

Contrato de Servicios (Expediente núm. MT260312) Contrato sometido a las Instrucciones internas de contratación del grupo Correos			
☒ Procedimiento general		☐ Procedimiento especial	
☒ Ordinario	☐ Simplificado	☐ Con invitación a un único licitador	☐ 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.	5
5. Condiciones de participación.	6
6. Licitación del contrato.	7
6.1. Comunicaciones y notificaciones electrónicas.	7
6.2. Resolución de consultas relacionadas con la licitación.	8
6.3. Envío de ofertas por medios electrónicos.	8
6.4. Documentación confidencial.	8
6.5. Adjudicación de los contratos	8
6.5.1. Procedimiento General	8
6.5.1.1. Procedimiento General Ordinario:	8
6.6. Contenido de las ofertas.	9
6.6.1. Sobre 1: documentación administrativa.	9
6.6.2. Sobre 2: Criterios de adjudicación de evaluación automática o con arreglo a fórmulas matemáticas y/o proposición económica.	10
7. Adjudicación y perfección del contrato.	10
7.1. Procedimiento de apertura de sobres y valoración de ofertas.	10
7.2. Ofertas anormalmente bajas.	11
7.3. Documentación a presentar por el propuesto como adjudicatario.	11
7.4. Adjudicación del contrato.	12

7.5. Perfección del contrato.	12
7.6. Constitución de garantías	13
8. Ejecución del contrato.....	14
8.1. Obligaciones del adjudicatario.....	14
8.1.1. Obligaciones en materia fiscal, laboral y medioambiental. .	14
8.1.2. Obligaciones relativas a la gestión de permisos, licencias y autorizaciones.....	14
8.1.3. Obligaciones del adjudicatario en materia de protección de datos	14
8.1.4. Aceptación y adhesión a las políticas de prevención de imputaciones delictivas.....	17
8.1.5. Evaluación de proveedores.....	17
8.1.6. Obligaciones esenciales del contrato.....	17
8.1.7. Condiciones especiales de ejecución.	19
8.1.8. Régimen de confidencialidad.....	20
8.2. Modificaciones del contrato.....	20
8.3. Cesión y Subcontratación.....	20
8.3.1. Cesión del contrato.....	20
8.3.2. Régimen de subcontratación.....	21
9. Cumplimiento del contrato.....	21
9.1. Responsable del contrato. Representante del contratista.....	21
9.2. Régimen de penalidades.....	21
9.3. Abonos al contratista. Facturación.	22
9.4. Recepción y liquidación.....	23
9.5. Plazo de garantía.....	24
10. Resolución del contrato.....	24
10.1. Causas de resolución.....	24
10.2. Procedimiento.....	25
11. Protección de Datos	25
11.1 Cláusula informativa de protección de datos personales recabados a través del Canal Ético	25
11.2 Información a representantes, trabajadores y personas de contacto	25
12. Régimen jurídico del contrato y reclamaciones contra este pliego...	26
Anexo I.- Características técnicas específicas del contrato.....	28
Anexo II.- Descripción y limitaciones a la licitación por lotes.....	37

Anexo III.- Resumen de metodología seguida para el cálculo del presupuesto base de licitación y el valor estimado del contrato.	38
Anexo IV.- Forma de acreditación de la solvencia económica y financiera, y técnica o profesional.	40
Anexo V.- Modelo de aval.	41
Anexo VI. - Instrucciones y recomendaciones para la presentación electrónica de las ofertas.	42
Anexo VII.- Instrucciones para cumplimentar el DEUC.	43
Anexo VIII.- Modelo de proposición económica.	45
Anexo IX.- Régimen de penalidades.	47
Anexo X. – Evaluación de Proveedores.	51
Anexo XI.- Requerimientos de seguridad.	52
Anexo XII.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad.	60
Anexo XIII. Consideraciones sobre el uso de IA en los servicios	61
Anexo XIV.- Contrato de encargo de tratamiento de datos personales	66
Anexo XV.- Declaración responsable en materia de Protección de Datos	80
Anexo XVI.- Criterios de adjudicación de evaluación automática	84

La presentación de oferta 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	Sociedad Estatal Correos y Telégrafos, S.A. S.M.E.
Órgano de contratación	Secretaría General y de Políticas Públicas mancomunadamente con la Dirección Financiera
Dirección/Subdirección gestora de la necesidad UGC	Dirección de Tecnología y Transformación Digital Subdirección de Desarrollo TI UGC28
Perfil de contratante	https://www.correos.com/perfil-contratante/
Dirección de contacto	C/Conde de Peñalver, 19 Bis. 28006, Madrid.
Responsable del contrato	Dirección/Subdirección/Área: Dirección de Tecnología y Transformación Digital Subdirección de Desarrollo TI Área de Sistemas de Gestión Comercial
	Datos de contacto: expdtesit@correos.com

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	El objeto es la contratación de una plataforma SaaS para la gestión integral de las redes sociales y su integración con la plataforma Salesforce Service Cloud, como parte del ecosistema de Atención al Cliente de la Sociedad Estatal Correos y Telégrafos S.A., S.M.E. (Correos en adelante). Adicionalmente, también se incluyen los servicios de mantenimiento y soporte y la contratación de servicios profesionales bajo demanda.
Código CPV	48900000-7 - Paquetes de software y sistemas informáticos diversos
Lotes	☒ NO ☐ SI (Ver Anexo II) Justificación de la no división en Lotes: El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica en el artículo 99.3 b) LCSP, “El hecho de que, la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución del mismo desde el punto de vista técnico” En este caso, se cumple la justificación del citado supuesto, en la medida en que no se contempla la división del contrato

	por lotes porque se mantiene un solo sistema de suscripciones del producto que afecta a los entornos de producción, preproducción y desarrollo, de forma que, la realización independiente de las diversas suscripciones comprendidas en el objeto del contrato dificultaría la correcta ejecución del mismo desde el punto de vista técnico ya que el mantenimiento del sistema, de realizarse por distintos operadores, podría provocar un riesgo para la correcta ejecución del contrato. Por lo tanto, la naturaleza del servicio imposibilita su división en partes y, en consecuencia, su división en lotes.
¿Se admite oferta integradora (lotes)?	☒ NO ☐ SI (Ver condiciones)

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	20	☐ días ☒ meses ☐ años	☐ día siguiente a la firma de aceptación de la Resolución de adjudicación ☐ día siguiente a la comunicación de inicio del contrato por la entidad contratante ☒ fecha que figure en el acuerdo de aceptación.
Prorrogable	☒ NO ☐ SI	Nº de prórrogas: Duración máxima de cada prórroga (en meses):	
El plazo máximo de ejecución será de 20 meses, a contar desde la fecha que conste en el documento de acuerdo de aceptación, suponiendo su inicio el 1 de octubre del 2026 y en todo caso finalizará el 31 de mayo del 2028, inclusive.			

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Valor estimado del contrato	134.472,00 €	Ciento treinta y cuatro mil cuatrocientos setenta y dos euros, conforme al método de cálculo especificado en <u>Anexo III</u>		
Presupuesto base de licitación	162.711,12 €	IVA/impuesto equivalente	28.239,12 €	
Anualidades (IVA, o impuesto indirecto equivalente, incluido)	2026	2027	2028	Total
	24.406,67 €	97.626,67 €	40.677,78 €	162.711,12 €

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	☐ SI	☐ 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		
	☒ NO			
Solvencia económica o financiera	☒ Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, de al menos 80.683,20 euros. ☐ Otros: ... Sobre la forma de acreditar estos requisitos, ver Anexo IV En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote			
		LOTE 1	LOTE 2	LOTE 3
	Porcentaje/Cífra volumen anual negocio.			
	☐ Responsabilidad solidaria de la ejecución del contrato de las entidades que completen la solvencia económica y financiera del licitador			
Solvencia técnica o profesional	☐ Haber realizado ... servicios de igual o similar naturaleza que 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, esto es €.			

	☒ Haber realizado un servicio de igual o similar naturaleza que 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 a 80.683,20 €. ☐ Disponibilidad de los siguientes perfiles relativos al personal: ... ☐ Cumplimiento de las medidas de aseguramiento de la calidad durante la ejecución del contrato que a continuación se relacionan: ... ☐ Acreditación del cumplimiento de las siguientes medidas de gestión medioambiental: ... ☐ Disponibilidad de la siguiente maquinaria, material y equipo técnico: ... ☒ Otros: Declaración responsable que acredite que el proveedor dispone de los perfiles con conocimientos técnicos y funcionales suficientes de las herramientas de la plataforma y sus interfaces con otros sistemas. Sobre la forma de acreditar estos requisitos, ver Anexo IV. En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote
Adscripción de medios	☐ Sí. Medios a adscribir: ... ☒ No. No aplica.

Se exige 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 incursos 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 **tres días naturales antes de la finalización del plazo para la presentación de ofertas**.

6.3. Envío de ofertas por medios electrónicos.

Las ofertas se presentarán en **plazo de 30 días naturales** 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 el [Anexo VI](#)).

Cada licitador no podrá presentar más de una proposición. Tampoco podrá suscribir una proposición en unión temporal con otras empresas si lo ha hecho individualmente o figurar en más de una UTE. La contravención de este principio dará lugar a la exclusión de todas las presentadas.

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

6.5.1.1. Procedimiento General Ordinario:

A. Sin negociación:

Se propone como procedimiento de contratación el Procedimiento General sin negociación en base a lo dispuesto en el punto 11 de las Instrucciones aplicables a la Contratación de las entidades que forman parte del Grupo Correos, siendo el único criterio de adjudicación la mejor relación coste-eficacia, de acuerdo con lo establecido en las citadas instrucciones.

En el procedimiento general sin negociación, cualquier operador económico interesado podrá presentar una oferta en respuesta a un anuncio de licitación, por ello se considera que es el procedimiento más adecuado para garantizar la mayor

conurrencia competitiva posible.

