III OTRAS RESOLUCIONES

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

RESOLUCIÓN de 6 de julio de 2016, de la Consejera, por la que se ordena la publicación en el Diario Oficial de Extremadura del Acuerdo de Encomienda de Gestión entre la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio y la Consejería de Hacienda y Administración Pública para la gestión de los requisitos de seguridad de la información en el Organismo Pagador de la Comunidad Autónoma de Extremadura en la prestación de servicios TIC de la Dirección General de Administración Electrónica y Tecnologías de la Información, de 10 de junio de 2016.

(2016061028)

Por acuerdo del Consejo de Gobierno del 31 de mayo de 2016 se autorizó la firma del Acuerdo de encomienda de gestión entre la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio y la Consejería de Hacienda y Administración Pública para la gestión de los requisitos de seguridad de la información en el organismo pagador de la Comunidad Autónoma de Extremadura, en la prestación de servicios TIC de la Dirección General de Administración Electrónica y Tecnologías de la Información, que fue suscrito el 10 de junio de 2016.

En virtud de lo dispuesto en el artículo 75 de la Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura el presente acuerdo de encomienda de gestión debe ser publicado en el Diario Oficial de Extremadura, tal y como se recoge asimismo en la cláusula séptima del mismo.

Por todo lo cual, se

R E S U E L V E :

Ordenar la publicación en el Diario Oficial de Extremadura del Acuerdo de encomienda de gestión entre la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio y la Consejería de Hacienda y Administración Pública para la gestión de los requisitos de seguridad de la información en el organismo pagador de la Comunidad Autónoma de Extremadura, en la prestación de servicios TIC de la Dirección General de Administración Electrónica y Tecnologías de la Información, de 10 de junio de 2016, que se inserta como Anexo a la presente resolución.

Mérida, 6 de julio de 2016.

La Consejera de Hacienda y Administración Pública,
PILAR BLANCO-MORALES LIMONES

A N E X O

ACUERDO DE ENCOMIENDA DE GESTIÓN ENTRE LA CONSEJERÍA DE MEDIO AMBIENTE Y RURAL, POLÍTICAS AGRARIAS Y TERRITORIO Y LA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA PARA LA GESTIÓN DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN EN EL ORGANISMO PAGADOR DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA EN LA PRESTACIÓN DE SERVICIOS TIC DE LA DIRECCIÓN GENERAL DE ADMINISTRACIÓN ELECTRÓNICA Y TECNOLOGÍAS DE LA INFORMACIÓN

En Mérida, a 10 de junio de 2016.

REUNIDOS

D.ª Begoña García Bernal, Consejera de Medio Ambiente y Rural, Políticas Agrarias y Territorio, en ejercicio de las competencias atribuidas por el Decreto del presidente 36/2015, de 14 de septiembre (DOE num.178 de 15/09/2015), asumiendo las funciones de Director/a del Organismo Pagador en función del Decreto 299/2015, de 27 de noviembre (DOE num.233 de 3/12/2015) y por el Real Decreto 521/2006, de 28 de abril, en el Reglamento (UE) núm.1306/2013, del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013 por los que se designa a la Consejería competente en materia de agricultura como el Organismo Pagador de los gastos correspondientes al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Extremadura.

D.ª Pilar Blanco-Morales Limones, Consejera de Hacienda y Administración Pública, en ejercicio de las competencias atribuidas por el Decreto del presidente 18/2015, de 6 de julio (DOE num.129 de 07/07/2015).

EXPONEN

Primero

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establece, en su artículo 15, la encomienda de gestión como instrumento para confiar la realización de actividades materiales a órganos o entidades de la misma Administración Pública.

Segundo

En virtud del artículo 15.1 de la mencionada Ley 30/1992, la realización de actividades de carácter material, técnico o de servicios de la competencia de órganos de la Administración de la Comunidad Autónoma o de las entidades de derecho público de ella dependientes, podrá ser encomendada a otros órganos o entidades de la misma o distinta Administración por razones de eficacia o cuando no se posean los medios técnicos, personales o materiales idóneos para el desempeño en los términos y con el carácter previsto en esta Ley y, en su defecto, en la legislación básica del régimen Jurídico de las Administraciones Públicas.” Del mismo modo, la Ley 1/2002, de 28 de febrero, de Gobierno y Administración

de la Comunidad Autónoma de Extremadura, en su artículo 75, regula la figura de la encomienda de gestión, estableciendo en sus apartados 3 y 4 que para la encomienda a órganos pertenecientes o dependientes de distinta Consejería será precisa la autorización por el Consejo de Gobierno, y servirá de instrumento de formalización la resolución o acuerdo que la formalice. La presente encomienda de gestión ha sido autorizada por Consejo de Gobierno en su reunión de 31 de mayo de 2016.

