

Contrato de Servicios (Expediente núm SV260405)			
Contrato sometido a las <a href="#">Instrucciones internas de contratación del grupo Correos</a>			
<input checked="" type="checkbox"/> Procedimiento general		<input type="checkbox"/> Procedimiento especial	
<input checked="" type="checkbox"/> Ordinario	<input type="checkbox"/> Simplificado	<input type="checkbox"/> Con invitación a un único licitador	<input type="checkbox"/> Con invitación a varios licitadores

## PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

1.	Entidad contratante.....	4
2.	Objeto del contrato.....	4
3.	Duración del contrato.....	5
4.	Aspectos económicos.....	6
5.	Condiciones de participación.....	6
6.	Licitación del contrato.....	9
6.1.	Comunicaciones y notificaciones electrónicas.....	9
6.2.	Resolución de consultas relacionadas con la licitación.....	9
6.3.	Envío de ofertas por medios electrónicos.....	10
6.4.	Documentación confidencial.....	10
6.5.	Adjudicación de los contratos.....	10
6.6.	Ofertas integradoras.....	11
6.7.	Contenido de las ofertas.....	11
7.	Adjudicación y perfección del contrato.....	12
7.1.	Procedimiento de apertura de sobres y valoración de ofertas.....	12
7.2.	Ofertas anormalmente bajas.....	13
7.3.	Documentación a presentar por el propuesto como adjudicatario.....	13
7.4.	Adjudicación del contrato.....	15
7.5.	Perfección del contrato.....	15
7.6.	Constitución de garantías.....	15
8.	Ejecución del contrato.....	17
8.1.	Obligaciones del adjudicatario.....	17
8.2.	Modificaciones del contrato.....	23

8.3. Cesión y Subcontratación. ....	24
9. Cumplimiento del contrato.....	25
9.1. Responsable del contrato. Representante del contratista. ....	25
9.2. Régimen de penalidades. ....	25
9.3. Abonos al contratista. Facturación. ....	26
9.4. Recepción y liquidación.....	28
9.5. Plazo de garantía.....	28
10. Resolución del contrato.....	28
10.1. Causas de resolución.....	28
10.2. Procedimiento .....	29
11. Protección de Datos.....	29
11.1. Cláusula informativa de protección de datos personales recabados a través del Canal Ético.....	29
11.2. Información a representantes, trabajadores y personas de contacto .....	30
12. Régimen jurídico del contrato y reclamaciones contra este pliego. ....	31
Anexo I.- Características técnicas específicas del contrato. ....	33
Anexo II.- Descripción y limitaciones a la licitación por lotes. ....	55
Anexo III.- Resumen de metodología seguida para el cálculo del valor estimado del contrato.....	56
Anexo IV.- Forma de acreditación de la solvencia económica y financiera, y técnica o profesional.....	57
Anexo V.- Modelo de aval. ....	58
Anexo VI.- Instrucciones y recomendaciones para la presentación electrónica de las ofertas. ....	59
Anexo VII.- Instrucciones para cumplimentar el DEUC. ....	60
Anexo VIII.- Criterios de adjudicación cuya evaluación depende de un juicio de valor. ....	63
Anexo IX.- Criterios de adjudicación de evaluación automática.....	64
Anexo X.- Modelo de proposición económica. ....	65
Anexo XI.- Información sobre condiciones de subrogación de contratos de trabajo. ....	66
Anexo XII.- Modificaciones previstas del contrato.....	67
Anexo XIII.- Régimen de penalidades. ....	68
Anexo XIV - Evaluación de Proveedores.....	71
Anexo XV.- Contrato de encargo de tratamiento de datos personales .....	72
Anexo XVI.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. ....	89
Anexo XVII.- Requisitos de seguridad.....	90

**ANEXO XVIII.- Compromiso de adscripción de personal al contrato. Declaración responsable..... 98**

La presentación de ofertas en el presente procedimiento supondrá la aceptación incondicionada de la totalidad de las cláusulas y condiciones del presente Pliego, sin salvedad o reserva alguna, sancionándose con la exclusión del procedimiento a los licitadores que introduzcan cualquier condicionante en sus ofertas que altere el régimen establecido.

### 1. Entidad contratante.

Entidad contratante	S.E. CORREOS Y TELÉGRAFOS, S.A., S.M.E.
Órgano de contratación	SECRETARÍA GENERAL Y DE POLÍTICAS PÚBLICAS Y DIRECCION FINANCIERA
Dirección/Subdirección gestora de la necesidad UGC	DIRECCIÓN DE ESTRATEGIA, SOSTENIBILIDAD Y MARCA Subdirección de Relaciones Internacionales y ESG UGC36
Perfil de contratante	<a href="https://www.correos.com/perfil-contratante/">https://www.correos.com/perfil-contratante/</a>
Dirección de contacto	C/ Conde de Peñalver,19 Bis. 28006, Madrid.
Responsable del contrato	Dirección/Subdirección/ Área: Subdirección de Relaciones Internacionales y ESG
	Datos de contacto: <a href="mailto:sostenibilidad@correos.com">sostenibilidad@correos.com</a>

### 2. Objeto del contrato.

El objeto del contrato consistirá en la ejecución, en la forma descrita en el [Anexo I](#) relativo a sus características técnicas, de las prestaciones que a continuación se describen:

Descripción	Contratación de un servicio para el diseño, desarrollo e implementación de un sistema integral, robusto y auditable dentro de la Sociedad Estatal Correos y Telégrafos S.A., S.M.E., destinado a la cuantificación y reporte de las emisiones de Gases de Efecto Invernadero (GEI) generadas por las operaciones logísticas de Correos a lo largo de toda su cadena logística extremo a extremo (E2E), conforme a la norma ISO 14083:2023 y a la metodología establecida en el Marco GLEC v3.2, de acuerdo con las obligaciones establecidas en el Anexo I.
Código CPV	90714200-7 Servicios de auditoría medioambiental de empresas 90714100-6 Sistemas de información medioambiental
Lotes	<input checked="" type="checkbox"/> NO <input type="checkbox"/> SI (Ver <a href="#">Anexo II</a> ) Justificación de la no división en Lotes: El servicio objeto del contrato es único, y se ejecuta de forma conjunta y global. La correcta ejecución del contrato implica la necesidad de coordinar la ejecución de las diferentes

	prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes. Por ello y, al amparo de lo previsto en el artículo 99.3.b) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público se justifica la no división en lotes para este expediente.
¿Se admite oferta integradora (lotes)?	<input checked="" type="checkbox"/> NO <input type="checkbox"/> SI (Ver <a href="#">condiciones</a> )

La participación en esta licitación se encuentra reservada a:

<input type="checkbox"/>	Centros Especiales de Empleo de iniciativa social
<input type="checkbox"/>	Empresas de Inserción Social
<input checked="" type="checkbox"/>	No aplica

### 3. Duración del contrato.

El contrato se ejecutará en los términos, plazos y condiciones temporales que se expresan a continuación:

	Cantidad	Unidad de tiempo	Cómputo
Duración inicial	1	<input type="checkbox"/> días <input type="checkbox"/> meses <input checked="" type="checkbox"/> años	<input type="checkbox"/> día siguiente a la firma de aceptación de la Resolución de adjudicación <input type="checkbox"/> día siguiente a la comunicación de inicio del contrato por la entidad contratante <input checked="" type="checkbox"/> la fecha que figure en la resolución de adjudicación
Prorrogable	<input checked="" type="checkbox"/> NO <input type="checkbox"/> SI	Nº de prórrogas:	
En caso de acordarse, la prórroga será obligatoria para el contratista, siempre y cuando se le notifique con dos meses de antelación al vencimiento. Se condiciona la prórroga del contrato a que sus características permanezcan inalterables.			

#### 4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

<b>Valor estimado del contrato</b>	<b>60.000,00 €</b>	Sesenta mil euros, conforme al método de cálculo especificado en <a href="#">Anexo III</a>	
Presupuesto base de licitación	72.600,00 €	IVA/impuesto equivalente	12.600 €
Anualidades (IVA o impuesto indirecto equivalente incluido)	2026	2027	<b>Total</b>
	54.450,00 €	18.150,00 €	<b>72.600,00 €</b>

#### 5. Condiciones de participación.

Los licitadores deberán cumplir, en el momento de finalizar el plazo de presentación de ofertas, y subsistir en el momento de perfección del contrato, los siguientes requisitos de participación.

Dispensa de acreditar aptitud, solvencia y capacidad	<input type="checkbox"/> SI	<input type="checkbox"/> Contratistas que hubiesen resultado adjudicatarios de contratos en los dos últimos años, hubiesen acreditado entonces su aptitud y solvencia en contratos de similar naturaleza, y no hubieran cambiado sus circunstancias.
	<input checked="" type="checkbox"/> NO	
Habilitación profesional	No aplica	
Solvencia económica o financiera	<input checked="" type="checkbox"/> Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, de al menos 60.000,00 €. <input type="checkbox"/> Otros: ... Sobre la forma de acreditar estos requisitos, ver <a href="#">Anexo IV</a>	
Solvencia técnica o profesional	<input checked="" type="checkbox"/> Haber realizado servicios de igual o similar naturaleza a los que constituyen el objeto del contrato en los tres últimos años, cuyo importe anual acumulado en el año de mayor ejecución sea igual o superior al 70 por ciento de la anualidad media del contrato (42.000 €).  <input checked="" type="checkbox"/> Acreditación del cumplimiento de las siguientes medidas de gestión medioambiental:	

	<ul style="list-style-type: none"> <li>- Los licitadores deberán contar con sistemas de gestión medioambiental basados en las normas europeas o internacionales sobre esta materia (ISO 14001 o EMAS o equivalentes), certificados por organismos independientes acreditados por una entidad perteneciente a IAF y aplicables a la prestación del servicio objeto del contrato.</li> </ul> <p><input checked="" type="checkbox"/> Otros:</p> <ul style="list-style-type: none"> <li>- Disponer de certificación ISO 27001 o equivalente en materia de seguridad de la información.</li> <li>- Certificación Smart Freight Centre (SFC) o equivalente.</li> </ul> <p>Para considerar una acreditación equivalente a una normativa, -como ISO, o UNE-, esta acreditación debe implicar que el licitador ha realizado una auditoría. ejecutada por terceros reconocidos e independientes. y cuya superación genera la documentación pertinente.</p> <p>Sobre la forma de acreditar estos requisitos, ver <a href="#">Anexo IV</a></p>
<p>Adscripción de medios</p>	<p><input checked="" type="checkbox"/> Sí. Medios a adscribir:</p> <ul style="list-style-type: none"> <li>- <b>Director de proyecto:</b> será el responsable de la correcta ejecución del contrato y actuará como interlocutor principal entre el adjudicatario y Correos. Será la figura encargada de la planificación, coordinación y supervisión de las actividades incluidas en el alcance del contrato, asegurando el cumplimiento de los plazos, la calidad técnica de los trabajos y la adecuación de los entregables a los requisitos establecidos en el presente pliego. Así mismo, será responsable de la gestión de riesgos, incidencias y posibles desviaciones, de la coordinación del equipo técnico adscrito al contrato y de la validación final de los entregables antes de su presentación a Correos. Deberá de participar en las reuniones de seguimiento y facilitar información sobre el estado del avance del proyecto. El Director o Directora deberá de contar con 3 años de experiencia en proyectos similares.</li> <li>- <b>Técnico/Consultor de Huella de Carbono:</b> Será el responsable del diseño metodológico del cálculo de</li> </ul>

	<p>Huella de Carbono y de la correcta aplicación e implantación de la norma ISO 14083:2023 y del Marco GLEC v3.2 o equivalentes a los procesos de Correos. Deberá definir los límites de cálculo, los criterios de asignación y reparto de emisiones, la selección y validación de los factores de emisión entre otros. Así mismo, será el responsable de analizar los procesos logísticos y de las fuentes de datos necesarias para el cálculo, colaborando con Correos en la identificación de datos primarios, modelizados o por defecto, y en la definición de metodologías de estimación cuando resulte necesario. Prestará soporte técnico en la revisión y elaboración de informes de emisiones, así como en los procesos de verificación de auditoría externa del cálculo de la Huella de Carbono. El técnico deberá de contar con 3 años de experiencia en proyectos similares.</p> <ul style="list-style-type: none"><li>- <b>Técnico/Consultor de datos y reporte:</b> el técnico será el responsable de la integración, tratamiento y modelización de los datos necesarios para el cálculo de la Huella de Carbono, así como de la configuración y generación de los informes derivados del cálculo. Se encargará de gestionar las distintas fuentes de datos de actividad, asegurando su correcta integración con la metodología definida. Entre sus funciones se incluirá la configuración de los informes y outputs de la herramienta de cálculo, garantizando que estos sean flexibles y configurables conforme a los requerimientos de Correos y de los distintos clientes, así como la implementación de mecanismos de trazabilidad y métricas de calidad del dato. Así mismo, dará soporte a la automatización de los procesos de cálculo y reporte y colaborará en la adaptación de los informes a distintos esquemas de presentación y niveles de agregación. El técnico deberá de contar con 3 años de experiencia en proyectos similares.</li><li>- <b>Técnico encargado del mantenimiento y soporte de la herramienta:</b> será el responsable de asegurar el correcto funcionamiento, disponibilidad y continuidad operativa de la solución tecnológica utilizada para el cálculo y reporte de la Huella de</li></ul>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Carbono durante toda la vigencia del contrato. Asumirá tareas de mantenimiento correctivo de la herramienta y gestionará las incidencias técnicas que surjan durante el desarrollo e implementación de la herramienta. Será el responsable de la actualización de parámetros y factores de emisión cuando proceda, del soporte técnico de usuarios autorizados y de la implementación de los ajustes funcionales necesarios para garantizar el adecuado funcionamiento de la herramienta. El técnico deberá de contar con 3 años de experiencia en proyectos similares.</p> <p><input type="checkbox"/> No.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Se exime a los licitadores de la obligatoriedad de presentar los medios que acrediten su solvencia en el caso de que presenten su inscripción en el Registro Oficial de Licitadores y Empresas Clasificadas del Estado.

En dicha inscripción en el Registro Oficial de Licitadores y Empresas Clasificadas del Estado deben constar todos los datos relativos a su capacidad, solvencia económica-financiera y técnica o profesional, representación y habilitaciones exigidos en este pliego, haciendo constar, además, que no se hallan incurso en prohibición para contratar, comprometiéndose a poner a disposición del Órgano de Contratación, en cualquier momento, cuando así fuese requerido, la documentación justificativa de las indicadas circunstancias.

## 6. Licitación del contrato.

### 6.1. Comunicaciones y notificaciones electrónicas.

Sin perjuicio de la publicidad que pueda acordarse de determinadas actuaciones las comunicaciones y notificaciones a los licitadores se realizarán a través de la Plataforma de Contratación de Correos (<https://pcc.correos.es/licitacion/licitaciones>), utilizando para los avisos la dirección de correo electrónico que el licitador hubiera facilitado para su registro en dicha Plataforma.

### 6.2. Resolución de consultas relacionadas con la licitación.

Las dudas o consultas relacionadas con la interpretación del contenido de este Pliego se realizarán obligatoriamente a través de la Plataforma de Contratación de Correos (<https://pcc.correos.es/licitacion/licitaciones>), siendo éste el único canal mediante el que serán atendidas.

Los licitadores, podrán subir sus preguntas a la Plataforma de Contratación de Correos hasta un (1) día hábil antes de la finalización del plazo para la presentación de ofertas.

### 6.3. Envío de ofertas por medios electrónicos.

El plazo de presentación de ofertas será de 10 días hábiles a contar desde el día siguiente a aquél en que se publique el anuncio de licitación en el perfil de contratante.

Los licitadores, a excepción del Procedimiento Especial con un único licitador, deberán presentar obligatoriamente sus ofertas de forma electrónica a través de la Plataforma de Contratación de Correos (<https://pcc.correos.es/licitacion/licitaciones>) utilizando para ello la “Herramienta de Preparación y Presentación de Ofertas” que desde esa plataforma se pone a su disposición (ver instrucciones y recomendaciones en [Anexo VI](#)).

### 6.4. Documentación confidencial.

Los licitadores, al tiempo de presentar su oferta, indicarán expresamente qué documentos (o parte de los mismos) o datos, de los incluidos en las ofertas, tienen la consideración de «confidenciales», sin que resulten admisibles las declaraciones genéricas de confidencialidad de todos los documentos o datos de la oferta. La condición de confidencial deberá reflejarse claramente (sobreimpresa, al margen, o de cualquier otra forma claramente identificable) en el propio documento que tenga tal condición, señalando además los motivos que justifican tal consideración. No se considerarán confidenciales documentos o datos que no hayan sido expresamente calificados como tales por los licitadores.

### 6.5. Adjudicación de los contratos

#### 6.5.1. Procedimiento General Ordinario sin negociación

Único Criterio de Adjudicación: MEJOR RELACIÓN COSTE-EFICACIA.

Pluralidad de Criterios de Adjudicación: MEJOR RELACIÓN CALIDAD-PRECIO. La puntuación final estará compuesta por la suma de la puntuación asignada en los criterios de adjudicación que, en todo caso, serán evaluables mediante la mera aplicación de fórmulas matemáticas.

Tipología	Criterio	Ponderación
Criterios evaluables automáticamente ( <a href="#">Anexo IX</a> )		
	Económico	100%

## 6.6. Ofertas integradoras.

No aplica

## 6.7. Contenido de las ofertas.

### 6.7.1. Sobre 1: documentación administrativa.

- a) Documento Europeo Único en materia de Contratación (DEUC). Cumplimentado conforme a las indicaciones contenidas en el [Anexo VII](#), firmado por el licitador o su representante.
- b) En su caso, compromiso de adscripción de medios, según lo indicado en el Apartado 5.
- c) Compromiso de constitución de Unión Temporal de Empresarios (UTE), en su caso. Cuando dos o más empresas acudan a una licitación con el compromiso de constituirse en Unión Temporal, se deberá aportar una declaración indicando los nombres y circunstancias de los empresarios que la suscriban, la participación de cada uno de ellos y que asumen el compromiso de constituirse formalmente en Unión Temporal, caso de resultar adjudicatarios. El citado documento deberá estar firmado por los representantes de cada una de las Empresas componentes de la Unión. En estos casos cada una de las empresas deberá presentar su propio Documento Europeo Único en materia de Contratación (DEUC) a que se refiere el apartado a).
- d) En su caso, declaración de que la empresa a la que representa pertenece a un grupo empresarial, con indicación de las sociedades que forman parte del mismo
- e) Las empresas no españolas deberán aportar declaración de que se somete a la Jurisdicción de los Juzgados y Tribunales españoles de cualquier orden, para todas las incidencias que de modo directo o indirecto pudieran surgir del contrato, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponder al licitador.
- f) Las empresas de Estados que no sean miembros de la Unión Europea o signatarios del Acuerdo sobre el Espacio Económico Europeo deberán aportar un informe que acredite su capacidad de obrar, expedido por la Misión Diplomática Permanente u Oficina Consular de España del lugar del domicilio de la empresa, en el que se haga constar, previa acreditación por la empresa, que figuran inscritas en el Registro local profesional, comercial o análogo o, en su defecto que actúan con habitualidad en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.
- g) Otra documentación:

- Aquella documentación de carácter técnico (sin referencias a aspectos económicos) que los licitadores consideren necesaria para la exposición de su propuesta. Dicha documentación deberá incluir al menos:
  - Solución técnica propuesta: descripción de la solución técnica propuesta que acredite el cumplimiento de los requisitos establecidos en el Anexo I del presente Pliego de Condiciones Técnicas y Particulares, de forma que se detalle cada uno de los aspectos del servicio demandados en la presente contratación. Asimismo, la propuesta deberá incluir los recursos técnicos asignados, tanto a nivel cualitativo como cuantitativo, para dar respuesta a todos los requerimientos y condiciones de ejecución.
- **Cuestionario para la privacidad de Proveedores: Anexo XIX: Declaración responsable protección de datos personales**

**6.7.2. Sobre 2: oferta técnica y criterios de adjudicación cuya evaluación depende de un juicio de valor.**

**NO APLICA**

**6.7.3. Sobre 3: Criterios de adjudicación de evaluación automática o con arreglo a fórmulas matemáticas y/o proposición económica.**

Los criterios de adjudicación de evaluación automática y/o con arreglo a fórmulas serán los establecidos en el [Anexo IX](#).

La proposición económica se ajustará al modelo que se incluye como [Anexo X](#).

La documentación que incluya los valores de los criterios de adjudicación cuya evaluación puede realizarse de manera automática deberá presentarse en archivo electrónico, en una o varias carpetas, comprimidas si no es posible por tamaño, con el nombre "SOBRE N° 3" en archivo ejecutable con formatos \*.pdf, \*.doc, \*.docx, \*.xls, \*.xlsx, \*.odt, \*.ods).

Sin perjuicio de la posibilidad de solicitar la pertinente aclaración de ofertas, no se aceptarán aquellas que tengan omisiones o errores que impidan conocer claramente sus términos esenciales.

## **7. Adjudicación y perfección del contrato.**

### **7.1. Procedimiento de apertura de sobres y valoración de ofertas.**

Una vez concluido el plazo de presentación de ofertas, se procederá a la apertura de la documentación administrativa presentada por los licitadores, verificándose que constan los documentos requeridos, o en caso contrario, procediendo a solicitar su subsanación para que el licitador presente la documentación requerida en el plazo de 3 días hábiles.

La evaluación de las ofertas conforme a los criterios cuantificables mediante la mera

aplicación de fórmulas se realizará, en su caso, tras efectuar previamente la de aquellos otros criterios en que no concurra esta circunstancia.

En su caso, técnicamente las ofertas presentadas se considerarán aptas o no, en virtud de que cumplan con todos los requisitos exigidos en el presente pliego. La evaluación de las ofertas se realizará en acto interno, pudiendo desecharse las ofertas técnicamente inadecuadas o que no garanticen adecuadamente con su oferta la correcta ejecución del contrato.

Una vez recibidas y tras la apertura de sobres, se valorarán y posteriormente se otorgará la mayor puntuación a la mejor oferta y las demás ofertas se puntuarán de forma proporcional a la de mayor puntuación.

Una vez valoradas las ofertas, se remitirá al órgano de contratación la correspondiente propuesta de clasificación y de adjudicación, en la que figurarán ordenadas las ofertas de forma decreciente, incluyendo la puntuación otorgada a cada una en aplicación de los criterios de adjudicación e identificando la mejor oferta puntuada.

## 7.2. Ofertas anormalmente bajas.

Para la identificación de ofertas anormalmente bajas se atenderá a los siguientes parámetros:

<input checked="" type="checkbox"/>	Se considerará que una proposición económica es anormalmente baja cuando incluya un porcentaje de baja que, respecto de la media aritmética de los porcentajes de baja de todas las ofertas admitidas, o del presupuesto de licitación en caso de licitador único, exceda de diez unidades porcentuales.
<input type="checkbox"/>	Otra...