☒ Único Criterio de Adjudicación: MEJOR RELACIÓN COSTE-EFICACIA.

Como criterio de adjudicación se considera la mejor relación coste-eficacia al ser empleados únicamente criterios automáticos y no utilizarse criterios sujetos a juicio de valor.

Debido a que se pretende contratar un servicio de contratación de suscripciones, con las prestaciones perfectamente definidas técnicamente y no es posible introducir modificaciones de ninguna clase, es por consiguiente el precio el único factor determinante de la adjudicación.

Relación coste-eficacia sobre la base del precio, porque se pretende conseguir el precio más favorable. De esta forma los operadores económicos que intervengan en la licitación presentarán su mejor oferta, todo ello, con la finalidad de que Correos, obtenga el mejor precio posible del mercado.

La puntuación final estará compuesta por la suma de la puntuación asignada en los criterios evaluables mediante fórmula o automáticamente.

En caso de incurrir en empate entre varias ofertas tras aplicación de los criterios de adjudicación, se acudirá a lo dispuesto en el art. 147.2 LCSP relativo a los criterios de desempate.

Tipología	Criterio	Ponderación
Criterios sujetos a un juicio de valor	Técnico	0%
Criterios evaluables mediante fórmula o automáticamente (Anexo XVI)	Técnico	0%
	Económico	100%

6.6. Contenido de las ofertas.

6.6.1. Sobre 1: documentación administrativa.

- Documento Europeo Único en materia de Contratación (DEUC). Complimentado conforme a las indicaciones contenidas en el [Anexo VII](#), firmado por el licitador o su representante.
- En su caso, compromiso de adscripción de medios, según lo indicado en el Apartado 5.
- 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) Declaración responsable en materia de Protección de Datos, Anexo XV

6.6.2. Sobre 2: Criterios de adjudicación de evaluación automática o con arreglo a fórmulas matemáticas y/o proposición económica.

La proposición económica se ajustará al modelo que se incluye como ejemplo en el [Anexo VIII](#).

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

El importe sin impuestos total de la oferta no debe superar el importe de la base del presupuesto base de licitación establecido en el [Anexo III](#) del Pliego. La superación la base del presupuesto base de licitación de licitación dará lugar a la exclusión del licitador.

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 Nº 2", en archivo ejecutable con formatos *.pdf, *.doc, *.docx, *.xls.

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.

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:

☒	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.
☐	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.

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:

☒	Los que acrediten la personalidad del empresario y su ámbito de actividad.
☒	Los que acrediten la representación.
☒	Resguardo de haber constituido la garantía definitiva y, en su caso, complementaria.
☐	En el caso de contratos reservados, documentación que acredite oficialmente su condición como entidad que le faculta para resultar adjudicataria del contrato reservado.
☐	Los que acrediten disponer de la habilitación empresarial o profesional para la realización de la prestación objeto de contrato.
☒	Documentos que acrediten su solvencia económica, financiera y técnica o profesional por los medios que se especifiquen en el Anexo IV . 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,
☒	Acreditación de la inexistencia de deudas tributarias y con la Seguridad Social, mediante la presentación de los correspondientes certificados emitidos por los organismos competentes.
☐	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
☒	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.
☒	Contrato de Encargo de Tratamiento de Datos, conforme al modelo consignado en el Anexo XIV .
☒	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 (Anexo XII).
☐	Otros

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 del acuerdo de aceptación 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 la 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	☒ 5% del importe de adjudicación del contrato o el lote o lotes adjudicados (IVA excluido).		Si el licitador la constituye mediante aval, deberá utilizar el modelo incluido como Anexo V. Si utiliza otro medio, 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	☐ NO ☒ SI	Importe	☒ 5% sobre el importe de adjudicación (en caso de oferta anormalmente baja (IVA excluido). ☐ Otros: ...
Constitución de garantía provisional	☒ NO ☐ SI	Importe	3% del Presupuesto Base de Licitación (IVA excluido)
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. 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.			

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:

☒ NO procede subrogación de trabajadores
☐ SI procede la 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 XIV](#) 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.
2. Si el desarrollo del servicio objeto de licitación implicase una comunicación de datos ya sea de la entidad contratante (como cedente) al adjudicatario (como cesionario), del adjudicatario (como cedente) a la entidad contratante (como cesionario) o recíproca, el adjudicatario se compromete a regular la comunicación de datos a través de una adenda cuyo cumplimiento garantice que la comunicación de datos se realiza bajo las exigencias previstas en la normativa de protección de datos vigente y, entre otras, recoja los siguientes aspectos:

El compromiso por parte del cedente de que:

- I. Los datos personales han sido obtenidos conforme con la legislación vigente, siendo lícita su comunicación y posterior tratamiento para las finalidades enumeradas en el Pliego.
- II. Los datos personales son tratados de conformidad con la normativa vigente en materia de protección de datos, y en particular, el RGPD y LOPDGDD.

El compromiso por parte del cesionario de:

- I. Utilizar los datos personales exclusivamente para las finalidades expuestas en el Pliego y, en caso de querer utilizarlos para otras finalidades, solicitar el previo consentimiento del cedente o de los propios interesados (en caso de ser éste necesario).
- II. Tratar los datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular, el RGPD y la LOPDGDD.

El compromiso por ambas partes de prestarse asistencia mutua y colaborar activamente en todos aquellos procedimientos que afecten a la comunicación de datos, incluyendo su uso posterior, especialmente en lo que respecta a: Análisis de Riesgo y Evaluaciones de Impacto, Gestión de Derechos, Notificación de Brechas de Seguridad e interlocución ante el organismo regulador.

Que cada una de las partes será responsable del incumplimiento de las obligaciones que le correspondan, según lo previsto en el mismo,

respondiendo 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 de este 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 X](#).

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:

☐	Mantenimiento de adscripción de medios personales o materiales
☒	Condiciones especiales de ejecución del contrato
☐	Aspectos que se hayan considerado como criterios de adjudicación
☐	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
☒	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: https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf
☒	Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia.
☒	Otras: Tareas propias de la gestión del servicio que permitan conocer en todo momento el cumplimiento de los niveles de servicio de este.

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
Condiciones especiales de ejecución del contrato	Anualmente. Durante el periodo de ejecución del contrato	Según se indica en el punto 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: https://cwwetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf	Anualmente. Durante el periodo de ejecución del contrato	Los proveedores deben proporcionar la documentación que respalde el cumplimiento del programa de prevención de riesgos penales establecido por Correos
Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia.	Se deben realizar auditorías y controles anuales para asegurar el cumplimiento continuo	Los proveedores deben proporcionar la presentación de documentación que respalde el cumplimiento de las obligaciones legales, como políticas de privacidad, registros de tratamiento de datos, informes de auditoría.
Tareas propias de la gestión del servicio que permitan conocer en todo momento el cumplimiento de los niveles de servicio de este	Verificaciones periódicas, que serán mensuales	Mediante realización de reuniones de seguimiento y presentación de informes sobre el

		servicio.
--	--	-----------

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:

☐	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
☐	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 https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf
☐	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 deeuros
☐	Establecimiento de un plan de formación para los empleados adscritos a la ejecución del contrato en materias relacionadas con: ☐ Prevención de riesgos laborales específicos en el marco del servicio a prestar ☐ Otro
☐	Establecimiento de un sistema de gestión diferenciada para los residuos que pueda generar la prestación del servicio.
☐	Establecimiento de medidas que garanticen la igualdad de trato y no discriminación, así como la inclusión de miembros de grupos vulnerables.
☒	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.
☒	Condición de carácter social o medioambiental: Emplear en la ejecución del contrato un porcentaje de trabajadores fijos igual o superior al 20 por 100.

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	Verificaciones anuales	Informe detallado y certificaciones que demuestren el cumplimiento con la normativa de protección de datos
Condición de carácter social o medioambiental: Emplear en la ejecución del contrato un porcentaje de trabajadores fijos igual o superior al 20 por 100	ANUALMENTE. Durante el periodo de ejecución del contrato	A través de registro de empleados

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

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

☐ NO ☒ SI

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.

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 IX](#). 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, al tratarse de suscripciones, se efectuará al comienzo de la contratación 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/Ad ministrativeCentre/CentreC ode
Descripción de la operación		Facturae/Invoices/Invoice/A dditionalData/InvoiceAdditi onallInformation
Fecha de la operación		Facturae/Invoices/Invoice/I nvoiceIssueData/Operation Date
Grupo Gestor		Facturae/Parties/BuyerPart y/AdministrativeCentres/Ad ministrativeCentre/CentreC ode (RoleTypeCode 02)
Nº línea del pedido		Facturae/Invoices/Invoice/I tems/InvoiceLine/Sequence Number
Referencia legal		Facturae/Invoices/Invoice/I tems/InvoiceLine/Additional LineItemInformation

La adjudicación conlleva la aceptación del requisito de facturación electrónica.

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.

☐	SIN PLAZO DE GARANTÍA.
☒	GENERAL, de tres meses desde la recepción de conformidad del servicio.
☐	ESPECÍFICO, de meses desde la recepción de conformidad del servicio...

Durante el periodo de garantía se debe reportar las incidencias y en el plazo máximo en horas (a contar desde la fecha/hora de comunicación de la incidencia por parte de Correos) al que se compromete para la resolución de las incidencias detectadas, en las mismas condiciones que durante el período de vigencia del contrato.

Por cada incumplimiento durante el período de garantía de cualquiera de estos plazos (o de los ofertados si fueran mejores) en cualquier incidencia, la devolución del importe total de la fianza se disminuirá de igual manera que durante la vigencia del contrato.