En virtud de lo anterior, suscriben el siguiente

ACUERDO DE ENCOMIENDA DE GESTIÓN ENTRE LA CONSEJERÍA DE MEDIO AMBIENTE Y RURAL, POLÍTICAS AGRARIAS Y TERRITORIO Y LA CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Primera

La Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio, como Organismo Pagador de los gastos correspondientes al FEAGA y al FEADER en la Comunidad Autónoma de Extremadura, y la Consejería de Hacienda y Administración Pública, a través de la Dirección General de Administración Electrónica y Tecnologías de la Información, acuerdan, en el marco de lo dispuesto en el artículo 15 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en el artículo 75 de la Ley 1/2002, de 28 de febrero de Gobierno y Administración de la Comunidad Autónoma de Extremadura, que la citada Consejería de Hacienda y Administración Pública lleve a cabo, por razones de eficacia y competencia, la realización de los servicios descritos en los siguientes puntos como proveedor interno de servicios TIC al Organismo Pagador.

Segunda

En virtud de lo dispuesto en el artículo 6 del Decreto 261/2015 de 7 de agosto, por el que se establece la estructura orgánica de la Consejería de Hacienda y Administración Pública (DOE Extraordinario número 5 de 8 de agosto), corresponde a la Dirección General de Administración Electrónica y Tecnologías de la Información (en adelante DGAETI), bajo la superior dirección de la persona titular de la Consejería y la coordinación de la Secretaría General de Administración Pública, el diseño, ejecución, gestión, supervisión e impulso de las políticas de la Junta de Extremadura en materia de tecnologías de la información y comunicación de carácter corporativo e interadministrativo, así como el seguimiento y análisis de todos los recursos y sistemas informáticos para garantizar la eficiencia de la Administración.

Tercera

Para el cumplimiento de las políticas y normativas, vigente en el Organismo Pagador, que conforman el marco normativo del sistema de gestión de seguridad de la Información basado en el estándar UNE-ISO/IEC 27001, la Dirección General de Administración Electrónica y Tecnologías de la Información, como proveedor que presta servicios internos TIC a la Junta de Extremadura en base a las competencias descritas en el Decreto 261/2015, de 7 de agosto, por el que se establece la estructura orgánica de la Consejería de Hacienda y

Administración Pública, proveerá la gestión de los requisitos de seguridad de la información de los servicios prestados al Organismo Pagador (OP), en las siguientes áreas:

1. Seguridad en el desarrollo y mantenimiento de los sistemas de información que prestan soporte a las actividades y procesos de negocio del OP, incluyendo las siguientes responsabilidades:

   — Definición e implantación de los requisitos de seguridad

   — Control de versiones y gestión del cambio

   — Gestión de las vulnerabilidades

2. Incidentes TIC, incluyendo las siguientes responsabilidades:

   — Detección y comunicación de incidentes de seguridad TIC

   — Análisis de los incidentes.

   — Coordinación de las actividades de resolución.

3. Continuidad TI, incluyendo las siguientes responsabilidades:

   — Desarrollo y prueba de los planes de recuperación TI acorde a la estrategia de continuidad del OP

   — Gestión de las operaciones de copias de seguridad

4. Seguridad en las comunicaciones, incluyendo las siguientes responsabilidades:

   — Securización de los perímetros de seguridad

   — Operación y mantenimiento de la infraestructura de comunicaciones

   — Aseguramiento de la continuidad de las comunicaciones.

5. Seguridad lógica de activos TIC, incluyendo las siguientes responsabilidades:

   — Mantenimiento del inventario TIC

   — Gestión de las vulnerabilidades de las infraestructuras

   — Administración de los dispositivos de gestión de acceso lógico

   — Mantenimiento de la seguridad de los sistemas TIC que soportan los sistemas de información del OP

   — Garantizar la segregación de entornos.

6. Protección contra código malicioso: incluyendo las siguientes responsabilidades:

   — Gestión de la detección y mitigación frente a código malicioso.

En la ejecución de los servicios descritos, la Dirección General de Administración Electrónica y Tecnologías de la Información, estará sujeta a las cláusulas de seguridad que se especifican en el ANEXO II – Cláusulas de Seguridad.

