



RESOLUCIÓN de 6 de noviembre de 2024, de la Consejera, por la que se dispone la publicación del Acuerdo de encomienda de gestión entre la Consejería de Agricultura, Ganadería y Desarrollo Sostenible y la Consejería de Economía, Empleo y Transformación Digital para la prestación de servicios TIC al Organismo Pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) de la Comunidad Autónoma de Extremadura, suscrito el 5 de noviembre de 2024. (2024063739)

La Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura, en su artículo 75 regula la figura de la encomienda de gestión como instrumento para el ejercicio de competencia por los órganos de la Administración de la Comunidad Autónoma, estableciendo en sus apartados 3 y 4 que para la encomienda a órganos pertenecientes o dependientes de diferente Consejería será precisa la autorización por el Consejo de Gobierno, y servirá de instrumento de formalización, la resolución o acuerdo que la autorice.

Por Acuerdo de Consejo de Gobierno de 29 de octubre de 2024 se autorizó el Acuerdo de encomienda de gestión entre la Consejería de Agricultura, Ganadería y Desarrollo Sostenible y la Consejería de Economía, Empleo y Transformación Digital para la prestación de servicios TIC al Organismo Pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) de la Comunidad Autónoma de Extremadura, suscrito el 5 de noviembre de 2024.

El acuerdo será publicado, para su eficacia, en el Diario Oficial de Extremadura, de conformidad con lo establecido en el artículo 11.3.a) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el artículo 75.5 de la Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura y en la cláusula séptima del mismo.

Por lo expuesto,

RESUELVO:

Ordenar la publicación en el Diario Oficial de Extremadura del Acuerdo de encomienda de gestión entre la Consejería de Agricultura, Ganadería y Desarrollo Sostenible y la Consejería de Economía, Empleo y Transformación Digital para la prestación de servicios TIC al Organismo Pagador de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) de la Comunidad Autónoma de Extremadura, suscrito el 5 de noviembre de 2024, que se inserta como anexo a la presente resolución.

Mérida, 6 de noviembre de 2024.

La Consejera de Agricultura, Ganadería
y Desarrollo Sostenible,

MERCEDES MORÁN ÁLVAREZ

**ANEXO**

ACUERDO DE ENCOMIENDA DE GESTION ENTRE LA CONSEJERÍA DE AGRICULTURA, GANADERÍA Y DESARROLLO SOSTENIBLE Y LA CONSEJERÍA DE ECONOMÍA, EMPLEO Y TRANSFORMACIÓN DIGITAL PARA LA PRESTACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN (TIC) AL ORGANISMO PAGADOR DE LOS GASTOS FINANCIADOS POR EL FONDO EUROPEO AGRÍCOLA DE GARANTÍA (FEAGA) Y POR EL FONDO EUROPEO AGRÍCOLA DE DESARROLLO RURAL (FEADER) DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA.

REUNIDOS:

Doña Mercedes Morán Álvarez, Consejera de Agricultura, Ganadería y Desarrollo Sostenible, cargo para el que fue nombrada por el Decreto de la Presidenta 19/2023, de 20 de julio (DOE número 140, de 21 de julio), en ejercicio de las competencias atribuidas por el Decreto de la Presidenta 16/2023, de 20 de julio, por el que se modifican la denominación y las competencias de las Consejerías que conforman la Administración de la Comunidad Autónoma de Extremadura (DOE número 140, de 21 de julio) y de conformidad con el Decreto 233/2023, de 12 de septiembre, por el que se establece la estructura orgánica de la Consejería de Agricultura, Ganadería y Desarrollo Sostenible (DOE extraordinario número 3, de 16 de septiembre), asumiendo las funciones de Directora del Organismo Pagador de conformidad con el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo, de 2 de diciembre de 2021 sobre la financiación, la gestión y el seguimiento de la política agrícola común, el Real Decreto 1046/2022, de 27 de diciembre, por el que se regula la gobernanza del Plan Estratégico de la Política Agrícola Común en España y de los fondos europeos agrícolas FEAGA y FEADER, y el Decreto 4/2023, de 20 de enero, por el que se regula la estructura de gobernanza del Plan Estratégico de la Política Agrícola Común 2023-2027 en la Comunidad Autónoma de Extremadura (DOE número 51, de 15 de marzo), debidamente autorizada por el Consejo de Gobierno en su reunión de fecha 5 de noviembre de 2024.

