

PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

ÍNDICE.

1. Entidad contratante.....	4
2. Objeto del contrato.....	4
3. Duración del contrato.....	5
4. Aspectos económicos.....	6
5. Condiciones de participación.....	6
6. Licitación del contrato.....	7
6.1. Comunicaciones y notificaciones electrónicas.....	7
6.2. Resolución de consultas relacionadas con la licitación.	7
6.3. Envío de ofertas por medios electrónicos.	7
6.4. Documentación confidencial.	7
6.5. Procedimiento de licitación y Criterios de adjudicación.....	8
6.6. Ofertas integradoras.....	9
6.7. Contenido de las ofertas.	9
6.7.1. Sobre 1: Documentación administrativa.	9
6.7.2. 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. Preferencia de ofertas comunitarias.	11
7.4. Documentación a presentar por el propuesto como adjudicatario.....	12
7.5. Adjudicación del contrato.....	13
7.6. Perfección del contrato.....	13
7.7. 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.....	15
8.1.3. Obligaciones del adjudicatario en materia de protección de datos. .	15
8.1.4. Aceptación y adhesión a las políticas de prevención de imputaciones delictivas	18
8.1.5. Evaluación de proveedores	19
8.1.6. Obligaciones esenciales del contrato	19

8.1.7.	Condiciones especiales de ejecución.....	20
8.1.8.	Régimen de confidencialidad	21
8.2.	Modificaciones del contrato.....	21
8.3.	Cesión y Subcontratación	21
8.3.1.	Cesión del contrato	21
8.3.2.	Régimen de subcontratación.....	21
9.	Cumplimiento del contrato.	22
9.1.	Responsable del contrato. Representante del contratista	22
9.2.	Régimen de penalidades	22
9.3.	Abonos al contratista. Facturación	23
9.4.	Recepción y liquidación	24
9.5.	Plazo de garantía	25
10.	Resolución del contrato	25
10.1.	Causas de resolución	25
10.2.	Procedimiento	26
11.	Protección de Datos	26
11.1.	Cláusula informativa de protección de datos personales recabados a través del Canal Ético	26
11.2.	Información a representantes, trabajadores y personas de contacto.....	26
12.	Régimen jurídico del contrato y reclamaciones contra este pliego	27
Anexo I.-	Características técnicas específicas del contrato.....	29
Anexo II.-	Descripción y limitaciones a la licitación por lotes	34
Anexo III.-	Resumen de metodología seguida para el cálculo del valor estimado del contrato	35
Anexo IV.-	Forma de acreditación de la solvencia económica y financiera, y técnica o profesional	36
Anexo V.-	Modelo de aval	37
Anexo VI. -	Instrucciones y recomendaciones para la presentación electrónica de las ofertas.....	38
Anexo VII.-	Instrucciones para cumplimentar el DEUC.....	39
Anexo IX.-	Criterios de adjudicación de evaluación automática	41
Anexo X.-	Modelo de proposición económica	42
Anexo XI.-	Información sobre condiciones de subrogación de contratos de trabajo	44
Anexo XII.-	Modificaciones previstas del contrato.....	45
Anexo XIII.-	Régimen de penalidades	46

Anexo XV.- Contrato de encargo de tratamiento de datos personales	55
Anexo XVI.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la ley 9/2017, de 8 de noviembre, de contratos del sector público	56
Anexo XVII Adscripción de medios	57
Anexo XVIII. Compromiso de adscripción de personal al contrato.....	58
Anexo XIX – Requerimientos Arquitectura	59
Anexo XX – Requerimientos Ciberseguridad	75
Anexo XXI. Cláusula sobre el uso de IA en contratos con Correos.	84

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

1. Entidad contratante.

Entidad contratante	Sociedad Estatal Correos y Telégrafos S.A. S.M.E.
Órgano de contratación	Comité de Inversiones
Dirección/Subdirección gestora de la necesidad UGC	Dirección de Tecnología y Transformación Digital Subdirección de Ciberseguridad 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 de Tecnología y transformación digital Subdirección de Ciberseguridad Área Inteligencia y Ciberdefensa Jefe de área de Inteligencia y Ciberdefensa
	Datos de contacto: expdtes.ciberseguridad@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	Adquisición de hardware y licencias asociadas a los proxies Bluecoat de Broadcom (Symantec Web Protection) de las que es titular la S.E. Correos y Telégrafos, S.A. SME (en adelante "Correos"), junto con los derechos de uso, actualizaciones y los servicios de mantenimiento y soporte asociados.
Código CPV	Principales: 48730000-4 (Paquetes de software de seguridad). 48820000-2 (Servidores appliance para la plataforma). Secundario: 48218000-9 (Paquetes de software de gestión de licencias).
Lotes	☒ NO ☐ SI (Ver Anexo II) El presente procedimiento de licitación no se divide en lotes, de conformidad con lo establecido en el artículo 52.3 b) del Real Decreto-Ley 3/2020 de 4 de febrero: "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; o bien que el riesgo para la correcta ejecución del contrato proceda de la naturaleza del objeto del mismo, al implicar la

	necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes. Ambos extremos deberán ser, en su caso, justificados debidamente en el expediente” El contrato no se divide en lotes al concurrir estos motivos válidos: (I) interdependencia técnica entre los elementos de hardware y las licencias asociadas; (II) riesgo operativo por multiplicación de interlocutores y pérdida de trazabilidad en actualizaciones y RMA (Autorización de Devolución de Mercancía, por sus siglas del inglés de Return Merchandise Authorization); y (III) necesidad de coordinación unificada, ya que un mantenimiento fragmentado puede generar incompatibilidades temporales y soluciones parciales, aumentando el esfuerzo total y el consumo de recursos. En consecuencia, la no división garantiza coherencia técnica, continuidad de servicio y control eficaz del entorno.[
¿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	36	☐ 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. ☒ desde la fecha que se indique en el contrato.
Prorrogable	☒ NO ☐ SI	N° de prórrogas: Duración máxima de cada prórroga (en meses):	