Cuarta

En el caso de que el Organismo Pagador requiera de la realización de alguna actividad en materia de seguridad de la información en el ámbito TIC que no esté reflejada en los puntos anteriores, se enviará una petición con la descripción de la actividad a realizar a la DG de Administración Electrónica y Tecnologías de la Información, quién evaluará la viabilidad de su ejecución y la realizará en su caso.

Quinta

Los servicios anteriormente descritos pueden afectar a la confidencialidad, integridad y disponibilidad de la información perteneciente al Organismo Pagador, por lo que se requiere definir los niveles de acuerdo de servicio, en lo relativo a la seguridad de la información, así como los indicadores necesarios que permitan evaluar el correcto cumplimiento.

Los acuerdos de nivel de servicio se especifican en el ANEXO I – Acuerdos de nivel de servicio.

Asimismo, en el Anexo II se establecen las cláusulas de seguridad.

Sexta

Para un adecuado seguimiento del cumplimiento de los acuerdos de niveles de servicio, la DG de Administración Electrónica y Tecnologías de la Información realizará un informe, cada dos meses, que incluirá un resumen de los servicios prestados y una evaluación del cumplimiento, durante el mes en curso con los datos de los dos meses anteriores, que será enviado al Responsable de Seguridad del Organismo Pagador.

Se crea una Comisión de Seguimiento formada por 5 miembros de entre los que formen parte del Comité de Gestión y Coordinación de Seguridad de la Información que funcionará conforme a la normativa interna del mismo y que se reunirá, al menos, semestralmente para evaluar el seguimiento de la encomienda.

En caso de detección, en el control de los acuerdos de nivel de servicio, de desviaciones o tendencias que puedan afectar a la consecución de los objetivos de seguridad de la información establecidos por el Organismo Pagador, la Comisión de Seguimiento lo pondrá en conocimiento de su Directora, quien convocará extraordinariamente al Comité de Gestión y Coordinación para la Seguridad de la Información para decidir las acciones correctivas que correspondan, pudiendo modificar los acuerdos de nivel de servicio si así se consensúa.

Séptima

La presente encomienda de gestión permanecerá vigente mientras no se vean alteradas las competencias de las Consejerías que conforman la Administración de la Comunidad Autónoma de Extremadura, tal y como se recoge en el Decreto del Presidente 16/2015, de 6 de julio, a contar desde la fecha de publicación en el Diario Oficial de Extremadura.

Serán causas de resolución de esta encomienda de gestión el mutuo acuerdo de las partes y el desistimiento, a instancia de cualquiera de ellas, mediante el preaviso con un mes de antelación a la fecha que la parte denunciante desee darlo por finalizado. Las partes deberán acordar, a propuesta de la comisión de seguimiento, todos los aspectos que resulten pendientes de las actuaciones no finalizadas. Asimismo, se resolverá por la desaparición o destrucción sobrevenida del objeto del mismo. En todo caso, deberá tramitarse la preceptiva autorización para la resolución, correspondiendo la misma al mismo órgano autorizante. Finalmente se procederá a la correspondiente publicación en el Diario Oficial de Extremadura.

Octava

La encomienda de gestión no supone cesión de la titularidad de las competencias ni de los elementos sustantivos de su ejercicio, atribuidas a la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio, como organismo pagador de los gastos correspondientes al FEAGA y al FEADER.

Novena

Es responsabilidad de la Consejería de Medio Ambiente y Rural, Políticas Agrarias y Territorio, como Organismo Pagador de los gastos correspondientes al FEAGA y al FEADER en Extremadura, el establecimiento, implantación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información en el Organismo Pagador.

LA DIRECTORA DEL ORGANISMO PAGADOR	LA CONSEJERA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA
FDO.: Begoña García Bernal	FDO.: Pilar Blanco-Morales Limones

A N E X O I

ACUERDOS DE NIVEL DE SERVICIO

Los tiempos establecidos se atenderán en días laborables de Lunes a Viernes, y no computarán los tiempos en los que las acciones o decisiones dependan del personal propio del Organismo Pagador.