En los casos en que se identifique una oferta anormalmente baja se solicitará al licitador su justificación por escrito de forma razonada y detallada, en un plazo de 5 días hábiles. Si transcurrido este plazo no se hubiera recibido dichas justificaciones, se entenderá que la empresa licitadora ha retirado su oferta.

A la vista de la justificación de la oferta, la entidad contratante decidirá sobre su aceptación o rechazo. En el caso de rechazarse, se propondrá la adjudicación en favor del siguiente mejor, sin realizar una nueva clasificación.

En el caso de que una de las ofertas consideradas *a priori* como anormalmente bajas resulte adjudicataria el licitador deberá constituir una garantía complementaria si así se hubiera contemplado.

## 7.3. Documentación a presentar por el propuesto como adjudicatario.

Al licitador que haya presentado la mejor oferta se le requerirá para que en el plazo de

10 días hábiles a contar desde el siguiente a aquel en el que haya recibido el requerimiento, presente la siguiente documentación original o copias compulsadas:

<input checked="" type="checkbox"/>	Los que acrediten la personalidad del empresario y su ámbito de actividad.
<input checked="" type="checkbox"/>	Los que acrediten la representación.
<input checked="" type="checkbox"/>	Resguardo de haber constituido la garantía definitiva y, en su caso, complementaria.
<input type="checkbox"/>	En el caso de contratos reservados, documentación que acredite oficialmente su condición como entidad que le faculta para resultar adjudicataria del contrato reservado.
<input type="checkbox"/>	Los que acrediten disponer de la habilitación empresarial o profesional para la realización de la prestación objeto de contrato.
<input checked="" type="checkbox"/>	Documentos que acrediten su solvencia económica, financiera y técnica o profesional por los medios que se especifiquen en el <a href="#">Anexo IV</a> . La acreditación de la solvencia mediante medios externos exigirá demostrar que para la ejecución del contrato dispone efectivamente de esos medios mediante la exhibición del correspondiente documento de compromiso de disposición.
<input checked="" type="checkbox"/>	Acreditación de la inexistencia de deudas tributarias y con la Seguridad Social, mediante la presentación de los correspondientes certificados emitidos por los organismos competentes.
<input checked="" type="checkbox"/>	Los que acrediten la efectiva disposición de los medios que se exijan adscribir a la ejecución o, en su caso, se hubiesen comprometido a dedicar a la ejecución del contrato.
<input checked="" type="checkbox"/>	Cuando se ejerzan actividades sujetas al Impuesto sobre Actividades Económicas: Alta, referida al ejercicio corriente, o último recibo, junto con una declaración responsable de no haberse dado de baja en la matrícula del citado Impuesto o, en su caso, declaración responsable de encontrarse exento.
<input checked="" type="checkbox"/>	Declaración relativa al lugar en el que estarán los servidores en los que se almacenan datos personales y desde dónde se van a prestar los servicios asociados a los mismos, (Esta declaración deberá presentarse con carácter previo cada vez que se producen cambios en las anteriores circunstancias).
<input checked="" type="checkbox"/>	Contrato de Encargo de Tratamiento de Datos, conforme al modelo consignado en el <a href="#">Anexo XV</a> .
<input checked="" type="checkbox"/>	Declaración responsable sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
<input checked="" type="checkbox"/>	Otros: documentación de carácter técnico que los licitadores consideren necesaria para la exposición de su propuesta

En los supuestos en que la propuesta de adjudicación de un contrato recaiga sobre una

unión de empresarios o sobre una agrupación de estos con el compromiso de constituir una sociedad, el plazo para presentar la documentación será de veinte días hábiles.

De no cumplimentarse adecuadamente el requerimiento en el plazo señalado por causas imputables al contratista, se entenderá que el licitador ha retirado su oferta. En tal supuesto, se procederá a recabar la misma documentación al licitador siguiente, por el orden en que hayan quedado clasificadas las ofertas.

Una vez presentada la documentación, se verificará que el propuesto como adjudicatario cumple los requisitos de participación exigidos.

#### **7.4. Adjudicación del contrato.**

Una vez adoptado, el acuerdo de adjudicación se notificará al adjudicatario y al resto de los licitadores, y se publicará en el perfil de contratante.

#### **7.5. Perfección del contrato.**

El contrato quedará perfeccionado con su adjudicación. La formalización se realizará mediante la firma de aceptación por el contratista de la resolución de adjudicación donde ha de constar de forma expresa la fecha de inicio del contrato.

Si se tratara de una UTE, su representante deberá presentar ante el órgano de contratación la escritura pública de su constitución, CIF asignado y nombramiento de representante con poder suficiente.

Cuando por causas imputables al adjudicatario no se hubiese formalizado el contrato dentro del plazo de 5 días hábiles desde notificación de la adjudicación, el contrato quedará automáticamente resuelto y se adjudicará al siguiente licitador por el orden en que hubieran quedado clasificadas las ofertas, previa presentación de la documentación establecida para los propuestos como adjudicatarios.

Si el adjudicatario desea que el contrato se formalice en documento público podrá solicitarlo corriendo con los gastos que se deriven de ello y facilitando una copia de la escritura a la entidad contratante.

La formalización de los contratos deberá asimismo publicarse en el perfil de contratante.

#### **7.6. Constitución de garantías.**

RÉGIMEN DE GARANTÍAS		
Constitución de garantía definitiva	<input checked="" type="checkbox"/> 5% del importe de adjudicación del contrato o el	Si el licitador la constituye mediante aval, deberá utilizar el modelo incluido como <a href="#">Anexo V</a> . Si utiliza otro medio,

	lote o lotes adjudicados (IVA excluido)		consultará las condiciones que debe reflejar el documento de constitución con la entidad contratante.  Además de por la correcta ejecución del contrato, la garantía definitiva responderá de los daños y perjuicios que se ocasionen a la entidad contratante y de los gastos que puedan derivarse de las reclamaciones fehacientes de cumplimiento o ejecución de las garantías, así como por los restantes conceptos indicados en el artículo 110 de la LCSP.
Constitución de garantía complementaria	<input type="checkbox"/> NO <input checked="" type="checkbox"/> SI	Importe	<input checked="" type="checkbox"/> 5% sobre el importe de adjudicación (en caso de oferta temeraria). (IVA excluido) <input type="checkbox"/> Otros: ....
Constitución de garantía provisional	<input checked="" type="checkbox"/> NO <input type="checkbox"/> SI	Importe	3% del Presupuesto Base de Licitación (IVA excluido)
<p>Cuando varíe el importe del contrato por cualquier causa, el contratista vendrá obligado a ajustar el importe de las garantías constituidas en la proporción que corresponda en el plazo de 10 días hábiles desde que se le notifique la causa determinante de la variación del importe del contrato. De no cumplirse este requisito por causas imputables al contratista en el plazo establecido, la entidad contratante podrá resolver el contrato, con pérdida de la garantía que tuviera constituida el contratista.</p> <p>En el caso de que se impongan penalidades al contratista y deban hacerse efectivas contra la garantía definitiva constituida, el adjudicatario quedará obligado a reponer esta garantía en los diez días hábiles siguientes a que se comunique la ejecución de la garantía inicial.</p>			

La empresa adjudicataria deberá depositar la correspondiente garantía definitiva a favor del órgano de contratación que haya promovido la licitación. En el caso de que una de las ofertas consideradas a priori como anormalmente bajas resulte adjudicataria, el licitador deberá constituir una garantía complementaria.

El contratista dispondrá de 10 días hábiles para la constitución de la garantía definitiva y, cuando corresponda, complementaria.

Al licitador que presente la mejor oferta le será requerido el resguardo de la garantía definitiva procedente con carácter previo a la adjudicación del contrato.

En caso de no constituir la garantía definitiva en el plazo señalado al efecto, se entenderá que el licitador ha retirado su oferta y se procederá a la adjudicación del licitador siguiente por el orden en que hayan quedado clasificado las ofertas.

## 8. Ejecución del contrato.

### 8.1. Obligaciones del adjudicatario.

#### 8.1.1. Obligaciones en materia fiscal, laboral y medioambiental.

Serán de cuenta del contratista todos los tributos de cualquier índole que graven las operaciones necesarias para la ejecución del contrato y cualquier otra que resulte de aplicación según las disposiciones vigentes. En este sentido, tanto en las ofertas que formulen los licitadores como en las propuestas de adjudicación, se entenderán comprendidos, a todos los efectos, los tributos de cualquier índole que graven los diversos conceptos, excepto el Impuesto sobre el Valor Añadido, que será repercutido como partida independiente de acuerdo con la legislación vigente.

El adjudicatario del contrato cumplirá con las condiciones salariales de los trabajadores conforme al Convenio Colectivo sectorial de aplicación. El personal que el adjudicatario deba contratar para atender sus obligaciones dependerá exclusivamente de este, sin que a la extinción del contrato pueda producirse en ningún caso la consolidación de las personas que hayan realizado los trabajos como personal de la entidad contratante.

Para la ejecución de este contrato:

SI procede la subrogación de trabajadores (ver información sobre condiciones de subrogación en [Anexo XI](#))

NO procede subrogación de trabajadores

En el caso de que, debido a actuaciones u omisiones de la empresa, de sus contratistas o subcontratistas, la entidad contratante fuese sancionada por incumplimientos de las disposiciones vigentes en materia laboral, de seguridad social, de integración social de personas con discapacidad, de prevención de riesgos laborales, de protección del medio ambiente o cualesquiera otra que resulten de aplicación en ejecución del contrato, bien en exclusiva o con carácter solidario, el adjudicatario abonará a la entidad contratante la cantidad que resulte de dicha sanción, al primer requerimiento, y sin perjuicio de las acciones legales que posteriormente le pudieran corresponder.

### **8.1.2. Obligaciones relativas a la gestión de permisos, licencias y autorizaciones.**

El contratista estará obligado, salvo que el órgano de contratación decida encargarse directamente y así se lo haga saber de forma expresa, a gestionar los permisos, licencias y autorizaciones establecidas en las ordenanzas municipales y en las normas de cualquier otro organismo público o privado que sean necesarias para el inicio y ejecución del servicio, solicitando de la entidad contratante los documentos que para ello sean necesarios.

### **8.1.3. Obligaciones del adjudicatario en materia de protección de datos.**

La empresa que resulte adjudicataria se compromete a adoptar las medidas legales, organizativas y técnicas que resulten necesarias para dar cumplimiento a la normativa de protección de datos. En este sentido:

1. Si el desarrollo del servicio objeto de licitación implicase un acceso del adjudicatario a los datos de carácter personal de los que la entidad contratante resulte Responsable del Tratamiento el adjudicatario, en calidad de Encargado del Tratamiento, se compromete a firmar un Contrato de Acceso a Datos por cuenta de la Entidad contratante debiendo ajustarse al modelo que se incorpora como Anexo XV del presente Pliego, cumpliendo con las exigencias previstas en la normativa de protección de datos vigente y, entre otras, recoja el compromiso del adjudicatario a:

- Llevar a cabo del tratamiento de datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular el RGPD y la LOPDGDD.

- Actuar sujeto a las instrucciones que, en cada momento, le indique la entidad contratante y no utilizar los datos con una finalidad distinta a la prestación del Servicio al que se hace referencia en el presente Pliego.

- Adoptar todas aquellas

- medidas técnicas y organizativas que resulten necesarias para garantizar un nivel de seguridad adecuado, guardar bajo su control y custodia los datos personales suministrados por la entidad contratante y no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas.

- No subcontratar ninguna de las prestaciones que formen parte del objeto de este Pliego que comporten el tratamiento de datos personales o realizar Transferencias Internacionales de Datos, salvo previa autorización expresa y otorgada por escrito por parte de la entidad contratante.

- Asistir a la entidad contratante en la realización de los análisis de riesgo, la presentación de consultas previas a la AEPD, en el proceso de notificación de violaciones de seguridad y de respuesta a solicitudes de derechos.

- Mantener secreto y confidencialidad respecto de los datos personales a los que

acceda y garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que les informará convenientemente.

- Poner a disposición de la entidad contratante toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como permitir la realización de auditorías con acceso físico directo a sus instalaciones o los subcontratistas autorizados y colaborar activamente en su desarrollo.

- Poner a disposición de la entidad contratante, con carácter previo a la formalización del Contrato, una declaración escrita que contenga la información acerca de

- (i) La ubicación de los servidores en los que se almacenarán los datos personales tratados por cuenta de la entidad contratante; y

- (ii) Lugar de prestación de servicios objeto la licitación.

- Si fuera necesario subcontratar los servidores o los servicios asociados a los mismos, el adjudicatario reflejará esta circunstancia en su oferta, junto con el nombre completo del subcontratista o, en su defecto, la referencia al perfil empresarial del mismo, definido por referencia a las condiciones de solvencia profesional o técnica del mismo.

- Comunicará a la entidad contratante cualquier cambio que se produzca con respecto a los términos y condiciones en los que accederá y tratará los datos personales por cuenta de la entidad contratante, y especialmente aquellas relacionadas con la información presentada en la declaración previa recogida en el punto octavo de la presente cláusula.

- En caso de incumplimiento: Responder de los daños y perjuicios que pudiesen ocasionarse y, en especial, de las sanciones que les pudiera imponer la Agencia Española de Protección de Datos o cualquier otro órgano competente ya sea español o europeo, como consecuencia del incumplimiento de las obligaciones establecidas en el presente Pliego.

#### **8.1.4. Aceptación y adhesión a las políticas de prevención de imputaciones delictivas.**

La empresa adjudicataria vendrá obligada a contar con una política propia de prevención de imputaciones delictivas similar a la establecida por la entidad contratante, o directamente adherirse a los procedimientos y políticas internas implantados por la misma. A estos efectos, la empresa adjudicataria podrá consultar el Código General de Conducta para el correcto cumplimiento del mismo que aparece en el documento “programa de prevención de riesgos penales” accesible a través de la web:

<https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS->

[Codigo-General-de-Conducta.pdf](#)

### 8.1.5. Evaluación de proveedores.

Durante la ejecución del contrato se realizará una evaluación continua del proveedor en materia de cumplimiento de las condiciones del contrato. Los parámetros sobre los que se realizará dicha evaluación se encuentran definidos en el [Anexo XIV](#).

### 8.1.6. Obligaciones esenciales del contrato.

Tendrán la consideración de obligaciones esenciales del contrato cuyo incumplimiento constituirá -en todo caso- causa de resolución, las siguientes:

<input checked="" type="checkbox"/>	Mantenimiento de adscripción de medios personales o materiales
<input checked="" type="checkbox"/>	Condiciones especiales de ejecución del contrato
<input checked="" type="checkbox"/>	Aspectos que se hayan considerado como criterios de adjudicación
<input type="checkbox"/>	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
<input checked="" type="checkbox"/>	El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento “programa de prevención de riesgos penales” accesible a través de la web <a href="https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREO S-Codigo-General-de-Conducta.pdf">https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREO S-Codigo-General-de-Conducta.pdf</a>
<input checked="" type="checkbox"/>	Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia.
<input checked="" type="checkbox"/>	El sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 LCSP.
<input type="checkbox"/>	Otras:

El cumplimiento de dichas condiciones será exigible durante la vida del contrato, el control que Correos ejercerá para velar por ese cumplimiento será el siguiente:

Condición esencial	Frecuencia	Forma de acreditación del cumplimiento
Mantenimiento de adscripción de medios personales o materiales	Mensual	Mediante reunión de seguimiento con el equipo
Condiciones especiales de ejecución del contrato	Ver epígrafe 8.1.7	

El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento “programa de prevención de riesgos penales” accesible a través de la web corporativa de Correos	Anual	Certificado de cumplimiento
Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia.	Mensual	Mediante reunión de seguimiento con el equipo
El sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 LCSP.	Mensual	Mediante reunión de seguimiento con el equipo

No obstante, en cualquier momento durante la vida del contrato, Correos podrá exigir al adjudicatario el cumplimiento de dichas condiciones.

#### 8.1.7. Condiciones especiales de ejecución.

Tendrán la consideración de condiciones especiales de ejecución incumplimiento dará lugar a la imposición de la penalidad que corresponda, en los casos en que no proceda la resolución del contrato, las siguientes:

<input type="checkbox"/>	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
<input type="checkbox"/>	El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento “programa de prevención de riesgos penales” accesible a través de la web <a href="https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREO S-Codigo-General-de-Conducta.pdf">https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREO S-Codigo-General-de-Conducta.pdf</a>

<input type="checkbox"/>	La suscripción de un seguro de responsabilidad civil por los daños que pueda causar el contratista, su personal, subcontratistas o proveedores, por un importe mínimo de .....euros.
<input type="checkbox"/>	Establecimiento de un plan de formación para los empleados adscritos a la ejecución del contrato en materias relacionadas con: <input type="checkbox"/> Prevención de riesgos laborales específicos en el marco del servicio a prestar <input type="checkbox"/> Régimen de protección de datos de carácter personal. <input type="checkbox"/> Otro ..... .....
<input type="checkbox"/>	Establecimiento de un sistema de gestión diferenciada para los residuos que pueda generar la prestación del servicio.
<input checked="" type="checkbox"/>	Sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos Destrucción de datos: Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado. No obstante, el adjudicatario encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.
<input checked="" type="checkbox"/>	Establecimiento de medidas que garanticen la igualdad de trato y no discriminación, así como la inclusión de miembros de grupos vulnerables.
<input checked="" type="checkbox"/>	Condición de carácter social o medioambiental: Implementación de al menos un plan de sensibilización y formación en materia medioambiental.
<input checked="" type="checkbox"/>	Otras: Cumplimiento de los plazos establecidos en el Anexo I.

El cumplimiento de dichas condiciones será exigible durante la vida del contrato, el control que Correos ejercerá para velar por ese cumplimiento será el siguiente:

Condición especial	Frecuencia	Forma de acreditación del cumplimiento
Sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos Destrucción de datos: Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado.	Anual	Certificado de eliminación

Establecimiento de medidas que garanticen la igualdad de trato y no discriminación, así como la inclusión de miembros de grupos vulnerables	Mensual	Mediante reunión de seguimiento con el equipo
Implementación de planes de sensibilización y formación en materia medioambiental.	Anual	Certificación de ejecución a la finalización de la formación
Cumplimiento de los plazos detallados en el Anexo I.	De acuerdo con los plazos establecidos en el Anexo I	Reuniones de seguimiento y entrega de los archivos y reportes especificados en el Anexo I

No obstante, en cualquier momento durante la vida del contrato, Correos podrá exigir al adjudicatario el cumplimiento de dichas condiciones.

Todas las condiciones especiales de ejecución que formen parte del contrato serán exigidas igualmente a todos los subcontratistas que participen de la ejecución del mismo, respondiendo el contratista principal en caso de incumplimiento por parte de aquellos.

#### 8.1.8. Régimen de confidencialidad.

El contratista, así como todas las personas que intervengan en la ejecución del contrato (incluidos subcontratistas y proveedores), estarán sujetos al deber de confidencialidad al que se refiere el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 en relación con el tratamiento de datos personales.

Igualmente deberán respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le indique por el responsable del contrato, se hubiese dado el referido carácter en los pliegos de condiciones o en el contrato, o que por su propia naturaleza deba ser tratada como tal, obligación que se mantendrá durante un plazo de cinco años desde el conocimiento de la información, salvo que se establezca un plazo mayor.

#### 8.2. Modificaciones del contrato.

En el presente contrato:

NO están previstas modificaciones.

Sí se han previsto la posibilidad de acordar modificaciones en los supuestos descritos en el [Anexo XII](#))

Además, se prevé la posibilidad de acudir a lo dispuesto en el artículo 205 de la LCSP

respecto de las modificaciones no previstas en el presente Pliego.

### **8.3. Cesión y Subcontratación.**

#### **8.3.1. Cesión del contrato**

Para que los contratistas puedan ceder sus derechos y obligaciones a terceros será necesario el cumplimiento de los siguientes requisitos:

- Autorización expresa y previa del órgano de contratación.
- Que el cedente tenga ejecutado al menos un 20 por 100 del importe del contrato.
- Que el cesionario tenga capacidad para contratar con la Administración y la solvencia que resulte exigible en función de la fase de ejecución del contrato, debiendo estar debidamente clasificado si tal requisito ha sido exigido al cedente, y no estar incurso en una causa de prohibición de contratar.
- Que la cesión se formalice, entre el adjudicatario y el cesionario, en escritura pública.

#### **8.3.2. Régimen de subcontratación.**

Subcontratación permitida:

NO  SI

El contratista podrá concertar con terceros la realización parcial de la prestación bajo las siguientes condiciones:

- Los licitadores deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial de los subcontratistas a los que se vaya a encomendar su realización.
- El adjudicatario comunicará su intención de celebrar subcontratos, señalando la parte de la prestación que se pretende subcontratar y la identidad, datos de contacto y representante o representantes legales del subcontratista, y justificando suficientemente la aptitud de este para ejecutarla por referencia a los elementos técnicos y humanos de que dispone y a su experiencia, y acreditando que el mismo no se encuentra incurso en causa de prohibición de contratar. Cualquier cambio respecto de los subcontratos que se produzca durante la ejecución del contrato deberá ser comunicado también a la entidad contratante.
- En el caso de que la subcontratación afecte al tratamiento de datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, el

subcontratista quedará sometido a las mismas obligaciones que el contratista y deberá suscribir un Contrato de encargo de tratamiento de datos personales conforme al modelo consignado en el [Anexo XV](#).

No obstante lo anterior y en atención a su consideración como “tareas críticas” debidamente justificadas, no podrán ser objeto de subcontratación las siguientes prestaciones:

<input checked="" type="checkbox"/>	Las interlocuciones con Correos, así como las reuniones de seguimiento del proyecto.

## 9. Cumplimiento del contrato.

### 9.1. Responsable del contrato. Representante del contratista.

El órgano de contratación designará un responsable del contrato con facultades de supervisión y capacidad para dictar instrucciones sobre la ejecución del contrato y para aprobar la recepción del contrato. El responsable del contrato podrá apoyarse en otras unidades para realizar el seguimiento de la ejecución del servicio.

Por su parte, el adjudicatario designará a su propio representante y lo comunicará al responsable del contrato. Este será el único interlocutor válido con la entidad contratante en la fase de ejecución y período de garantía.

### 9.2. Régimen de penalidades.

El régimen de penalidades aplicable en caso de incumplimiento de obligaciones establecidas en este pliego será el descrito en el [Anexo XIII](#). Los procedimientos para la imposición de penalidades deberán iniciarse antes de la aprobación del acta de conformidad con el servicio prestado (informe fin de ejecución), y su tramitación no se demorará más allá de un mes en caso de infracciones leves, tres meses, en caso de infracciones graves, o seis meses, en caso de infracciones muy graves.

Las cuantías de cada una de las penalidades impuestas, por cada incumplimiento efectuado, no podrán ser superiores al 10 por ciento del precio del contrato, IVA excluido, ni el total de las mismas superar el 50 por ciento del precio del contrato.

Las penalidades por incumplimientos leves y graves se impondrán por acuerdo del responsable del contrato, y por los muy graves, del órgano de contratación, adoptado a propuesta del responsable del contrato, dando audiencia al contratista con carácter previo.