Don Guillermo Santamaría Galdón, Consejero de Economía, Empleo y Transformación Digital, cargo para el que fue nombrado por el Decreto de la Presidenta 20/2023, de 20 de julio (DOE número 140, de 21 de julio), en ejercicio de las competencias atribuidas por el Decreto de la Presidenta 16/2023, de 20 de julio, por el que se modifican la denominación y las competencias de las Consejerías que conforman la Administración de la Comunidad Autónoma de Extremadura (DOE número 140, de 21 de julio) y de conformidad con el Decreto 234/2023, de 12 de septiembre, por el que se establece la estructura orgánica de la Consejería de Economía, Empleo y Transformación Digital (DOE extraordinario número 3, de 16 de septiembre), debidamente autorizado por el Consejo de Gobierno en su reunión de fecha 5 de noviembre de 2024.

**MANIFIESTAN:**

Primero. Que a la Consejería de Agricultura, Ganadería y Desarrollo Sostenible le corresponden las competencias en materia de agricultura y ganadería, diversificación y formación del medio rural, conservación de la naturaleza y áreas protegidas y evaluación y protección ambiental; en materia de planificación y coordinación hídrica; las competencias en materia de industria, energía y minas. También se le asignan las competencias en materia sociedades cooperativas y sociedades laborales y de política demográfica y poblacional.

Por su parte, a la Dirección General de Política Agraria Comunitaria le corresponde, bajo la superior dirección de la persona titular de la Consejería, la gestión integrada de las ayudas directas del FEAGA, de los derechos de pago de ayudas del FEAGA, la gestión de las ayudas agroambientales cofinanciadas por el FEADER, así como la gestión del cese anticipado de la actividad agraria, según el artículo 14.3 del Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica básica de la Administración de la Comunidad Autónoma de Extremadura (DOE número 145, de 28 de julio).

Que a la Consejería de Economía, Empleo y Transformación Digital le corresponden las competencias en materia de planificación y coordinación económica y estadística, comercio e inversiones y la política empresarial, promoción de la empresa y apoyo al emprendedor; así como las competencias en materia de trabajo y políticas de empleo, las de sociedad de la información y telecomunicaciones. Así mismo ejercerá las competencias de política tecnológica de carácter corporativo y administración electrónica.

Por su parte, a la Secretaría General de Transformación Digital y Ciberseguridad le corresponde, bajo la superior dirección de la persona titular de la citada Consejería, la coordinación de la Dirección General de Digitalización de la Administración y de la Dirección General de Digitalización Regional. Igualmente le corresponde impulsar y coordinar la ejecución de medidas horizontales para la implantación de la administración digital y las que se derivan del marco vigente sobre administración electrónica, rediseño de procedimientos administrativos y de gestión interna. En el ámbito de competencias de la citada Consejería residen, además, las funciones del Responsable de Privacidad y Seguridad de la Información y Delegado de Protección de Datos de la administración autonómica, en virtud de lo dispuesto en el Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica básica de la Administración de la Comunidad Autónoma de Extremadura (DOE número 145, de 28 de julio).

A la Dirección General de Digitalización de la Administración le corresponde, bajo la superior dirección de la persona titular de la Consejería y la coordinación de la Secretaría General de Transformación Digital y Ciberseguridad, las competencias sobre políticas digitales corporativas y seguridad de la información, la gestión centralizada de las infraestructuras y sistemas



que soporten los servicios administrativos y las comunicaciones corporativas de la administración autonómica, la gestión del inventario de activos tecnológicos; así como el análisis de requerimiento, el diseño, la gestión y supervisión de los medios y servicios que fueran necesarios para la ejecución de las políticas digitales corporativas que se establezcan para implantar la administración digital. Asimismo, asume las funciones de asistir al Responsable de Privacidad y Seguridad de la Información conforme a lo dispuesto en la política respectiva, así como las funciones de asistencia, coordinación y supervisión de recursos, infraestructuras y soluciones digitales de todas las Consejerías de la Junta de Extremadura. Y todo ello en virtud del artículo 17.7 del Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica básica de la Administración de la Comunidad Autónoma de Extremadura (DOE número 145, de 28 de julio).