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Valor estimado del contrato	605.495,82 euros		Seiscientos cinco mil cuatrocientos noventa y cinco euros y ochenta y dos céntimos, conforme al método de cálculo especificado en Anexo III		
Presupuesto base de licitación	732.649,94 euros		IVA/impuesto equivalente		127.154,12 euros
Anualidades (IVA o impuesto indirecto equivalente incluido)	2026	2027	2028	2029	Total
	73.532,38 euros	243.993,82 euros	244.662,30 euros	170.461,44 euros	732.649,94 euros

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:

Habilitación profesional			
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 200.000,00 euros. En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote		
		LOTE 1	LOTE 2
	Porcentaje/Cifra volumen anual negocio.		
	Sobre la forma de acreditar estos requisitos, ver Anexo IV		
Solvencia técnica o profesional	☒ Haber realizado dos 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. (141.282,35 euros) Sobre la forma de acreditar estos requisitos, ver Anexo IV		
Adscripción de medios:	☐ Sí. Medios a adscribir ☒ No.		

Los candidatos y licitadores no estarán obligados a aportar aquellos documentos justificativos u otra prueba documental de los datos que ya obraran en poder de la entidad contratante o aquellos otros que pudieran obtenerse de forma directa y gratuita, bien a través del registro oficial de licitadores y empresas clasificadas del sector público, o bien a

través de una base de datos nacional de un estado miembro de la unión europea, como un expediente virtual de la empresa, un sistema de almacenamiento electrónico de documentos o un sistema de precalificación.

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 del sector público, 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 seis (6) días naturales antes de la finalización del plazo para la presentación de ofertas.

6.3. Envío de ofertas por medios electrónicos.

El plazo de presentación de ofertas será de 30 días naturales a contar desde el día siguiente a aquel en que se publique el anuncio de licitación en el perfil de contratante.

Los licitadores, a excepción del procedimiento especial con un único licitador, deberán presentar obligatoriamente sus ofertas de forma electrónica a través de la plataforma de contratación de Correos (<https://pcc.correos.es/licitacion/licitaciones>) utilizando para ello la "herramienta de preparación y presentación de ofertas" que desde esa plataforma se pone a su disposición (ver instrucciones y recomendaciones en [Anexo VI](#)).

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 estos) 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. Procedimiento de licitación y Criterios de adjudicación.

Se propone que la contratación del presente expediente se realice mediante el procedimiento de licitación abierto, conforme a lo dispuesto en el artículo 82 del Real Decreto-ley 3/2020, que establece:

“En los procedimientos abiertos, cualquier operador económico interesado podrá presentar una oferta en respuesta a un anuncio de licitación”.

Este procedimiento se considera el más adecuado para garantizar la máxima concurrencia competitiva, permitiendo que cualquier operador económico interesado presente su mejor oferta en igualdad de condiciones.

Las características técnicas, operativas y de prestación del servicio no admiten variantes en la configuración ni en la forma de prestación del servicio, al tratarse de suministros estandarizados ofrecidos en condiciones cerradas definidas por el fabricante, por lo que:

- No se admiten variantes en la configuración ni en la forma de prestación del servicio.
- No se permiten mejoras técnicas ni modificaciones en los plazos de entrega, al tratarse de una solución estándar ofrecida en condiciones cerradas.

En consecuencia, para el presente expediente, la adjudicación se efectuará utilizando como único criterio de adjudicación el precio, aplicado bajo el principio de mejor relación coste-eficacia.

El único criterio de adjudicación será el precio, dado que:

- Las características del servicio están plenamente definidas y no admiten modificaciones.
- Tampoco se admiten variantes en los plazos de entrega ni en la forma de prestación del servicio.

Tipología	Criterio	Ponderación
Criterios sujetos a un juicio de valor	Técnicos	0%
Criterios evaluables mediante formula o automáticamente	Técnico	0%
	Económico	100%

En caso de incurrir en empate entre varias ofertas tras la aplicación de los criterios de adjudicación, se acudirá a lo dispuesto en el artículo 66.11 del Real Decreto Ley 3/2020 de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, relativo a los criterios de desempate.