Para la imposición de penalidades se deberá observar su adecuación a la gravedad y perjuicio que supone para la entidad contratante el hecho constitutivo de penalidad. La graduación de la penalidad considerará especialmente los siguientes criterios:

- a) El grado de culpabilidad o la existencia de intencionalidad.
- b) La continuidad o persistencia en la conducta que da lugar al incumplimiento.
- c) La naturaleza de los perjuicios causados.
- d) La reincidencia, por sucederse en el término de un año más de un incumplimiento de la misma naturaleza, que hubiese sido penalizado con anterioridad.

El importe de las penalidades se hará efectivo mediante deducción de las cantidades que, en concepto de pago total o parcial, deban abonarse al contratista o sobre la garantía que, en su caso, se hubiese constituido, cuando no puedan deducirse de los mencionados pagos.

El pago de las penalizaciones no sustituirá al resarcimiento de daños y perjuicios por incumplimiento del adjudicatario, ni eximirá de cumplir con las obligaciones contractuales, pudiendo exigirse, conjuntamente el cumplimiento de dichas obligaciones y la satisfacción de las penas pecuniarias estipuladas que se imputarán a factura y/o fianza, sin perjuicio de poder optar por la resolución del contrato y la reclamación de daños y perjuicios al adjudicatario.

### **9.3. Abonos al contratista. Facturación.**

El pago del servicio se efectuará con periodicidad mensual, a la realización conforme de los entregables establecidos en el Anexo I, previa presentación de la correspondiente factura. Para el pago de facturas giradas por el adjudicatario, la entidad contratante utilizará los siguientes medios de pago:

- Transferencia bancaria. Correos ordenará la transferencia para el pago de la factura en los 60 días naturales siguientes a la fecha de su recepción, coincidente con el calendario de pagos de la entidad contratante.
- Confirming. La entidad contratante dispone del servicio de confirming con entidades financieras que facilita al adjudicatario el anticipo del importe de sus facturas. En ningún caso se considerará como medio de pago el uso de servicios de factoring, cesiones de crédito o cualquier otro de similar naturaleza, sin perjuicio de la utilización del servicio de confirming de la entidad contratante.

En caso de que el adjudicatario no estuviera interesado en el anticipo de sus facturas, el importe de las mismas se abonará mediante transferencia bancaria en los 60 días naturales siguientes a la fecha de su recepción, coincidente con el calendario de pagos de la entidad contratante.

Las facturas contendrán la información establecida en la normativa que resulte de

aplicación, y se tramitarán por vía electrónica con arreglo a las siguientes especificaciones y formato:

- Se requiere que el proveedor adjudicatario del contrato gestione la facturación del mismo mediante factura electrónica en el formato factura que determine la entidad contratante (actualmente es 3.2) y a través de la plataforma se le indique (actualmente se utiliza la VAN de EDICOM (EDIWIN), para la recepción y envío de facturas).
- Como campos específicos de Correos, como mínimo se proporcionarán los siguientes:

Campo		Facturae 3.2
Expediente		
Lote		
Grupo Gestor		Facturae/Parties/BuyerPart y/ AdministrativeCentres/ AdministrativeCentre/CentreCode
Descripción de la operación		Facturae/Invoices/Invoice/AdditionalData/InvoiceAdditionalInformation
Fecha de la operación		Facturae/Invoices/Invoice/InvoiceIssueData/OperationDate
Grupo Gestor		Facturae/Parties/BuyerPart y/ AdministrativeCentres/ AdministrativeCentre/CentreCode (RoleTypeCode 02)
Nº línea del pedido		Facturae/Invoices/Invoice/Items/InvoiceLine/SequenceNumber
Referencia legal		Facturae/Invoices/Invoice/Items/InvoiceLine/AdditionalLineItemInformation

La entidad contratante tendrá derecho a retener y compensar las cantidades pendientes de pago al proveedor, en la cuantía que éste, a su vez, adeude a la propia entidad contratante o a cualesquiera de las sociedades del Grupo al que pertenece.

#### 9.4. Recepción y liquidación.

El contratista deberá prestar el servicio dentro del plazo estipulado, efectuándose por el responsable del contrato un examen de la prestación realizada antes de darla por recibida. El responsable del contrato podrá solicitar, en su caso, la realización de las prestaciones contratadas y la subsanación de los defectos observados.

La recepción, total o parcial, se consignará en un documento en el que se detallarán las condiciones de recepción. Si los trabajos efectuados no se adecuan a la prestación contratada, como consecuencia de vicios o defectos imputables al contratista, el responsable del contrato podrá optar por exigir el cumplimiento íntegro de lo contratado o por rechazar la misma quedando liberada la entidad contratante de la obligación de pago o teniendo derecho, en su caso, a la recuperación del precio satisfecho.

Aprobadas la recepción y liquidación del contrato, así como, transcurrido el plazo de garantía (si existiese), se procederá, si se han cumplido todas las obligaciones incluidas en el contrato, a cancelar la garantía dentro del plazo de tres meses, contados a partir de la fecha de la indicada liquidación o finalización del plazo de garantía.

#### 9.5. Plazo de garantía.

<input type="checkbox"/> SIN PLAZO DE GARANTÍA.
<input checked="" type="checkbox"/> GENERAL, de tres meses desde la recepción de conformidad del servicio.
<input type="checkbox"/> ESPECÍFICO, de .... meses desde la recepción de conformidad del servicio.

Transcurrido dicho plazo sin que la entidad contratante haya formalizado ningún reparo, el contratista quedará relevado de toda responsabilidad por razón de la prestación efectuada, procediéndose a la devolución o cancelación de la garantía definitiva.

### 10. Resolución del contrato.

#### 10.1. Causas de resolución.

Serán causa de resolución del contrato:

<input checked="" type="checkbox"/>	Las previstas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
<input checked="" type="checkbox"/>	El incumplimiento de obligaciones calificadas expresamente como «esenciales» en este Pliego, de acuerdo con lo establecido en el Apartado 8.1.6.
<input checked="" type="checkbox"/>	Cuando teniendo que llevar a cabo una modificación en el mismo que, no estando prevista en el pliego, no concurrieran las circunstancias establecidas en

	el artículo 205 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
<input checked="" type="checkbox"/>	La imposición de penalidades por demora en la ejecución, cada vez que alcancen un múltiplo del 5 por 100 del precio del contrato, IVA excluido.
<input checked="" type="checkbox"/>	El cumplimiento defectuoso de la prestación, cuando afecte a más del 20% de dicha prestación.
<input checked="" type="checkbox"/>	El incumplimiento por el contratista de los plazos de pago a sus proveedores o subcontratistas.
<input checked="" type="checkbox"/>	La falta de renovación o prórroga de la Póliza de seguro de responsabilidad civil, en los casos en que fuera exigible o lo hubiera ofrecido el adjudicatario.
<input checked="" type="checkbox"/>	El desistimiento de la ejecución del servicio por la entidad contratante por circunstancias sobrevenidas, aun cuando se hubiera comenzado dicha ejecución.
<input checked="" type="checkbox"/>	Incumplimiento de las condiciones especiales de ejecución, de modo que se frustre el objeto del contrato.
<input checked="" type="checkbox"/>	Incumplimiento de las obligaciones de carácter esencial recogidas en las letras a) a e) del artículo 122.2 LCSP.

## 10.2. Procedimiento

La resolución del contrato se acordará por el órgano de contratación, adoptado a propuesta del responsable del contrato, sobre la que se dará audiencia al contratista por plazo no inferior a diez días hábiles.

## 11. Protección de Datos

### 11.1. Cláusula informativa de protección de datos personales recabados a través del Canal Ético

En cumplimiento con lo establecido en la Ley de Protección del Informante (Ley 2/2023, de 20 de febrero) le informamos de que sus datos personales, de cualquier categoría, o los datos personales de sus empleados y/o representantes pueden ser comunicados a Correos con motivo de la interposición de una comunicación en la que sea parte, en cuyo caso sus datos se habrán obtenido a través del Canal Ético y serán tratados con la finalidad de gestionar las comunicaciones recibidas por Correos. Puede ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento o portabilidad en:

- Dirección Postal: Conde De Peñalver 19, 28006, Madrid
- Correo Electrónico: [derechos.protecciondatos.correos@correos.com](mailto:derechos.protecciondatos.correos@correos.com)

Puede consultar más información en la [Política de Protección de Datos del Canal Ético para Clientes y Proveedores](#).

## 11.2. Información a representantes, trabajadores y personas de contacto

Los datos de carácter personal de las personas de contacto de los licitantes y, en su caso, de sus trabajadores serán tratados por la entidad contratante con la finalidad de gestionar su participación en la presente contratación, y en caso de resultar adjudicatario del contrato, con la finalidad de gestionar la relación contractual que se formalice entre las partes, siendo la base legitimadora del tratamiento la ejecución del contrato y el cumplimiento de la normativa de aplicación. En este sentido, le informamos que los datos facilitados no se cederán a terceros, salvo obligación legal.

Estos datos se conservarán hasta que se produzca la adjudicación del contrato y, en caso de resultar adjudicatario, durante la realización del servicio. Transcurrido este período se procederá a su bloqueo y, prescritas las acciones derivadas, a su eliminación.

Los interesados podrán ejercitar sus derechos de acceso, rectificación, oposición, supresión, limitación al tratamiento y portabilidad, mediante comunicación a las siguientes direcciones:

- Dirección Postal: Conde De Peñalver 19, 28006, Madrid
- Correo Electrónico: [derechos.protecciondatos.correos@correos.com](mailto:derechos.protecciondatos.correos@correos.com)

Asimismo, podrán ponerse en contacto con el delegado de protección de datos en la dirección: [dpdgrupocorreos@correos.com](mailto:dpdgrupocorreos@correos.com) o presentar una reclamación ante la autoridad de control (en España, la AEPD) en caso de que considere infringidos sus derechos.

El licitante se compromete expresamente a informar a sus trabajadores y resto de personas de contacto de los términos de la presente cláusula manteniendo indemne a la entidad contratante.

En lo que respecta al tratamiento de datos personales que pudiera derivar de la prestación del servicio, los licitadores y la entidad contratante acuerdan someterse de manera expresa a la normativa vigente en materia de protección de datos en España y, en particular, al 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 o “RGPD”) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (“LOPDGDD”).

Este acuerdo ostenta el carácter de obligación esencial, por lo que su incumplimiento, por cualquiera de las partes, facultará a la otra parte a resolver el contrato y, en su caso, reclamar la indemnización por daños y perjuicios a que pudiera haber lugar.

## 12. Régimen jurídico del contrato y reclamaciones contra este pliego.

El contrato se registrará, en cuanto a su preparación y adjudicación, por lo dispuesto en el presente Pliego y en las Instrucciones Internas de Contratación del Grupo Correos. El resto de cuestiones relativas a los efectos, cumplimiento y extinción del contrato se registrarán por lo previsto en la documentación que revista carácter contractual y por el Derecho Privado.

A esos efectos, tendrán carácter contractual, a todos los efectos, con el siguiente orden de prelación, los siguientes documentos:

<input checked="" type="checkbox"/>	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos
<input checked="" type="checkbox"/>	Aceptación de la resolución de adjudicación
<input checked="" type="checkbox"/>	Los proyectos o programas de trabajo que se hubiera presentado el adjudicatario
<input checked="" type="checkbox"/>	La totalidad de la oferta presentada por el adjudicatario.

El presente pliego podrá ser objeto de recurso de alzada en el plazo de un mes a contar desde su publicación, o en su defecto de la notificación, de acuerdo con lo previsto en el art. 321.5 de la Ley 9/2017 de Contratos del Sector Público y el art. 121 de la Ley 39/2015, ante la Sociedad Estatal de Participaciones Industriales (SEPI), C/ Velázquez no 134, 28006 Madrid. SEPI.

Madrid, a 12 de marzo de 2026

CONFORME:

DIRECTOR DE ESTRATEGIA,  
SOSTENIBILIDAD Y MARCA

SUBDIRECTORA DE SOSTENIBILIDAD  
Y RELACIONES INTERNACIONALES

Fdo.: D. José Miguel Moreno Moreno

Fdo.: D.<sup>a</sup> Elena Fernández Rodríguez

## **Anexo I.- Características técnicas específicas del contrato.**

El cálculo de huella de carbono deberá garantizar el **cumplimiento regulatorio vigente**, responder a las necesidades de información de clientes y grupos de interés, y permitir demostrar de manera verificable el avance en los objetivos de descarbonización de Correos.

### **SERVICIOS REQUERIDOS:**

Con el objetivo de cumplir con la normativa en materia de cálculo de huella y de reducción de Gases de Efecto Invernadero (GEI), tanto a nivel nacional como europeo, Correos necesita realizar la contratación de un servicio que le permita realizar el cálculo de huella por envío de acuerdo con la norma ISO 14083:2023 y la metodología establecida en el Marco GLEC v3.2.

El servicio consistirá en la provisión de una herramienta SaaS (Software as a Service) para el cálculo de la huella de carbono con total operatividad por parte de Correos, con un caso de uso concreto, así como en la provisión de servicios de consultoría para la realización del cálculo de huella a lo largo de toda la cadena logística de extremo a extremo (E2E) acorde al estándar ISO 14083:2023 y al Marco GLEC v3.2 para su posterior verificación, incluyendo asesoramiento para la realización de los cálculos, datos necesarios, posibles aproximaciones, e informes necesarios para la certificación del cálculo.

Para cumplir con las necesidades de Correos, el adjudicatario deberá proporcionar las siguientes prestaciones:

### **Bloque I: Herramienta SaaS para el cálculo de la huella de carbono en base a la ISO 14083:2023 y GLEC v3.2 para un caso de uso concreto, consultoría y formación para ponerla en marcha con total operatividad y soporte durante su uso:**

Este Bloque I se centrará en el cálculo de la huella de carbono en la cadena logística completa de Correos limitado a un caso de uso concreto basado en paquetería registrada con el siguiente orden de magnitud estimado en términos de volúmenes mensuales:

- Volumen nominal promedio estimado de envíos mensuales: 4.000.000 de envíos.

La solución debe garantizar un correcto funcionamiento tanto en escenarios de carga normal como en escenarios pico, donde el volumen estimado puede llegar a alcanzar los

5.000.000 de envíos mensuales, independientemente de los registros que estos volúmenes puedan generar.

El adjudicatario deberá:

- Definir las variables, parámetros y fuentes de información necesarios para la cuantificación de las emisiones de GEI en cada fase de la cadena logística.
- Establecer la metodología de cálculo y reporte de las emisiones de GEI conforme a los requerimientos establecidos en la ISO 14083:2023 y el Marco GLEC v3.2, proporcionando documentación completa y trazable sobre hipótesis, factores de emisión, fuentes de datos primarios, algoritmos y procesos de cálculo utilizados.
- Proveer a Correos de una herramienta SaaS certificada propia, previamente desarrollada, que permita la realización del cálculo de huella y generar informes mensuales de emisiones a nivel de cliente y producto, escalable y adaptable a distintos formatos y requisitos específicos solicitados por los clientes, aumentando progresivamente el nivel de granularidad y detalle. En caso de que el proveedor no disponga de una herramienta certificada en la ISO 14083:2023 y el Marco GLEC v3.2 será necesaria una verificación externa del cálculo, mediante auditoría externa, a solicitud del adjudicatario.
- Definir los procesos de integración con la herramienta que proporcione para la realización del cálculo de huella objeto del contrato siguiendo las directrices de integración para una solución SaaS que se recogen en este documento.
- Prestar soporte a Correos durante la duración íntegra del contrato (12 meses) para el uso de su herramienta, de forma que permita reportar mensualmente, así como para la interpretación de los resultados obtenidos.

En el marco de estas obligaciones, el Bloque I comprende las siguientes prestaciones específicas:

#### 1.1 Definición de la metodología ISO 14083:2023/GLEC v3.2:

Por parte de Correos se presentará al adjudicatario el detalle de la necesidad a cubrir en el caso de uso, plazos y salida esperada del *output*.

El adjudicatario realizará una presentación de las necesidades para la realización del cálculo de la huella del caso de uso anteriormente referido.

Entregables:

- Inventario de entidades necesarias para el cálculo, entendidas como categorías de datos. (detallado en el siguiente apartado 1.2).
- Metodología de cálculo para la huella de carbono siguiendo la ISO 14083:2023 y el Marco GLEC v3.2 Correos requerirá el entregable con la metodología de cálculo que incluya:

- Declaración de alineación con la ISO 14083:2023 y el Marco GLEC v3.2.
- Definición de los límites organizativos y operacionales del cálculo, así como el alcance de la cadena logística E2E.
- Identificación de los datos de actividad empleados, indicando el uso de datos primarios, secundarios, modelizados o por defecto en cada una de las fases del cálculo.
- Descripción de las fuentes de datos.
- Detalle de los factores de emisión empleados (origen, año, base metodológica).
- Explicación de los criterios de asignación y reparto de emisiones conforme a la ISO 14083:2023 y el Marco GLEC v3.2.
- Metodología de cálculo de las emisiones diferenciando WTT, TTW, WTW, así como emisiones de origen fósil y biogénico.
- Descripción de hipótesis, supuestos y aproximaciones y trazabilidad del cálculo.

Durante la vigencia del contrato, el adjudicatario deberá realizar los cálculos estimados para aquellas categorías de las que no se disponga información.

Para este apartado el adjudicatario dispondrá de un **plazo de 15 días** desde el inicio del contrato.

### 1.2 Análisis de procesos y categorías de datos:

Se establecerá de manera conjunta un análisis de datos y levantamientos de procesos, que redunden en el caso de uso en cuestión.

Por parte de Correos se aportará el conocimiento y el trabajo previo realizado respecto de los procesos de Negocio y de las fuentes de datos que serán objeto de análisis, y por parte del Adjudicatario, se aportará el conocimiento sobre las entidades necesarias para la realización del cálculo de la huella según ISO 14083:2023 y el Marco GLEC v3.2.

Entregables:

- Inventario detallado de entidades y categorías de datos necesarias, para la realización del cálculo de la huella cumpliendo la ISO 14083:2023 y con el Marco GLEC v3.2.
- Informe de entidades y atributos de datos, existentes y disponibles en Correos, con la granularidad requerida para el cálculo de la huella según ISO14083:2023 y el Marco GLEC v3.2, y para aquellas que no estén disponibles, la metodología del cálculo para poder realizar las aproximaciones necesarias. Todas las estimaciones deberán de estar documentadas y justificadas, indicando las fuentes de información empleadas, los criterios técnicos empleados, los factores de emisión,

conversión o equivalencia empleados, así como los límites metodológicos que se han empleado.

- Identificación de las entidades de entrada distinguiendo entre maestras y variables. En el caso de las entidades variables, acuerdo de integración mediante los mecanismos definidos en la documentación técnica del pliego en cuestión, para el traspaso de información al adjudicatario del contrato, de manera que permita la realización del cálculo referido en el Bloque 1.1. Este acuerdo podrá plantear distintas fases/evoluciones. En caso necesario se podrá realizar una primera integración rápida con la periodicidad que se estime oportuna, según el volumen de datos a manejar y la periodicidad de los informes requeridos (por ejemplo, una integración diaria vía intercambio de ficheros), para garantizar la puesta en marcha de la herramienta con total operatividad en el menor tiempo posible y esta fase finalizará a medida que se implementa la solución definitiva de acuerdo de integración.

Si así se precisa, el adjudicatario deberá realizar las acciones necesarias para la incorporación de esta información a sus herramientas de cálculo (adaptaciones en APIs actuales, etc.).

Para este apartado el adjudicatario dispondrá de un **plazo de 1 mes** a contar desde la finalización de la prestación 1.1.

### 1.3 Provisión de una herramienta SaaS para el cálculo mensual para el caso de uso en cuestión, formación en la herramienta y soporte durante su uso:

El adjudicatario deberá proporcionar una herramienta SaaS para el cálculo de huella de carbono para el caso de uso suministrado. El cálculo se realizará al inicio de cada mes, con los datos del mes anterior. Es un cálculo mensual, donde se deberá proporcionar el dato agregado y el detalle de las emisiones o huella de carbono de los envíos incluidos en el caso de uso.

Las entradas variables y maestras que componen el referido cálculo, serán las definidas en el punto 1.2. En cualquier caso, Correos se encargará de disponibilizar los datos que se estimen necesarios para el cálculo de huella y que estén disponibles en la compañía en el menor tiempo posible. Mientras tanto, la herramienta deberá realizar el cálculo de huella con las aproximaciones que se establezcan oportunas.

Estarán incluidas en el contrato tantas pruebas en un entorno no productivo y ajustes (por ejemplo, pruebas de carga de datos, pruebas de rendimiento, ajustes sobre los resultados devueltos por la herramienta) como el adjudicatario deba realizar sobre la herramienta como paso previo a la entrega a Correos de la herramienta con total operatividad para su uso productivo.

El adjudicatario impartirá un mínimo de 3 horas de formación, incluida en el precio de la oferta a los empleados de Correos que sean usuarios de dicha plataforma en formato online y/o presencial. La formación deberá permitir a los usuarios:

- Comprender el funcionamiento general de la herramienta de cálculo de huella de carbono.
- Interpretar los resultados del cálculo de emisiones conforme a la ISO 14083:2023 y el Marco GLEC v3.2.
- Utilizar las funcionalidades de consulta, análisis y explotación de la información.
- Acceder y comprender la trazabilidad del dato, incluyendo el origen de los datos de actividad, factores de emisión y criterios de cálculo.
- Generar, consultar y analizar los informes y resultado de emisiones, tanto a nivel agregado como a nivel de envío.
- Diferenciar y utilizar adecuadamente las funcionalidades de cada uno de los perfiles de usuario.

El adjudicatario deberá proporcionar materiales que faciliten la comprensión y el uso posterior de la herramienta, tales como manuales de usuario o guías operativas, en formato digital.

El proveedor proporcionará soporte a Correos durante la duración del contrato en relación con el uso de la herramienta incluyendo, entre otros aspectos, consultas relativas a la carga de datos, a la interpretación de los resultados propuestos por la herramienta o a problemas operativos durante su uso, como ralentización o caída del servicio.

La herramienta deberá permitir gestionar distintos niveles de acceso, usuario administrador y usuario visualizador:

- Usuario administrador:
  - Tiene acceso completo a la plataforma.
  - Puede llegar al origen del dato (funcionalidad de trazabilidad).
  - Tiene capacidad de gestionar informes, ver información detallada por envío y configurar la herramienta.
  - Puede consultar certificados auditables (emisiones totales, por alcance y por envío).
- Usuario visualizador
  - Acceso solo de consulta.
  - No puede editar información.
  - No puede acceder a la trazabilidad del dato.
  - Su uso se limita a visualizar información de emisiones y filtros

La herramienta debe permitir la interacción de los usuarios a través de una interfaz web ligera, intuitiva y dinámica que permita la carga de datos y la visualización/exportado de informes.