Segundo. La seguridad de la información es el conjunto de medidas, tanto preventivas como reactivas, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, con el objetivo de mantener su confidencialidad, disponibilidad e integridad.

La Dirección del Organismo Pagador de los gastos financiados por los fondos europeos agrícolas FEAGA y FEADER de la Comunidad Autónoma de Extremadura (en adelante Organismo Pagador) es consciente de que la información es un activo esencial para el cumplimiento adecuado de sus competencias y asume, por ello, la Gestión de la Seguridad de la Información como una función clave para su protección frente a las amenazas que puedan afectarla, con el objeto del cumplimiento de sus objetivos, así como de la satisfacción de las condiciones adecuadas en la prestación de sus servicios.

En concreto, el Reglamento Delegado (UE) 2022/127 de la Comisión, de 7 de diciembre de 2021, que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro establece como uno de los requisitos para los Organismos Pagadores con un volumen superior a los 400 millones de euros anuales a que la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems Requirements (ISO) (Sistema de gestión de la seguridad de la información-Requisitos) (ISO).

De esta forma, con la presente encomienda se pretende garantizar que el Organismo Pagador cumpla los requisitos de seguridad de la información a través de un sistema de gestión de seguridad de la Información basado en el estándar UNE-ISO/IEC 27001, si bien en el marco de las políticas digitales y de seguridad corporativas de la administración autonómica.

Tercero. En virtud de las competencias de los distintos departamentos de la Junta de Extremadura, en la seguridad de los sistemas de información del Organismo Pagador concurren



varios órganos, el Organismo Pagador de los gastos financiados por los fondos europeos agrícolas FEAGA y FEADER, la Secretaría General de Transformación Digital y Ciberseguridad y la Dirección General de Digitalización de la Administración, por lo que, por razones de eficacia y competencia, es necesario establecer un sistema de organización y coordinación en dicho ámbito que facilite su realización.

Cuarto. La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece en su artículo 11 que la realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las entidades de Derecho Público podrá ser encomendada a otros órganos o entidades de Derecho Público de la misma o distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño.

Quinto. La Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura, en su artículo 75 regula la figura de la encomienda de gestión como instrumento para el ejercicio de competencia por los órganos de la Administración de la Comunidad Autónoma, estableciendo en sus apartados 3 y 4 que para la encomienda a órganos pertenecientes o dependientes de diferente Consejería será precisa la autorización por el Consejo de Gobierno, y servirá de instrumento de formalización, la resolución o acuerdo que la autorice.

En virtud de lo anterior, suscriben el siguiente Acuerdo:

CLÁUSULAS:

Primera. Objeto.

El presente Acuerdo tiene por objeto establecer las condiciones en las que la Consejería de Agricultura, Ganadería y Desarrollo Sostenible, como Organismo Pagador de los gastos correspondientes al FEAGA y al FEADER en la Comunidad Autónoma de Extremadura, encomienda a la Consejería de Economía, Empleo y Transformación Digital, por razones de eficacia y al no disponer de los medios técnicos, personales o materiales idóneos para su desempeño, la realización de las actividades de carácter material o técnico de su competencia descritas en los siguientes puntos, identificándose así como proveedor interno de servicios TIC del Organismo Pagador, y ello en el marco de lo dispuesto en el artículo 11 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector y 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.

Segunda. Naturaleza jurídica.

El presente acuerdo tiene naturaleza administrativa, rigiéndose en su aplicación e interpretación por su propio contenido y por las normas administrativas que le sirven de fundamento



jurídico, especialmente la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como por la Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura, sin perjuicio de las demás normas legales y reglamentarias, vigentes y aplicables. Las controversias que puedan surgir en la interpretación de lo acordado en el presente acuerdo de encomienda de gestión o de las normas aplicables al mismo, serán resueltas en el seno de la Comisión de Seguimiento.

La encomienda de gestión no supone cesión de la titularidad de las competencias ni de los elementos sustantivos de su ejercicio, atribuidos a la Consejería de Agricultura, Ganadería y Desarrollo Sostenible, como Organismo Pagador de los gastos correspondientes al FEAGA y al FEADER.