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:

☒	Las previstas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público
☒	El incumplimiento de obligaciones calificadas expresamente como «esenciales» en este Pliego, de acuerdo con lo establecido en el Apartado 8.1.5
☒	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
☒	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
☒	El cumplimiento defectuoso de la prestación, cuando afecte a más del 20% de dicha prestación
☒	El incumplimiento por el contratista de los plazos de pago a sus proveedores o subcontratistas
☒	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
☒	El desistimiento de la ejecución del servicio por la entidad contratante por circunstancias sobrevenidas, aun cuando se hubiera comenzado dicha ejecución.

☒	Incumplimiento de las condiciones especiales de ejecución, de modo que se frustre el objeto del contrato
-------------------------------------	--

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:

Para Correos:

- Dirección Postal: Conde De Peñalver 19, 28006, Madrid
- Correo Electrónico: 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:

Para Correos:

- Dirección Postal: Conde de Peñalver 19, 28006, Madrid
- Correo Electrónico: derechos.protecciondatos.correos@correos.com

Asimismo, podrán ponerse en contacto con el delegado de protección de datos en la dirección: 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 regirá, 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 las cuestiones relativas a los efectos, cumplimiento y extinción del contrato se regirán 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:

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos
☒	Aceptación del acuerdo de aceptación de adjudicación
☒	Los proyectos o programas de trabajo que se hubiera presentado el adjudicatario
☒	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

En Madrid, a 30 de julio de 2026
CONFORME:

RESPONSABLE DEL ÁREA DE
SISTEMAS DE GESTIÓN COMERCIAL

EL SUBDIRECTOR DE DESARROLLO
TI

FDO. JUANA M^a FERNÁNDEZ MAÑAS

FDO. CARLOS SUAREZ ÁLVAREZ

RESPONSABLE DE UNIDAD DE
TRANSFORMACIÓN Y ATENCIÓN AL CLIENTE

FDO. NORBERTO RUIZ ESPINOSA

V^ºB^º:
LA DIRECTORA DE TECNOLOGÍA Y
TRANSFORMACIÓN DIGITAL

V^ºB^º
LA DIRECTORA COMERCIAL

FDO. CRISTINA TARRERO MARTOS

FDO. YOLANDA ORCAJADA DE LA TORRE

Anexo I.- Características técnicas específicas del contrato.

La plataforma Salesforce Service Cloud está compuesta por diversas herramientas nativas que dan cobertura a los diferentes canales de contacto de los clientes. Desafortunadamente, no cuenta con una herramienta que permita dar cobertura al canal de Redes Sociales, por lo que es necesario contratar una aplicación que permita gestionar y atender este canal por parte del área de Atención al Cliente.

El proveedor deberá proveer a Correos de los servicios de suscripción, mantenimiento y soporte, en modalidad de contratación de “Software como servicio” (SaaS – de sus siglas en inglés “Software as a Service”), durante el plazo de ejecución del presente expediente, así como atender los requerimientos de Correos relativos a la evolución de la solución, de los siguientes servicios:

- **Plataforma de gestión de redes sociales:** La plataforma de gestión integral de redes sociales deberá tener las siguientes características técnicas y funcionales:
 - Debe disponer de una conexión nativa o certificada con Salesforce Service Cloud.
 - Debe soportar picos de volumen sin degradación del funcionamiento.
 - La plataforma debe presentar una interfaz clara, intuitiva y con baja curva de aprendizaje.
 - Debe permitir una gestión inteligente de la bandeja de entrada, centralizando todas las interacciones, comentarios públicos, mensajes privados, respuestas a historias, menciones, formularios o mensajes generados desde anuncios y comentarios de múltiples redes sociales (Instagram, Facebook y Twitter/X, con posibilidad de ampliación a otras) en un único lugar, optimizando así la gestión de los mensajes.
 - La bandeja de entrada tiene que ser capaz de:
 - Identificar automáticamente los mensajes que requieren respuesta: casos urgentes, quejas, preguntas frecuentes, conversaciones repetidas.
 - Priorizar según el sentimiento, número de seguidores y etiquetas.
 - Enrutar y asignar automáticamente casos a colas o agentes según reglas configurables.
 - Crear flujos escalables.
 - Mostrar de forma clara si una interacción es pública o privada y tener fácil visualización cuando están asociadas.
 - Poder visualizar de forma clara la conversación completa.
 - Crear y aplicar etiquetas personalizadas a los mensajes entrantes.
 - A la hora de redactar las respuestas, la plataforma debe permitir:
 - Utilizar plantillas de respuestas.
 - Reutilizar respuestas ya guardadas.
 - La configuración y envío de mensajes automáticos.
 - Disponer de detección de idioma y análisis de sentimiento.
 - Automatizaciones de respuestas basadas en reglas avanzadas para, por ejemplo, detectar casos relacionados con una incidencia y mandar un mensaje automático.
 - Tener un acortador de enlaces integrado.

- La plataforma debe mantener:
 - Visualización de:
 - Publicación original.
 - Otros comentarios del hilo.
 - Perfil completo del usuario (incluyendo post recientes en el caso de X).
 - Respuesta en público con posibilidad de mover conversación a privado y eliminar las menciones no relevantes.
 - Contador de caracteres por red social.
 - Gestión correcta de visibilidad privada/pública sin inconsistencias.
- Integración entre Salesforce y redes sociales: Se tiene que poder conectar perfiles de redes sociales con los contactos y clientes potenciales de Salesforce, permitiendo una vista unificada del cliente (Cliente 360).
- Para la integración con Salesforce, se tiene que poder automatizar flujos y configurar el enrutamiento automático de casos, y las respuestas dadas a los casos en Salesforce deben poder enviarse a la red social correspondiente a través de la plataforma.
- La creación automática de casos tiene que permitir distintos criterios tales como:
 - Tema.
 - Tipo de mensaje.
 - Idioma.
 - Sentimiento.
 - Palabras clave (incluida detección de comentarios sensibles).
 - Número de seguidores.
 - Estado VIP del usuario.
- La plataforma debe mantener el historial completo del cliente, incluyendo datos tales como:
 - Conversaciones anteriores, aunque sean en distintas redes sociales.
 - Notas internas y comentarios de los agentes.
 - Datos básicos del usuario tales como Nick y datos de contacto.
- La plataforma tiene que permitir asociar a cada caso un contacto de identidad social, independientemente de la red social que provenga, y que permita las siguientes posibilidades:
 - Vincular varios perfiles sociales al mismo contacto general, incluyendo mínimo Nick y número de seguidores.
 - Calificar contactos (por ejemplo, detectar trolls o calificación de perfiles problemáticos) y poder aplicar medidas restrictivas.
 - Posibilidad de asociar el perfil de redes sociales al contacto general de Salesforce, de cara a poder asociar todos los contactos de un mismo usuario.
- El enrutamiento y asignación automática de casos debe tener las siguientes características:
 - Clasificar los mensajes entrantes y asignarlos al equipo adecuado.
 - Crear reglas automáticas (por palabra clave, idioma, red social, prioridad, etc.).

- Poder configurar flujos escalables (automatizar asignaciones basadas en reglas avanzadas, configurar flujos para derivar casos según criterios operativos).
- Se tiene que poder enviar leads a Salesforce y crear nuevos contactos que conecten con nuestros canales de redes sociales.
- La plataforma debe tener capacidades de monitoreo y escucha social para poder así rastrear palabras clave, menciones de marca, competidores y tendencias del sector y estar al día sobre lo que se comenta en las redes sociales.
- Debe tener capacidad de realizar análisis e informes detallados sobre el rendimiento de las redes sociales, configurar paneles de control con distintas métricas para hacer seguimiento y que sean adaptables a distintos roles de usuarios, permitir informes personalizados y creación rápida de los mismos a partir de plantillas, exportación, proporcionar evaluaciones comparativas del sector y los competidores.
- Se valorará positivamente que la plataforma sea capaz de integrarse con Salesforce para obtener datos y así poder crear informes de gestión de casos que incluyan métricas tales como:
 - Tiempo de primera respuesta.
 - Tiempo de resolución.
 - Tiempo medio de cierre.
 - Tipo de mensaje.
 - Cierres y reaperturas.
 - Productividad por agente.
 - Volumen de casos separados por red social.
 - Satisfacción del cliente.
- La plataforma debe permitir la creación de encuestas de satisfacción que puedan ser enviadas a los clientes en formato URL para la valoración de la atención recibida, y que estas puedan ser enviadas de forma automática dependiendo del tipo de caso.
- La plataforma debe permitir acceso federado desde Salesforce que evite que el usuario se tenga que estar logando en los dos sistemas si accede desde Salesforce.
- La plataforma debe incluir funciones de seguridad, cumplimiento y gobernanza que garanticen y proporcionen:
 - Protección de datos según normativa europea de privacidad.
 - Gestión y configuración de permisos por roles.
 - Trazabilidad de acciones.
 - Auditoría.
 - Capacidades avanzadas de compliance y governance.
 - Registro de actividad de usuarios y suscripciones.

El proveedor deberá colaborar en todo momento con la empresa que está realizando las tareas de mantenimiento y evolución de Salesforce para que los trabajos que haya que realizar de manera conjunta se lleven a cabo de una forma diligente, efectiva y satisfactoria.

El proveedor deberá proporcionar las suscripciones de **40 usuarios** de la plataforma ofertada **durante 20 meses**.

La plataforma que resulte seleccionada debe incluir las configuraciones iniciales y puesta en marcha incluida en el precio.