6.6. Ofertas integradoras.

6.7. Contenido de las ofertas.

6.7.1. Sobre 1: Documentación administrativa.

- a) Documento europeo único en materia de contratación (DEUC). Cumplimentado conforme a las indicaciones contenidas en el [anexo VII](#), firmado por el licitador o su representante.
- b) En su caso, compromiso de adscripción de medios, según lo indicado en el apartado 5 (según [anexo XVIII](#)).
- c) Compromiso de constitución de unión temporal de empresarios (UTE), en su caso. cuando dos o más empresas acudan a una licitación con el compromiso de constituirse en unión temporal, se deberá aportar una declaración indicando los nombres y circunstancias de los empresarios que la suscriban, la participación de cada uno de ellos y que asumen el compromiso de constituirse formalmente en unión temporal, caso de resultar adjudicatarios. el citado documento deberá estar firmado por los representantes de cada una de las empresas componentes de la unión. en estos casos cada una de las empresas deberá presentar su propio documento europeo único en materia de contratación (DEUC) a que se refiere el apartado a).
- d) En su caso, declaración de que la empresa a la que representa pertenece a un grupo empresarial, con indicación de las sociedades que forman parte del mismo.
- e) Las empresas no españolas deberán aportar declaración de que se somete a la jurisdicción de los juzgados y tribunales españoles de cualquier orden, para todas las incidencias que de modo directo o indirecto pudieran surgir del contrato, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponder al licitador.

- f) Las empresas de estados que no sean miembros de la Unión Europea o signatarios del acuerdo sobre el espacio económico europeo deberán aportar un informe que acredite su capacidad de obrar, expedido por la misión diplomática permanente u oficina consular de España del lugar del domicilio de la empresa, en el que se haga constar, previa acreditación por la empresa, que figuran inscritas en el registro local profesional, comercial o análogo o, en su defecto que actúan con habitualidad en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.

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

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

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

La documentación que incluya los valores de los criterios de adjudicación cuya evaluación puede realizarse de manera automática deberá presentarse en archivo electrónico, en una o varias carpetas, comprimidas si no es posible por tamaño, con el nombre "SOBRE N° 2" en archivo ejecutable con formatos *.pdf, *.doc, *.docx, *.xls, *.xlsx *.odt *.ods).

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

CORREOS se reserva el derecho de solicitar las aclaraciones que estime oportunas al respecto durante el proceso de valoración de ofertas.

Los importes reflejados deberán indicarse solo con dos decimales y redondeados al segundo decimal.

Se deberá incluir en la oferta los importes de cada uno de los conceptos en los que se desglosa la misma, indicando el importe total o global, sin impuestos y con impuestos, con la suma de todos los conceptos de los que se compone.

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.

En su caso, técnicamente las ofertas presentadas se considerarán aptas o no, en virtud de que cumplan con todos los requisitos exigidos en el presente pliego. La evaluación de las ofertas se realizará en acto interno, pudiendo desecharse las ofertas

técnicamente inadecuadas o que no garanticen adecuadamente con su oferta la correcta ejecución del contrato.

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.

Para la evaluación de las ofertas se analizará la documentación entregada por los licitadores y, en general, todo aquello que sirva para un mejor conocimiento de las ofertas presentadas.

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 si así se hubiera contemplado.

7.3. Preferencia de ofertas comunitarias.

De conformidad con lo dispuesto en el art. 70 del Real Decreto Ley 3/2020, cualquier oferta presentada para la adjudicación de un contrato de suministro podrá rechazarse cuando la parte de los productos originarios de los países terceros, determinados de conformidad con el Reglamento (CEE) número 952/2013 del Parlamento Europeo y del Consejo, de 9 de octubre de 2013, por el que se aprueba el Código Aduanero

Comunitario, sea superior al 50 por 100 del valor total de los productos que componen esta oferta.

7.4. 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.
☐	Declaración relativa al lugar en el que estarán los servidores en los que se almacenan datos personales y desde dónde se van a prestar los servicios asociados a los mismos, (Esta declaración deberá presentarse con carácter previo cada vez que se producen cambios en las anteriores circunstancias).
☐	Contrato de Encargo de Tratamiento de Datos, conforme al modelo consignado en el Anexo XV .
☒	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.
☐	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 (20) 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.

7.5. 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.

7.6. 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 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 y en el Diario Oficial de la Unión Europea.

7.7. Constitución de garantías.

RÉGIMEN DE GARANTÍAS		
Constitución de garantía definitiva	☒ SI. 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 temeraria). (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.

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.

Para la ejecución de este contrato:

☒ NO procede subrogación de trabajadores
☐ SI procede la subrogación de trabajadores (ver información sobre condiciones de subrogación en Anexo XI)

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.

El desarrollo del servicio objeto de la licitación, no requiere ni de una comunicación de datos, ni de un acceso por parte del adjudicatario a los datos de carácter personal bajo la responsabilidad de la entidad contratante. No obstante, 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. Por ello, la empresa que resulte adjudicataria se compromete a:

- a) Evitar todo acceso a datos, informando expresamente a sus trabajadores y profesionales de que el mismo se encuentra prohibido.
- b) En caso de acceso accidental o simple visionado por necesidad de acceso a las instalaciones:
 - i. Guardar la más estricta confidencialidad y secreto sobre los datos accedidos.
 - ii. Adoptar las medidas oportunas para evitar su reiteración.
 - iii. Proceder a la inmediata destrucción de las copias accidentales que se hayan podido realizar.
- c) 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 (AEPD) o cualquier otro órgano competente ya sea español o europeo, como consecuencia del incumplimiento de las obligaciones establecidas en el presente contrato.

