.

1. El Responsable Sectorial de Seguridad de la Información del Organismo Pagador será el encargado de la coordinación de las actuaciones en materia de seguridad de la información derivadas de las decisiones de las Comisiones SDSIOP y SSSIOP.

2. Para el desempeño de sus funciones estará apoyado por personal del Organismo Pagador experto en las distintas materias afectadas por la ejecución de esas actuaciones y de la Secretaría General, en función de las competencias y actuaciones en materia de seguridad de la información que afecten globalmente a la Consejería y por tanto, también al Organismo Pagador.

3. El Responsable Sectorial de Seguridad de la Información del Organismo Pagador tiene las siguientes funciones en materia de seguridad de la información:

a. Coordinar y supervisar la ejecución de las actuaciones derivadas de las decisiones de la Comisión SSSIOP.

b. Coordinar la realización de auditorías y presentar los resultados de las Comisiones SDSIOP y SSSIOP.

c. Impulsar las contrataciones que sean necesarias.

d. Promover la elaboración de los planes de continuidad de los servicios y sus pruebas de verificación.

e. Promover la realización y mantenimiento de catálogos de activos y servicios.

f. Promover la realización de revisiones de los accesos vigentes a los distintos servicios, aplicaciones y recursos.

g. Promover la realización de las actuaciones que sean pertinentes relativas a ficheros no automatizados.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

h. Elaborar informes de situación y proponer acciones de mejora a las Comisiones SDSIOP y SSSIOP.

i. Coordinar la participación de los responsables de las unidades de gestión en la elaboración de análisis de riesgos, valoración de los sistemas, auditorías y otras actividades relacionadas con al gestión de la seguridad.

j. Ejercer de interlocutor principal con el Responsable de Seguridad de la Información de la Comunidad Autónoma de Cantabria y con otras unidades de gestión, organismos públicos o entidades de la Comunidad Autónoma de Cantabria o de otras instituciones del estado.

k. Promover la concienciación y formación del personal del Organismo Pagador en la materia.

l. Coordinar, impulsar o realizar aquellas otras tareas que le sean asignadas por parte de la persona titular de la Dirección del Organismo Pagador en materia de seguridad de la información o de la continuidad de los servicios prestados por el Organismo Pagador en el ejercicio de sus competencias.

Artículo 5. Integración administrativa.

La Comisión Sectorial de Dirección de la Seguridad de la Información del Organismo Pagador, la Comisión Sectorial de Seguimiento de la Seguridad de la Información del Organismo Pagador y el Responsable Sectorial de Seguridad de la Información del Organismo Pagador, queda integrado en la Consejería de Medio Rural, Pesca y Alimentación, de quien depende el Organismo Pagador de Cantabria, aunque sin participar en su estructura jerárquica.

Artículo 6. Composición de la Comisión Sectorial de Dirección de la Seguridad de la Información del Organismo Pagador.

1. La Comisión estará compuesta por:

a) Presidente: La persona titular de la Dirección del Organismo Pagador.

b) Vocales: Las personas titulares de la Secretaría General de la Consejería de Medio Rural, Pesca y Alimentación, la Dirección General de Ganadería, la Dirección General de Pesca y Alimentación, la Dirección General de Medio Natural y la Dirección General de Organización y Tecnología, el o la Responsable Sectorial de Seguridad de la Información del Organismo Pagador y el o la Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria (artículo 14, Decreto 31/2015).

c) Secretario: El o la Responsable Sectorial de Seguridad de la Información del Organismo Pagador, que al tener también la condición de vocal, contará con voz y voto.

2. En el caso de modificación de la estructura orgánica de las Consejerías implicadas, que supongan un cambio en los puestos de trabajo representados en la Comisión, pasarán a formar parte de ella los titulares de los puestos de trabajo, nuevos o existentes, que asuman las competencias en materia de seguridad de los Sistemas de Información que ostentan los actuales.

3. Las funciones del Presidente, el Secretario y los demás miembros de la Comisión, así como el régimen jurídico de las convocatorias, sesiones y actas de la misma se regirán por lo establecido con carácter general en los artículos 68 a 72 de la Ley de Cantabria 6/2002, de 10 de diciembre, de Régimen Jurídico del Gobierno y de la Administración de la Comunidad Autónoma de Cantabria:

4. En caso de ausencia obligada prolongada o inexistencia del Presidente, será sustituido por el Secretario General de la Consejería de Medio Rural, Pesca y Alimentación.

5. En caso de ausencia del Responsable Sectorial de Seguridad de la Información del Organismo Pagador, ejercerá de secretario el vocal designado por el presidente.

Artículo 7. Periodicidad de las reuniones

1. La Comisión SDSIOP se reunirá cuando la convoque el Presidente, a iniciativa propia o a propuesta del Responsable Sectorial de Seguridad de la Información del Organismo Pagador y de sus reuniones se levantará acta que custodiará su secretario.

2. Habrá al menos una reunión al año.

Artículo 8. Composición de la Comisión Sectorial de Seguimiento de la Seguridad de la Información del Organismo Pagador.