El suministro de la plataforma deberá incorporar una garantía integral que asegure la resolución de todas las incidencias propias del producto, garantizando de esta forma su correcto funcionamiento y disponibilidad a lo largo de toda la vigencia del contrato. El objetivo de esta garantía es solicitar que el proveedor, se comprometa a responder y solucionar de forma eficaz los problemas inherentes al producto, asegurando el soporte del fabricante, manteniendo los niveles de servicio acordados. Estas garantías deberán abarcar:

1. Soporte implícito y correctivo, entendido como reparaciones resultantes de avería, incidencias o anomalías que afecten a los elementos que conforman la solución presentada, o a los servicios soportados por la misma, con el objetivo de sostener la solución plenamente operativa, mediante la corrección de disfunciones e ineficiencias que puedan ponerse de manifiesto y que impliquen corrección de la infraestructura que tenga incidencia o problema, para conseguir la restitución del servicio.
2. La administración, gestión y resolución de todas las incidencias que supongan problema de funcionamiento de la solución, tanto las detectadas preventivamente, como las producidas y escaladas por las áreas técnicas de Correos (Arquitectura, Ingeniería, Seguridad). La comunicación de incidencias y de los problemas se centralizará a través de un canal entre Correos y el adjudicatario, y se gestionará en una herramienta denominada POST perteneciente a los sistemas de Correos. El adjudicatario, de conformidad con lo establecido con Correos, deberá cumplir el procedimiento propuesto para la comunicación, seguimiento y documentación de las incidencias.
3. Actualizaciones de versiones, mejoras técnicas y funcionales. En este sentido, la empresa adjudicataria deberá informar previamente y con la antelación suficiente a Correos, acerca de la evaluación y el diagnóstico del posible impacto que cualquier actualización pueda tener sobre los sistemas y aplicaciones de Correos.
4. Facilitar las explicaciones funcionales y técnicas sobre el funcionamiento de las herramientas con el nivel de detalle que se requiera en cada momento.

➤ **Servicios profesionales de 500 horas, en modalidad bajo demanda:**

Adicionalmente y dadas las especiales características técnicas, así como la criticidad que estos servicios tienen para Correos, se hace necesaria la realización de labores de mejora de la plataforma y puesta en marcha de nuevas configuraciones para optimización de determinadas funcionalidades tales como:

- ✓ Implementación y puesta en marcha.
- ✓ Asistencia técnica avanzada.
- ✓ Configuración avanzada de integración en Salesforce.

- ✓ Formación a usuarios.

Para la realización de estas labores de mejora de la plataforma y puesta en marcha de configuraciones “ad hoc” se han estimado un máximo de 500 horas durante el plazo de ejecución del proyecto de las que solo serán abonadas las realizadas a solicitud de Correos (modalidad bajo demanda).

CONCEPTO	UNIDADES
Servicios profesionales (horas)	500

➤ **Cambio de plataforma de gestión de redes sociales:**

El proveedor deberá comenzar sus servicios el día 1 de octubre de 2026 para que se puedan realizar todas las configuraciones iniciales necesarias para poner en marcha la plataforma el día 25 de octubre de 2026 y de esta forma poder continuar dando el servicio de atención en redes sociales en Correos sin ningún tipo de interrupción.

En caso de que el adjudicatario proponga utilizar herramientas de Inteligencia Artificial para cualquiera de las tareas incluidas en la prestación de estos servicios, deberá ajustarse a lo indicado en el Anexo XIII.- Consideraciones sobre el uso de IA en los servicios.

SEGUIMIENTO Y GESTIÓN DEL SUMINISTRO

Las suscripciones y los servicios a prestar deben estar basados en una garantía de efectividad por parte del adjudicatario, puesto que, como consecuencia de la elevada complejidad técnica de las labores a desarrollar, deberá tener presente una elevada especialización.

Por lo tanto, el adjudicatario se compromete a poner en marcha el sistema de seguimiento del **Acuerdo de Nivel de Servicio, ANS**, en un plazo máximo de 15 días hábiles desde la fecha de inicio del servicio.

A estos efectos, el adjudicatario deberá utilizar el sistema corporativo de gestión de peticiones e incidencias, utilizado como fuente de información para el seguimiento del ANS, sistema que actualmente se denomina POST, basado en ITSM Remedy, o la herramienta que, en su caso, determine Correos. En esta línea, el proveedor se compromete a cumplir las siguientes directrices:

- Integrarse como grupo de soporte en la citada herramienta. Para ello, el proveedor deberá disponer de los perfiles acreditables con conocimientos técnicos y funcionales suficientes sobre las herramientas de la plataforma y sus interfaces con otros sistemas de Correos garantizando que el servicio esté siempre cubierto con independencia de vacaciones, bajas y demás circunstancias ajenas a Correos.
- Realizar y liderar la gestión de incidencias y peticiones a través de la herramienta corporativa, no estando permitido el intercambio de correos electrónicos para esta gestión, salvo autorización expresa de Correos. En este sentido, no se certificará ninguna tarea que no haya sido registrada en la citada herramienta,

al ser ésta la fuente de información para la obtención del ANS.

- Se establecerá una reunión mensual, o con la periodicidad que se decida de mutuo acuerdo entre Correos y el adjudicatario, al objeto de revisar la medición y cumplimiento del ANS.
- No obstante, el proveedor se compromete a aportar un sistema complementario, si el seguimiento de los indicadores de los acuerdos de nivel de servicio acordados inicialmente o, en su caso, del que resulte de modificaciones posteriores lo requiera. Este sistema complementario deberá ser autorizado, de manera previa y expresamente por Correos.

CONDICIONES DE PRESTACIÓN DEL SERVICIO

Los trabajos se llevarán a cabo de forma habitual en las propias oficinas del adjudicatario, el cual se obliga a disponer de la infraestructura técnica (Comunicaciones, Software y Hardware) adecuada para poder desarrollar los trabajos de forma remota. Dicha infraestructura deberá seguir los estándares que Correos fije al respecto, cumpliendo las normas de seguridad y arquitectura definidas.

En cualquier caso, todos los costes de la mencionada infraestructura serán a cargo del adjudicatario, no debiendo afectar al precio de la oferta.

Si bien la actividad del equipo de trabajo se desarrollará normalmente dentro de un horario de oficina, los licitantes deberán comprometerse a una total disponibilidad horaria del equipo de trabajo (incluyendo noches, sábados, domingos y festivos) cuando la criticidad o urgencia de las peticiones así lo exijan (ej. para la apertura de incidencias normales y/o críticas vía correo electrónico, o por teléfono)

La realización del trabajo fuera del horario habitual no tendrá una consideración especial a efectos de cómputo de horas o tarifa aplicable a las mismas. Esta circunstancia ha de tener la aprobación previa del Director Técnico de Correos.

Las condiciones estándar de prestación de los diferentes servicios será el siguiente:

- Soporte 24x7 para la apertura de incidencias a nivel de servidor/hosting.
- Soporte 8x5 (en horario de oficina) para resolución de incidencias/consultas a nivel de proyecto.

PUESTOS CLIENTES DEL EQUIPO DE TRABAJO

La empresa adjudicataria deberá proveerse de sus propias licencias/suscripciones de software cliente para el desempeño de tareas ofimáticas en el entorno de Correos por parte del equipo de trabajo encargado de la prestación de los servicios objeto del presente contrato (por ejemplo, Office 365 y/o similares).

ECOSISTEMA SOFTWARE

Mediante la aceptación de la presente cláusula, el adjudicatario se compromete a no realizar modificaciones del ecosistema software de Correos, que no se detallen específicamente en el pliego, tales como la activación/modificación/desactivación de opciones, productos y servicios de las licencias ya existentes, o la descarga,

instalación, activación y suscripción de cualquier software. Cualquier modificación del ecosistema software no especificada en el contrato debe ser previamente solicitada y autorizada por parte de Correos.

El adjudicatario será responsable de velar por el cumplimiento de esta norma por parte de todo su personal al servicio de Correos durante toda la ejecución del contrato, asumiendo los posibles costes y demás responsabilidades de toda índole que pudieran derivarse de su incumplimiento, independientemente de la causa del mismo, ya sea por desconocimiento, falta de formación y/o de experiencia, negligencia o mala praxis. Tras la adjudicación y antes del inicio del servicio Correos, en el caso de que el adjudicatario así lo solicitase, facilitará una descripción de las plataformas software a las que tendrá acceso el personal del adjudicatario encargado de prestar el citado servicio, incluyendo información de las licencias de software en el caso de solicitarlo. Correos también facilitará al adjudicatario los permisos pertinentes para que, bajo su supervisión, pueda acceder a las citadas plataformas software. Adicionalmente, si el adjudicatario lo estima oportuno, podrá pedir a Correos las aclaraciones y/o información adicional que requiera para conocer la citada configuración del ecosistema software en el que prestará su servicio.

ACUERDO DE NIVEL DE SERVICIO (ANS)

Dentro de la presente contratación, las prestaciones que se indican a continuación se regularán por el sistema de “Acuerdo de Nivel de Servicio”. En consecuencia, las tareas correspondientes deberán realizarse ajustándose a los “Indicadores de nivel de servicio (INS)” y “valores objetivos” (VO) detallados a continuación.

Estos INS y VO tienen carácter obligatorio y de mínimos, aun así, el adjudicatario se compromete a ampliar los indicadores que Correos le solicite y a establecer de común acuerdo VO para todos ellos. Dentro de su oferta, el adjudicatario podrá mejorar los Valores Objetivo mínimos establecidos.

El adjudicatario, dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los VO establecidos, con independencia de los recursos que para ello tenga que incorporar en cada momento.

Para la prestación de los servicios objeto de este contrato se deberán establecer unos niveles de servicios mínimos que el adjudicatario se comprometerá a garantizar durante el periodo de ejecución de este.

DISPONIBILIDAD DEL SERVICIO:

El indicador utilizado para medir la disponibilidad del servicio es el Optime. El Uptime es el porcentaje de tiempo durante el cual la plataforma está disponible para Correos, es decir el software trabaja sin interrupciones, excluyendo las operaciones de mantenimiento programadas.

Se considerará no disponible solo si es completamente inaccesible o si el mal funcionamiento del software por causa de la plataforma impide por completo su uso por parte de Correos.