Es responsabilidad de la Consejería de Agricultura, Ganadería y Desarrollo Sostenible dictar los actos o resoluciones que den soporte o en los que se integre la concreta actividad material objeto de la presente encomienda de gestión.

Tercera. Actividades a las que afecta la encomienda de gestión.

Para el cumplimiento de las políticas y requisitos que conforman el marco normativo del sistema de gestión de seguridad de la información, basado en el estándar UNE-ISO/IEC 27001, la Consejería de Economía, Empleo y Transformación Digital, a través de la Dirección General de Digitalización de la Administración y la Secretaría General de Transformación Digital y Ciberseguridad, como centro directivo competente en materia de Tecnologías de la Información y la Comunicación en la Junta de Extremadura y conforme a lo regulado en el Decreto 77/2023, de 21 de julio, por el que se establece la estructura orgánica de la Consejería de Economía, Empleo y Transformación Digital, prestará los servicios tecnológicos necesarios para el normal funcionamiento del Organismo Pagador, observando los requisitos de seguridad que éste demande y motivados en el cumplimiento del estándar mencionado, para lo cual el Organismo Pagador aportará en el Comité de Gestión y Coordinación de Seguridad de la Información, de manera continua y actualizada, la información relativa al análisis de contexto y declaración de alcance, así como la documentación elaborada para la gestión de riesgos del OP. La prestación de servicios tecnológicos se llevará a cabo 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:
 - a) Implantación de los requisitos de seguridad.
 - b) Control de versiones y gestión del cambio.
 - c) Gestión de las vulnerabilidades.



2. Incidentes TIC, incluyendo las siguientes responsabilidades:
 - a) Detección y comunicación de incidentes de seguridad TIC
 - b) Análisis de los incidentes TIC.
 - c) Coordinación de las actividades de resolución.
3. Continuidad TI, incluyendo las siguientes responsabilidades:
 - a) Desarrollo y prueba de los planes de recuperación de los sistemas de información de soporte a la actividad del OP.
 - b) Gestión de las operaciones de copias de seguridad.
4. Seguridad en las comunicaciones, incluyendo las siguientes responsabilidades:
 - a) Securización de los perímetros de seguridad.
 - b) Operación y mantenimiento de la infraestructura de comunicaciones.
 - c) Aseguramiento de la continuidad de las comunicaciones.
5. Seguridad lógica de activos TIC, incluyendo las siguientes responsabilidades:
 - a) Mantenimiento del inventario TIC.
 - b) Gestión de las vulnerabilidades de las infraestructuras.
 - c) Administración de los dispositivos de gestión de acceso lógico.
 - d) Mantenimiento de la seguridad de los sistemas TIC que soportan los sistemas de información del OP.
 - e) Garantizar la segregación de entornos.
6. Protección contra código malicioso, incluyendo la responsabilidad de:
 - a) Gestión de la detección y mitigación frente a código malicioso.

Cuarta. Seguridad de la información y datos de carácter personal.

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 que se especifican en el anexo I adjunto serán de aplicación en el mismo momento de firma de la presente encomienda. No obstante, dichos acuerdos de nivel de servicio podrán ser modificados de conformidad con lo determinado en la cláusula quinta de este documento.

En la ejecución de los servicios descritos, tanto la Dirección General de Digitalización de la Administración como la Secretaría General de Transformación Digital y Ciberseguridad, estarán sujetas a las cláusulas de seguridad que se especifican en el anexo II – Cláusulas de Seguridad.

En todo caso, la Consejería de Economía, Empleo y Transformación Digital tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la presente encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal.

En el desarrollo del presente Acuerdo de Encomienda de gestión las partes adoptarán las medidas de seguridad requeridas por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como lo indicado en el Esquema Nacional de Seguridad (ENS) establecido en el Real Decreto 3/2010, de 8 de enero, y sus modificaciones; así como, aquella otra normativa reguladora de la protección de datos de carácter personal que sea de aplicación durante su vigencia.

Las partes se comprometen a cumplir la política de seguridad y confidencialidad de la información y a someterse a los sistemas de verificación establecidos, de acuerdo con la legislación que resulte aplicable en cada caso.

Quinta. Comisión de seguimiento.