Los informes deberán cumplir los siguientes requisitos:

- Periodicidad y periodo de referencia:
  - Los informes se elaborarán con periodicidad mensual durante 12 meses.
  - Cada informe deberá identificar de forma expresa la fecha de inicio del periodo de cálculo, la fecha de fin del periodo de cálculo y la fecha de realización del cálculo.
  - El cálculo se realizará utilizando los datos correspondientes al mes natural inmediatamente anterior al de la entrega del informe.
- Nivel de resolución y estructura del informe:
  - Nivel agregado, con el total de emisiones por el periodo, especificando el código o identificación del cliente, por producto cuando resulte aplicable, especificando el código o identificación del producto.
  - Nivel de envío individual, permitiendo identificar las emisiones asociadas a envíos concretos.
  - Para cada operación del transporte (TOC) y nodo logístico (HUB) se deberán indicar las emisiones totales de GEI, la intensidad de emisiones de GEI y la actividad asociada (tonelada kilómetro, tonelada procesada, etc.).
  - Se debe disponer de identificador a nivel de envío / paquete / viaje / contenedor.
- Identificación metodológica:
  - Identificación del estándar metodológico utilizado para el cálculo. Declaración expresa de alineación con la norma ISO 14083:2023 y el Marco GLEC V3.2.
  - Identificación del criterio de asignación, utilizado en el reparto de emisiones, cuando aplique.
  - Método de asignación utilizado en el cálculo de emisiones de GEI en caso de transporte combinado de mercancías. Valores aceptados: volumen, peso, tamaño.
- Trazabilidad del dato, para conocer las emisiones generadas en cada punto de la cadena de suministros, así como el origen y el modo de calcular el mismo. Se deben de incluir tanto la cadena de operación del transporte (TOC) como los nodos logísticos (HUB).
- Emisiones totales y desagregación por fases: los informes deberán de incluir las emisiones de Gases de Efecto Invernadero en toneladas de CO<sub>2</sub> equivalente (TCO<sub>2</sub>e) o kilogramos de CO<sub>2</sub> equivalente (KgCO<sub>2</sub>e) diferenciando de forma explícita entre emisiones Well-to- Tank (WTT), emisiones Tank-to-Wheel (TTW) y emisiones Well-to-Wheel (WTW). Esta diferenciación deberá realizarse tanto para el total de emisiones como para los distintos desgloses incluidos en el informe.

- Naturaleza: las emisiones deberán desglosarse en función de su naturaleza, diferenciando entre emisiones de origen fósil y emisiones de origen biogénico. Expresadas en toneladas de CO<sub>2</sub> equivalente (TCO<sub>2</sub>e) o kilogramos de CO<sub>2</sub> equivalente (KgCO<sub>2</sub>e)
- Desglose por tipología de transporte: los informes deberán de incluir el desglose de emisiones por modo de transporte utilizado, incluyendo al menos: transporte terrestre; transporte ferroviario; transporte aéreo; transporte marítimo; emisiones asociadas a nodos logísticos o hubs. Para cada modalidad de transporte deberán identificarse las emisiones WTT, TTW y WTW cuando resulte aplicable.
- Datos de actividad: los informes deberán de incluir información sobre los datos de actividad utilizados para el cálculo: número total de envíos; distancias recorridas. Consumos energéticos y otras magnitudes relevantes utilizadas como variables de entrada. Para cada dato de actividad se deberán de indicar las unidades de medida.
- Formato y exportación: Los informes deberán ser exportables en formatos estándar, tales como: Excel, CSV, PDF y otros formatos equivalentes acordados con Correos. Así mismo, los ficheros de datos deberán estructurarse de tal forma que permitan realizar el reporte a clientes, análisis internos y procesos de verificación y auditoría externos.

Los informes estarán sujetos a revisión y validación por parte de Correos. En caso de detectarse errores o desviaciones metodológicas, el adjudicatario deberá proceder a su corrección sin coste adicional. La correcta entrega y validación de los informes constituirá condición necesaria para la conformidad del servicio.

La selección de la información a incluir en cada informe no alterará la capacidad de cálculo de la herramienta ni el cumplimiento de la metodología establecida en la norma ISO 14083:2023 y el Marco GLECC V3.2.

Una vez finalizado el contrato, todos los datos de Correos que estén en posesión del adjudicatario deberán ser devueltos a su origen, quedando estrictamente prohibido su tratamiento posterior y obligando al borrado seguro y definitivo de cualquier dato almacenado en su infraestructura, emitiendo, en caso de ser requerido, un certificado que acredite dicha eliminación.

Entregables:

- Herramienta SaaS para el cálculo mensual de huella para el caso de uso en cuestión con total operatividad para Correos.

El primer mes para la realización del cálculo es julio 2026 y continuará durante el plazo de ejecución del contrato.

## **Bloque II: Asesoramiento en el cálculo de la huella de carbono del conjunto Logístico de Correos de acuerdo con la metodología ISO14083:2023 y el Marco GLEC v3.2**

En el marco de estas obligaciones, el Bloque II comprende las siguientes prestaciones específicas:

### 2.1 Diagnóstico de la ISO 14083:2023 y Marco GLEC v3.2:

Estado de situación de la compañía respecto a la metodología ISO14083:2023 y el Marco GLEC v3.2 para cuantificar y reportar las emisiones de Gases de Efecto Invernadero (GEI) de la cadena logística.

Entregables:

- Informe del estado actual, AS/IS.

### 2.2 Análisis de procesos y categorías de datos:

Se establecerá de manera conjunta un análisis de datos y levantamientos de procesos. Por parte de Correos se aportará el conocimiento respecto de los procesos de Negocio y de las fuentes de datos que serán objeto de análisis dentro del conjunto logístico de la Compañía, y por parte del Adjudicatario se aportará el conocimiento sobre las entidades necesarias para la realización del cálculo de la huella de carbono según ISO 14083:2023, en el Marco GLEC v3.2.

Entregables:

- Requisitos funcionales:
  - Inventario detallado de entidades y categorías de datos necesarias, para la realización del cálculo de la huella del conjunto Logístico de Correos cumpliendo la ISO 14083:2023 y el Marco GLEC v3.2.
  - Informe de entidades y atributos de datos, existentes y disponibles en Correos, con la granularidad requerida para el cálculo de la huella según ISO 14083:2023 y el Marco GLEC v3.2, y para aquellas que no estén disponibles, la metodología del cálculo para poder realizar las aproximaciones necesarias. Todas las estimaciones deberán de estar documentadas y justificadas, indicando las fuentes de información empleadas, los criterios técnicos empleados, los factores de emisión, conversión o equivalencia empleados, así como los límites metodológicos que se han empleado.
  - Metodología de cálculo para la huella de carbono según ISO 14083:2023 y el Marco GLEC v3.2
  - Informes de los Output necesarios para la certificación ISO14083:2023 y el Marco GLEC v3.2.
- Plan de transición operativa:

- Inventario de proyectos de desarrollo tecnológicos y de los cambios de los procesos operativos, que Correos tendría que acometer para llegar a un cálculo de huella certificable por la norma ISO 14083:2023 y el Marco GLEC v3.2.
- Definición de la secuencia de proyectos anteriores y los cambios operativos, faseado según impacto.

Para este bloque el adjudicatario dispondrá de un **plazo de 6 meses** desde el inicio del contrato. Transcurrido este período y durante la vigencia del contrato, el adjudicatario deberá prestar soporte a Correos en cuantas cuestiones, dudas, refieran sobre los apartados anteriores.

Para la ejecución de estas tareas, Correos aportará en el plazo más breve posible la siguiente información:

- Datos de actividad de la compañía, necesarios para dicho cálculo.
- Tipología de los envíos para los que se realizará el cálculo
- Modos de transporte utilizados:
  - Terrestre.
  - Marítimo.
  - Aéreo.
- Fuentes de emisión: deberán tenerse en consideración tanto las emisiones directas como las indirectas, con un enfoque Well to Wheel y clasificándolas en biogénicas y no biogénicas.
- Cualquier otra información necesaria para la correcta ejecución de las tareas establecidas.

La transferencia de datos entre ambas partes se realizará de forma que se garantice por ambas partes la seguridad, la confidencialidad y la protección de los datos de carácter personal que pudieran incluir.

#### **ANEXO 1.2 REQUERIMIENTOS DE LA SOLUCIÓN TECNOLÓGICA EN SAAS APORTADA POR EL ADJUDICATARIO.**

1. Los componentes tecnológicos que forman parte de la solución deben estar soportados por los fabricantes durante todo el periodo que Correos use la solución SaaS.
2. En el supuesto de que la solución SaaS preste su servicio desde varios centros de datos dispersos geográficamente, estos deben estar en el marco de la Unión Europea. El adjudicatario debe indicar en su oferta si se despliega el servicio en

- un CPD alternativo, y este CPD debe estar bajo el marco legal de la Union Europea.
3. El adjudicatario debe garantizar la alta disponibilidad de la solución, preferiblemente disponiendo de varias áreas geográficas desde las cuales se pueda seguir dando servicio en caso de que una de ellas no esté disponible.
  4. La solución debe garantizar rápida escalabilidad del servicio, en caso de que Correos necesite usar servicios adicionales de la solución, o incrementar el uso de los mismos, sin afectar al servicio prestado.
  5. La solución debe garantizar su normal funcionamiento ante aumentos en la carga de trabajo, proporcionando un servicio sin degradación en las épocas de mayor actividad y garantizando que la plataforma soporte un incremento de hasta el 100% de la carga. En este caso, Correos debe avisar al adjudicatario con aviso previo de 48 horas. El servicio de soporte asociado a la solución debe estar dimensionado y preparado para estos eventuales aumentos en la carga de trabajo.
  6. Se deberá disponer de sistemas de protección anti-DDoS, así como de filtrado del tráfico, incorporando características WAF.
  7. El prestatario debe garantizar la portabilidad de los datos que residen en su solución, así como el código fuente y configuraciones específicas de Correos en la solución, para facilitar la integración con Correos, o bien en otras plataformas de las que disponga el fabricante.
  8. La solución debe contar con medios de protección que garanticen la mitigación de riesgos asociados a la fuga de información, y deben ser explicados a Correos en la oferta del adjudicatario.

El adjudicatario deben considerar para presentar su oferta que, si recurren a una solución para el cálculo de huella basada en soluciones de mercado y/o herramientas de terceros, e independientemente de su actuación como intermediarios o partners de cualquier fabricante (en caso de resultar empresa adjudicataria) dicha solución y todos los componentes (sean cuales fuere al inicio y durante la ejecución del contrato) deben adquirirse a nombre de Correos de forma que, Correos será titular del derecho de uso de todos y cada uno de los componentes para futuras renovaciones y proveerá a Correos de usuarios, contraseñas y demás aspectos que se requieran para que si así lo estimase, Correos directamente pueda renovar el uso de estos componentes en un futuro. Esto aplica tanto a licencias, como suscripciones y cualquier otro modelo de uso, independientemente de la solución propuesta.

### **ANEXO 1.3 REQUISITOS DE INTEGRACIÓN PARA UNA SOLUCIÓN SAAS**

1. La solución SaaS ofrecida debe albergar la posibilidad de integración con servicios y aplicaciones de Correos, mediante los mecanismos de integración estandarizados en Correos, descritos a continuación:
  - a. API (REST, y SOAP)
  - b. Mensajería asíncrona mediante colas MQ
  - c. Intercambio de ficheros con grandes volúmenes de datos (SFTP)
2. Estas integraciones podrán ser en ambos sentidos:
  - a. La solución debe exponer mecanismos de integración para que puedan ser invocados por los sistemas de Correos. Por ejemplo, exponer una API.
  - b. La solución debe ser capaz de invocar a los sistemas de Correos para obtener información o ejecutar procesos. Por ejemplo, invocar a un servicio REST.
3. La solución debe tener la capacidad de adaptarse a las necesidades de integración desde un punto de vista volumétrico, en caso de que se requiriera un intercambio de mucha información, que haya que realizar de una forma óptima.
4. La solución debe permitir la realización de pruebas de integración en entornos no productivos.

#### ANEXO 1.4 REQUERIMIENTOS GOBIERNO DEL DATO.

El adjudicatario será el encargado de cumplir todos los procesos y requisitos que marca el Área Inteligencia Artificial y Analítica de Datos de Correos en el marco de este pliego de condiciones técnicas, dónde deberá tener en cuenta los siguientes apartados:

##### 1. Desarrollo de integraciones de datos

El adjudicatario será el encargado de la realización de las integraciones de datos que requiera Correos, en aras de dar solución a las necesidades informacionales y analíticas de la compañía. Para llevarlo a cabo será necesario cumplir los Requisitos de Arquitectura de Correos (ver Anexo 1.4), siguiendo los mecanismos técnicos determinados para tal efecto.

##### 2. Gestión y gobernanza

El adjudicatario asumirá entre sus tareas aquellas conducentes a la **implementación de las políticas y procedimientos** indicados por Correos para la gestión de los datos a lo largo de su ciclo de vida, desde la creación hasta la eliminación de estos, que serán marcados desde el Área Inteligencia Artificial y Analítica de Datos de Correos.

Así mismo, se deberá definir la organización con **roles y responsabilidades** en el marco de la/s aplicaciones/sistemas de información de las que proporcione el servicio a Correos.

3. El adjudicatario estará obligado a aplicar los procedimientos y normativas establecidos en el marco del Gobierno del Dato establecido en el Área Inteligencia Artificial y Analítica de Datos, así como al uso de la herramienta de gobierno vigente en cada momento. Las implicaciones se expresan en términos de cumplimentación de las plantillas y documentación necesaria para mantenimiento del glosario de términos de negocio, catálogo datos, clasificación, linaje y reglas de calidad del dato de la compañía, con el objetivo de crear un vocabulario empresarial común recogido en un **glosario empresarial** y cumpliendo el **diccionario de datos** de la organización.

#### 4. Calidad de datos

El adjudicatario será el responsable de mantener la Calidad del Dato que maneje dentro del marco de la aplicación/es o sistema/s de información del que es responsable. Deberá cumplir con las reglas globales y de dominio, y solucionar las incoherencias de estos.

#### 5. Seguridad y privacidad

El adjudicatario será el responsable de proteger los datos contra accesos no autorizados y garantizar el cumplimiento de las normativas de privacidad tal y como se determinan en los requisitos de Seguridad de la Información (confidencialidad, integridad y disponibilidad) (ver Anexo 1.6).

### ANEXO 1.5 REQUISITOS DE MANTENIMIENTO, OPERACIÓN Y MONITORIZACIÓN DE LOS SISTEMAS

1. Los cambios en la configuración del servicio, los despliegues de las actualizaciones, los procesos de *tuning* interno, y resto de acciones de mejora continua del servicio, serán comunicados a Correos con una antelación de:
  - a. 15 días, si el cambio no implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.
  - b. 6 meses, si el cambio implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.
2. El adjudicatario debe responsabilizarse de la ejecución de implementaciones, configuraciones y acciones predictivas, que permitan la recuperación del servicio ante cualquier desastre. Correos exige que este tiempo de recuperación de los servicios sea de menos de 4 horas.
3. La solución debe dar servicio a Correos, sin perjuicio en el rendimiento o la disponibilidad del servicio, ante un incremento de hasta el 100% de la carga, y con un aviso previo de al menos 48 horas por parte de Correos.
4. El servicio debe ser convenientemente monitorizado por el prestatario del servicio, y esta monitorización ha de ser extremo a extremo, es decir, desde el nivel físico (hardware) hasta los procesos de negocio.

5. Al detectarse una incidencia en el servicio, el adjudicatario debe solucionarla y enviará un informe que incluya:
  - a. La ventana temporal de afectación del servicio.
  - b. Una explicación de las causas que han producido la incidencia
  - c. Acciones puestas en marcha para solucionar la incidencia.
  - d. Dentro de las 48 horas posteriores a la resolución de una incidencia, se enviará un análisis de la causa raíz (RCA), para eventos críticos.
6. Aquellos eventos que puedan afectar al servicio, incluyendo degradación de rendimiento, actualizaciones críticas o incidentes de seguridad, serán notificados de manera proactiva por parte del prestatario a Correos, indicando el impacto previsto y el plan de mejoras a implementar. El adjudicatario debe indicar el tiempo estimado de resolución de la incidencia.
7. La solución, o en su defecto el adjudicatario del servicio, deben proveer a Correos de información respecto a los parámetros del servicio prestado. Correos debe tener disponible tanto datos operativos como las métricas del servicio. Debe proveerse esta información a través de cuadros de mando, y esta información debe poder exportarse en algún formato estándar y consensuado con Correos, como XML, JSON o CSV.
8. En caso de que la solución tenga versiones del producto *on premises* y *cloud*, debe facilitar la migración de información entre las versiones del producto. El proceso de migración de datos, procesos y configuraciones específicas que ha implementado Correos en la plataforma, debe ser exportable en la plataforma origen, e importable en la plataforma destino, con algún mecanismo manual o automático que facilite esta migración.

#### ANEXO 1.6 REQUISITOS SOBRE ACUERDOS A NIVEL DE SERVICIO

1. La disponibilidad del servicio debe ser **99.9%** o mayor. En esta métrica deben incluirse fines de semana sólo si Correos va a usar el servicio durante estos días.
2. Si el adjudicatario fuera capaz de mejorar los ANS exigidos por Correos, deberá presentar en su oferta dicha propuesta de nuevos ANS específicos para Correos, incluyendo indicadores y métricas del servicio. Una vez que Correos haya validado los indicadores propuestos por el adjudicatario y el cumplimiento de los mínimos requeridos, ambas partes suscribirán el correspondiente Acuerdo de Niveles de Servicio Definitivo, que será de aplicación durante todo el periodo de vigencia del contrato.
3. RTO (Return Time Objective) o tiempo máximo de restablecimiento del servicio una vez que ya no se ha cumplido el ANS contratado, y Correos podrá aplicar KPIs incrementales a fin de evitar que la persistencia de una incidencia no se

refleje adecuadamente en los indicadores una vez que ya ha contabilizado como tal.

4. RPO. (Return Point Objective) o período de tiempo máximo asumible sobre el que se puede perder datos. Desde Correos por defecto, la tendencia debe ser igual a cero.
5. Correos será el propietario de todos los datos, y el adjudicatario se compromete a la devolución de los mismos, sin que el adjudicatario pueda conservarlos, ni obtener copia de los mismos o facilitarlos a terceros. El adjudicatario sólo podrá consultar o extraer estos datos con la autorización expresa de Correos.

## **ANEXO 1.7 REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN**

### **1. Normativa y Conformidad**

La ejecución del expediente incluirá la elaboración y entrega de todos aquellos documentos cuya existencia venga derivada del cumplimiento de la legislación vigente, del marco normativo de seguridad establecido para los sistemas de información de Correos o, en su caso, sean necesarios para llevar a cabo una gestión adecuada del servicio, la aplicación o el sistema. Esto se hará extensivo a la cadena de suministro del proveedor.

El adjudicatario contará con un proceso formal de control y homologación de proveedores de tal manera que toda su cadena de suministro cumpla con los niveles adecuados de ciberseguridad de acuerdo con los estándares de mercado. En concreto y como mínimo, el proveedor deberá trasladar y hacer cumplir todos los requisitos de ciberseguridad establecidos por Correos a aquellos subcontratistas que puedan ser parte del servicio, haciéndose responsable de su verificación previa.

Asimismo, aquellos servicios que impliquen desarrollos se someterán a las recomendaciones y directrices establecidas sobre buenas prácticas en el desarrollo de sistemas, acorde a los estándares de mercado existentes.

El adjudicatario deberá informar a Correos de las herramientas que utilice en el desarrollo del servicio, en particular de Inteligencia Artificial, la finalidad de su uso, el tipo de datos que utiliza y las medidas técnicas y organizativas que ha implementado para realizar un tratamiento seguro de la información y garantizar un acceso autorizado.

### **2. Control de Acceso y SSO**

El control de acceso a las aplicaciones objeto del presente pliego, por parte de los usuarios, ya sea personal interno o proveedor de servicio, deben integrarse (delegar los procesos de autenticación y autorización) con el Sistema Corporativo de Gestión de Identidades (SGId), y con el Sistema de Single Sign On, permitiendo la gestión centralizada de usuarios, logon único y autenticación segura, asegurando la confidencialidad e integridad de la información transmitida.

En el caso de que las aplicaciones tengan un modelo de arquitectura en la nube, el mecanismo de autenticación y autorización debe basarse en la federación de identidades. La infraestructura de federación de identidades de Correos se fundamenta en el uso de protocolos OAuth 2.0 + OIDC o SAML2.0, integrados en una herramienta de mercado que garantiza el uso de estándares.

Los usuarios administradores no federados deben tener habilitado el inicio de sesión con autenticación multifactor (MFA) para garantizar una capa adicional de seguridad. Además, sus cuentas deben cumplir con una política de contraseñas robusta, que incluya una longitud mínima, uso de caracteres complejos (mayúsculas, minúsculas, números y símbolos), y la obligación de cambiar la contraseña de forma periódica o ante cualquier indicio de compromiso. Cada administrador debe poder actualizar su contraseña de manera segura y autónoma. Para reducir riesgos, el número de usuarios administradores no federados debe ser limitado a un máximo de tres (3) cuentas activas.

En todo momento estas integraciones deben ser tuteladas y asistidas por personal de Correos, que cuenta con experiencia en este tipo de integraciones con otras aplicaciones contratadas en similar modalidad.

El coste de dicha integración debe ser asumido por el proveedor de la aplicación.

El modelo para controlar el acceso debe estar basado en roles (RBAC), de manera que las aplicaciones permitan el establecimiento de distintos grupos de usuarios en función de las actividades que se realicen en el mismo. Dichos grupos deben estar identificados y detallados en base a los privilegios de los mismos y sus responsabilidades asociadas.

Asimismo, el adjudicatario tiene la obligación de notificar a Correos el alta, modificación y/o baja de los usuarios prestadores del servicio, para garantizar el bloqueo y posterior eliminación de las cuentas asociadas a los mismos.

### **3. Respaldo y recuperación**

Los componentes de la solución ofertada deberán disponer de un plan de contingencia ante desastres alineado con la estrategia corporativa de respaldo, siendo responsabilidad del proyecto elaborar un Plan de Contingencia que incluya las tareas y prioridades de recuperación de los componentes que permiten dar servicio al activo, ante los distintos escenarios de desastre contemplados en el Plan de Recuperación de Desastres.

En este sentido, el prestatario del servicio deberá garantizar la recuperación de los sistemas bajo unas condiciones de Tiempo de Recuperación Objetivo (RTO) y de Punto de Recuperación Objetivo (RPO), valores proporcionados por el licitador, debiendo practicar tres pruebas anuales de restauración de los activos implicados en el servicio y donde se deberá constatar, entre otras cuestiones, los valores de RTO y RPO obtenidos en la misma y las mediciones de tiempos de reacción y recuperación del servicio.

### **4. Comunicaciones**

Se deben definir protocolos ligeros, que no sobrecarguen las líneas de comunicaciones, que intercambien solo y exclusivamente la información necesaria para el fin que es recabada, que posean mecanismos de cifrado de la información en tránsito, y que sean fácilmente procesables en un entorno de tiempo real como el que nos ocupa.