Update	Disponibilidad (%)
Mensual	99.00%
Trimestral	99.50%
Anual	99.99%

- ✓ **El Uptime mensual** se calcula sobre meses naturales y usa la fórmula:

(30 [días] * 24[horas] * 60 [minutos])

- ✓ **El Uptime trimestral** se calcula cada tres meses usando estos grupos:

Enero Febrero Marzo
Abril Mayo Junio
Julio Agosto Septiembre
Octubre Noviembre Diciembre

Utiliza la fórmula: **(3 [meses] * 30 [días] * 24 [horas] * 60 [minutos])**

- ✓ **El Uptime anual** se calcula sobre años naturales. Utiliza la fórmula

(365 [días] * 24 [horas] * 60 [minutos])

En caso de incumplimiento de este ANS, el adjudicatario aplicará un crédito de nivel de servicio en la próxima factura equivalente a un máximo del **5% del precio de los servicios de mantenimiento y soporte correspondiente al mes en el que se produce cada Incumplimiento comunicado y probado.**

DEFINICIONES DE CRITICIDAD

La descripción de categorización de deficiencias es la que sigue a continuación:

Crítica. La solución está en producción y es de misión crítica para su negocio. Está inoperable y la situación está provocando una interrupción total del trabajo. No hay ninguna solución alternativa disponible.

Alta. Se define como un incidente en el que las funcionalidades críticas del software pueden seguir funcionando de forma restringida, aunque la productividad a medio/largo plazo puede verse afectada.

Media. Se define como un incidente que causa una pérdida parcial y no crítica de la funcionalidad del software. También puede ser un defecto de software (error) o un impacto al realizar ciertas acciones y no existe una solución conocida.

Baja. No hay pérdida de servicio. Se define como: (1) una solicitud de información o consulta, (2) solicitudes de características para el software o (3) un defecto de software y una solución alternativa que tiene un impacto bajo en la funcionalidad.

TIEMPO DE REACCIÓN

Se define como Tiempo de reacción: Plazo máximo transcurrido desde que la incidencia es comunicada por Correos, desde que quede registrada en el sistema corporativo de gestión de incidencias (POST), hasta que se obtiene una respuesta por parte del proveedor. Los indicadores a tener en cuenta son:

Indicador de Servicio	Tiempo de respuesta		
	Horas de Cobertura	Valor Objetivo (valor mensual)	Porcentaje de Cumplimiento mínimo (PCm)
Plazo máx. de reacción de una incidencia Crítica	24x7	≤ 2 horas	95 %
Plazo máx. de reacción de una incidencia Alta	8x5	≤ 6 horas hábiles	95 %
Plazo máx. de reacción de una incidencia Media	8x5	≤ 24 horas hábiles	95 %
Plazo máx. de reacción de una incidencia Baja	8x5	≤ 48 horas hábiles	95 %

Los valores están expresados en los períodos comprendidos de lunes a viernes, referidos siempre a períodos laborables.

Se considera:

- PCm: el porcentaje de cumplimiento mínimo establece el porcentaje de casos (incidencias, consultas) de un periodo que deben cumplir el valor objetivo para que Correos no aplique una penalización.
- El porcentaje de cumplimiento (en adelante, PC) señala el porcentaje de casos respondidos dentro del valor objetivo, sobre el total de los respondidos del mes, tanto si se han iniciado en el mes como en meses anteriores. Se calcula conforme a la siguiente fórmula:

El grado de cumplimiento (en adelante, GC) se calculará sobre el tiempo de respuesta total de incidencias mensualmente de la siguiente forma:

- $GC = 100$, si $PC \geq PCm$
- $GC = 0$, para $PC = 0$
- Para valores intermedios de GC: $GC = 100 \times PC / PCm$

Se considerará que ha habido incumplimiento cuando $GC < 100$. La forma de calcular la penalización por los incumplimientos se realizará según se indica en la siguiente tabla:

	Número de Incumplimientos	Número de Incumplimientos	Número de Incumplimientos
	>0 y ≤2	>2 y ≤4	>4
Gravedad del incumplimiento	Leve	Grave	Muy Grave
Implica Penalización	SI	SI	SI
% Penalización	5%	7%	10%

Este porcentaje de corrección se aplicará sobre el importe mensual total del servicio de mantenimiento permanente y se calculará mensualmente.

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

El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica en el artículo 99.3 b) LCSP, **“El hecho de que, la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución del mismo desde el punto de vista técnico”**.

En este caso, se cumple la justificación del citado supuesto, en la medida en que no se contempla la división del contrato por lotes porque se mantiene un solo sistema de suscripciones del producto que afecta a los entornos de producción, preproducción y desarrollo, de forma que, la realización independiente de las diversas suscripciones comprendidas en el objeto del contrato dificultaría la correcta ejecución del mismo desde el punto de vista técnico ya que el mantenimiento del sistema, de realizarse por distintos operadores, podría provocar un riesgo para la correcta ejecución del contrato. Por lo tanto, la naturaleza del servicio imposibilita su división en partes y, en consecuencia, su división en lotes.

Anexo III.- Resumen de metodología seguida para el cálculo del presupuesto base de licitación y el valor estimado del contrato.

Se establece como **Presupuesto base de Licitación**, incluido IVA o cualquier otro impuesto indirecto equivalente, la cantidad de **162.711,12 Euros (CIENTO SESENTA Y DOS MIL SETECIENTOS ONCE EUROS CON DOCE CÉNTIMOS)**, de acuerdo con la siguiente distribución:

Base del Presupuesto base de Licitación: 134.472,00 Euros (CIENTO TREINTA Y CUATRO MIL CUATROCIENTOS SETENTA Y DOS EUROS), excluido IVA o cualquier otro impuesto indirecto equivalente.

Importe del IVA o cualquier otro impuesto indirecto equivalente: **28.239,12 Euros (VEINTIOCHO MIL DOSCIENTOS TREINTA Y NUEVE EUROS CON DOCE CÉNTIMOS)**.

El presupuesto se ha obtenido de la siguiente manera:

Año	Base Imponible	Coste Directo 84%	Coste Indirecto 10%	Beneficio Industrial 6%	IVA o impuesto indirecto equivalente 21%	Presupuesto base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2026	20.170,80 €	16.943,47 €	2.017,08 €	1.210,25 €	4.235,87 €	24.406,67 €
2027	80.683,20 €	67.773,89 €	8.068,32 €	4.840,99 €	16.943,47 €	97.626,67 €
2028	33.618,00 €	28.239,12 €	3.361,80 €	2.017,08 €	7.059,78 €	40.677,78 €
TOTAL	134.472,00 €	112.956,48 €	13.447,20 €	8.068,32 €	28.239,12 €	162.711,12 €

Se estima que, sobre el importe total de licitación, los costes directos suponen un 84%, los costes indirectos un 10% y el beneficio industrial un 6% del total.

Respecto a los costes directos que asumirá el prestador del servicio, se han estimado unos costes salariales en torno al 20% por considerarse que los costes en mantenimiento y soporte suponen la mayor carga económica del conjunto de servicios a contratar. En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes salariales están conformados únicamente por el gasto en personal. El Convenio Colectivo que se ha tenido en cuenta como referencia para el cálculo económico es el XIX Convenio Colectivo Estatal de Empresas de Consultoría, de Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública, publicado el pasado 16 de abril de 2025 en BOE (Disposición 7766 del BOE núm. 92 de 2025), con efectos desde el 01 de enero de 2025, vigente desde el 17 de abril de 2025 hasta el 31 de diciembre de 2027 (prorrogable). Además, se ha tenido en cuenta el grado de especialización y el catálogo de servicios contemplados en la presente contratación.

Se establece como **Valor Estimado** de la contratación, la cantidad de **134.472,00 Euros**. El valor del contrato se ha evaluado de la siguiente forma:

VALOR ESTIMADO DEL CONTRATO			
Importe de Licitación			134.472,00 €
Plazo de Ejecución (meses)	20		6.723,60 €
Modificación 20%	NO		0,00 €
Prórrogas (meses)	NO	0	0,00 €
VALOR ESTIMADO DEL CONTRATO			134.472,00 €

El contrato no podrá ser prorrogado ni podrá ser objeto de ninguna modificación.

Los precios unitarios establecidos en el presente expediente tienen carácter de precios máximos de licitación, no pudiendo los licitadores presentar ofertas que los superen para cada una de las partidas definidas.

Nombre del servicio	Cantidad (suscripciones u horas)	Duración (meses)	Coste Unitario (€)	Importe total sin impuestos (€)
Suscripciones	40	20	111,84€	89.472,00€
Servicios Profesionales	500	20	90,00€	45.000,00€
TOTAL				134.472,00€

Asimismo, los volúmenes de servicios indicados tienen carácter meramente estimativo, constituyendo una previsión de necesidades basada en datos históricos y en la planificación operativa del servicio, sin que supongan un compromiso de contratación o de ejecución por parte de Correos.

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:

☒	Certificado de correcta ejecución de los servicios o trabajos realizados, expedidos o visados por la entidad para la que hayan sido realizados
☐	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.
☐	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: ...
☐	Indicación de las medidas de gestión medioambiental que el empresario aplicará al ejecutar el contrato.
☐	Documentación acreditativa de la maquinaria, material y equipo técnico del que se dispondrá para la ejecución de los trabajos.
☒	Otros. Declaración responsable que acredite que se dispone de los perfiles con conocimientos técnicos y funcionales suficientes de las herramientas de la plataforma y sus interfaces con otros sistemas.

Anexo V.- Modelo de aval.