No obstante a lo anterior:

1. Si el desarrollo del servicio objeto de licitación implicase un acceso del adjudicatario a los datos de carácter personal de los que la entidad contratante resulte responsable del tratamiento el adjudicatario, en calidad de encargado del tratamiento, se compromete a firmar un contrato de acceso a datos por cuenta de la entidad contratante debiendo ajustarse al modelo que se incorpora como [Anexo XV](#) del presente pliego, cumpliendo con las exigencias previstas en la normativa de protección de datos vigente y, entre otras, recoja el compromiso del adjudicatario a:
 - Llevar a cabo del tratamiento de datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular el RGPD y la LOPDGDD.
 - Actuar sujeto a las instrucciones que, en cada momento, le indique la entidad contratante y no utilizar los datos con una finalidad distinta a la prestación del Servicio al que se hace referencia en el presente Pliego.
 - Adoptar todas aquellas medidas técnicas y organizativas que resulten necesarias para garantizar un nivel de seguridad adecuado, guardar bajo su control y custodia los datos personales suministrados por la entidad contratante y no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas.
 - 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 (AEPD) 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 (AEPD) o cualquier otro órgano competente ya sea español o europeo, como consecuencia del incumplimiento de las obligaciones establecidas en el presente pliego.

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

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

<https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf>

8.1.5. Evaluación de proveedores

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

8.1.6. Obligaciones esenciales del contrato

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

☐	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.
☐	El sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 LCSP.
☐	Otras

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

Condición esencial	Frecuencia	Forma de acreditación del cumplimiento
Condiciones especiales de ejecución del contrato	Evaluación trimestral.	Auditorías internas y revisiones de cumplimiento.
El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista.	Anual.	Documentación acreditativa del cumplimiento de la condición especial de ejecución relativa a la prevención de delitos y códigos de conducta, conforme a lo establecido en el pliego de cláusulas administrativas particulares.

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 de ...euros.
☐	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 ☐ Régimen de protección de datos de carácter personal. ☐ 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.
☒	Condición de carácter social o medioambiental: Porcentaje de trabajadores fijos igual o superior al 20 por 100.
☐	Otras:

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

Condición especial	Frecuencia	Forma de acreditación del cumplimiento
Porcentaje de trabajadores fijos igual o superior al 20 por 100.	Al principio de la prestación.	Presentación de documentación oficial emitida por la tesorería general de la seguridad social (TGSS) o por el servicio público de empleo estatal (SEPE).

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

Todas las condiciones especiales de ejecución que formen parte del contrato serán exigidas igualmente a todos los subcontratistas que participen de la ejecución del

mismo, respondiendo el contratista principal en caso de incumplimiento por parte de aquellos.

8.1.8. Régimen de confidencialidad

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

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

8.2. Modificaciones del contrato

En el presente contrato:

☒ NO están previstas modificaciones.

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

Además, se prevé la posibilidad de acudir a lo dispuesto en el artículo 205 de la LCSP respecto de las modificaciones no previstas en el presente pliego.

8.3. Cesión y Subcontratación

8.3.1. Cesión del contrato

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

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

8.3.2. Régimen de subcontratación

Subcontratación permitida:

☐ NO ☒ SI

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

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

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

No existen tareas críticas que no puedan ser objeto de subcontratación.

9. Cumplimiento del contrato.

9.1. Responsable del contrato. Representante del contratista

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

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

9.2. Régimen de penalidades

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

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

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

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

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

9.3. Abonos al contratista. Facturación

El pago del servicio se efectuará a la realización conforme del mismo 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 estas 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		AI260016
Lote		
Grupo Gestor		Facturae/Parties/BuyerParty/AdministrativeCentres/AdministrativeCentre/CentreCode
Descripción de la operación		Facturae/Invoices/Invoice/AdditionalData/InvoiceAdditionalInformation
Fecha de la operación		Facturae/Invoices/Invoice/InvoiceIssueData/OperationDate
Grupo Gestor		Facturae/Parties/BuyerParty/AdministrativeCentres/AdministrativeCentre/CentreCode (RoleTypeCode 02)
Nº línea del pedido		Facturae/Invoices/Invoice/Items/InvoiceLine/SequenceNumber
Referencia legal		Facturae/Invoices/Invoice/Items/InvoiceLine/AdditionalLineItemInformation

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

9.4. Recepción y liquidación

El contratista deberá prestar el servicio dentro del plazo estipulado, efectuándose por el responsable del contrato un examen de la prestación realizada antes de darla por

recibida. El responsable del contrato podrá solicitar, en su caso, la realización de las prestaciones contratadas y la subsanación de los defectos observados.

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

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

9.5. Plazo de garantía

☐	SIN PLAZO DE GARANTÍA.
☐	GENERAL, de tres meses desde la recepción de conformidad del servicio.
☒	ESPECÍFICO, de 12 meses desde la recepción de conformidad del servicio.

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

10. Resolución del contrato

10.1. Causas de resolución

Serán causa de resolución del contrato:

☒	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 8.1.6.
☒	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.
☒	Incumplimiento de las obligaciones de carácter esencial recogidas en las letras a) a e) del artículo 122.2 LCSP.