No están permitidas aquellas conexiones que pretendan intercambiar información con componentes internos de Correos de manera directa sin “delegar” esta comunicación en componentes (gateways) de los perímetros externos.

El adjudicatario debe facilitar a Correos un diagrama de componentes (físicos y lógicos) de comunicaciones y seguridad, en el cual se ubiquen todos los elementos de la aplicación en sus distintas capas y los flujos de información necesarios para la comunicación entre componentes la misma.

Los protocolos de comunicaciones en los que viaje el usuario y la contraseña en claro quedan expresamente prohibidos, como por ejemplo ftp, http y telnet.

El acceso de forma remota a los recursos corporativos a través de una red pública, sea realizado con la finalidad de realizar un soporte o por teletrabajo, deberá cumplir los requerimientos sobre autenticación, cifrado, filtrado de redes y puestos de usuario que establezca la normativa de seguridad de Correos, así como cualquier otro requerimiento que pudiera establecer la Subdirección de Ciberseguridad.

Todos los accesos remotos que sean necesarios para la prestación del servicio se realizarán a través de la plataforma Corporativa ARCO (acceso remoto seguro), basada en VPN-SSL.

No están permitidas las conexiones directas entrantes a la red de CORREOS ni el uso de VPNs convencionales. Tampoco se permite el establecimiento de VPNs salientes desde el entorno de Correos hacia redes externas. En caso de necesidad, únicamente se permitirá el uso de VPNs dedicadas previamente autorizadas. Adicionalmente, deberá informarse con antelación del rango de direcciones IP externas requeridas para el acceso, no pudiendo superar un máximo de 20 IPs. Todos los accesos desde el exterior deberán realizarse a través de una zona desmilitarizada (DMZ).

Los canales por los que se podrá acceder a este servicio podrán ser la red de Internet o enlaces privados punto a punto. En el caso de que la solución de prestación del servicio sea incompatible con la comunicación descrita, el adjudicatario deberá proveer de un enlace de comunicaciones dedicado para el acceso remoto, cuyo coste será asumido por el propio adjudicatario.

El acceso remoto de Correos proveerá de un Terminal de trabajo en remoto, desde el cual se realizarán los trabajos objeto del contrato y se accederá a los recursos internos de Correos que sean necesarios. En ningún caso se permitirá la conexión de estaciones de trabajo del proveedor con los Sistemas de Información de Correos.

El intercambio de información entre el proveedor y Correos que no se realice mediante soportes físicos, se llevará a cabo a través de un servicio seguro de intercambio de

ficheros que garantizará la protección de las operaciones y de la información intercambiada. En ningún caso se permitirá el intercambio de información entre estaciones de trabajo del proveedor y el Terminal de trabajo en remoto.

## 5. Integridad y confidencialidad

Se deben implementar los mecanismos necesarios para garantizar la integridad y confidencialidad de los datos manejados por los distintos componentes que conformen la solución ofertada, tanto en tránsito como almacenados.

- Para datos en tránsito se debe utilizar la capa SSL/TLS, en su versión 1.3 o superior, para asegurar la integridad y confidencialidad de los datos transmitidos, siendo obligatorio su uso para todas las operaciones de administración y aquellas otras, que lo requiera el nivel de confidencialidad de la información transmitida.
- Para datos almacenados de carácter confidencial o secreto así como para las contraseñas y claves de cifrado nunca se deben almacenar en claro, debiendo aplicar mecanismos de cifrado robustos (AES 256, XML Encryption), y de integridad (RSA, SHA-2, XML Signature).
- Se debe detallar a qué recursos va a requerir permisos de acceso la aplicación, teniendo en cuenta siempre políticas de mínimo privilegio, es decir, solo se debe poder acceder a los recursos que sean estrictamente necesarios, justificándolos de manera pertinente.

## 6. Tratamiento de la información

Se deben adoptar las medidas de índole técnica y organizativa necesarias establecidas en el Reglamento General de Protección de Datos (RGPD) para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Así mismo, se deben detallar todos los flujos de datos desde que son recogidos hasta que se eliminan del sistema. Es necesario disponer de un diseño con el flujo de los datos (dibujo visual) del proceso que contenga los datos que se van a tratar, determinar los sistemas afectados, identificar ubicaciones y proveedores (todos los que intervienen en el proceso) y documentar todos los interfaces existentes con Correos y terceros (origen/destino de datos).

En el caso de servicios en la nube gestionados por el adjudicatario, se debe informar del país de ubicación de los CPDs donde resida la información de Correos, el tratamiento de los datos solo podrá llevarse a cabo dentro del Espacio Económico Europeo o en aquellos países que hayan sido declarados de nivel adecuado mediante una decisión de adecuación de la Comisión Europea.

Cualquier acuerdo con otras organizaciones que incluya compartir información deberá incluir un procedimiento para clasificar la información según su organización y la nuestra.

## 7. Desarrollo Seguro

El adjudicatario debe poder evidenciar el uso de estándares y recomendaciones de seguridad, sobre todo aquellos destinados a evitar ataques conocidos en aplicaciones expuestas a internet (SQL Injection, XSS, etc.), garantizando así un nivel mínimo de seguridad en el desarrollo de la aplicación y el código utilizado, y cumpliendo así con las buenas prácticas vigentes en Correos. Se debe confirmar la realización de pruebas de seguridad periódicas en la solución ofertada.

En caso de que el sistema disponga de una página web pública a Internet, se debe incluir una herramienta de detección de Phishing y Pharming (TrapCode) ofuscado que el Jefe de proyecto debe solicitar a Correos.

El acceso a aplicativos desde fuera de la red de Correos debe incluir un sistema de detección y limitación de ataques de descubrimiento de credenciales mediante técnicas de probada eficacia como por ejemplo captcha y/o retrasos en las transacciones después de un login fallido.

Correos debe poder establecer exigencias de auditoría, funcionales y técnicas, sobre el nivel de cumplimiento de los principios del desarrollo seguro, para comprobar la no existencia de vulnerabilidades explotables desde el exterior. En caso de detectar alguna vulnerabilidad el adjudicatario debe asumir la resolución de las mismas y los costes asociados.

Adicionalmente, el adjudicatario debe restringir el acceso al código fuente del programa.

El soporte de la aplicación y las actualizaciones de la aplicación debe garantizar la compatibilidad con la versión de los sistemas usados en Correos.

## 8. Desarrollo de APIs

En el desarrollo de APIs es fundamental implementar mecanismos de autenticación robustos, como JWT o API keys, que permitan verificar de forma segura la identidad de los usuarios o aplicaciones consumidoras. De forma complementaria, se debe establecer un sistema de autorización que controle de manera precisa el acceso a los recursos y operaciones disponibles según los permisos asignados, aplicando el principio de mínimo privilegio. Asimismo, es recomendable definir límites de tasa (rate limiting) para prevenir ataques de fuerza bruta y mitigar el uso abusivo o indebido de la API.

Toda la comunicación entre clientes y servidores debe realizarse exclusivamente a través de HTTPS (SSL/TLS), garantizando el cifrado de los datos transmitidos y la protección frente a ataques de intermediarios. Además, es imprescindible implementar medidas de seguridad contra vulnerabilidades comunes como Cross-Site Request Forgery (CSRF) y Cross-Site Scripting (XSS), utilizando mecanismos como tokens anti-CSRF y asegurando la validación y sanitización de todas las entradas de usuario para prevenir inyecciones de código malicioso.

Desde el punto de vista de la infraestructura, los accesos a la API desde el exterior deben canalizarse a través de una zona desmilitarizada (DMZ), reforzada mediante firewalls y controles de seguridad en la capa de red, con el objetivo de aislar los sistemas internos y reducir la superficie de ataque. Adicionalmente, se debe mantener un registro detallado de las solicitudes y respuestas de la API para facilitar el monitoreo, la auditoría y la detección temprana de posibles intrusiones, así como controlar cuidadosamente la información expuesta en los mensajes de error. Estas medidas deben complementarse con la realización periódica de pruebas de seguridad y pruebas de penetración para identificar vulnerabilidades y mejorar de forma continua la seguridad de la API.

### **9. Sistemas operativos y software base**

Todos los elementos que formen parte de la aplicación deben tener implantados procedimientos de securización para el software, de manera que se garantice la eliminación de usuarios, configuraciones por defecto y minimicen los riesgos, actuando sobre los siguientes ámbitos: control de acceso, instalación, configuración, auditoría, monitorización, integridad y confidencialidad.

Correos debe poder solicitar los controles aplicados en cada ámbito, así como los resultados de las auditorías de cumplimiento llevadas a cabo por terceras empresas.

### **10. Eventos de auditoría**

Los componentes de la solución ofertada deberán generar eventos de Auditoría y almacenarse en local, y se revisará la posibilidad de integrarse con el gestor de eventos (SIEM) de Correos. El proyecto deberá asumir todas las tareas derivadas de la integración, aportando el conector específico o realizando la transformación del log para su adaptación al conector genérico.

Los eventos de seguridad mínimos que debe generar cualquier sistema en explotación de Correos son los siguientes:

- Autenticación en el sistema
- Accesos a los datos del sistema
- Cambios en las cuentas y grupos de usuarios y contraseñas
- Cambios de accesos y modificaciones del sistema de log o auditoría
- Acciones realizadas con privilegios de administración
- Accesos a los Servicios de integración e intercambio de datos con sistemas internos y externos.
- En general toda la actividad de sobre la información catalogada como CONFIDENCIAL. En especial en este caso se deberá generar un evento por cada actividad concreta (lectura, modificación... etc.).

Cada evento debe generar, al menos, la siguiente información:

- Identificador de la aplicación.
- Identificador del usuario (usuario del login, sea o no del dominio).
- Fecha y hora en la que se generó el evento.

- Tipo de acción realizada (modificación, consulta, login...)
- Objeto o datos sobre el que se realiza la acción (acceso a..., ejecución de..., modificación de..., lectura de..., borrado de..., etc.).
- Resultado de la acción (éxito / fallo).
- Identificación del terminal desde el que se ha realizado la acción (dirección IP de origen, MAC, nombre DNS/NetBIOS....).

La generación de los citados eventos y trazas de auditoría del sistema deberán permitir el cumplimiento de las políticas de auditoría corporativa:

- Registro de accesos
- Control de privilegios administrativos
- Cumplimiento de la LOPD/RGPD
- Gestión única de Identidades

Los posibles métodos de recepción de los eventos de auditoría (SFTP, Syslog, etc.) se definirán con la Subdirección de Ciberseguridad de Correos.

### **11. Respuesta ante incidentes**

Se establecerá un procedimiento de notificación de incidentes de seguridad entre Correos y la empresa adjudicataria con el objetivo de comunicar la información existente respecto a la naturaleza del incidente, las áreas afectadas, el momento en que se ha producido, el estado actual y el grado de control del incidente por parte de la organización. Para ello Correos deberá exigir el cumplimiento de los Acuerdos de Nivel de Servicios - SLA acordados previamente con proveedor.

El proveedor de servicios/adjudicatario deberá mostrarse en todo momento diligente y proactivo en todas las comunicaciones y en especial, en supuestos de incidentes de seguridad y/o brechas de seguridad, propios o producidos en su cadena de suministro, que puedan impactar en el desarrollo normal del servicio.

El proveedor deberá proporcionar un interlocutor y un canal de comunicación específico para la gestión de incidentes de seguridad con el área de ciberseguridad de Correos.

### **12. Auditabilidad**

El proveedor de servicios deberá aplicar los principios y requerimientos establecidos sobre seguridad de la información por la comunidad internacional, así como el marco legal vigente en cada momento sobre protección de datos de carácter personal y cualquier otro que sea aplicable por razón de la materia objeto de regulación. En este sentido Correos podrá establecer exigencias de auditoría sobre el nivel de cumplimiento de los mismos de acuerdo a los servicios contratados.

Correos podrá auditar, por sí misma o a través de un tercero, con el único requisito de preavisar con una antelación de un mes y, de forma presencial o en remoto, todas aquellas medidas y controles que considere necesarios para verificar la seguridad de la información. Además, Correos podrá exigir al proveedor del servicio afectado la

aportación de ciertas evidencias de cumplimiento o, en su defecto, la realización una auditoría interna cuyo informe deberá ser firmado por una persona autorizada y con poder de representación de la empresa prestadora del servicio.

En el caso de que en alguno de estos supuestos se detecte una no conformidad y no se haya visto resuelta, el proveedor deberá realizar una auditoría, a su costa, y proporcionar un informe de auditoría (test de penetración o hacking ético) realizado por un tercero en el último año, junto con el compromiso, en su caso, de solucionar las vulnerabilidades encontradas antes del arranque del servicio.

### **13. Formación y concienciación**

El adjudicatario deberá contar con un plan de formación y concienciación en materia de seguridad, alineado con las políticas de seguridad de Correos, adquirir las conductas adecuadas y ampliar las competencias para mejorar el servicio prestado de forma continua.

### **14. Compromiso de aceptación de políticas de acceso y uso de infraestructuras de correos**

El acceso a la red de Correos por parte de un colaborador a través de un equipo no corporativo se llevará a cabo, siendo el proveedor garante y responsable de su cumplimiento y verificación, bajo el sometimiento de las siguientes premisas:

El proveedor responsable, garantizará que el dispositivo dispone de software de Seguridad en el EndPoint actualizado y permanentemente monitorizado, así como un proceso desatendido de gestión de parches de Seguridad. En ningún caso, el usuario del dispositivo dispondrá de permisos o privilegios de administrador en el mismo.

Asimismo, es responsabilidad del proveedor que el software instalado esté autorizado por la empresa, esté debidamente licenciado y sea el necesario, exclusivamente, para el cumplimiento efectivo de las funciones que tenga que desarrollar en Correos.

Correos se reserva el derecho de verificar y solicitar las evidencias que permitan comprobar que todos los puntos de este documento son cumplidos con exactitud.

El uso inadecuado por un usuario de los recursos que represente un riesgo para la información y/o infraestructuras que la soportan, determinará de forma automática la cancelación y/o limitación de su uso por el Área de Seguridad de la información de Correos.

Asimismo, en el caso de producirse un incidente de seguridad que tenga origen en un dispositivo ajeno a Correos, el área de seguridad podrá solicitar toda la información necesaria para controlar y mitigar los efectos del mismo y el titular/es del dispositivo se obliga a prestar apoyo en la resolución del incidente, así como entregar la información registrada en el dispositivo afectado que permita la investigación y resolución del incidente.

Todo responsable de equipos de personas y de usuarios debe gestionar de forma activa el alta/baja de las personas de las que es responsable y de sus permisos asociados, así como de verificar y controlar un uso adecuado de las credenciales de acceso a los sistemas, personales e intransferibles, debiendo velar por que el desarrollo del servicio se realice en todo momento conforme a unas buenas prácticas de seguridad de la información.

El usuario deberá realizar un uso responsable de sus credenciales de acceso (usuario/contraseña), son personales y la gestión es exclusiva de su titular, estando prohibido su comunicación a terceros y siendo responsable de las acciones que se realice con ellas.

### **15. Ubicación de los datos**

En el caso de tratarse de un SaaS, se tiene que explicar en un apartado específico en qué país van a residir los datos. En caso de que el SaaS se preste desde algún proveedor de Cloud, se deberá indicar cuál es ese proveedor. Así mismo, el proveedor tiene totalmente prohibida la cesión total o parcial a terceros de los datos de Correos.

GDPR. La aplicación o Servicio contratados tendrán que cumplir con la normativa Europea de protección de datos (GDPR).

## Anexo II.- Descripción y limitaciones a la licitación por lotes.

El servicio objeto del contrato es único, y se ejecuta de forma conjunta y global. La correcta ejecución del contrato implica la necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes. Por ello y, al amparo de lo previsto en el artículo 99.3.b) de la Ley 9/2017 de Contratos del Sector Público se justifica la no división en lotes para este expediente.

En cumplimiento del art. 100.2 de la Ley 9/2017, de 8 de noviembre, el desglose del presupuesto base de licitación es el siguiente:							
	Costes directos		Costes indirectos (35%)	Beneficio Industrial (7%)	Presupuesto	IVA o impuesto indirecto equivalente	Presupuesto IVA Incluido
	Costes de personal (51%)	Otros (7%)					
2026	25.500,00	3.500,00	17.500,00	3.500,00	50.000,00	10.500,00	60.500,00
2027	5.100,00	700,00	3.500,00	700,00	10.000,00	2.100,00	12.100,00
<b>TOTAL</b>	<b>30.600,00</b>	<b>4.200,00</b>	<b>21.000,00</b>	<b>4.200,00</b>	<b>60.000,00</b>	<b>12.600,00</b>	<b>72.600,00</b>

\*Se ha tenido en cuenta para la estimación de costes de personal el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública.

### **Anexo III.- Resumen de metodología seguida para el cálculo del valor estimado del contrato.**

El Valor Estimado de la contratación se establece en un máximo de **60.000,00 €** (SESENTA MIL EUROS), IVA o impuestos indirectos equivalentes excluidos.

	Cantidades en euros IVA no incluido
Presupuesto de ejecución	60.000€
Importe de modificaciones previstas	No procede
Importe de prórrogas previstas	No procede
<b>Valor estimado del contrato</b>	60.000 €

## Anexo IV.- Forma de acreditación de la solvencia económica y financiera, y técnica o profesional.

- Forma de acreditación de la solvencia económica y financiera:

El volumen anual de negocios del licitador se acreditará por medio de sus cuentas anuales aprobadas y depositadas en el Registro Mercantil, si el empresario estuviera inscrito en dicho registro, y en caso contrario por las depositadas en el registro oficial en que deba estar inscrito. Los empresarios individuales no inscritos en el Registro Mercantil acreditarán su volumen anual de negocios mediante sus libros de inventarios y cuentas anuales legalizados por el Registro Mercantil.

- Forma de acreditación de la solvencia técnica y profesional:

<input checked="" type="checkbox"/>	Certificados de correcta ejecución de los servicios o trabajos realizados, expedidos o visados por la entidad para la que hayan sido realizados
<input checked="" type="checkbox"/>	<p>Descripción de las medidas que se emplearán para garantizar la calidad. Se admitirán como justificativas del cumplimiento de los requisitos exigidos los siguientes certificados emitidos por instituciones o servicios oficiales:</p> <ul style="list-style-type: none"> <li>• Los licitadores deberán contar con sistemas de gestión medioambiental basados en las normas europeas o internacionales sobre esta materia (ISO 14001 o EMAS o equivalentes), certificados por organismos independientes acreditados por una entidad perteneciente a IAF y aplicables a la prestación del servicio objeto del contrato.</li> </ul>
<input checked="" type="checkbox"/>	Otros: Acreditación de estar en posesión de las certificaciones ISO27001 y Smart Freigh Centre. En caso de que se trate de certificaciones equivalentes se presentará documento que acredite dicho carácter.

- Forma de acreditación del compromiso de adscripción de medios:

<input checked="" type="checkbox"/>	Relación y perfil o <i>Curriculum Vitae</i> del personal, integradas o no en la empresa, que participará en el contrato. Se aportará el CV ciego del personal o equipo humano (es decir, sin referencia a datos de carácter personal) disponible para el cumplimiento del mismo en el que se recoja la formación y años de experiencia que guarden relación con las funciones a desempeñar por el personal o equipo humano bajo el contrato.
-------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Anexo V.- Modelo de aval.

LA ENTIDAD .....

AVALA

Solidariamente a la empresa .....con domicilio social en ..... NIF .....

Ante ..... (en adelante, la entidad contratante), con renuncia a cualquier beneficio que pudiera corresponderle, y en especial al de orden, previa excusión y división de bienes, por la cantidad de .....Euros ( ..... €), para responder de todas y cada una de las obligaciones y eventuales responsabilidades de toda índole que se deriven del cumplimiento del contrato «...».

El presente aval será ejecutable por la entidad contratante a PRIMERA DEMANDA O PETICIÓN, bastando para ello el simple requerimiento a la entidad avalista, dándole cuenta del incumplimiento contractual en que haya incurrido la empresa avalada.

El suscriptor del aval se encuentra especialmente facultado para su formalización según poderes otorgados ante el notario de....., D. .... el día ..... al número de su protocolo y que no le han sido revocados ni restringidos o modificados en forma alguna.

Este aval, que ha sido inscrito con esta misma fecha en el Registro Especial de Avals con el número ....., estará en vigor hasta tanto no se hayan extinguido y liquidado todas y cada una de las obligaciones contraídas por la empresa avalada, y la entidad contratante autorice expresamente su cancelación.

*(Nombre de la entidad avalista, identificación de su representante legal facultado para emitir el aval, fecha y firma)*

## **Anexo VI.- Instrucciones y recomendaciones para la presentación electrónica de las ofertas.**

Los licitadores deberán preparar y presentar obligatoriamente todos los sobres de sus proposiciones de forma telemática a través del Portal de Contratación de Correos (<https://pcc.correos.es/>).

En dicho portal podrán consultarse los requisitos técnicos necesarios, así como manuales y videotutoriales de ayuda:

- Requisitos técnicos: <https://pcc.correos.es/html/requisitos-tecnicos>

La presentación de ofertas se realiza directamente a través del navegador web (no es necesaria la descarga de una aplicación adicional), siendo imprescindible utilizar un navegador compatible. En esta página también se indican las recomendaciones sobre requisitos de ordenador.

Asimismo, será necesario que las empresas dispongan de un certificado electrónico válido para la identificación y firma electrónica. Para ello será preciso tener instalada la aplicación AutoFirma.

- Manuales y videotutoriales: disponibles en el portal, donde se explican los pasos para el acceso al sistema, la presentación de ofertas, la recepción de notificaciones, el registro de personas usuarias y la configuración de certificados.

Toda proposición que, por cualquier causa, no sea presentada por medios telemáticos a través del portal será automáticamente inadmitida en el procedimiento de licitación.

En el caso de que cualquiera de los documentos de una proposición no pueda visualizarse correctamente, se permitirá que, en un plazo de 24 horas desde la notificación de la incidencia, el licitador presente nuevamente dicho documento en formato digital. El documento presentado posteriormente no podrá sufrir modificación respecto al original incluido en la proposición. Si la entidad contratante comprueba que el documento ha sido alterado, la proposición del licitador no será tenida en cuenta.

Cuando se requiera la firma electrónica de sobres o documentos, esta deberá realizarse con certificados electrónicos emitidos por proveedores de servicios de certificación reconocidos, así como compatibles con la aplicación AutoFirma.

No obstante, las personas extranjeras podrán firmar con otros certificados siempre que justifiquen que los mismos son generalmente aceptados en la contratación pública de su país.

Asimismo, los licitadores podrán presentar, en el registro de la entidad contratante y en soporte físico electrónico, una copia de seguridad de dichos documentos, de acuerdo con lo previsto en la Disposición adicional decimoquinta de la LCSP.

## Anexo VII.- Instrucciones para cumplimentar el DEUC.

El DEUC consiste en una declaración responsable de la situación financiera, las capacidades y la idoneidad de las empresas para participar en un procedimiento de contratación pública, de conformidad con el artículo 59 Directiva 2014/14, (Anexo 1.5) y el Reglamento de Ejecución de la Comisión (UE) 2016/7 de 5 de enero de 2016 que establece el formulario normalizado del mismo y las instrucciones para su cumplimentación.