LA ENTIDAD

AVALA

Solidariamente a la empresacon
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 deEuros (..... €), 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/espd-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: MT260301: renovación de las suscripciones. SUSE Linux Enterprise Server with SUSE Multi-Linux Manager Lifecycle Management+, X86-64, SUSE Linux Enterprise Server for SAP Applications, x86-64 y Long Term Service Pack Support, x86-64 del fabricante SUSE para la Sociedad Estatal Correos y Telégrafos S.A., S.M.E y la entidad contratante: Sociedad Estatal Correos y Telégrafos S.A., S.M.E)

☒ **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.- 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, 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 de acuerdo con la siguiente oferta:

Nombre del servicio	Cantidad (suscripciones u horas)	Duración (meses)	Coste Unitario (€)	Importe total sin impuestos (€)	Impuesto aplicable	Impuestos (€)	Importe total con impuestos (€)
Suscripciones	40	20					
Servicios Profesionales	500	20					
TOTAL							

* Todos los importes estarán expresados en euros y constarán de 2 decimales. En caso de que las ofertas se presenten con más de dos decimales, ello supondrá la exclusión automática del licitador que incurra en esta actuación. Además, la suma de los precios unitarios indicados con 2 decimales debe ser exacta al total.

Los precios unitarios establecidos en el presente expediente tienen carácter de precios máximos de licitación, no pudiendo los licitadores presentar ofertas que los superen para cada una de las partidas definidas.

**SERVICIOS
CON TRATAMIENTO DE DATOS
INSTRUCCIONES
Procedimiento: GENERAL SIN NEGOCIACIÓN
Expediente núm.: MT260312**



Nombre del servicio	Cantidad (suscripciones u horas)	Duración (meses)	Coste Unitario (€)	Importe total sin impuestos (€)
Suscripciones	40	20	111,84€	89.472€
Servicios Profesionales	500	20	90€	45.000€
TOTAL				134.472€

Asimismo, los volúmenes de servicios indicados tienen carácter meramente estimativo, constituyendo una previsión de necesidades basada en datos históricos y en la planificación operativa del servicio, sin que supongan un compromiso de contratación o de ejecución por parte de Correos.

Lugar, fecha, sello del licitador y firma autorizada.

Anexo IX.- 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 establecidos de ejecución total o parciales o de disponibilidad de la plataforma, cuando no exceda del 3 por ciento del plazo.	☐ Penalidades diarias en la proporción de 1 euros por cada 1.000 euros del precio del contrato, IVA excluido ☒ Penalidades sobre el precio en la misma proporción que suponga el retraso respecto del plazo inicial, IVA excluido. ☐ Otras penalidades por incumplimiento de plazo
Incumplir las comunicaciones de incidentes de seguridad	No entrega de informe forense en 3 meses tras la detección del incidente	3% facturación total de la adjudicación, con un mínimo de 5.000€
detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 10 o más vulnerabilidades Baja (CVSS < 4.0)	2% facturación anual de la adjudicación, con un mínimo de 5.000€
Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro	No asistir a una reunión dentro del plazo de 30 días	3% facturación anual de la adjudicación, con un mínimo de 5.000€
Pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación	Renovación de la certificación en más de 30 días naturales	1% facturación anual de la adjudicación, con un mínimo de 1.000€

B).- INCUMPLIMIENTOS GRAVES.

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Plazos	Por el incumplimiento de los plazos establecidos de ejecución total o parciales o	☐ Penalidades diarias en la proporción de 1 euros por

	de disponibilidad de la plataforma, cuando no exceda del 5 por ciento del plazo.	cada 1.000 euros del precio del contrato, IVA excluido. ☒ Penalidades sobre el precio en la misma proporción que suponga el retraso respecto del plazo inicial, IVA excluido. ☐ Otras penalidades por incumplimiento de plazo
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.
Subcontratación	Incumplimiento de las condiciones de subcontratación	Penalidad de hasta un 50 por 100 del importe del subcontrato.
ANS	Incumplimiento de los acuerdos de nivel de servicio	Lo indicado en el Anexo I del presente pliego
Incumplir las comunicaciones de incidentes de seguridad	Ausencia de actualizaciones durante el incidente	5% facturación total de la adjudicación, con un mínimo de 10.000€
detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 5 o más vulnerabilidades Media (4.0 ≤ CVSS < 7.0)	3% facturación anual de la adjudicación, con un mínimo de 5.000€
Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro	No ejecutar una prueba técnica específica o no entregar los resultados de esta dentro del plazo de 30 días	5% facturación anual de la adjudicación, con un mínimo de 10.000€
Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro	No facilitar las evidencias necesarias para la auditoría o evaluación dentro del plazo de 15 días	5% facturación anual de la adjudicación, con un mínimo de 10.000€
Pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación	Renovación de la certificación en más de 90 días naturales	3% facturación anual de la adjudicación, con un mínimo de 3.000€
Pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación	Renovación de la certificación en más de 60 días naturales	2% facturación anual de la adjudicación, con un mínimo de 2.000€

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 establecidos de ejecución total o parciales o de disponibilidad de la plataforma, 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.	☐ 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. ☒ penalidades sobre el precio en la misma proporción que suponga el retraso respecto del plazo inicial, IVA excluido. ☐ Otras penalidades por incumplimiento de plazo
Criterios de adjudicación	Por el incumplimiento de características de la oferta vinculadas a los criterios de adjudicación diferentes al plazo de ejecución	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
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.
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.
Incumplir las comunicaciones de incidentes de seguridad	Incidente no comunicado y detectado por terceros o por Correos	10% facturación total de la adjudicación, con un mínimo de 20.000€
Incumplir las comunicaciones de incidentes de seguridad	Retraso en el primer comunicado	10% facturación total de la adjudicación, con un mínimo de 20.000€
Incumplir las comunicaciones de incidentes de seguridad	Retraso en el segundo comunicado	10% facturación total de la adjudicación, con un mínimo de 10.000€
detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 1 o más vulnerabilidades Críticas (CVSS $\geq$ 9.0)	5% facturación anual de la adjudicación, con un mínimo de 10.000€
detección de vulnerabilidades de ciberseguridad en procesos y	Detectar 1 o más vulnerabilidades Altas ($7.0 \leq$ CVSS < 9.0)	5% facturación anual de la adjudicación, con un mínimo de 10.000€

soluciones de terceros*		
Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro	No subsanar las no conformidades o no implementar los controles requeridos dentro del plazo de 90 días	10% facturación anual de la adjudicación, con un mínimo de 20.000€
Pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación	Retraso en la notificación de la pérdida/caducidad/suspensión de la certificación en el plazo de 72 horas	5% facturación anual de la adjudicación, con un mínimo de 5.000€

*Asimismo, se considerará como un incumplimiento la superación de los plazos máximos de subsanación establecidos en función de la criticidad del hallazgo, conforme a la siguiente tabla:

SUPUESTO	GRAVEDAD	TIEMPO DE RESOLUCIÓN	PENALIZACIÓN
Vulnerabilidades Críticas ($CVSS \geq 9.0$)	Muy grave	15 días	2.000€ por día de retraso
Vulnerabilidades Altas ($7.0 \leq CVSS < 9.0$)	Muy grave	27 días	2.000€ por día de retraso
Vulnerabilidades Medias ($4.0 \leq CVSS < 7.0$)	Grave	33 días	1.000€ por día de retraso
Vulnerabilidades Bajas ($CVSS < 4.0$)	Leve	35 días	500€ por día de retraso

Anexo X. – Evaluación de Proveedores.

Parámetro a Evaluar	Indicador	Valor objetivo	Nivel de cumplimiento
Plazo	Plazos totales o parciales exigidos al adjudicatario en pliego	Indicados según los términos contractuales en el pliego (3 y 5% en función del tipo de incumplimiento)	
Penalizaciones	Incumplimientos que resultan en sanciones económicas u otras medidas	Evitar incumplimientos contractuales para mantener el rendimiento	
ANS	Tiempo de reacción inicial	Garantizar Grado de cumplimiento del 95%	
Encuestas de satisfacción	Opiniones de usuarios sobre la calidad del servicio	Alcanzar altos niveles de satisfacción de los usuarios.	
Auditorías a realizar	Evaluación sistemática de operaciones y procesos	Realizar auditorías anuales para garantizar la conformidad y eficiencia	

Anexo XI.- Requerimientos de seguridad.

1. REQUERIMIENTOS DE SEGURIDAD

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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 en reposo.

- 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).
- 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.

1.6 Tratamiento de datos

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.

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.

1.7 Uso de la inteligencia artificial

Cualquier uso de tecnología de Inteligencia Artificial deberá seguir las directrices a nivel de proceso de Asesoría Jurídica, el Área de Privacidad y, a nivel tecnológico, de la Dirección de Tecnología.

No se debe compartir información confidencial o sensible de Correos a través de ninguna herramienta de Inteligencia Artificial, en adelante IA, como puede ser credenciales, información financiera, etc.

No utilizar información corporativa como credenciales, emails y números de teléfono.

No utilizar información de clientes y proveedores, tanto actuales como futuros.

Debe existir un procedimiento de borrado seguro de la información en caso de la baja del modelo de IA.

1.8 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.

1.9 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.

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

1.10 Eventos de auditoría

Los componentes de la solución ofertada deberán generar y almacenar eventos de Auditoría, y 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.

1.11 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.

1.12 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.

1.13 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.

1.14 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 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, 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.

1.15 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 nueva normativa Europea de protección de datos (GDPR).

2. DIRECCIÓN TÉCNICA DEL SERVICIO

La Dirección de Tecnología y Transformación Digital de la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. designará un director técnico del Proyecto, quien asumirá la dirección y control del proyecto y actuará como principal interlocutor con la empresa adjudicataria. Asimismo, la empresa adjudicataria designará a un responsable del proyecto, que actuará como interlocutor único con Correos, debiendo proporcionar al

director técnico de Correos los reportes de actividad requeridos en cada momento sobre el avance de los trabajos, cumplimiento de hitos, justificación de posibles retrasos, horas incurridas, cumplimiento del nivel de servicio estipulado y cualquier otra información solicitada, en la forma requerida.