10.2. Procedimiento

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

11. Protección de Datos

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

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

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

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 siguiente dirección:

- 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: dpggrupocorreos@correos.com o presentar una reclamación ante la autoridad de control (en España, la AEPD) en caso de que considere infringidos sus derechos.

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

En lo que respecta al tratamiento de datos personales que pudiera derivar de la prestación del servicio, los licitadores y la entidad contratante acuerdan someterse de manera expresa a la normativa vigente en materia de protección de datos en España y, en particular, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o "RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD").

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

12. Régimen jurídico del contrato y reclamaciones contra este pliego

El contrato se registrará, en cuanto a su preparación y adjudicación, por lo dispuesto en el presente Pliego y en el Real Decreto Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la UE en el ámbito de la contratación pública, así como en la Directiva 2014/25/UE de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales.

Las disposiciones de este pliego relativas a la modificación del contrato y las condiciones de subcontratación, resolución y especiales de ejecución se ajustarán igualmente a la normativa señalada. El resto de las cuestiones relativas a los efectos, cumplimiento y extinción del contrato se registrarán por lo previsto en la documentación que revista carácter contractual y por el Derecho Privado.

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

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos.
☒	Aceptación del contrato.
☒	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 reclamación, conforme a lo dispuesto en los artículos 119 y siguientes del Real Decreto Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, en el plazo de quince días hábiles a contar desde la publicación del anuncio de licitación en el perfil de contratante de la entidad.

Madrid, 10 de julio de 2026.

EL RESPONSABLE DE
ÁREA INTELIGENCIA Y CIBERDEFENSA

CONFORME:
EL SUBDIRECTOR DE
CIBERSEGURIDAD

Fdo.: Óscar Sanz Gallardo

Fdo.: Jesús Mayor Sendra

VºBº
LA DIRECTORA DE TECNOLOGÍA Y TRANSFORMACIÓN DIGITAL DE CORREOS

Fdo.: Cristina Tarrero Martos

Anexo I.- Características técnicas específicas del contrato.

ENTORNO TECNOLÓGICO

En la actualidad, Correos dispone de un contrato vigente para el suministro del mantenimiento hardware las licencias asociadas al Proxy Bluecoat de Broadcom (Symantec Web Protection) de las que es titular, dotando así a Correos de la suscripción con los derechos de uso, actualizaciones y los servicios de mantenimiento y soporte asociados y prestados con el respaldo del propio fabricante.

PART NUMBER/SKU	Descripción	Cantidad
SSP-S410-20B	Hardware: SYMANTEC S410-20B HW PLATFORM	2
PREMIUM-PLUS	Soporte Hardware: End Customer Support Level 1->3 Software Support & 24x7x4 Hour Parts Replacement Hardware Support	2
WEB-PROTECT-SUB	Licencias: Web Protection Suite	5.000

En concreto, Correos dispone de 2 equipos (SSP-S410-20B) con capacidad de función Proxy y de Servicio de Central de Autenticación (CAS) en cada uno, pudiendo configurarse alta disponibilidad entre los dos (HA). Para cada uno de estos equipos, Correos tiene contratado el soporte PREMIUM-PLUS que le dota de una cobertura de reemplazo de componentes de 24x7x4 horas.

Asociado a este hardware, Correos tiene contratada la suscripción de licencias Web Protection Suite, que incluye todos estos componentes:

- Puerta de enlace web segura (SWG) local: Software SWG local entregado como dispositivo virtual en su centro de datos.
- Cloud Secure Web Gateway (entregado como servicio): Protección Cloud SWG para cada usuario, entregada como servicio.
- Análisis de contenido e inspección profunda de archivos: Inspección multicapa y sandboxing bloquea amenazas que eluden el análisis tradicional.
- Servicio de Firewall Cloud: Firewall en la nube de próxima generación para una seguridad más allá de los puertos web estándar (80 y 443).
- Centro de Gestión (MC) y Reporter (RP): gestión de informes centralizados para infraestructura de red de Symantec.
- Reporter para SWG Cloud: Registros de tráfico basados en la nube desde cualquier ubicación.
- Proxy inverso: El proxy local aísla de forma segura el uso general de servidores desde el acceso directo a Internet.
- Aislamiento de Alto Riesgo (HRI): Aislamiento y ejecución remota de contenidos desde sitios desconocidos y de alto riesgo.

- Servicios de Inteligencia Avanzados (BCIS-A): Protección, categorización y aplicación en tiempo real control de contenidos web.

PRESTACIONES A REALIZAR

El contrato tiene por objeto el suministro de hardware y licencias asociadas a los proxies Bluecoat de Broadcom (Symantec Web Protection) de las que es titular Correos, junto con los derechos de uso, actualizaciones y los servicios de mantenimiento y soporte asociados que dará solución a las nuevas necesidades de capacidad.