El formulario del Documento Europeo Único de Contratación (DEUC) es accesible a través de la siguiente dirección:

<https://visor.registrodelicitadores.gob.es/esp-d-web/filter#>

El órgano de contratación podrá hacer uso de sus facultades de comprobación de los extremos incluidos en el DEUC requiriendo al efecto la presentación de los correspondientes justificantes documentales, en los términos del artículo 69 de la Ley 39/2015.

En cualquier caso, la presentación del DEUC por el licitador conlleva el compromiso de que, en caso de que la propuesta de adjudicación del contrato recaiga a su favor, se aportarán los documentos justificativos a los que sustituye .

Los requisitos que en el documento se declaran deben cumplirse, en todo caso, el último día de plazo de licitación y subsistir hasta la perfección del contrato. La declaración debe estar firmada por quien tenga poder suficiente para ello.

Deberán cumplimentarse necesariamente los apartados (del Índice y Estructura del DEUC) que se encuentran marcados en este Anexo.

PARTE I: INFORMACIÓN SOBRE EL PROCEDIMIENTO DE CONTRATACIÓN Y EL PODER ADJUDICADOR (Identificación del contrato y la entidad contratante; estos datos deben ser facilitados o puestos por el poder adjudicador)

PARTE II: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

Sección A: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

- Identificación

Como nº de IVA se deberá indicar el NIF o CIF (ciudadanos o empresas españolas), el NIE (ciudadanos extranjeros residentes en España), y el VIES o DUNS (empresas extranjeras).

- Información general

- Forma de participación

Sección B: INFORMACIÓN SOBRE LOS REPRESENTANTES DEL OPERADOR ECONÓMICO

- Representación, en su caso (datos del representante)

Sección C: INFORMACIÓN SOBRE EL RECURSO A LA CAPACIDAD DE OTRAS ENTIDADES

- Recurso (Sí o No)

Sección D: INFORMACIÓN RELATIVA A LOS SUBCONTRATISTAS

- Subcontratación (Sí o No y, en caso afirmativo, indicación de los subcontratistas conocidos)

PARTE III: MOTIVOS DE EXCLUSIÓN (en el servicio electrónico DEUC los campos de los apartados A, B y C de esta parte vienen por defecto con el valor 'No' y tienen la utilidad de que el operador pueda comprobar que no se encuentra en causa de prohibición de contratar o que, en caso de encontrarse en alguna, puede justificar la excepción)

Sección A: MOTIVOS REFERIDOS A CONDENAS PENALES. Motivos referidos a condenas penales establecidos en el art. 57, apartado 1, de la Directiva 2014/24/UE.

Sección B: MOTIVOS REFERIDOS AL PAGO DE IMPUESTOS O DE COTIZACIONES A LA SEG. SOCIAL. Pago de impuestos o de cotizaciones a la Seguridad Social (declara cumplimiento de obligaciones)

Sección C: MOTIVOS REFERIDOS A LA INSOLVENCIA, LOS CONFLICTOS DE INTERESES O LA FALTA PROFESIONAL. Información relativa a toda posible insolvencia, conflicto de intereses o falta profesional

Sección D: OTROS MOTIVOS DE EXCLUSIÓN QUE ESTÉN PREVISTOS EN LA LEGISLACIÓN NACIONAL. Motivos de exclusión puramente nacionales (si los hay, declaración al respecto)

PARTE IV: CRITERIOS DE SELECCIÓN

OPCIÓN 1: INDICACIÓN GLOBAL DE CUMPLIMIENTO DE TODOS LOS CRITERIOS DE SELECCIÓN

OPCIÓN 2: El poder adjudicador exige la declaración de cumplimiento de los criterios específicamente (cumplimentar todas las secciones)

- Sección A: IDONEIDAD: (información referida a la inscripción en el Registro Mercantil u oficial o disponibilidad de autorizaciones habilitantes).
- Sección B: SOLVENCIA ECONÓMICA Y FINANCIERA (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección C: CAPACIDAD TÉCNICA Y PROFESIONAL (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección D: SISTEMAS DE ASEGURAMIENTO DE LA CALIDAD Y NORMAS DE GESTIÓN MEDIOAMBIENTAL.

PARTE V: REDUCCIÓN DEL NÚMERO DE CANDIDATOS CUALIFICADOS.

PARTE VI: DECLARACIONES FINALES (declaración responsable de veracidad y disponibilidad de documentos acreditativos de la información facilitada, y consentimiento de acceso a la misma por el poder adjudicador)

**Anexo VIII.- Criterios de adjudicación cuya evaluación depende de un juicio de valor.**

NO APLICA

## Anexo IX.- Criterios de adjudicación de evaluación automática

Criterio de adjudicación 1			
Descripción	Oferta económica	Ponderación	100 puntos
Formula de valoración	$PE = PEm (1 - ((Pon - Pse)/PL))$  Donde: PE = Puntuación oferta "n" PEm = Ponderación asignada al criterio económica Pon = Presupuesto oferta "n" Pse = Presupuesto oferta más económica PL: Presupuesto de Licitación		

## Anexo X.- Modelo de proposición económica.

- Don/Doña:
- Con domicilio en:
- Calle/Plaza, nº:
- Teléfono:
- NIF ó DNI:
- Correo electrónico:

En caso de actuar en representación

- Como apoderado/a de:
- Con domicilio en:
- Calle/Plaza, nº:

Enterado de las condiciones y requisitos para concurrir al procedimiento convocado por la Sociedad Estatal Correos y Telégrafos S.A, S.M.E., para adjudicar la contratación del Expediente: ....., cree que se encuentra en situación de acudir como licitador del mismo. A este efecto hace constar que conoce los Pliegos que sirven de base a la convocatoria, que acepta incondicionalmente sus cláusulas, que reúne todas y cada una de las condiciones exigidas para contratar y que se compromete en nombre (propio o de la empresa a la que representa) a realizar el objeto del contrato con estricta sujeción a los expresados requisitos y condiciones d acuerdo con la siguiente oferta:

Importe: .....( IVA o cualquier otros impuesto indirectos equivalente Excluido)

IVA que aplica:.....%

Importe .....( IVA o cualquier otros impuesto indirectos equivalente Incluido)

Lugar, fecha, sello del licitador y firma autorizada.

SERVICIOS TRATAMIENTO DE DATOS  
INSTRUCCIONES  
Procedimiento: General Ordinario  
Expediente núm: SV260405



**Anexo XI.- Información sobre condiciones de subrogación de contratos de trabajo.**

NO APLICA

SERVICIOS TRATAMIENTO DE DATOS  
INSTRUCCIONES  
Procedimiento: General Ordinario  
Expediente núm: SV260405



## **Anexo XII.- Modificaciones previstas del contrato.**

**NO APLICA**

## Anexo XIII.- Régimen de penalidades.

### A).- INCUMPLIMIENTOS LEVES.

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Obligaciones generales	Incumplimiento de las obligaciones establecidas en este pliego y que no hayan sido tipificados como incumplimientos graves o muy graves	Hasta 1.000 euros
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, cuando no exceda del 3 por ciento del plazo.	<input checked="" type="checkbox"/> penalidades diarias en la proporción de 1 euros por cada 1.000 euros del precio del contrato, IVA excluido. <input type="checkbox"/> penalidades sobre el precio en la misma proporción que suponga el retraso respecto del plazo inicial, IVA excluido. <input type="checkbox"/> Otras penalidades por incumplimiento de plazo <i>(añadir aquí la cuantía para cada penalización por incumplimiento leve)</i>
<input type="checkbox"/> Otras	<i>(añadir aquí relación de penalizaciones por incumplimiento leve)</i>	<i>(añadir aquí la cuantía para cada penalización por incumplimiento leve)</i>

### B).- INCUMPLIMIENTOS GRAVES.

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, cuando no exceda del 5 por ciento del plazo.	<input checked="" type="checkbox"/> penalidades diarias en la proporción de 1 euros por cada 1.000 euros del precio del contrato, IVA excluido. <input type="checkbox"/> penalidades sobre el precio en la misma proporción que suponga el retraso respecto

		del plazo inicial, IVA excluido.  <input type="checkbox"/> Otras penalidades por incumplimiento de plazo <i>(añadir aquí la cuantía para cada penalización por incumplimiento leve)</i>
Adscripción de medios	Por el incumplimiento de los compromisos de adscripción de medios	Penalidad de hasta el 2 por ciento del precio del contrato, IVA excluido.
Subcontratación	Incumplimiento de las condiciones de subcontratación	Penalidad de hasta un 50 por 100 del importe del subcontrato.
Reincidencia	La comisión de una tercera infracción de carácter leve en el plazo de un año	Penalidad de hasta el 2 por ciento del precio del contrato, IVA excluido.
<input type="checkbox"/> Otras	<i>(añadir aquí relación de penalizaciones por incumplimiento grave)</i>	<i>(añadir aquí la cuantía para cada penalización por incumplimiento grave)</i>

### C).- INCUMPLIMIENTOS MUY GRAVES.

Sin perjuicio de su configuración eventual como causas de resolución del contrato, tendrán la consideración de incumplimientos muy graves:

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, o cuando la demora en el cumplimiento de aquellos haga presumir razonablemente la imposibilidad de cumplir el plazo total, o cuando superen el 5 por ciento del plazo.	<input checked="" type="checkbox"/> penalidades diarias en la proporción de 1 euros por cada 1.000 euros del precio del contrato, IVA excluido, hasta un máximo del 10 por ciento del precio.  <input type="checkbox"/> penalidades sobre el precio en la misma proporción que suponga el retraso respecto del plazo inicial, IVA excluido.

		<input type="checkbox"/> Otras penalidades por incumplimiento de plazo <i>(añadir aquí la cuantía para cada penalización por incumplimiento leve)</i>
Cumplimiento defectuoso	Por el cumplimiento defectuoso de la prestación objeto del contrato	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido, siempre y cuando el cumplimiento defectuoso no afectase a más del 20% de la prestación.
Condiciones especiales de ejecución	Por el incumplimiento de condiciones especiales de ejecución	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
Reincidencia	La comisión de una tercera infracción de carácter grave en el plazo de un año	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
<input type="checkbox"/> otras	<i>(añadir aquí relación de penalizaciones por incumplimiento muy)</i>	<i>(añadir aquí la cuantía para cada penalización por incumplimiento muy grave)</i>

SERVICIOS TRATAMIENTO DE DATOS  
INSTRUCCIONES  
Procedimiento: General Ordinario  
Expediente núm: SV260405



## **Anexo XIV - Evaluación de Proveedores.**

NO APLICA (NA)

## **Anexo XV.- Contrato de encargo de tratamiento de datos personales**

En \_\_\_\_\_, a \_\_ de \_\_\_\_\_ de 20\_\_.

### **REUNIDOS**

DE UNA PARTE,

La mercantil [-] con NIF [-] y domicilio social en calle [-] (en lo sucesivo, el “RESPONSABLE DEL TRATAMIENTO” o “[...]”), sociedad inscrita en el Registro Mercantil de Madrid al tomo [-], folio [-], sección [-], hoja [-], inscripción [-]; representada en este acto por [-], de nacionalidad española, mayor de edad y con N.I.F. [-], en virtud de la escritura de poder otorgada ante el Notario don [-], el [-], bajo el número [-] de su protocolo.

Y DE OTRA,

La mercantil [Denominación social del adjudicatario] con NIF [-] y domicilio social en [-], (en lo sucesivo, el “ENCARGADO DEL TRATAMIENTO”), sociedad inscrita en el Registro Mercantil de Madrid al tomo [-], folio [-], sección [-], hoja [-], inscripción [-]; representada en este acto por [-], de nacionalidad española, mayor de edad y con N.I.F. [-], en virtud de la escritura de poder otorgada ante el Notario don [-], el [-], bajo el número [-] de su protocolo.

Ambas partes reconociéndose capacidad jurídica y de obrar suficiente para el otorgamiento del presente Contrato de encargo de tratamiento y, al efecto,

### **EXPONEN**

- I. Que la prestación de los servicios objeto de licitación exigen el acceso del adjudicatario a los datos de carácter personal de los que resulta responsable del tratamiento CORREOS.
- II. Que con el fin de dar cumplimiento a la normativa de Protección de Datos Personales ambas partes convienen en firmar el presente Contrato de Encargo del Tratamiento, el cual comprende las siguientes:

### **CLÁUSULAS**

#### **1. Posición de las partes**

CORREOS ostenta la posición de RESPONSABLE DEL TRATAMIENTO con las funciones, derechos y obligaciones que le son propias. Y de otro lado, el adjudicatario ostenta la posición de ENCARGADO DEL TRATAMIENTO con las funciones, derechos y obligaciones que le son propias.

**DATOS OBJETO DE TRATAMIENTO**

<b>OBJETO DEL CONTRATO</b>	Se debe incluir el objeto del contrato
<b>TRATAMIENTO A REALIZAR</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Recogida</li> <li><input type="checkbox"/> Registro</li> <li><input type="checkbox"/> Estructuración</li> <li><input type="checkbox"/> Modificación</li> <li><input type="checkbox"/> Conservación</li> <li><input type="checkbox"/> Extracción</li> <li><input type="checkbox"/> Consulta</li> <li><input type="checkbox"/> Comunicación por transmisión</li> <li><input type="checkbox"/> Difusión</li> <li><input type="checkbox"/> Interconexión</li> <li><input type="checkbox"/> Cotejo</li> <li><input type="checkbox"/> Limitación</li> <li><input type="checkbox"/> Supresión</li> <li><input type="checkbox"/> Destrucción</li> <li><input type="checkbox"/> Comunicación</li> <li><input type="checkbox"/> Otros: .....</li> </ul>
<b>FINALIDAD DEL TRATAMIENTO</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Gestión de clientes, contable, fiscal y administrativa</li> <li><input type="checkbox"/> Gestión de nóminas</li> <li><input type="checkbox"/> Servicios económico-financieros y de seguros</li> <li><input type="checkbox"/> Publicidad y prospección comercial</li> <li><input type="checkbox"/> Videovigilancia</li> <li><input type="checkbox"/> Recursos humanos</li> </ul>

	<input type="checkbox"/> Prevención de riesgos laborales <input type="checkbox"/> Prestación de servicios de comunicaciones electrónicas <input type="checkbox"/> Comercio electrónico <input type="checkbox"/> Seguridad y control de acceso a edificios <input type="checkbox"/> Otros: .....
<b>TIPO DE DATOS</b>	<input type="checkbox"/> Datos de carácter identificativo <input type="checkbox"/> Características personales <input type="checkbox"/> Académicos y profesionales <input type="checkbox"/> Información comercial <input type="checkbox"/> Circunstancias sociales <input type="checkbox"/> Detalles del empleo <input type="checkbox"/> Transacciones de bienes o servicios <input type="checkbox"/> Categorías especiales de datos <input type="checkbox"/> Otros: .....
<b>CATEGORÍAS DE INTERESADOS</b>	<input type="checkbox"/> Empleados <input type="checkbox"/> Clientes y usuarios <input type="checkbox"/> Proveedores <input type="checkbox"/> Personas de contacto <input type="checkbox"/> Beneficiarios <input type="checkbox"/> Cargos públicos <input type="checkbox"/> Otros: .....

## 2. Obligaciones del adjudicatario

El adjudicatario llevará a cabo el tratamiento de datos personales derivado de la prestación del servicio contratado, de conformidad con las siguientes obligaciones:

- Llevar a cabo del tratamiento de datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular 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 (en adelante, RGPD) y Ley Orgánica 3/2018, de

5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

- Tratar los datos de acuerdo con las instrucciones de CORREOS y no destinarlos para ninguna otra finalidad.
- En el supuesto de que el adjudicatario, como Encargado del Tratamiento, reciba una solicitud legalmente vinculante mediante la cual deba comunicar datos personales dentro del alcance del presente encargo, con carácter previo, se lo notificará a CORREOS sin dilación indebida. No obstante, no existirá obligación de comunicar este tipo de notificaciones a CORREOS en caso de que el adjudicatario deba tratar esta información como confidencial (por ejemplo y entre otras, para preservar la confidencialidad de una investigación policial). El adjudicatario rechazará aquellas solicitudes que impliquen comunicar datos personales del Responsable del Tratamiento y que no sean legalmente vinculantes.
- Mantener actualizado un registro de todas las actividades de tratamiento efectuadas por cuenta de CORREOS, que contenga al menos: identificación de autorizados; categorías de tratamientos y una descripción general de las medidas técnicas y organizativas de seguridad adoptadas.
- Guardar secreto y la más estricta confidencialidad con respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo.
- Garantizar que las personas autorizadas para tratar datos personales observan las instrucciones y protocolos remitidos por CORREOS, así como las medidas de seguridad legales, técnicas y organizativas establecidas y asegurar que se comprometen, de forma expresa y por escrito, a respetar la confidencialidad de los datos y a cumplir con las instrucciones de CORREOS.
- Comprometerse a guardar bajo su control y custodia los datos personales accedidos y a no comunicarlos en modo alguno a terceros.
- Poner a disposición de CORREOS toda la información necesaria para demostrar el cumplimiento de sus obligaciones, según el proceso establecido en el punto 5.
- Asistir a CORREOS en la realización de los análisis de riesgo, la presentación de consultas previas a la AEPD, en el proceso de notificación de violaciones de seguridad y de respuesta a solicitudes de derechos.
- Gestión de derechos: Dar traslado de las solicitudes de derechos de protección de datos o quejas o reclamaciones por esta materia que puedan formular los interesados de forma inmediata a V y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción.
- El deber de secreto y confidencialidad obliga al adjudicatario durante su vigencia y perdurará indefinidamente en el tiempo una vez finalizada la relación.

- En el caso de que el adjudicatario recabe datos personales por cuenta de CORREOS se obliga a realizarlo conforme las instrucciones de V, siguiendo la redacción y formato indicado y custodiando o dando traslado a V (según proceda) de las evidencias recogidas para acreditar el cumplimiento del deber de información y, en su caso, de obtención del consentimiento.

### 3. Declaración previa

Como Adenda al presente Anexo se incluye la siguiente información facilitada por el adjudicatario:

- (i) Ubicación de los servidores en los que se almacenarán los datos personales tratados por cuenta de ; y
- (ii) Lugar de prestación de servicios objeto de licitación.

### 4. Obligaciones de CORREOS

Corresponden a CORREOS las siguientes obligaciones:

- Permitir al adjudicatario el acceso a los datos objeto de tratamiento de conformidad con lo establecido en la presente cláusula.
- Realizar el análisis de riesgos que puedan derivar de la actividad de tratamiento que va a ser objeto de encargo y, en base a tal análisis, indicar al adjudicatario las medidas técnicas y organizativas que deberá implementar para la prestación del servicio que conlleva el encargo de tratamiento.
- Realizar, si fuese necesario, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el adjudicatario.
- Realizar a la autoridad de control las consultas previas que correspondan.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del adjudicatario.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- Facilitar el derecho de información en el momento de la recogida de los datos personales y/o en el momento de dirigirse a los interesados, en caso de que se dieran estos supuestos en la prestación del servicio. El adjudicatario deberá solicitar a CORREOS dicho texto con carácter previo a dirigirse a los interesados.

### 5. Medidas de seguridad

El adjudicatario implantará las medidas de seguridad y mecanismos establecidos en el artículo 32 del RGPD y deberá adoptar todas aquellas medidas técnicas y organizativas que, a tenor del análisis de riesgo efectuado por CORREOS, éste considere que resultan

necesarias para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

## **6. Derecho de auditoría**

CORREOS, y/o sus clientes en calidad de responsables del tratamiento, a efectos de verificar el nivel de cumplimiento por parte del adjudicatario de lo establecido en la normativa aplicable y en la presente cláusula, podrá exigir la realización de auditorías, ya sea por sí mismo o por medio de auditor independiente, autorizado por CORREOS.

CORREOS notificará al adjudicatario, con al menos cinco (5) días hábiles de antelación a la fecha en que desee llevarlas a cabo.

CORREOS, y/o sus clientes en calidad de responsables del tratamiento podrán solicitar al adjudicatario la información necesaria para evaluar su nivel de cumplimiento.

Si como consecuencia de la realización de la auditoría CORREOS detectase cualquier clase de incumplimiento, de conformidad con lo establecido en la normativa aplicable y en la presente cláusula, podrá, a su sola discreción y en función de la gravedad de los mismos:

Requerir al adjudicatario la resolución inmediata del incumplimiento detectado mediante la elaboración por su parte de un plan de corrección que deberá hacerse efectivo en un plazo determinado, que no podrá exceder de un mes, debiendo el adjudicatario aportar aquellas evidencias que acrediten su resolución.

Terminar anticipadamente la prestación o prestaciones de Servicios cuyos tratamientos de datos personales se vean afectados por el incumplimiento detectado. En este caso, el adjudicatario deberá devolver a CORREOS la parte proporcional de los importes percibidos correspondientes a los Servicios que no hubieran sido efectivamente ejecutados.

## **7. Notificación de violaciones de seguridad**

El adjudicatario deberá notificar a CORREOS las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, incluyendo toda la información relevante para la documentación y comunicación de la incidencia a la autoridad de control.

La notificación de la violación de seguridad por parte del adjudicatario deberá llevarse a cabo sin dilación indebida y, en todo caso, en el plazo máximo de 24 horas a contar desde que tuvo o debió tener conocimiento de la misma aplicando el nivel de diligencia exigible a un ordenado empresario, incluyendo toda la información relevante para la documentación y comunicación de la incidencia, en la que se incluirá como mínimo:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Toda aquella otra información que resulte relevante para el conocimiento de la violación de seguridad, sus efectos sobre los derechos y libertades de las personas, así como para cumplir con el deber de notificación a los interesados y al organismo regulador que la normativa de protección de datos imponga al RESPONSABLE DEL TRATAMIENTO.

Si no fuera posible facilitar la información simultáneamente con la notificación, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

## **8. Destrucción o devolución de los datos una vez finalizado el contrato**

Una vez cumplida la correspondiente prestación del servicio objeto del Contrato, el adjudicatario se compromete a devolver a CORREOS o a la persona que éste determine aquella información que contenga datos de carácter personal a la que haya accedido el adjudicatario con motivo de la prestación del servicio.

La devolución implicará la entrega o puesta a disposición de los datos tratados en un formato de uso común e interoperable. La entrega o puesta a disposición de los soportes originales, que a su vez fueron entregados o puestos a disposición del adjudicatario por CORREOS con motivo de la prestación del servicio, en los que se almacenen o contengan datos de carácter personal.