- Dirección de Tecnología y Transformación Digital
- Área de oficina de proyectos y relación con negocio

No se permitirán contactos directos entre el equipo de trabajo del contratista y el usuario final sin el conocimiento previo y autorización del director técnico.

Correos llevará a cabo la certificación de los trabajos y servicios prestados. Para ello, se podrán establecer reuniones de control con la periodicidad y soporte documental que Correos considere oportunos, en las que se revisarán todos los aspectos de los trabajos y servicios realizados y se decidirá, cuando corresponda, la posibilidad de llevar a cabo la certificación total o parcial de los mismos.

Cuando, a juicio del director técnico, el grado de cumplimiento del Acuerdo de Nivel de Servicio (ANS) lo justifique, Correos podrá aplicar las correcciones a la certificación y consiguiente facturación, detalladas en el epígrafe correspondiente. Esto implica una minoración en el importe de la facturación equivalente al importe de la penalización a imponer.

Para la certificación de los trabajos realizados, se prestará especial atención al cumplimiento del nivel de servicio estipulado.

Los productos y servicios descritos en este Pliego se considerarán recibidos de conformidad por Correos una vez haya transcurrido un periodo de un mes de funcionamiento real pleno y satisfactorio, sin requerimientos u observaciones por parte de Correos que indiquen deficiencias o anomalías en la prestación de los servicios.

Las rectificaciones o modificaciones en los trabajos derivadas de decisiones sobrevenidas que no tengan como origen errores u omisiones del adjudicatario se certificarán según se acuerde en cada caso, ya sea como “proyectos cerrados” o como horas de trabajo y/o suministros, dentro de la asistencia.

Una vez aceptada por el director técnico la porción de los trabajos a certificar y establecido el importe, el adjudicatario emitirá la correspondiente factura.

Anexo XII.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad.

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 XIII. Consideraciones sobre el uso de IA en los servicios

Condiciones en materia de inteligencia artificial

A los efectos de la presente cláusula, se entenderá por sistema de inteligencia artificial y modelo de uso general lo dispuesto en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, el “Reglamento de Inteligencia Artificial” o “RIA”).

En el supuesto de que la prestación de los servicios por parte del Adjudicatario/Proveedor a CORREOS pueda requerir el uso de sistemas o modelos de inteligencia artificial, el Adjudicatario/Proveedor se obliga a cumplir las siguientes condiciones, que resultarán de aplicación respecto de toda la información confidencial de CORREOS, incluyendo, de forma expresa y no limitativa, datos personales, información corporativa, operativa, técnica, estratégica, comercial y de seguridad, a la que tenga acceso con ocasión de la prestación de los servicios:

- (i) Deberá informar a CORREOS de forma completa y previa acerca de cualesquiera decisiones automatizadas que, en su caso, se adopten mediante el uso de sistemas o modelos de inteligencia artificial en el marco de los servicios, cuando dichas decisiones afecten a interesados cuyos datos personales sean tratados, incluyendo una explicación suficiente de la lógica aplicada, el funcionamiento general del sistema y las consecuencias previstas, en los términos exigidos por la normativa de protección de datos y el RIA.
- (ii) Deberá abstenerse de tratar, mediante sistemas o modelos de inteligencia artificial, la información confidencial de CORREOS —y en particular los datos personales— de forma incompatible con las finalidades expresamente autorizadas por CORREOS y comunicadas en el marco contractual o mediante instrucciones documentadas.
- (iii) No podrá generar ni inferir nuevos datos personales relativos a las categorías de interesados cuyos datos sean tratados por cuenta de CORREOS, salvo instrucción expresa, previa y por escrito de CORREOS, y siempre que dicha generación resulte conforme con la normativa aplicable en materia de protección de datos.
- (iv) Deberá colaborar activamente con CORREOS en el cumplimiento de cualesquiera obligaciones que resulten de aplicación en materia de inteligencia artificial, protección de datos y seguridad de la información, en la medida en que guarden relación con el uso de sistemas o modelos de inteligencia artificial y el tratamiento de información confidencial, incluyendo, en su caso, evaluaciones de riesgos, evaluaciones de impacto, medidas de mitigación y atención a derechos de los interesados.

- (v) Deberá comunicar a CORREOS, con carácter previo a su despliegue o utilización, la intención de implementar cualesquiera sistemas o modelos de inteligencia artificial distintos de los expresamente autorizados, cuando dichos sistemas o modelos vayan a tratar información confidencial de CORREOS o datos personales por su cuenta. Dicha comunicación deberá incluir, al menos:
- identificación del sistema o modelo de inteligencia artificial;
 - identificación del proveedor o desarrollador del sistema o modelo;
 - documentación técnica relevante;
 - finalidad prevista del sistema o modelo;
 - clasificación o nivel de riesgo del sistema o modelo conforme al RIA u otra normativa aplicable.
- (vi) No podrá utilizar, ni permitir que terceros utilicen, la información confidencial de CORREOS —incluidos los datos personales tratados por su cuenta— con fines de entrenamiento, desarrollo, ajuste o mejora de modelos de inteligencia artificial de uso general o de sistemas de inteligencia artificial, ya sean propios o de terceros, salvo autorización previa, expresa y por escrito de CORREOS, y únicamente cuando dicho uso resulte estrictamente necesario para la correcta ejecución de las instrucciones de CORREOS.

Las obligaciones establecidas en la presente cláusula serán plenamente exigibles a lo largo de toda la cadena de suministro del Adjudicatario/Proveedor y deberán trasladarse contractualmente a cualesquiera terceros que intervengan en la prestación de los servicios, con independencia de que dichos terceros tengan la consideración de sub-encargados del tratamiento, encargados del tratamiento o responsables independientes conforme a la normativa de protección de datos, garantizando en todo caso un nivel de protección equivalente al aquí previsto.

El Adjudicatario/Proveedor responderá frente a CORREOS de cualesquiera daños, perjuicios, sanciones administrativas, reclamaciones, multas, costes y responsabilidades de cualquier naturaleza que se deriven directa o indirectamente del incumplimiento de las obligaciones establecidas en la presente cláusula, del Reglamento de Inteligencia Artificial, de la normativa de protección de datos personales o de las instrucciones documentadas de CORREOS en relación con el uso de sistemas o modelos de inteligencia artificial.

En particular, el Adjudicatario/Proveedor mantendrá indemne a CORREOS frente a cualquier reclamación formulada por terceros, incluidas autoridades de control o interesados, que tenga su origen en un uso no autorizado, negligente o contrario a Derecho de sistemas o modelos de inteligencia artificial, o en un tratamiento ilícito o no conforme de la información confidencial de CORREOS, incluidos los datos personales.

Medidas de seguridad en el uso de Inteligencia Artificial

Cumplimiento Normativo y Estándares

El Adjudicatario/Proveedor garantiza el cumplimiento de la normativa aplicable, incluyendo (sin carácter limitativo) el Reglamento (UE) 2016/679 (RGPD), incluyendo el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el Esquema Nacional de Seguridad (ENS), la normativa sectorial que resulte de aplicación y el Reglamento Europeo de Inteligencia Artificial (AI Act), en su versión vigente y aplicable al caso concreto.

Adoptará buenas prácticas y estándares técnicos y organizativos reconocidos en el sector, tales como ISO/IEC 27001 (seguridad de la información), ISO/IEC 27036 (gestión de la seguridad en relaciones con proveedores), ISO/IEC 42001 (sistema de gestión de inteligencia artificial) y el NIST AI Risk Management Framework 1.0, o aquellos estándares equivalentes que resulten aplicables, evidenciando si le es requerido su aplicación a CORREOS.

Deberá clasificar el sistema de IA conforme a las categorías de riesgo establecidas por el AI Act, fundamentando dicha clasificación en los criterios previstos en los artículos 5 y 6 del mismo y, en caso de ser clasificado como de alto riesgo, se deberá realizar la Evaluación de Conformidad y la Evaluación de Impacto sobre los Derechos Fundamentales (FRIA) conforme a los artículos 27 y 43.

Directrices generales de seguridad

El Adjudicatario/Proveedor deberá proporcionar documentación técnica y funcional suficiente sobre el sistema de IA, las métricas de desempeño, sesgos conocidos y las medidas adoptadas para su mitigación, así como la versión del modelo y un registro de cambios relevantes. Este punto no será de aplicación en aquellos usos de herramientas de IA que sean meramente operativos/ofimáticos y que no traten información clasificada de CORREOS.

Deberá aplicar medidas técnicas y organizativas proporcionales al riesgo del sistema, incluyendo, entre otras, cifrado de datos en tránsito y en reposo, control de accesos, registro de eventos, segregación de entornos, y anonimización o seudonimización de datos según corresponda, así como realizar pruebas de seguridad periódicas, incluyendo adversarial testing cuando sea pertinente.

Deberá notificar a CORREOS sin demora, y en todo caso dentro de las 24 horas siguientes a su detección, cualquier incidente de seguridad o brecha que afecte al sistema de IA, proporcionando toda la información necesaria para su investigación, contención y remediación.

CORREOS tendrá derecho a auditar, directamente o mediante un tercero independiente, los procesos y controles del Adjudicatario/Proveedor relacionados con el sistema de IA, incluyendo datos de entrenamiento, validación, seguridad y

cumplimiento, con preaviso razonable y sin acceso a secretos industriales no estrictamente necesarios.

Deberá comunicar por escrito, con antelación razonable, cualquier actualización sustancial del modelo, dataset o arquitectura que pueda afectar precisión, sesgo, explicabilidad o cumplimiento, y no ejecutará cambios de alto impacto sin la aprobación previa de CORREOS cuando afecten procesos críticos.

Deberá establecer, documentar y mantener un sistema de gestión de riesgos que abarque todo el ciclo de vida del sistema. Este sistema deberá identificar los riesgos razonablemente previsibles, analizarlos y evaluarlos, y establecer controles técnicos y organizativos adecuados para su mitigación.