El adjudicatario del presente contrato deberá proveer a Correos de los siguientes suministros:

PART NUMBER/SKU	Descripción	Cantidad
SSP-S210-10	Hardware: SYMANEC S210-10 HW PLATFORM	2
PREMIUM-PLUS	Soporte Hardware: End Customer Support Level 1->3 Software Support & 24x7x4 Hour Parts Replacement Hardware Support	2
ADVANCED	Soporte Hardware: End Customer Support Level 1->3 Software Support & Next Business Day Delivery Hardware Support	2
NETWORK-PROTECT-SUB	Licencias: Symantec Enterprise Cloud for SSE - Core Network Protection (Minimum quantity 200)	10.000

Estos suministros deberán proveerse, con el respaldo directo del propio fabricante, de la siguiente manera:

- Hardware:
 - ✓ Incorporar a la configuración actual 2 nuevos equipos de menor tamaño (SSP-S210-10) con capacidad de Proxy + CAS en cada uno.
 - ✓ El proveedor realizará las tareas de instalación y configuración del equipamiento contando con el apoyo de los equipos de sistemas que administran la infraestructura actual.
- Soporte hardware:
 - ✓ Soporte oficial PREMIUM-PLUS para los 2 equipos actuales SSP-S410-20B.
 - ✓ Soporte oficial ADVANCED para los 2 nuevos equipos SSP-S210-10.
- Licencias:
 - ✓ Suministro de la suscripción con los derechos de uso, actualizaciones, así como los servicios asociados de mantenimiento y soporte de las 10.000 licencias NETWORK-PROTECT-SUB que incluyen los mismos componentes que las

licencias WEB-PROTECT-SUB actuales (indicados más arriba), y añaden las siguientes capacidades y mejoras:

- ZTNA (Zero Trust Network Access): Acceso seguro a aplicaciones internas basado en identidad y contexto, sin exponer la red completa.
 - Remote Browser Isolation: Navegación web aislada en un entorno remoto para evitar que amenazas lleguen al dispositivo.
 - Advanced On-premises Sandboxing: Análisis local de archivos sospechosos en un entorno aislado para detectar amenazas avanzadas.
 - Enhanced Reporting Log Retention: Informes avanzados y mayor retención de logs para auditoría, análisis y cumplimiento.
- ✓ Se incluye en la provisión de licencias asociadas al hardware las tareas necesarias para la implantación de estas, incluyendo la migración de configuraciones o instalación de nuevos appliances si fuera necesario.

El adjudicatario se compromete a proporcionar las licencias en un plazo máximo de 7 días hábiles, a contar desde el día siguiente de la fecha de comunicación de la resolución de adjudicación.

A la recepción del hardware y del software objeto del contrato, se firmará por ambas partes un acta de recepción del suministro y de comienzo de la fase de prestación de los servicios de soporte y mantenimiento hardware.

CONDICIONES DE PRESTACIÓN DE LOS SERVICIOS

Con carácter general, los trabajos se llevarán a cabo en las propias oficinas del adjudicatario, el cual se obliga a disponer de toda la infraestructura técnica (comunicaciones, software y hardware) necesaria para poder desarrollar los trabajos de manera remota. Dicha infraestructura deberá seguir los estándares que Correos fije al respecto, cumpliendo las normas de seguridad, arquitectura y comunicaciones definidas, y que se detallan más abajo, en el punto “Cumplimiento de normativas internas”.

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

La actividad del equipo de trabajo se desarrollará normalmente dentro de un horario de oficina, a través de la herramienta corporativa de gestión de incidencias, consultas y peticiones de Correos. Las condiciones estándar de prestación de los diferentes servicios será el siguiente:

- Soporte para resolución de incidencias/consultas a nivel de proyecto: de 9:00 a 18:00 horas de lunes a viernes, en días laborables según el calendario laboral de la ciudad de Madrid.
- Soporte 24x7 para situaciones críticas: Para incidencias críticas de producción no programadas fuera del horario de soporte, soporte telefónico proporcionando asistencia las 24 horas del día.

- Atención y operación del Sistema: de lunes a viernes de 07.30 a 19:30 excluyendo los días festivos, locales, autonómicos y nacionales de la ciudad de Madrid. El servicio se realiza remotamente mediante conexión directa a la plataforma.

No obstante, si fuera necesario, Correos podrá requerir la presencia de técnicos del adjudicatario en sus dependencias, ubicadas en Madrid, facilitando un número limitado de puestos de trabajo para uso del adjudicatario en momentos puntuales. Los recursos que el adjudicatario determine para su trabajo presencial en dependencias de Correos deberán tener la solvencia técnica y funcional necesaria para que se garantice la respuesta rápida a las necesidades que se planteen, o la resolución inmediata de una situación crítica si este fuera el caso.

La empresa que resulte 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 pliego (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, servicios de las licencias ya existentes, o la descarga, instalación, activación, 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, mala praxis, etc.

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 de Correos a las que tendrá acceso el personal del adjudicatario encargado de prestar el citado servicio, incluyendo información de las licencias de software o, 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 de Correos. Adicionalmente, si el adjudicatario lo estima oportuno, podrá pedir a Correos las aclaraciones o información adicional que requiera para conocer la citada configuración del ecosistema software en el que prestará su servicio.

CUMPLIMIENTO DE NORMATIVAS INTERNAS

El adjudicatario del presente contrato quedará obligado a que todos los trabajos que realice en el marco de la prestación de los diferentes servicios cumplan en todo momento y durante toda la duración del contrato, con las diferentes normativas y requerimientos

vigentes de uso interno (anexos [XIX](#) y [XX](#)), así como con las actualizaciones que de las mismas pudieran realizarse durante la duración del contrato.