Con el fin de articular la coordinación y el seguimiento de la ejecución de las medidas previstas en el presente Acuerdo de Encomienda de Gestión y proceder a su interpretación, se creará una Comisión de seguimiento integrada por:

- Presidente/a: La persona titular de la Jefatura de Servicio de Gestión de Recursos Humanos de la Consejería de Agricultura, Ganadería y Desarrollo Sostenible.
- Vocales:
 - La persona titular de la Jefatura de Servicio de Ayudas Sectoriales y Explotación Agraria de la Consejería de Agricultura, Ganadería y Desarrollo Sostenible.



- La persona titular del Servicio de la Dirección General de Digitalización de la Administración con competencias en el ámbito operativo de la Seguridad de la Información, o persona en quien delegue.
 - La persona titular del Servicio de la Dirección General de Digitalización de la Administración con competencias en materia de Protección de Datos y Seguridad de la Información, o persona en quien delegue.
 - La persona titular del Servicio de la Dirección General de Digitalización de la Administración con competencias en materia de desarrollo de sistemas de información agraria.
- Secretario/a: La persona responsable de Seguridad de la Información de Organismo Pagador de la Consejería de Agricultura, Ganadería y Desarrollo Sostenible.

Esta Comisión de seguimiento tendrá las siguientes funciones:

- 1) Seguimiento del cumplimiento de los acuerdos de niveles de servicio, para lo que la Dirección General de Digitalización de la Administración y/o Secretaría General de Transformación Digital y Ciberseguridad, realizará y remitirá a la Comisión de seguimiento el cálculo de los indicadores que miden los servicios prestados con los datos de los tres meses anteriores.
- 2) Poner en conocimiento de la Dirección del Organismo Pagador cualquier supuesto de ineficacia, desviación o tendencia que puedan afectar a la consecución de los objetivos de seguridad de la información establecidos por el Organismo Pagador y que hayan sido detectados durante el control de los acuerdos de nivel de servicio, con la finalidad de que aquella Dirección pueda convocar extraordinariamente al Comité de Gestión y Coordinación para la Seguridad de la Información. En su caso, consecuencia de lo anterior, la Comisión podrá acordar la modificación de los acuerdos de nivel de servicio y los indicadores necesarios que permitan evaluar el correcto cumplimiento.
- 3) Coordinar los trabajos para la consecución óptima del fin que se persigue.
- 4) Resolver cualquier discrepancia que se plantee en la interpretación y ejecución del acuerdo y de los diferentes instrumentos jurídicos, que para su aplicación dicten las partes.
- 5) Proponer la prórroga del acuerdo de encomienda de gestión.

La comisión se reunirá, al menos, trimestralmente, para evaluar el seguimiento de la encomienda.



En lo no contemplado por esta cláusula sobre el funcionamiento y actuaciones de la comisión, se estará a lo dispuesto por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, sobre órganos colegiados de las distintas administraciones públicas.

Sexta. Régimen económico.

Este acuerdo de encomienda de gestión no comporta obligaciones económicas entre las partes firmantes del mismo.

Séptima. Publicidad.

El presente acuerdo será publicado para su eficacia en el Diario Oficial de Extremadura, de conformidad con lo establecido en el artículo 11.3.a) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y el artículo 75.5 de la Ley 1/2002, de 28 de febrero, del Gobierno y de la Administración de la Comunidad Autónoma de Extremadura.

Octava. Plazo de vigencia.

El Acuerdo, actualmente en vigor, de 10 de junio de 2016 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, publicado en DOE núm. 132 de 11 de julio de 2016, continuará en vigor mientras existan actuaciones pendientes que necesiten de la cobertura de las actividades encomendadas en el período de programación FEADER 2014-2020.

La actual encomienda permanecerá vigente durante cuatro años desde su publicación, pudiendo prorrogarse por mutuo acuerdo de las partes, de conformidad con lo determinado en la cláusula quinta, por periodos sucesivos de hasta cuatro años.

Novena. Modificación y extinción.

Las partes podrán acordar por unanimidad la modificación de las cláusulas del presente acuerdo requiriéndose, para su eficacia, autorización del Consejo de Gobierno.