Deberá disponer de un modelo de gobernanza de IA interno, que establezca un marco organizativo, normativo y operativo que garantice que su uso es seguro, ético y legal conforme a estándares internacionales.

Otras consideraciones de seguridad:

- Disponer de modos degradados no IA que permitan continuar operaciones críticas en caso de fallos del sistema o detección de sesgos excesivos.
- Aplicar cifrado de datos en tránsito y en reposo, así como protocolos seguros para la transmisión y almacenamiento de información sensible.
- Realizar pruebas de seguridad periódicas, incluyendo análisis de vulnerabilidades y pruebas de resistencia frente a ataques adversariales (adversarial testing) cuando sea pertinente.
- Mantener planes de contingencia y protocolos de recuperación ante desastres que garanticen la continuidad del servicio y la mitigación de riesgos operativos.

Control de acceso, uso adecuado y limitaciones

El Adjudicatario/Proveedor deberá establecer controles de acceso y perfiles de uso del sistema de IA, adecuados al nivel de riesgo y al principio de necesidad de conocer y mínimo privilegio.

Deberá garantizar que todo el personal que participe en el diseño, implementación, operación, supervisión o mantenimiento involucrado ha recibido formación específica en buenas prácticas para el uso seguro de herramientas de IA.

Deberá asegurar una supervisión humana efectiva durante toda la vida operativa del sistema, especialmente cuando existan decisiones con impacto legal, financiero, sanitario, laboral o de derechos fundamentales, definiendo los límites de autonomía del sistema, estableciendo protocolos de intervención y disponiendo de mecanismos para la detección de comportamientos anómalos.

Los siguientes usos para la IA se consideran prohibidos:

- Manipulación subliminal del comportamiento de una persona que tenga por objeto o efecto causar daños físicos o psicológicos a dicha persona o a terceros.
- Explotación de las vulnerabilidades de grupos sociales o personas en situación de especial vulnerabilidad, con el fin de manipular su comportamiento de manera que pueda causarles perjuicios a ellos mismos o a terceros.

- Evaluación, clasificación o puntuación de individuos o grupos (social scoring) basada en su comportamiento social o en características personales, ya sean conocidas, inferidas o predichas.
- Identificación biométrica remota en tiempo real en espacios de acceso público, salvo en los supuestos expresamente autorizados por una base jurídica previa.
- Predicción del riesgo de que una persona cometa un delito basado exclusiva o principalmente en el análisis de su perfil, características personales o patrones de comportamiento.
- Reconocimiento, inferencia o alteración de las emociones de personas en el ámbito laboral o en centros educativos, salvo cuando el uso del sistema esté debidamente justificado por razones médicas o de seguridad.

Anexo XIV.- 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/CORREOS EXPRESS/CORREOS TELECOM].
- 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/CORREOS EXPRESS/CORREOS TELECOM] 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

OBJETO DEL CONTRATO	Se debe incluir el objeto del contrato
TRATAMIENTO A REALIZAR	☒ Recogida ☒ Registro ☒ Estructuración ☐ Modificación ☒ Conservación ☒ Extracción ☒ Consulta ☐ Comunicación por transmisión ☐ Difusión ☒ Interconexión ☒ Cotejo ☐ Limitación ☒ Supresión ☒ Destrucción ☐ Comunicación ☐ Otros:
FINALIDAD DEL TRATAMIENTO	☐ Gestión de clientes, contable, fiscal y administrativa ☐ Gestión de nóminas ☐ Servicios económico-financieros y de seguros ☐ Publicidad y prospección comercial ☐ Videovigilancia ☐ Recursos humanos ☐ Prevención de riesgos laborales ☐ Prestación de servicios de comunicaciones electrónicas ☐ Comercio electrónico ☐ Seguridad y control de acceso a edificios ☒ Otros: Servicios de Atención al Cliente
TIPO DE DATOS	☒ Datos de carácter identificativo ☒ Características personales ☐ Académicos y profesionales ☐ Información comercial ☒ Circunstancias sociales ☐ Detalles del empleo ☐ Transacciones de bienes o servicios ☒ Categorías especiales de datos ☐ Otros:
CATEGORÍAS DE INTERESADOS	☐ Empleados ☒ Clientes y usuarios ☐ Proveedores ☐ Personas de contacto ☐ Beneficiarios ☐ Cargos públicos

	☐ 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] sin dilación indebida. No obstante, no existirá obligación de comunicar este tipo de notificaciones a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM], 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/CORREOS EXPRESS/CORREOS TELECOM], 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/CORREOS EXPRESS/CORREOS TELECOM].
- 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/CORREOS EXPRESS/CORREOS TELECOM] toda la información necesaria para demostrar el cumplimiento de sus obligaciones, según el proceso establecido en el punto 5.
- Asistir a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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 [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] se obliga a realizarlo conforme las instrucciones de [CORREOS/CORREOS EXPRESS/CORREOS TELECOM], siguiendo la redacción y formato indicado y custodiando o dando traslado a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] (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 [CORREOS/CORREOS EXPRESS/CORREOS TELECOM]; y
- (ii) Lugar de prestación de servicios objeto de licitación.

4. Obligaciones de [CORREOS/CORREOS EXPRESS/CORREOS TELECOM]

Corresponden a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM], 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/CORREOS EXPRESS/CORREOS TELECOM], 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 EXPRESS/CORREOS TELECOM].

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

[CORREOS/CORREOS EXPRESS/CORREOS TELECOM], 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM]. 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 irre recuperables

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/CORREOS EXPRESS/CORREOS TELECOM] así como los servidores y servicios relacionados con los mismos comunicados a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] tendrá un plazo de 30 días para oponerse.

Transcurrido el plazo de 30 días sin que [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM]. 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] la documentación acreditativa de su vigencia.

11. Responsabilidad

El adjudicatario vendrá obligado a exonerar a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM].

12. Notificación de cambios

El adjudicatario comunicará a [CORREOS/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] 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 obligadas 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

Para Correos:

- *Dirección Postal: Conde De Peñalver 19, 28006, Madrid*
- *Correo Electrónico: derechos.protecciondatos.correos@correos.com*

Para Correos Express:

- *Dirección Postal: Avda. de Europa nº 8, Centro de Transportes de Coslada, 28.821, Coslada (Madrid)*
- *Correo* *Electrónico:*
derechos.protecciondatos.correosexpress@correosexpress.com

Para Correos Telecom:

- *Dirección Postal: C/Conde de Peñalver 19B, 28006 Madrid (España).*
- *Correo Electrónico: derechos.protecciondatos.telecom@correos.com*

Asimismo, podrán ponerse en contacto con los respectivos delegados de protección de datos en la dirección 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/CORREOS EXPRESS/CORREOS TELECOM] actúe como ENCARGADO DEL TRATAMIENTO y el adjudicatario como SUBENCARGADO DEL TRATAMIENTO, comprometiéndose con carácter adicional a las obligaciones previstas con anterioridad a:

- Por parte de [CORREOS/CORREOS EXPRESS/CORREOS TELECOM]: 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/CORREOS EXPRESS/CORREOS TELECOM] 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/CORREOS EXPRESS/CORREOS TELECOM] acuerdan someterse de manera expresa a la normativa vigente en materia de protección de datos en España y, en particular, al RGPD y LOPDGD.

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).
 - o Gestión de derechos y credenciales de acceso asignados a los usuarios.
 - o Gestión de privilegios especiales de acceso según el impacto que puede derivar de un uso inadecuado de los datos de carácter personal.
 - o Gestión de información confidencial de autenticación de usuarios.
 - o Política de retirada de cancelación de accesos y credenciales.
- Haber establecido un procedimiento de accesos a sistemas y aplicaciones que incluya:
 - o La restricción de acceso a la información.
 - o 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.
 - o 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:
 - o Forzar el uso de los identificadores de usuario (IDs) individuales y de las contraseñas para mantener la responsabilidad.
 - o Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada.
 - o 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:
 - o Controles físicos de entrada.
 - o Perímetro de seguridad.
 - o Protección contra amenazas externas o ambientales.
 - o 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:
 - o Identificación de las medidas de seguridad.
 - o Campos de eventos que deberían ser registrados.
 - o Tipología de eventos a registrar.
 - o 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:
 - o La realización de una copia de seguridad con una periodicidad mínima semanal en un segundo soporte distinto del destinado a los usos habituales.
 - o 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:
 - o Haga uso de las medidas físicas y lógicas necesarias para garantizar la irrecuperabilidad de la documentación destruida.
 - o 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 medida 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 por 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 restrinjan 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:
 - o La gestión de claves para la encriptación/desencriptación.
 - o Un sistema de etiquetado/cifrado que garantice el anonimato de los titulares de los datos.
 - o Un cifrado de información de dispositivos de almacenamiento (como pendrive, equipos informáticos o almacenamientos remotos).
 - o 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:
 - o La identificación y registro de los cambios significativos.
 - o La planificación y pruebas de los cambios.
 - o 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.
 - o La comunicación de los detalles de los cambios a las personas correspondientes.
 - o 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:
 - o Una evaluación de riesgos
 - o Un análisis de los efectos de los cambios
 - o Una especificación de los controles de seguridad necesarios.
 - o 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:
 - o Se deberá contar con un registro de ubicaciones de las cámaras y monitores de observación.
 - o 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 XV.- Declaración responsable en materia de Protección de Datos

En caso de obtener una puntuación de cero (0) en alguna de las preguntas del presente cuestionario de privacidad, el licitador será excluido del 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 su preguntas, la empresa adjudicataria deberá presentar a la SOCIEDAD ESTATAL CORREOS Y TELÉGRAFOS, 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 encargado 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>

Cuestionario 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:

1. Cuestiones generales

En caso de ser adjudicatario y realizará la prestación de servicios a [], 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 [], 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 [].

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 [].

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 [] 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 [], 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 [] 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.:

Anexo XVI.- 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		