ESTIMACIÓN DE IMPORTES

Con objeto de ayudar a establecer el alcance y facilitar el dimensionamiento de los recursos asociados a la ejecución de las tareas necesarias para la prestación de los servicios contratados, se facilita la siguiente estimación realizada por Correos a partir de los precios proporcionados por el fabricante (sin IVA):

SUMINISTRO	UNIDADES	PRECIO ANUAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)	% SOBRE EL TOTAL	PRECIO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
SSP-S210-10 (hardware)	2	13.996,83 €	13,87%	83.981,00 €
PREMIUM-PLUS (soporte hardware)	2	45.397,59 €	22,49%	136.192,78 €
ADVANCED (soporte hardware)	2	15.107,35 €	7,49%	45.322,04 €
NETWORK-PROTECT-SUB (Licencias)	10.000	113.333,33 €	56,15%	340.000,00 €
TOTAL		201.831,94 €	100,00%	605.495,82 €

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

El presente procedimiento de licitación no se divide en lotes, de conformidad con lo establecido en el artículo 52.3 b) del Real Decreto-Ley 3/2020 de 4 de febrero:

“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; o bien que el riesgo para la correcta ejecución del contrato proceda de la naturaleza del objeto del mismo, al implicar la necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes. Ambos extremos deberán ser, en su caso, justificados debidamente en el expediente”

El contrato no se divide en lotes al concurrir estos motivos válidos: (I) interdependencia técnica entre los elementos de hardware y las licencias asociadas; (II) riesgo operativo por multiplicación de interlocutores y pérdida de trazabilidad en actualizaciones y RMA (Autorización de Devolución de Mercancía, por sus siglas del inglés de Return Merchandise Authorization); y (III) necesidad de coordinación unificada, ya que un mantenimiento fragmentado puede generar incompatibilidades temporales y soluciones parciales, aumentando el esfuerzo total y el consumo de recursos.

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

El valor estimado del contrato se obtiene de la siguiente manera:

Presupuesto de ejecución	605.495,82 €		
Plazo de Ejecución (meses)	36		
Modificación 20%	No		
Prórroga (meses)	No		
VALOR ESTIMADO DEL CONTRATO	605.495,82 €		

No se contempla la posibilidad de modificación.

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.

Cuando se admita como forma de acreditar la solvencia, la suscripción de un seguro de responsabilidad civil se acreditará mediante la presentación de:

- ✓ Copia de la póliza o certificado de compañía aseguradora o el mediador de conformidad de la cobertura suscrita con el objeto de la licitación.
- ✓ Copia del último recibo de pago de la póliza
- ✓ Declaración responsable sobre su vigencia, y compromiso de renovación, donde deberán recogerse las siguientes condiciones:
 - La cobertura temporal de la póliza deberá comprender, como mínimo, el período de duración inicial del contrato, y contemplarse expresamente la posibilidad de prórroga de dicha póliza en caso de acordarse la prórroga del contrato.
 - La cobertura económica deberá ser equivalente a la
 - ☐ Anualidad media del contrato, o al presupuesto de licitación, en caso de contratos con una duración inferior a un año.
 - ☐ (Otra cantidad.....), atendiendo al riesgo estimable presente en el contrato

- 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 Curriculum Vitae 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.

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 Avaluos 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 será automáticamente inadmitida del 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 y la entidad contratante; estos datos deben ser facilitados o puestos por el poder adjudicador).

☒ PARTE II: Información sobre el operador económico.

☒ Sección A: Información sobre el operador económico.

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

☒ Sección B: Información sobre los representantes del operador económico.

- Representación, en su caso (datos del representante).

☒ Sección C: Información sobre el recurso a la capacidad de otras entidades.

- Recurso (Sí o No).

☒ Sección D: Información relativa a los subcontratistas.

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

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

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

☒ Sección B: Motivos referidos al pago de impuestos o de cotizaciones a la SEG. SOCIAL. Pago de impuestos o de cotizaciones a la Seguridad Social (declara cumplimiento de obligaciones).

☒ Sección C: Motivos referidos a la insolvencia, los conflictos de intereses o la falta profesional. Información relativa a toda posible insolvencia, conflicto de intereses o falta profesional.

☒ Sección D: Otros motivos de exclusión que estén previstos en la legislación nacional. Motivos de exclusión puramente nacionales (si los hay, declaración al respecto).

PARTE IV: CRITERIOS DE SELECCIÓN.

☒ OPCIÓN 1: Indicación global de cumplimiento de todos los criterios de selección.

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

- Sección A: Idoneidad: (información referida a la inscripción en el Registro Mercantil u oficial o disponibilidad de autorizaciones habilitantes).
- Sección B: Solvencia económica y financiera (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección C: Capacidad técnica y profesional (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección D: sistemas de aseguramiento de la calidad y normas de gestión medioambiental.

☐ PARTE V: Reducción del número de candidatos cualificados.