Para la extinción del presente acuerdo se requerirá autorización del Consejo de Gobierno, siendo causas de extinción del mismo las siguientes:

- Por mutuo acuerdo de las partes.
- Por incumplimiento grave por cualquiera de los firmantes de las concretas obligaciones asumidas en el mismo. En caso de incumplimiento por una de las partes de las obliga-



ciones y compromisos asumidos, la otra deberá comunicarlo a la Comisión de Seguimiento. La Comisión de Seguimiento, podrá requerir a la parte incumplidora para que, en el plazo máximo que a tal fin establezca, realice las actuaciones que le corresponden en virtud de la encomienda de gestión instrumentada por el presente Acuerdo. Si transcurrido el plazo indicado en el requerimiento persiste el incumplimiento, éste podrá considerarse como grave a efectos de declarar la extinción de este Acuerdo.

— Por la expiración del plazo de duración previsto en la cláusula octava.

Mérida, 5 de noviembre de 2024.

La Consejera de Agricultura, Ganadería y
Desarrollo Sostenible,
MERCEDES MORÁN ÁLVAREZ

El Consejero de Economía, Empleo y
Transformación Digital,
GUILLERMO SANTAMARÍA GALDÓN

**ANEXO I**

INDICADORES DE NIVEL DE SERVICIO

1. Servicio de seguridad en el desarrollo y mantenimiento de los sistemas de información.

[IND-026] Eficacia corrección de vulnerabilidades sistemas: [vulnerabilidades encontradas corregidas en plazo/vulnerabilidades encontradas]

- Valores: [0-1]
- Objetivo: $\geq 0,9$
- Frecuencia medición: Trimestral.

Observaciones: Se tiene en cuenta que la fecha máxima para la corrección esté en el periodo medido.
Tiempos de corrección:

- Críticas: 5 días.
- Graves: 15 días.
- Medio: 30 días.
- Leve: 60 días.

[IND-027] Pases a producción de sistemas seguros: [Pases de versiones mayores con escaneo de vulnerabilidades / Pases de versiones mayores]

- Valores: [0-1]
- Objetivo: $\geq 0,9$
- Frecuencia medición: Trimestral

Definición de versión mayor: La actualización que suponga la creación de una nueva base de datos.

- Se modifique el mecanismo de autenticación o de autorización que utiliza.
- Se realice una modificación sustancial en la aplicación o una ampliación de las funcionalidades de la misma que según la consideración del responsable de la aplicación lo haga ser versionado.
- La aplicación incorpore interacción con otras aplicaciones del Organismo Pagador que obliguen a establecer un paso de credenciales o de información a través de mecanismos web.
- La aplicación cambie de framework / plataforma de desarrollo o de ejecución.
- Se modifique la versión del motor de base de datos en la/s base de datos utilizada/s.
- Se modifique la versión del servidor de aplicaciones (WEB, CITRIX)
- Se modifique la versión del Sistema Operativo de los servidores que le dan soporte
- La aplicación incorpore una nueva librería externa a su desarrollo o una nueva versión de las mismas.
- Se corrija una vulnerabilidad específica de seguridad anteriormente detectada.
- Siendo la versión m.n, se entenderá como versión mayor el cambio de 'm'.