Finalizado el proceso de devolución, el adjudicatario deberá proceder a la destrucción de los datos existentes en los equipos informáticos y otros soportes por él utilizados. No obstante, el adjudicatario podrá conservar los datos e información tratada, debidamente bloqueados, en el caso que pudieran derivarse responsabilidades de su relación con CORREOS. Transcurrido el plazo de prescripción de las acciones que motivaron la conservación de datos, el ENCARGADO DEL TRATAMIENTO deberá proceder a su destrucción. Para ello, aplicará las medidas físicas y lógicas que resulten adecuadas para garantizar que los datos incorporados a los distintos soportes son irrecuperables

## 9. Subcontratación

El adjudicatario no podrá subcontratar ninguna de las prestaciones que formen parte del objeto de este Contrato que comporten el tratamiento de datos personales, salvo previa autorización expresa y otorgada por escrito por parte de CORREOS así como los servidores y servicios relacionados con los mismos comunicados a CORREOS durante el procedimiento de licitación.

Si fuera necesario subcontratar algún tratamiento o existiese alguna novedad respecto a los servidores o los servicios relacionados con los mismos, este hecho se deberá comunicar previamente y por escrito a CORREOS indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. Con carácter previo a cualquier actividad de tratamiento por parte del subencargado, CORREOS tendrá un plazo de 30 días para oponerse.

Transcurrido el plazo de 30 días sin que CORREOS hubiese manifestado su oposición se entenderá que acepta el subencargo comunicado.

Por el contrario, en caso de oposición, si el adjudicatario mantiene la necesidad de subcontratar con un tercero la correspondiente prestación pero no propone un nuevo subcontratista que cumpla con los extremos mencionados anteriormente, CORREOS podrá resolver libremente el Contrato de servicios y reclamar los daños y perjuicios a que hubiera lugar.

En caso de autorización, el subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el adjudicatario y las instrucciones que dicte CORREOS. Corresponde al adjudicatario regular la nueva relación de conformidad con el artículo 28 del RGPD, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En el caso de incumplimiento por parte del nuevo encargado, el adjudicatario seguirá siendo plenamente responsable ante CORREOS en lo referente al cumplimiento de las obligaciones.

## 10. Cláusulas de buenas prácticas

El adjudicatario se compromete a mantener durante la vigencia del contrato adjudicado su adhesión a todos aquellos Códigos de Conducta y mecanismos de certificación que hubiesen sido valorados en la adjudicación, así como a poner a disposición de CORREOS la documentación acreditativa de su vigencia.

## 11. Responsabilidad

El adjudicatario vendrá obligado a exonerar a CORREOS de cualquier tipo de responsabilidad frente a terceros, por reclamaciones de cualquier índole que tengan origen en el incumplimiento de las obligaciones de protección de datos de carácter personal que le incumben en su condición de encargado del tratamiento, y responderán frente a la indicada Sociedad del resultado de dichas acciones. El adjudicatario vendrá también obligado a prestar su plena ayuda en el ejercicio de las acciones que correspondan a CORREOS.

## 12. Notificación de cambios

El adjudicatario comunicará a CORREOS cualquier cambio que se produzca con respecto a los términos y condiciones en los que accederá y tratará los datos personales por cuenta de CORREOS y especialmente aquellas relacionadas con la información presentada en la declaración previa recogida en la cláusula tercera del presente Anexo a la mayor brevedad, y en todo caso con carácter previo a su adopción.

## 13. Tratamiento de datos de representantes y trabajadores

Los datos personales de los representantes de las partes, así como de sus trabajadores y resto de personas de contacto que puedan intervenir en la relación jurídica formalizada serán tratados, respectivamente, por CORREOS y por el adjudicatario, que actuarán, de forma independiente, como responsables del tratamiento de los mismos. Dichos datos serán tratados para dar cumplimiento a los derechos y obligaciones contenidas en la presente licitación, sin que se tomen decisiones automatizadas que puedan afectar a los interesados. En consecuencia, la base jurídica del tratamiento es dar cumplimiento a la mencionada relación contractual.

Los datos se mantendrán mientras esté en vigor la relación contractual que aquí se estipula, siendo tratados únicamente por las partes y aquellos terceros a los que aquéllas estén legal o contractualmente obligados a comunicarlos.

Los interesados de las partes podrán ejercer, en los términos establecidos por la legislación vigente, los derechos de acceso, rectificación y supresión de datos, así como solicitar que se limite el tratamiento de sus datos personales, oponerse al mismo, o solicitar la portabilidad de sus datos dirigiendo una comunicación por escrito a cada una de las Partes, a través de las direcciones especificadas en el encabezamiento o, mediante comunicación a las siguientes direcciones

- Dirección Postal: Conde De Peñalver 19, 28006, Madrid
- Correo Electrónico: [derechos.protecciondatos.correos@correos.com](mailto:derechos.protecciondatos.correos@correos.com)

Asimismo, podrán ponerse en contacto con los respectivos delegados de protección de datos en la dirección [dpdgrupocorreos@correos.com](mailto:dpdgrupocorreos@correos.com) o [-], según corresponda, o presentar una reclamación ante la Agencia Española de Protección de Datos u otra autoridad competente.

Las partes se comprometen expresamente a informar a sus trabajadores y resto de personas de contacto de los términos de la presente cláusula, manteniendo indemne a la contraparte.

#### **14. Actuación como subencargado**

El contenido del presente contrato se aplicará, mutatis mutandis, en aquellos casos supuestos en los que CORREOS actúe como ENCARGADO DEL TRATAMIENTO y el adjudicatario como SUBENCARGADO DEL TRATAMIENTO, comprometiéndose con carácter adicional a las obligaciones previstas anteriormente a:

- Por parte de CORREOS: Asegurar que el subencargo del servicio se encuentra permitido por el RESPONSABLE DEL TRATAMIENTO.
- Por parte del adjudicatario: Cumplir con las instrucciones que le pudiesen remitir tanto CORREOS como, de manera directa o indirecta, el RESPONSABLE DEL TRATAMIENTO

#### **15. Ley aplicable**

En lo que respecta al tratamiento de datos personales que pudiera derivar de la prestación del servicio, el adjudicatario y CORREOS acuerdan someterse de manera expresa a la normativa vigente en materia de protección de datos en España y, en particular, al RGPD y LOPDGDD.

Este acuerdo ostenta el carácter de obligación esencial, por lo que su incumplimiento, por cualquiera de las partes, facultará a la otra parte a resolver el contrato y, en su caso, reclamar la indemnización por daños y perjuicios a que pudiera haber lugar.

### **MEDIDAS DE SEGURIDAD**

#### **I. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES**

- Disponer de un organigrama de asignaciones en materia de seguridad de la información, incluyendo cargos y funciones atribuidas a cada puesto.
- Contar con un procedimiento de control de accesos que incluya, entre otros:
  - o Gestión de altas/bajas en el registro de usuarios de repositorios de información asegurando que se asigna un identificador único a cada

cuenta de usuario. Excepcionalmente, podrán permitirse identificadores de usuario (IDs) genéricos para ser utilizados por un individuo, en el caso de que las funciones accesibles o las acciones llevadas a cabo por ese identificador o necesiten ser detallada seguidas (por ejemplo, acceso de sólo lectura), o cuando están implantados otros controles (por ejemplo, si la contraseña para un ID genérico sólo se utiliza por una persona al mismo tiempo y se registra tal caso).

- Gestión de derechos y credenciales de acceso asignados a los usuarios.
- Gestión de privilegios especiales de acceso según el impacto que puede derivar de un uso inadecuado de los datos de carácter personal.
- Gestión de información confidencial de autenticación de usuarios.
- Política de retirada de cancelación de accesos y credenciales.
- Haber establecido un procedimiento de accesos a sistemas y aplicaciones que incluya:
  - La restricción de acceso a la información.
  - Procedimientos seguros de inicio de sesión en el que, como mínimo:
    - Se registre los intentos de entrada no satisfactorios.
    - Se limite el número máximo de intentos fallidos, de forma que La revisión de los privilegios de acceso de forma recurrente y después de cualquier cambio, tal como promoción, degradación o terminación del empleo.
  - Procedimiento de uso de herramientas de administración de sistemas de información, tanto propias como externas.
- La revisión de los privilegios de acceso de forma recurrente y después de cualquier cambio, tal como promoción, degradación o terminación del empleo.

## II. PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

- Contar con un procedimiento de gestión de contraseñas de usuario que incluya los siguientes aspectos:
  - Forzar el uso de los identificadores de usuario (IDs) individuales y de las contraseñas para mantener la responsabilidad.
  - Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada.
  - Forzar la elección de contraseñas de calidad.

- Ser fáciles de recordar.
  - No se basen en algo que alguien más pueda fácilmente adivinar u obtener usando la información relativa a la persona, por ejemplo nombres, números de teléfono, y fechas de nacimiento etc..
  - No sean vulnerables a ataques de diccionario (por ejemplo, que no consistan en palabras incluidas en diccionario).
  - No contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos
- Forzar el cambio de contraseñas, por lo menos, cada 6 meses y siempre que existan indicios de que su confidencialidad ha podido verse comprometida.
  - Forzar a los usuarios el cambio de las contraseñas temporales después de la primera entrada.
  - Mantener un registro de las contraseñas de usuarios anteriores y prevenir su reutilización.
  - No mostrar las contraseñas en la pantalla cuando se están introduciendo.
  - No incluir contraseñas en ningún proceso de registro automático, por ejemplo almacenamiento en una macro o en una función clave.
  - Almacenar los ficheros de contraseñas por separado de los datos de la aplicación del sistema.
  - Almacenar y transmitir las contraseñas de forma que se garantice su integridad y confidencialidad.
- Plantear el uso de contraseñas basadas sistemas de autenticación fuerte (p.ej. mediante el uso de tarjetas inteligentes combinado con una contraseña).

### III. GESTIÓN DE SOPORTES

- Llevar a cabo un inventariado de soportes y gestión de activos, incluyendo:
  - Un registro de propiedad de los activos.
  - Una política interna de usos aceptables de los activos.
  - Una política de devolución/sustitución de activo.
  - Un registro de asignación de activos al personal al cargo.
- Disponer de una política seguridad de equipos y de control de acceso a los repositorios físicos de información, garantizando que los mismos cuenten con las debidas garantías de seguridad respecto a:

- El acceso a los repositorios de la información, incluyendo un registro de entradas y salidas.
- Un procedimiento de salida de activos fuera del entorno de la entidad.
- Un procedimiento de puesto de trabajo despejado y bloqueos de equipo
- Un procedimiento de mantenimiento de activos.
- Contar con una política de mesas limpias que exija que:
  - El puesto de trabajo esté limpio y ordenado.
  - La documentación que no se esté utilizando se encuentre guardada correctamente (armario bajo llave para documentos en soporte papel y carpetas de red para soportes informáticos), especialmente en el momento en que se abandona temporalmente el puesto de trabajo y al finalizar la jornada.
  - Prohibir expresamente que haya usuarios o contraseñas apuntadas en post-it o similares o que se comparta esta información.
- Disponer de una serie de normas y procedimientos de control para los puestos de trabajo desatendidos que incluya:
  - El bloqueo automático de la pantalla transcurrido un cierto período de tiempo sin que se utilice.

El apagado de los ordenadores centrales, servidores y ordenadores personales de la oficina cuando la sesión termine.

#### **IV. ACCESO FÍSICO AL LOCAL**

- Contar con un procedimiento de control de entrada y “área segura” que incluya:
  - Controles físicos de entrada.
  - Perímetro de seguridad.
  - Protección contra amenazas externas o ambientales.
  - Una política de seguridad para oficinas, despachos y recursos.

#### **V. MONITORIZACIÓN DE EQUIPOS Y REGISTRO DE LOGS**

- Disponer de un procedimiento de monitorización de equipos que incluya:
  - Identificación de las medidas de seguridad.
  - Campos de eventos que deberían ser registrados.
  - Tipología de eventos a registrar.

- Procesos de recogida y protección de logs.
- Los registros de los logs del administrador y operador de sistemas deben ser revisados regularmente.
- Resulta recomendable contar con sistemas de detección de intrusión gestionados fuera del sistema de control y de los administradores de red, para controlar el cumplimiento de las actividades del sistema y de administración de la red.

## **VI. FICHEROS TEMPORALES**

- Solo se crearán ficheros temporales cuando resulte preciso para la realización de trabajos temporales o auxiliares.
- Finalizado el trabajo que justificó su creación el fichero deberá ser destruido.

## **VII. COPIAS DE SEGURIDAD Y RESPALDO Y RESILENCIA**

- Disponer de un procedimiento de copias de seguridad y respaldo que, incluya, como mínimo los siguientes aspectos:
  - La realización de una copia de seguridad con una periodicidad mínima semanal en un segundo soporte distinto del destinado a los usos habituales.
  - Las pruebas con datos reales deberán evitarse, salvo en aquellos supuestos en que sea inevitable su uso o suponga un esfuerzo desproporcionado atendiendo al nivel de riesgo que implica el tratamiento. En estos casos con carácter previo al desarrollo de pruebas con datos reales se procederá a la realización de una copia de seguridad.
- Disponer de un Plan de continuidad de servicios TI que abarque todos los sistemas y componentes TI que procesan datos personales, incluyendo otras ubicaciones y centros de procesamiento de datos.

## **VIII. DESTRUCCIÓN DE LA DOCUMENTACIÓN**

- Disponer de un procedimiento de destrucción segura de información que:
  - Haga uso de las medidas físicas y lógicas necesarias para garantizar la irrecuperabilidad de la documentación destruida.
  - Impida que se desechen documentos o soportes electrónicos que contengan datos personales sin garantizar su destrucción.

## **IX. AMENAZAS INFORMÁTICAS**

- SEGURIDAD DE REDES: Deberá contar con una política de gestión de seguridad en las redes que:
  - o Proponga mecanismos de seguridad asociados a servicios en red.
  - o Disponga de controles de red y políticas de segregación de redes.
- ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales. El sistema de cortafuegos deberá ser actualizado de forma periódica.
- FUGA O SALIDA DE INFORMACIÓN: Introducir medidas técnicas en los sistemas de información que restringan la posibilidad que datos personales puedan ser exportados de forma no autorizada (p.ej. Restricción de las funcionalidades de descarga, impresión y almacenamiento de datos en los sistemas de información que procesan los datos personales) e implementar medidas técnicas que permitan detectar transmisiones no autorizadas de datos personales dentro de la organización y hacia fuera de la misma (p.ej. Sistemas de prevención de fugas de información, herramientas de monitorización de actividades de usuarios en los sistemas de información).

## X. CIFRADO DE DATOS

- Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá contar con un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- Todo tratamiento de datos sensibles u otros cuya pérdida de integridad, confidencialidad y/o disponibilidad puedan tener un importante impacto en los derechos y libertades de las personas se realizará en base a una política de seudonimización de los mismo frente al acceso de terceros o para la realización

de pruebas con datos reales, de manera que garanticen la integridad y confidencialidad de los mismos. Dicha política debe incluir:

- La gestión de claves para la encriptación/descriptación.
- Un sistema de etiquetado/cifrado que garantice el anonimato de los titulares de los datos.
- Un cifrado de información de dispositivos de almacenamiento (como pendrive, equipos informáticos o almacenamientos remotos).
- Una política de envío seguro de información a través de documentación cifrada.

## **XI. CONTROL DE CAMBIOS EN T.I**

- Los sistemas operacionales y las aplicaciones de software deberían estar sometidas a un estricto control de la gestión del cambio. En particular, se deberían considerar los siguientes puntos:
  - La identificación y registro de los cambios significativos.
  - La planificación y pruebas de los cambios.
  - La evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de dichos cambios. d) el procedimiento de aprobación formal de los cambios propuestos.
  - La comunicación de los detalles de los cambios a las personas correspondientes.
  - Los procedimientos de colchón, incluyendo los procedimientos y responsabilidades de abortar y recuperar los cambios infructuosos y los eventos imprevistos.
- Los procedimientos y las responsabilidades formales de la Dirección deberían asegurar de una manera satisfactoria el control de todos los cambios en los equipos, en el software o en los procedimientos. Cuando los cambios son realizados, se debería conservar un registro de auditoría que contenga toda la información importante.

## **XII. CONTROL DE CAMBIOS EN APLICATIVOS**

- Los procedimientos de control de cambios deberían estar documentados y aplicarse para minimizar la corrupción de los sistemas de información.
- La introducción de nuevos sistemas o de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación,

pruebas, control de calidad e implementación gestionada. Este proceso debería incluir:

- Una evaluación de riesgos
- Un análisis de los efectos de los cambios
- Una especificación de los controles de seguridad necesarios.
- Las medidas necesarias para garantizar que los procedimientos existentes de seguridad y control no se vean en peligro y que los programadores de la asistencia técnica sólo tengan acceso a aquellas partes del sistema necesarias para su trabajo requiriendo de consentimiento y aprobación formal para cualquier cambio.

### **XIII. GESTIÓN DE INCIDENCIAS Y BRECHAS DE SEGURIDAD**

- Contar con un procedimiento de gestión de incidencias y brechas de seguridad que permita su identificación, tratamiento y notificación al Responsable, conforme a lo dispuesto en la normativa de protección de datos.

### **XIV. VIDEOVIGILANCIA**

- En caso de contar con sistemas de captación de imágenes con fines de seguridad:
  - Se deberá contar con un registro de ubicaciones de las cámaras y monitores de observación.
  - Se deberá conservar las imágenes por el plazo máximo de 1 mes, salvo que su conservación resulte necesaria para investigar un hecho que haya afectado a la seguridad de las personas, bienes e instalaciones.

**Anexo XVI.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.**

Don/Doña \_\_\_\_\_  
NIF \_\_\_\_\_  
Con domicilio en \_\_\_\_\_  
Calle/Plaza, nº \_\_\_\_\_  
Telf. contacto nº \_\_\_\_\_  
Correo electrónico \_\_\_\_\_

En caso de actuar en representación

Como apoderado de \_\_\_\_\_  
CIF \_\_\_\_\_  
Con domicilio en \_\_\_\_\_  
Calle/Plaza, nº \_\_\_\_\_  
Correo electrónico \_\_\_\_\_

DECLARA BAJO SU RESPONSABILIDAD:

Que de conformidad con los artículos 45 y siguientes, de la Ley Orgánica 3/2007, de 22 de marzo, de igualdad efectiva entre hombres y mujeres,

- CUMPLE con la obligación de contar con un plan de igualdad.
- La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

## **Anexo XVII.- Requisitos de seguridad**

### **1. Normativa y conformidad**

La ejecución del expediente incluirá la elaboración y entrega de todos aquellos documentos cuya existencia venga derivada del cumplimiento de la legislación vigente, del marco normativo de seguridad establecido para los sistemas de información de la Sociedad Estatal de Correos y Telégrafos, S.A (en adelante, Correos) o, en su caso, sean necesarios para llevar a cabo una gestión adecuada de la solución.

El adjudicatario del servicio deberá informar a sus empleados de las obligaciones legales existentes en el tratamiento de datos de carácter personal, así como de los requerimientos de seguridad exigidos por Correos.

La empresa adjudicataria exigirá a los técnicos que formen parte del equipo de trabajo objeto de este contrato, el cumplimiento de la normativa de seguridad Correos en materia de obligaciones y funciones del personal, quedando obligada, la empresa adjudicataria, frente a Correos por las responsabilidades que puedan derivar de su incumplimiento.

### **2. Control de accesos**

En los casos en los que el adjudicatario requiera acceder a los sistemas de información de Correos para la prestación de su servicio, se realizará bajo las directrices marcadas por la Subdirección de seguridad, ya sea mediante el uso de usuarios externos proporcionados por Correos o mediante las medidas de comunicación descritas en el apartado 5. Comunicaciones.

En los casos en los que se proporcione un usuario externo por parte de Correos, se deberán asignar los privilegios mínimos necesarios para la prestación del servicio.

Asimismo, el adjudicatario tiene la obligación de notificar a Correos el alta, modificación y/o baja de los usuarios prestadores del servicio, para garantizar el bloqueo y posterior eliminación de las cuentas asociadas a los mismos.

### **3. Acceso físico**

En los casos en los que se requiera de acceso físico a instalaciones de Correos, especialmente a zonas que puedan almacenar información sensible, se deberá seguir las directrices indicadas por el Área de Seguridad Física.

Asimismo, el adjudicatario tiene la obligación de notificar a Correos el alta, modificación y/o baja de los usuarios prestadores del servicio, para garantizar el bloqueo y posterior eliminación de los accesos de estos.

Si fuera necesario acceder remotamente a sistemas de Correos para ofrecer asistencia, se proveerá de un Terminal de trabajo en remoto desde el cual se realizarán los trabajos

objeto del contrato. En ningún caso se permitirá la conexión de estaciones de trabajo del proveedor con los Sistemas de Información de Correos.

#### 4. Respaldo y recuperación

El adjudicatario, para la prestación de sus servicios, deberá disponer de un plan de contingencia ante desastres alineado con la estrategia corporativa de respaldo, siendo responsabilidad del proyecto elaborar un Plan de Contingencia que incluya las tareas y prioridades de recuperación de los componentes que permiten dar servicio al activo, ante los distintos escenarios de desastre contemplados en el Plan de Recuperación de Desastres.

En este sentido, el prestatario del servicio deberá garantizar la recuperación de los sistemas bajo unas condiciones de Tiempo de Recuperación Objetivo (RTO) y de Punto de Recuperación Objetivo (RPO), valores proporcionados por el licitador, debiendo practicar tres pruebas anuales de restauración de los activos implicados en el servicio y donde se deberá constatar, entre otras cuestiones, los valores de RTO y RPO obtenidos en la misma y las mediciones de tiempos de reacción y recuperación del servicio.

#### 5. Comunicaciones

No están permitidas aquellas conexiones que pretendan intercambiar información con componentes internos de Correos de manera directa sin “delegar” esta comunicación en componentes (gateways) de los perímetros externos.

Los protocolos de comunicaciones en los que viaje el usuario y la contraseña en claro quedan expresamente prohibidos, como por ejemplo ftp, http y telnet.

Todos los accesos remotos que sean necesarios para la prestación del servicio se realizarán a través de la plataforma Corporativa ARCO (acceso remoto seguro) basado en VPN-SSL, en ningún momento se autorizarán accesos directos a la red de Correos, ni VPNs convencionales. Los canales por los que acceder a este servicio, podrán ser la red de Internet o enlaces privados punto a punto. En el caso de que la solución de prestación del servicio sea incompatible con la comunicación descrita, el adjudicatario deberá proveer de un enlace de comunicaciones dedicado para el acceso remoto, cuyo coste será asumido por el adjudicatario.

Para el acceso remoto de Correos, si fuera necesario, se proveerá de un Terminal de trabajo en remoto desde el cual se realizarán los trabajos objeto del contrato y se accederá a los recursos internos de Correos necesarios. En ningún caso se permitirá la conexión de estaciones de trabajo del proveedor con los Sistemas de Información de Correos.

El intercambio de información entre el proveedor y Correos que no se realice mediante soportes físicos, se llevará a cabo a través de un servicio seguro de intercambio de ficheros que garantizará la protección de las operaciones y de la información intercambiada. En ningún caso se permitirá el intercambio de información entre estaciones de trabajo del proveedor y el Terminal de trabajo en remoto.

## 6. Integridad y confidencialidad

Se deben implementar los mecanismos necesarios para garantizar la integridad y confidencialidad de los datos manejados por para la prestación del servicio.