Se establecen todos los servicios con las mismas prioridades

1. **Servicio de Gestión de la seguridad en el desarrollo y mantenimiento de los sistemas de información que prestan soporte a las actividades y procesos de negocio del O.P.**

CÓDIGO	IND-SGDES-001
INDICADOR	Eficacia corrección de vulnerabilidades sistemas
FÓRMULA	[vulnerabilidades encontradas corregidas en plazo/vulnerabilidades encontradas]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual
TIEMPOS DE CORRECCIÓN	Críticas: 15 días Graves: 20 días Medio: 30 días Leve: 60 días

CÓDIGO	IND-SGDES-002
INDICADOR	**Pases a producción de sistemas seguros:**
FÓRMULA	[Pases de versiones mayores con escaneo de vulnerabilidades/Pases de versiones mayores]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual
TIEMPOS DE CORRECCIÓN	Críticas: 15 días Graves: 20 días Medio: 30 días Leve: 60 días

2. **Servicio de gestión de incidentes TIC**

CÓDIGO	IND-SGINC-001
INDICADOR	**Notificación Temprana de incidentes TIC:**
FÓRMULA	[Incidentes TIC notificados en tiempo/incidentes TIC totales]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual
TIEMPOS DE CORRECCIÓN	24 horas

CÓDIGO	IND-SGINC-002
INDICADOR	**Tiempo de resolución incidentes de seguridad:**
FÓRMULA	[Incidentes resueltos en plazo/Incidentes totales]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual
TIEMPOS DE CORRECCIÓN	Críticas: 15 días Altos o Muy Altos: 20 días Medio: 30 días Bajo: 60 días

3. **Servicio de gestión de continuidad TI**

CÓDIGO	IND-SGCON-001
INDICADOR	**Completitud de pruebas continuidad TI**
FÓRMULA	[Pruebas ejecutadas/pruebas planificadas]
DOMINIO	[0-1]
OBJETIVO	1
FRECUENCIA	Anual

CÓDIGO	IND-SGCON-002
INDICADOR	**Disponibilidad de SI:**
FÓRMULA	[Tiempo de indisponibilidad/Tiempo total]
DOMINIO	[0-1]
OBJETIVO	0,95
FRECUENCIA	Bimensual

CÓDIGO	IND-SGCON-003
INDICADOR	**Eficacia sistema de copias:**
FÓRMULA	[copias con éxito/ copias planificadas]
DOMINIO	[0-1]
OBJETIVO	0,95
FRECUENCIA	Bimensual

4. **Servicio de gestión de la seguridad en las comunicaciones**

CÓDIGO	IND-SGCOM-001
INDICADOR	**Disponibilidad de equipamiento crítico de red**
FÓRMULA	[Tiempo activo/Tiempo total]
DOMINIO	[0-1]
OBJETIVO	0,999
FRECUENCIA	Bimensual

5. **Servicio de gestión de la seguridad lógica de activos TIC**

CÓDIGO	IND-SGSLOG-001
INDICADOR	**Eficacia corrección de vulnerabilidades infraestructura:**
FÓRMULA	[vulnerabilidades encontradas corregidas en plazo/vulnerabilidades encontradas]
DOMINIO	[0-1]
OBJETIVO	0,8
FRECUENCIA	Mensual
TIEMPOS DE CORRECCIÓN	• Críticas: 15 días • Graves: 20 días • Medio: 30 días • Leve: 60 días

CÓDIGO	IND-SGSLOG-002
INDICADOR	**Eficacia baja de permisos:**
FÓRMULA [Bajas procesadas en tiempo/bajas procesadas totales]	[Bajas procesadas en tiempo/bajas procesadas totales]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Mensual
TIEMPOS DE ACEPTACIÓN	1 día

CÓDIGO	IND-SGSLOG-003
INDICADOR	**Eficacia aplicación parches**
FÓRMULA	[parches windows aplicados en tiempo en equipamiento crítico/parches windows publicados totales]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual

CÓDIGO	IND-SGSLOG-004
INDICADOR	**Análisis de vulnerabilidades:**
FÓRMULA	[sistemas con análisis de vulnerabilidades/sistemas totales]
DOMINIO	[0-1]
OBJETIVO	1/5 de los sistemas en 2016. 1/3 de los restantes en años posteriores con respecto al ciclo de 3 años de certificación.
FRECUENCIA	Bimensual

6. **Servicio de gestión de la protección contra código malicioso**

CÓDIGO	IND-SGCMAL-001
INDICADOR	**Despliegue efectivo de los sistemas de protección contra código malicioso**
FÓRMULA	[Servidores con protección activa/Servidores totales]
DOMINIO	[0-1]
OBJETIVO	0,9
FRECUENCIA	Bimensual

ANEXO II

CLÁUSULAS DE SEGURIDAD

Confidencialidad de la información

El proveedor interno vendrá obligado a guardar la más estricta confidencialidad sobre el contenido del encargo, así como sobre los datos o información a la que pueda tener acceso como consecuencia de la ejecución del mismo, y a usar dicha información a los exclusivos fines de la ejecución del contrato y conforme a la Política de Seguridad del Organismo Pagador en los términos en que resulte aplicable. Esta obligación se mantendrá incluso después de la finalización de la relación.