2. Servicio de gestión de Incidentes TIC.

[IND-028] Notificación Temprana de incidentes TIC: [Incidentes TIC notificados en tiempo/incidentes TIC totales]
<ul style="list-style-type: none">• Valores: [0-1]• Objetivo: $\geq 0,9$• Frecuencia medición: Trimestral.• Tiempo de notificación: 1 día. <p>Observaciones:</p> <ul style="list-style-type: none">• El plazo temporal se calcula desde el momento en el que el responsable TIC registra el incidente en su herramienta, hasta que lo comunica al Organismo Pagador.• Se tienen en cuenta únicamente los incidentes notificados al OP durante el periodo de medición.
[IND-029] Tiempo de resolución incidentes de seguridad: [Incidentes resueltos en plazo / Incidentes totales resueltos]
<ul style="list-style-type: none">• Valores: [0-1]• Objetivo: $\geq 0,9$• Frecuencia medición: Trimestral. <p>Observaciones:</p> <ul style="list-style-type: none">• El plazo temporal se inicia desde el momento en el que el incidente se notifica, hasta que se resuelve.• Se tendrán en cuenta los incidentes en estado "Resuelto" durante el periodo de medición.• Tiempos de resolución:<ul style="list-style-type: none">– Críticas: 5 días.– Graves: 15 días.– Medio: 30 días.– Leve: 60 días.
[IND-030] Eficacia y eficiencia de los Sistemas: [T50 + T90 / 2]
<ul style="list-style-type: none">• Valores: [0,1]• Objetivo: = 1• Frecuencia medición: Anual <p>Observaciones:</p> <ul style="list-style-type: none">• T50: Si tiempo empleado para cerrar el 50% de los incidentes < 15 días = 1• T90: Si tiempo empleado para cerrar el 90% de los incidentes < 45 días = 1 <p>Dicha información se recopila y se envía mediante el Informe INES,</p> <ul style="list-style-type: none">• El plazo temporal se inicia desde el momento en el que el incidente se notifica, hasta que se resuelve.• Se tendrán en cuenta los incidentes en estado "Resuelto" durante el periodo de medición.• También se remitirá el número total de incidentes tratados.



3. Servicio de gestión de continuidad TI.

[IND-031] Disponibilidad de SI: [Tiempo de indisponibilidad/Tiempo total]
<ul style="list-style-type: none">• Valores: [0,1]• Objetivo: $\leq 0,05$• Frecuencia medición: Trimestral

[IND-032] Eficacia sistema de copias: [copias con éxito/ copias planificadas]
<ul style="list-style-type: none">• Valores: [0,1]• Objetivo: $\geq 0,95$• Frecuencia medición: Anual

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

[IND-033] Disponibilidad de equipamiento crítico de red: [Tiempo activo/Tiempo total]
<ul style="list-style-type: none">• Valores: [0,1]• Objetivo: $\geq 0,999$• Frecuencia medición: Trimestral

[IND-033] Disponibilidad de equipamiento crítico de red: [Tiempo activo/Tiempo total]
<ul style="list-style-type: none">• Valores: [0,1]• Objetivo: $\geq 0,999$• Frecuencia medición: Trimestral

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

[IND-034] Eficacia corrección de vulnerabilidades infraestructura: [vulnerabilidades encontradas corregidas en plazo/vulnerabilidades encontradas]
<ul style="list-style-type: none">• Valores: [0-1]• Objetivo: $\geq 0,8$• Frecuencia medición: Trimestral
Observaciones:
<ul style="list-style-type: none">• Tiempos de corrección:<ul style="list-style-type: none">– Críticas: 5 días– Graves: 15 días– Medio: 30 días– Leve: 60 días

**[IND-035] Mantenimiento del inventario TIC: [Número de activos correctos/ total de activos revisados]**

- Valores: [0-1]
- Objetivo: ≥ 0.99
- Frecuencia medición: Trimestral

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

[IND-036] Despliegue efectivo de los sistemas de protección contra código malicioso: [Servidores con protección activa/Servidores totales]

- Valores: [0-1]
- Objetivo: $\geq 0,9$
- Frecuencia medición: Trimestral

Observaciones: Se entiende por protección activa aquellos con agente de red antivirus instalado y con BD de virus activa y actualizada.

[IND-037] Eficacia aplicación parches: [parches windows aplicados en equipamiento crítico/parches windows publicados totales]

- Valores: [0-1]
- Objetivo: $\geq 0,9$
- Frecuencia medición: Trimestral

Observaciones: Bajo criterios técnicos puede decidirse que un parche no tiene que ser aplicado. En este caso se justificará y no será tenido en cuenta en el cálculo del indicador.

NOTA: Este indicador se mide cada 2 meses, pero el informe se realiza cada 3 con lo que se tomará el valor del último cálculo disponible.

Para la anterior relación de indicadores se desarrollará y mantendrá actualizado el correspondiente manual del indicador que los defina conteniendo, a su vez, el procedimiento de recopilación de información, de cálculo, de medición de la efectividad del indicador correspondiente, así como el procedimiento y herramientas para el intercambio de información en este ámbito, lo cual se llevará a cabo por la Comisión de Seguimiento definida en la cláusula quinta del presente acuerdo.



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 al proveedor interno 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.

• • •