Se debe detallar a qué recursos va a requerir permisos de acceso, teniendo en cuenta siempre políticas de mínimo privilegio, es decir, solo se debe poder acceder a los recursos que sean estrictamente necesarios, justificándolos de manera pertinente.

En los casos en los que el adjudicatario del servicio disponga de una herramienta o aplicación para la prestación del servicio, se deberá tener en cuenta lo siguiente con respecto a la integridad y la confidencialidad:

- Para datos en tránsito se debe utilizar la capa TLS, en su versión 1.3 o superior, para asegurar la integridad y confidencialidad de los datos transmitidos, siendo obligatorio su uso para todas las operaciones de administración y aquellas otras, que lo requiera el nivel de confidencialidad de la información transmitida.
- Para datos almacenados de carácter confidencial o secreto, así como para las contraseñas y claves de cifrado nunca se deben almacenar en claro, debiendo aplicar mecanismos de cifrado robustos (AES 256, XML Encryption), y de integridad (RSA, SHA-2, XML Signature).

## 7. Tratamiento de datos

En los casos en los que el adjudicatario, para la prestación de servicio almacene datos de Correos o exista la posibilidad de acceso a entornos de Correos, se establece que:

- Se deben adoptar las medidas de índole técnica y organizativa necesarias establecidas en el Reglamento General de Protección de Datos (RGPD) para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Se debe identificar un responsable de tratamiento, así como el tipo de datos que se tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.
- Se deben detallar todos los flujos de datos desde que son recogidos hasta que se eliminan del sistema. Para ello, se deberá disponer de un diseño con el flujo de los datos (dibujo visual) del proceso que contenga los datos que se van a tratar, determinar los sistemas afectados, identificar ubicaciones y proveedores (todos los que intervienen en el proceso) y documentar todos los interfaces existentes con Correos y terceros (origen/destino de datos).
- En el caso de servicios en la nube gestionados por el adjudicatario, se debe informar del país de ubicación de los CPDs donde resida la información de Correos, el tratamiento de los datos solo podrá llevarse a cabo dentro del Espacio Económico Europeo o en aquellos países que hayan sido declarados de nivel adecuado mediante una decisión de adecuación de la Comisión Europea.

- Cualquier acuerdo con otras organizaciones que incluya compartir información deberá incluir un procedimiento para clasificar la información según su organización y la nuestra.

#### 8. Desarrollo seguro

En los casos en los que para la prestación del servicio sea necesario realizar desarrollos software para cumplir con los requisitos exigidos por Correos para la prestación de dicho servicio, será necesario tener en cuenta lo siguiente:

- El adjudicatario debe poder evidenciar el uso de estándares y recomendaciones de seguridad de la solución que formará parte del servicio contratado, sobre todo aquellos destinados a evitar ataques conocidos en aplicaciones expuestas a internet (SQL Injection, XSS, etc.), garantizando así un nivel mínimo de seguridad en el desarrollo de la aplicación y el código utilizado. Se debe confirmar la realización de pruebas de seguridad periódicas en la solución ofertada.
- Correos debe poder establecer exigencias de auditoría, funcionales y técnicas, sobre el nivel de cumplimiento de los principios del desarrollo seguro, para comprobar la no existencia de vulnerabilidades explotables desde el exterior. En caso de detectar alguna vulnerabilidad el adjudicatario debe asumir la resolución de estas y los costes asociados.
- En caso de que el sistema disponga de una página web pública a Internet, se debe incluir una herramienta de detección de Phishing y Pharming.
- Adicionalmente, el adjudicatario debe restringir el acceso al código fuente del programa.
- El soporte de la aplicación y las actualizaciones de la aplicación debe garantizar la compatibilidad con la versión de los sistemas usados en Correos.

#### 9. Sistemas operativos y software base

En el caso de uso de herramientas o aplicaciones para la prestación de los servicios por parte del adjudicatario, se deben seguir los siguientes requisitos:

- Se debe conocer las versiones del sistema operativo y del software de la aplicación que va a estar instalado. El software de la aplicación debe estar actualizado con los últimos parches de seguridad recomendados por el suministrador, por lo que debe existir un procedimiento de actualización. Dicho procedimiento debe ser remitido a Correos y acordar el tiempo máximo de actualización entre la publicación de un parche de seguridad y la puesta en producción, en función de la criticidad de este.
- Todos los elementos que formen parte de la aplicación deben tener implantados procedimientos de securización para el software, de manera que se garantice la eliminación de usuarios, configuraciones por defecto y minimicen los riesgos, actuando sobre los siguientes ámbitos: control de acceso, instalación, configuración, auditoría, monitorización, integridad y confidencialidad.

- Correos debe poder solicitar los controles aplicados en cada ámbito, así como los resultados de las auditorías de cumplimiento llevadas a cabo por terceras empresas.
- El soporte de la aplicación y las actualizaciones debe garantizar la compatibilidad con la versión de los sistemas usados en Correos, en caso de que haya conexión entre ellos.

#### 10. Eventos de auditoría

En los casos en los que para la prestación del servicio por parte del adjudicatario sea necesario el uso de herramientas o aplicaciones, se deberá tener en cuenta que se requerirá la generación de eventos de auditoría de seguridad para su explotación y/o integración y que, como mínimo, deben registrarse los siguientes eventos y alertas:

- Autenticación y accesos a la solución (acertados y fallidos).
- Cambios en las cuentas y grupos de usuarios y contraseñas (acertados y fallidos).
- Cambios accesos y modificaciones del sistema de log o auditoría (acertados y fallidos).
- Acciones realizadas con privilegios de administrador.
- Cambios en los privilegios asociados a cada rol.
- Registro de accesos a Información Personal (cumplimiento LOPDGDD Ley Orgánica 3/2018 /RGPD Reglamento (UE) 2016/679).

La generación de los citados eventos y trazas de auditoría de la solución deberán permitir comprobar las siguientes políticas:

- Registro de accesos (detalles de identificación, de orígenes y resultado de los mismos).
- Control de privilegios administrativos.
- Cumplimiento de la LOPDGDD/RGPD.

Los eventos de auditoría generados deberán estar disponibles para Correos, en caso de que los solicite para su revisión o integración con su sistema de correlación de eventos (SIEM). En este sentido, el adjudicatario deberá facilitar tanto su consulta como la integración y no deberá borrar los logs y trazas al menos durante un periodo de tiempo razonable.

Los posibles métodos de recepción de los eventos de auditoría (SFTP, Syslog, etc.) se definirán con la Subdirección de Ciberseguridad de Correos.

#### 11. Gestión de incidentes

El adjudicatario deberá contar con un proceso formal de gestión y notificación de incidentes de seguridad (diferenciando brechas RGPD) que le permita actuar siempre en tiempo y forma, de modo que se cumplan los requisitos legales y de disponibilidad definidos. Adicionalmente, se deberá disponer de un contacto principal en caso de

comunicación de incidentes y resolución de consultas técnicas. La comunicación de incidentes de seguridad será bidireccional, y se han de conocer tanto la persona de contacto, un buzón de correo electrónico y un teléfono para garantizar una comunicación clara, acordada y efectiva.

Por otro lado, se establecerá un procedimiento de notificación de incidentes de seguridad entre Correos y la empresa adjudicataria con el objetivo de comunicar la información existente respecto a la naturaleza del incidente, las áreas afectadas, el momento en que se ha producido, el estado actual y el grado de control del incidente por parte de la organización. En caso de tratarse de un incidente de privacidad (RGPD), susceptible de ser notificado al a Agencia española de Protección de Datos (AEPD), se actuará con la diligencia debida, para cumplir los plazos tasados de notificación. Para ello, Correos establecerá los Acuerdos de Nivel de Servicios acordados previamente con proveedor.

Cuando se detecte una sospecha fundada de que la solución o datos hayan sido comprometidos o utilizados sin autorización dentro de la prestación del servicio, el adjudicatario deberá notificar inmediatamente a Correos, proporcionando en la medida de lo posible un informe de auditoría del incidente que identifique la causa del incidente e incluya revisiones forenses, así como las acciones de mitigación llevadas a cabo, los controles de seguridad establecidos actualmente para control de riesgos y el plan de acciones de remediación que se llevará a cabo en la respuesta de dicho incidente.

## 12. Auditabilidad

El proveedor de servicios deberá aplicar los principios y requerimientos de seguridad de la información establecidos en el estándar ISO/IEC 27001, así como en el marco legal vigente en materia de protección de datos de carácter personal y otros ámbitos de aplicación. En este sentido, Correos podrá establecer exigencias de auditoría sobre el nivel de cumplimiento de los servicios contratados respecto a los requisitos de seguridad establecidos en el presente documento.

Correos se reservará el derecho de auditar de manera unilateral, por sí misma o a través de un tercero, con el único requisito de preavisar con una antelación de un mes y, de forma presencial o en remoto, todas aquellas medidas y controles que considere necesarios para verificar la seguridad de la información.

El alcance de la Auditoría será única y exclusivamente sobre el servicio que proporcione el adjudicatario, incluyendo los procesos e infraestructura hardware y software que lo soportan. En su defecto, Correos podrá exigir al proveedor del servicio afectado la aportación de ciertas evidencias de cumplimiento o, en su defecto, la realización una auditoría interna cuyo informe deberá ser firmado por una persona autorizada y con poder de representación de la empresa prestadora del servicio.

En el caso del uso de una herramienta o aplicación para la prestación del servicio, el proveedor deberá realizar a su costa y proporcionar un informe de auditoría (test de

penetración o hacking ético) realizado/s por un tercero en el último año, junto con el compromiso, en su caso, de solucionar las vulnerabilidades encontradas antes del arranque del servicio.

#### 13. Formación y concienciación

El adjudicatario deberá contar con un plan de formación y concienciación en materia de seguridad, alineado con las políticas de seguridad de Correos, adquirir las conductas adecuadas y ampliar las competencias para mejorar el servicio prestado de forma continua.

#### 14. Compromiso y aceptación de políticas de acceso y uso de infraestructura de Correos

El acceso a la red de Correos por parte de un colaborador a través de un equipo no corporativo se llevará a cabo, siendo el proveedor garante y responsable de su cumplimiento y verificación, bajo el sometimiento de las siguientes premisas:

- El proveedor responsable, garantizará que el dispositivo dispone de software de Seguridad en el EndPoint actualizado y permanentemente monitorizado, así como un proceso desatendido de gestión de parches de Seguridad. En ningún caso, el usuario del dispositivo dispondrá de permisos o privilegios de administrador en el mismo.
- Asimismo, es responsabilidad del proveedor que el software instalado esté autorizado por la empresa, esté debidamente licenciado y sea el necesario, exclusivamente, para el cumplimiento efectivo de las funciones que tenga que desarrollar en Correos.
- Correos se reserva el derecho de verificar y solicitar las evidencias que permitan comprobar que todos los puntos de este documento son cumplidos con exactitud.
- El uso inadecuado por un usuario de los recursos que represente un riesgo para la información y/o infraestructuras que la soportan, determinará de forma automática la cancelación y/o limitación de su uso por la Subdirección de Ciberseguridad de Correos.
- Asimismo, en el caso de producirse un incidente de seguridad que tenga origen en un dispositivo ajeno a Correos, la Subdirección de Ciberseguridad podrá solicitar toda la información necesaria para controlar y mitigar los efectos del mismo y el titular/es del dispositivo se obliga a prestar apoyo en la resolución del incidente, así como entregar la información registrada en el dispositivo afectado que permita la investigación y resolución del incidente.
- Todo responsable de equipos de personas y de usuarios debe gestionar de forma activa el alta/baja de las personas de las que es responsable y de sus permisos asociados, así como de verificar y controlar un uso adecuado de las credenciales de acceso a los sistemas, personales e intransferibles, debiendo velar por que el desarrollo del servicio

se realice en todo momento conforme a unas buenas prácticas de seguridad de la información.

- El usuario deberá realizar un uso responsable de sus credenciales de acceso (usuario/contraseña), siendo personales y cuya gestión corresponde exclusivamente a su titular, estando prohibido su comunicación a terceros y siendo responsable de las acciones que se realice con ellas.

#### 15. Ubicación de los datos

Es necesario especificar en qué país van a almacenarse o residir los datos. Asimismo, en caso de que el servicio se preste desde algún proveedor de Cloud, se deberá indicar cuál es el proveedor. Además, el proveedor tiene totalmente prohibida la cesión total o parcial a terceros de los datos de Correos.

Siguiendo la normativa GDPR, la aplicación o servicio contratado tendrá que cumplir con la nueva normativa europea de protección de datos (GDPR).

#### 16. Inclusión en el proceso de seguridad en el ciclo de vida de los SSII de Correos

En los casos en los que para la prestación del servicio se requiera del uso de una herramienta o aplicación, esta deberá formar parte del proceso de Correos que incluye la Seguridad en el Ciclo de Vida de los Sistemas de Información. Este proceso fija una serie de requisitos de seguridad detallados a cada nuevo sistema de Información y los grandes evolutivos, en función de los parámetros de Exposición del Sistema, Criticidad de la Información, Tipología de Usuarios y Normativa Legal Aplicable.

En caso de que la Subdirección de Ciberseguridad de Correos no establezca este conjunto de requisitos, el adjudicatario deberá identificar en qué riesgos incurre Correos, qué medidas los mitigan y el plan de acción que tiene para mitigarlos. Para poder realizar este Análisis de Riesgos, Correos facilitará el valor de la información gestionada en la solución.

## ANEXO XVIII.- Compromiso de adscripción de personal al contrato. Declaración responsable

Don/Doña \_\_\_\_\_  
NIF \_\_\_\_\_  
Con domicilio en \_\_\_\_\_  
Calle/Plaza, nº \_\_\_\_\_  
Telf. contacto nº \_\_\_\_\_  
Correo electrónico \_\_\_\_\_

En caso de actuar en representación

Como apoderado de \_\_\_\_\_  
CIF \_\_\_\_\_  
Con domicilio en \_\_\_\_\_  
Calle/Plaza, nº \_\_\_\_\_  
Correo electrónico \_\_\_\_\_

DECLARA BAJO SU RESPONSABILIDAD / MANIFIESTA

1. Disponer, adscribir y mantener durante la ejecución del contrato el siguiente personal, preciso para su correcta realización, conforme a lo establecido en el Pliego de Condiciones que rige esta contratación:

▪ **Medios Humanos**

PUESTO	TITULACIÓN	EXPERIENCIA PROFESIONAL <sup>(1)</sup>	HABILIDADES ESPECÍFICAS DEL PUESTO
Director de proyecto			
Técnico/Consultor de Huella de Carbono			
Técnico/Consultor de datos y reporte			
Técnico encargado del mantenimiento y soporte de la herramienta			

(1) Relacionada con el objeto de la licitación

2. Ejecutar el contrato con estricto cumplimiento de las obligaciones y responsabilidades que con respecto del personal adscrito al mismo incumbe al contratista, conforme a lo establecido en el Pliego de Condiciones de esta licitación.

Lugar, fecha y firma de licitador

## Anexo XIX: Declaración responsable protección de datos personales

### Cuestionario de privacidad

**En caso de obtener una puntuación de cero (0) en alguna de las preguntas del presente cuestionario de privacidad, el licitador será excluido el procedimiento de contratación.** Si el licitador hubiera aportado la planificación exigida en la pregunta 4.3, éste se obliga a su ejecución en las fechas establecidas en la misma y, su incumplimiento, podrá dar lugar a la resolución del contrato, así como el pago de los daños y perjuicios causados a Correos por dicho incumplimiento.

Para aquellos contratos ya adjudicados y en vigor a la fecha de recibir el presente cuestionario, en caso de obtener una puntuación de cero (0) en alguna de sus preguntas, la empresa adjudicataria deberá presentar a la SOCIEDAD ESTATAL CORREOS Y TELÉFGRAFOS, S.A., S.M.E un compromiso de adaptación al Reglamento 2016/679/UE, de 27 de abril, de 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 (RGPD) en el plazo máximo de un mes a contar desde la recepción del mismo. Dicho documento (se adjunta modelo) deberá presentarse junto con el presente cuestionario de privacidad.

\*AVISO PARA PEQUEÑAS Y MEDIANAS EMPRESAS:

La AEPD dispone de una herramienta fácil y gratuita denominada « Facilita RGPD ».

La herramienta genera diversos documentos adaptados a la empresa concreta, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargo de tratamiento, el registro de actividades de tratamiento, y un anexo con medidas de seguridad orientativas consideradas mínimas.

El enlace a esta herramienta es el siguiente:  
<https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIwNTAwMDkxNTQ5NjEyMTMxMDMz?updated=true>

### Questionario para la Privacidad de Proveedores:

Marque y cumplimente lo que corresponda:

D. [ ] con NIF....., actuando en su propio nombre y derecho, como profesional autónomo,

D. [ ] con NIF....., actuando en nombre y representación de la Sociedad [ ], con NIF [ ], según se desprende de poder conferido al efecto que fue elevado a público en escritura otorgada ante el Notario de [ ], D. [ ] el [ ] con el número [ ] de su protocolo, inscrita en el Registro Mercantil de [ ] en el Tomo [ ], Folio [ ], Hoja [ ]; Inscripción [ ],

### DECLARA lo siguiente:

#### Cuestiones generales

1. En caso de ser adjudicatario y realizará la prestación de servicios a Correos, accederá a datos personales objeto de protección, considerándose que realiza una actividad de TRATAMIENTO DE DATOS PERSONALES (Ejemplo: transportar correspondencia o paquetería de una provincia a otra). A estos efectos, marque lo que proceda:

1.1. ¿Tiene identificadas las actividades de tratamiento dentro de su empresa? (artículo 30.2 RGPD)

0= no dispone del registro de actividades a pesar de ser obligatorio.

5= dispone del registro de actividades actualizado y completado.

A continuación os facilitamos el enlace del Registro de Actividades de la AEPD a fin de que pueda informarse en relación a qué debe contener un registro de actividades del tratamiento conforme a las exigencias establecidas en el RGPD:

<https://www.aepd.es/agencia/transparencia/registro-actividades-tratamiento/index.html>

1.2. ¿En su empresa hay nombrado un Delegado de Protección de Datos (DPO)? (artículo 37 RGPD)

0= no dispone de DPO siendo obligatorio.

3= no dispone de DPO siendo voluntario.

5= dispone de DPO siendo obligatorio. Identifíquelo: [ ]

## 2. Medidas de seguridad

Las medidas de seguridad que debe cumplir en el marco de la prestación de servicios a Correos, deben ser las necesarias para garantizar un nivel de seguridad adecuado a la actividad objeto de la contratación, con la finalidad de proteger los datos personales a los que accederá en su condición de proveedor.

2.1. Responda si tiene una metodología de análisis de riesgos que permita implementar las medidas de seguridad [Se entiende por metodología de análisis de riesgo todo aquello que sirve para identificar, evaluar y gestionar los riesgos en relación con los tratamientos de datos personales que realizará como proveedor en la ejecución del Contrato a suscribir con Correos.

0= no dispone de una metodología de análisis de riesgos implantada.

3= dispone de metodología de análisis de riesgos pero no está implantada. Detalle sus principales características, en función de las distintas actividades que realiza para Correos

5= dispone de una metodología de análisis de riesgos implantada. Detalle sus principales características: [\_\_\_\_\_].

A continuación os facilitamos el enlace de la Guía de Análisis de Riesgos que facilita la AEPD:

<https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>

2.2. ¿Dispone de un procedimiento (o pautas establecidas) para la notificación de violaciones de seguridad de datos personales al responsable del tratamiento? (artículo 33 RGPD).

0= no dispone de un procedimiento de notificación de violaciones de la seguridad de los datos al responsable.

5= dispone de un procedimiento de notificación de violaciones de la seguridad de los datos al responsable.

A continuación os facilitamos el enlace de la Guía para la Gestión y Notificación de Brechas de Seguridad que facilita la AEPD:

<https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>

2.3. A pesar de ser algo voluntario, ¿Ha obtenido alguna certificación o está adherido a algún código de conducta en materia de privacidad?

1= No disponer de un certificado de privacidad o estar adherido a un código de conducta cuando el mismo resulta adecuado y pertinente atendiendo al nivel de riesgo del tratamiento y al servicio prestado.

5= disponer de un certificado de privacidad o estar adherido a un código de conducta cuando el mismo resulta adecuado y pertinente atendiendo al nivel de riesgo del tratamiento y al servicio prestado.

### 3. Confidencialidad

¿Puede garantizar que las personas autorizadas para tratar datos personales en el marco del Contrato a suscribir con Correos se comprometen a respetar la confidencialidad conforme a lo establecido en el artículo 28 del RGPD?

0= no

3= sí, disponen de código de conducta, o están sujetos a una obligación de naturaleza estatutaria.

5= sí, los empleados que van a realizar actividades en el marco del contrato a suscribir con Correos, han firmado un compromiso de confidencialidad.

### 4. Accountability y rendición de cuentas

A fin de valorar que tiene controles periódicos para la revisión del cumplimiento de la normativa de protección de datos, por favor, marque lo que corresponda:

¿Tiene implantados controles periódicos para la revisión del cumplimiento de la normativa de protección de datos? (artículo 24 RGPD)

0= no tiene implantados controles periódicos.

3= definidos no aplicados. **Presentar planificación de aplicación con plazo determinado.**

5= tiene definidos e implantados controles periódicos.

### 5. Subcontratación

En el caso de que parte del servicio objeto del contrato a suscribir con Correos se vaya a subcontratar con un tercero, debe garantizar que el nuevo Encargado del Tratamiento cumpla con las mismas medidas de seguridad a las que como proveedor principal está obligado (Artículo 28.4 RGPD). A tal efecto, marque lo que corresponda:

- 0= se va a subcontratar el servicio contratado sin cumplir con las obligaciones de autorización previa.
- 5= se va a subcontratar el servicio y estará debidamente regulado.
6. Transferencias internacionales  
¿Se realiza un tratamiento de datos fuera del Espacio Económico Europeo?  
Artículos 44 a 49 RGPD
- 0= se realiza Transferencias Internacionales de Datos a un país sin nivel adecuado de protección y sin ninguna garantía habilitante.
- 3= se realiza Transferencias Internacionales de Datos a un país con nivel adecuado de protección y utilizando alguna de las garantías habilitantes (cláusulas contractuales tipo, BCR's, etc.). Indique cuál/cuáles: [ \_\_\_\_\_ ]
- 5= no se realiza Transferencias Internacionales de Datos.
7. Sanciones y procedimientos inspectores
- 7.1 ¿Ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años?
- 1= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos idénticos a los prestados en este caso. **Aportar documentación justificativa de haber corregido el motivo de la infracción.**
- 3= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos distintos a los prestados en este caso.
- 5= no ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años.

7.2 ¿Tiene en la actualidad algún procedimiento sancionador/investigación abierta con la Autoridad de control?

- 1= tiene abierto procedimiento sancionador por tratamientos idénticos a los prestados en este caso.
- 3= tiene abierto procedimiento sancionador por tratamientos distintos a los prestados en este caso.
- 5= no tiene abiertos procedimientos sancionadores por infracciones de la normativa de protección de datos.

Fdo.: [\_\_\_\_\_]