El deber de confidencialidad sobre la información del Organismo Pagador será extensible a todo el personal del proveedor interno o colaborador con éste que participe en la prestación del servicio.

Todo el personal del proveedor interno protegerá, en la medida de sus posibilidades, la información propiedad del Organismo Pagador y los sistemas de información a los que tenga acceso con el fin de evitar revelación, alteración o uso indebido de la información.

El acceso y posesión de información del Organismo Pagador por parte del proveedor interno es estrictamente temporal y vinculado a las atribuciones propias del desempeño del puesto de trabajo o servicio contratado, sin que ello confiera derecho alguno de posesión, de titularidad de copia o de transmisión sobre dicha información.

El proveedor interno, una vez finalizadas las tareas que han originado el acceso a la información, deberá devolver los soportes y documentación que se le hubiese facilitado.

El proveedor interno no puede transmitir, enviar, compartir o poner a disposición de otras entidades información propiedad del Organismo Pagador, a no ser que de manera previa haya sido expresamente autorizado para hacerlo, independientemente del medio o formato de la información y de su contenido.

Auditoría

El Organismo Pagador podrá exigir a la Dirección General de Administración Electrónica y Tecnologías de la Información cualquier evidencia de cumplimiento con los requisitos de seguridad impuestos por parte del Organismo Pagador. Para ello se reserva el ejercicio de los siguientes derechos:

- Revisar o auditar el cumplimiento por parte del proveedor interno de la legislación aplicable de acuerdo a lo dispuesto por la encomienda firmada por ambas partes.

- Requerir al proveedor interno los documentos derivados de los procesos de auditoría llevados a cabo por éste, así como cualquier otra evidencia sobre el cumplimiento con el marco legal aplicable y con los requisitos de seguridad de la información impuestos por la presente encomienda.

- Solicitar la implantación de cualquier mecanismo organizativo, técnico o jurídico que considere adecuado para garantizar la Seguridad de la Información.

Para facilitar el ejercicio de los anteriores derechos por parte del Organismo pagador, el proveedor interno se compromete a facilitar y participar activamente en el desarrollo de las actividades anteriormente descritas.

Cumplimiento con la política de seguridad de la información del Organismo Pagador

El Organismo Pagador dispone de una Política de Seguridad de la Información, así como normativas para su desarrollo, los cuales establecen los controles de seguridad que se deben aplicar con objeto de garantizar la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información. Es obligación del proveedor interno el conocimiento, cumplimiento e implantación de aquellas medidas de seguridad establecidas en el Marco Normativo que, en base a la naturaleza de los servicios TIC prestados, sea de aplicación.

Transmisión de información por parte del proveedor interno a otras entidades

El proveedor interno no puede transmitir, enviar, compartir o poner a disposición de otras entidades información propiedad del Organismo Pagador, a no ser que de manera previa haya sido expresamente autorizado para hacerlo, independientemente del medio o formato de la información y de su contenido. En el caso de existir dicha autorización se deberá velar por el cumplimiento de las siguientes normas:

- Deben extenderse al receptor de la información todas las obligaciones del proveedor interno en materia de Seguridad de la Información impuestas por el Organismo Pagador.
- El proveedor interno será responsable del uso y protección de la información del Organismo Pagador que le haya sido proporcionada, así como de los perjuicios ocasionados al Organismo Pagador en los casos en los que la seguridad de la información hubiera sido comprometida.
- Se podrá transmitir única y exclusivamente la información estrictamente necesaria para que el proveedor interno autorizado pueda llevar a cabo su cometido.
- La información sólo podrá ser transmitida a los destinatarios autorizados, que han de estar unívocamente identificados, y por medios que garanticen la identidad del destinatario.
- En la transmisión de la información se deben aplicar mecanismos que imposibiliten el acceso a ella por parte de otras entidades no autorizadas. Igualmente en el almacenamiento de la información en dispositivos portátiles o extraíbles se deben aplicar mecanismos que imposibiliten dichos accesos.