1. La Comisión estará compuesta por:

a) Presidente: El Responsable Sectorial de Seguridad de la Información del Organismo Pagador.

b) Vocales:

— Por parte del Organismo Pagador, las personas titulares de los servicios gestores de ayudas incluidas en el Programa de Desarrollo Rural (PDR) vigente en cada momento. Actualmente, estos servicios son Supervisión de Gastos de la PAC, Ayudas del Sector Agrario, Agricultura y Diversificación Rural, Producción Animal, Reforma de Estructuras, Electrificación Rural, Industria y Calidad Agroalimentaria, Montes y Conservación de la Naturaleza. También se incluye a las personas titulares de la unidad de auditoría interna y del Servicio de Administración General.

- Por parte de la Dirección General de Organización y Tecnología, las personas titulares del Servicio de Informática, del Servicio de Centro de Proceso de Datos, de la Sección de Coordinación Técnica y el o la Responsable de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria (artículo 14, Decreto 31/2015).

c) Secretario: El Jefe de Sección de Actuaciones Administrativas del Servicio de Ayudas del Sector Agrario, que tendrá derecho a voz pero sin voto, o, en su defecto, el Jefe de Sección de Coordinación Técnica de la DGOT, que al tener también la condición de vocal, contará con voz y voto.

2. En el caso de modificación de la estructura orgánica de las Consejerías implicadas, que supongan un cambio en los puestos de trabajo representados en la Comisión, pasarán a formar parte de ella los titulares de los puestos de trabajo, nuevos o existentes, que asuman las competencias en materia de seguridad de los Sistemas de Información que ostentan los actuales.

3. Las funciones del Presidente, el Secretario y los demás miembros de la Comisión, así como el régimen jurídico de las convocatorias, sesiones y actas de la misma se regirán por lo establecido con carácter general en los artículos 68 a 72 de la Ley de Cantabria 6/2002, de 10 de diciembre, de Régimen Jurídico del Gobierno y de la Administración de la Comunidad Autónoma de Cantabria:

4. En caso de ausencia del Jefe de Sección de Actuaciones Administrativas del Servicio de Ayudas al Sector Agrario o del Jefe de Sección de Coordinación Técnica de la DGOT, ejercerá de secretario el vocal designado por el Presidente.

Artículo 9. Periodicidad de las reuniones

1. La Comisión SSSIOP se reunirá cuando la convoque el Presidente y de sus reuniones se levantará acta que custodiará su secretario.

2. Habrá al menos dos reuniones al año.

Artículo 10. Continuidad de los servicios

1. La responsabilidad máxima en materia de continuidad de los servicios prestados por el Organismo Pagador en el ejercicio de sus competencias, corresponderá a la persona titular de la Dirección del Organismo Pagador.

2. Por Orden de la Consejería de Presidencia y Justicia se definirá y aprobará la "Política de Continuidad del Organismo Pagador", en la que se recogerán al menos los siguientes extremos: finalidad, alcance, principios rectores, estructura para la gestión de continuidad de los servicios y asignación de funciones.

LUNES, 1 DE AGOSTO DE 2016 - BOC NÚM. 147

Disposición adicional primera. Asignación de funciones a unidad administrativa.

La Comisión SDSIOP determinara por acuerdo de la misma, la unidad administrativa a la que se le encomendaran las funciones y tareas de Responsable Sectorial de Seguridad de la Información del Organismo Pagador.

Disposición adicional segunda. Adecuación de las relaciones de puestos de trabajo.

La Consejería de Presidencia y Justicia procederá a las modificaciones y adaptaciones necesarias del puesto de trabajo al que se le asignan el desempeño de las funciones y tareas encomendadas al Responsable Sectorial de Seguridad de la Información del Organismo Pagador.

Disposición transitoria única. Desempeño temporal de funciones de Responsable Sectorial de Seguridad de la Información.

Hasta que se proceda a la modificación y adaptación de la unidad administrativa a la que se le encomiendan las funciones de Responsable Sectorial de Seguridad de la Información del Organismo Pagador, estas serán desempeñadas provisionalmente por titular de ese puesto de trabajo.

Disposición derogatoria única. Derogación normativa.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongán a la presente Orden y en particular, la Resolución de 28 de abril de 2006 de la Dirección del Organismo Pagador, por la que se crean los Comités de Dirección y de Seguridad de los SSII del Organismo Pagador de Cantabria, modificada por Resolución de 1 de octubre de 2012.

Disposición final primera. Facultad para dictar instrucciones para la aplicación.

La Dirección General competente en materia de seguridad de la información, y la Dirección del Organismo Pagador, quedan facultadas para que en el ámbito de sus correspondientes competencias adopten las acciones y dicten las instrucciones que sean necesarias para la aplicación de la presente orden.

Disposición final segunda. Entrada en vigor.

La presente Orden entrará en vigor el día siguiente de su publicación en el Boletín Oficial de Cantabria.

Santander, 22 de julio de 2016.
El consejero de Presidencia y Justicia,
Rafael de la Sierra González.

2016/6833

CVE-2016-6833