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

Anexo IX.- Criterios de adjudicación de evaluación automática

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

Anexo X.- Modelo de proposición económica

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

En caso de actuar en representación

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

Enterado de las condiciones y requisitos para concurrir al procedimiento convocado por la Sociedad Estatal Correos y Telégrafos S.A, 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 el siguiente modelo de oferta (ver definición para cada lote a continuación):

Descripción del suministro	Importe anual sin impuestos (€)	Nº de meses que comprende el contrato	Importe total sin impuestos (€)	Impuesto aplicable (%)	Importe total con impuestos (€)
Hardware					
Referencias y cantidad de los equipos hardware		36			
...		36			
Soporte hardware					
Referencias y cantidad de los servicios objeto del soporte hardware		36			
..		36			
Licencias asociadas al hardware					
Referencias y cantidad de los servicios objeto del soporte hardware		36			
..		36			
Importes totales		36			

Los importes reflejados deberán indicarse solo con dos decimales y redondeados al segundo decimal.

Se deberá incluir en la oferta los importes de cada uno de los conceptos en los que se desglosa la misma, indicando el importe total o global, sin impuestos y con impuestos, con la suma de todos los conceptos de los que se compone.

La oferta deberá incluir cualquier coste asociado a la prestación (soporte, mantenimiento, reemplazos, logística, acceso a portales). No se admitirán incrementos de precio por conceptos no cotizados; la oferta se considerará cerrada y vinculante.

NOTA 1. – Cualquier oferta deberá indicar expresamente que acata el siguiente plan de facturación:

Hardware

- Importe fijo a la finalización de su puesta en producción (1 anualidad).

Soporte hardware

- Importe mensual fijo a la finalización de cada periodo (36 mensualidades).

Licencias asociadas al hardware

- Importe mensual fijo a la finalización de cada periodo (36 mensualidades).

NOTA 2. – Cualquier oferta presentada debe incorporar al final de la misma:

Lugar, fecha firma autorizada.

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

NO APLICA

Para la ejecución de este contrato procede la subrogación en contratos de trabajo prevista en (indicar *convenio colectivo de aplicación y pactos en vigor aplicables a los trabajadores a los que afecte la subrogación*) respecto de los siguientes:

<i>número de trabajadores</i>	<i>categoría</i>	<i>tipo de contrato</i>	<i>vencimiento del contrato</i>	<i>jornada</i>		<i>fecha de antigüedad</i>	<i>salario bruto anual</i>	<i>Otras condiciones</i>

Sin perjuicio de la aplicación, en su caso, de lo establecido en el artículo 44 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, el contratista anterior responderá de los salarios impagados a los trabajadores afectados por subrogación, así como de las cotizaciones a la Seguridad social devengadas, aún en el supuesto de que se resuelva el contrato y aquellos sean subrogados por el nuevo contratista, sin que en ningún caso dicha obligación corresponda a este último. En tal caso, la entidad contratante, una vez acreditada la falta de pago de los citados salarios, procederá a la retención de las cantidades debidas al contratista anterior para garantizar el pago de los citados salarios, y a la no devolución de la garantía definitiva en tanto no se acredite el abono de éstos.

Anexo XII.- Modificaciones previstas del contrato

NO APLICA

Anexo XIII.- Régimen de penalidades

A).- INCUMPLIMIENTOS LEVES

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Suministro de licencias	Retraso en la entrega de licencias (> 7 días hábiles).	0,5% del importe del suministro por día de retraso (máx. 5%).
Despliegue	- Retraso en instalación/configuración de nuevo HW (SSP-S210). - Implantación incompleta (migración/configuración no finalizada).	0,5% del importe del HW por día (máx. 5%). - Hasta 3% del contrato afectado.
Soporte y mantenimiento para los dispositivos SSP-S410-20B	- Incidencias críticas no atendidas en plazo. - Incumplimiento soporte 24x7 (hardware). - Incumplimiento soporte NBD / 4h replacement.	- Hasta 2.000 € por incidencia. - Hasta 5% de la facturación mensual. - Hasta 3% mensual.
Soporte y mantenimiento para los dispositivos SSP-S210-10	- Incidencias críticas no atendidas en plazo. - Incumplimiento soporte NBD (Next Business Day).	- Hasta 1.000 € por incidencia. - Hasta 3% mensual.
Indisponibilidad	Disponibilidad < 99,9%.	99,5–99,9%: 1% mensual. 99–99,5%: 3% mensual. < 99%: 6% mensual.
Incumplimiento funcional	- Fallo en políticas de filtrado. - Bloqueos indebidos o bypass de seguridad.	- Hasta 1.000 € por evento. - Hasta 2.000 € por incidente.
Cumplimiento defectuoso del ANS	Por el cumplimiento defectuoso de la prestación objeto del contrato, según lo indicado en los ANS relativos a este asunto descritos en el Anexo XIV .	- Incumplimiento puntual: hasta 1% mensual - Incumplimiento reiterado: hasta 10% del contrato
Seguridad	Fallo en políticas de filtrado. Bloqueos indebidos o bypass de seguridad.	- Hasta 1.000 € por evento. - Hasta 2.000 € por incidente.
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	Detectar 10 o más vulnerabilidades Baja (CVSS < 4.0)	2% facturación anual de la adjudicación, con un mínimo de 5.000€

soluciones de terceros*		
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 de ejecución total o parciales establecidos, considerados como grave según lo descrito en Anexo XIV .	☐ 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: Penalidad de hasta un 6 por ciento sobre el importe de la facturación mensual IVA excluido
Cumplimiento defectuoso	Por el cumplimiento defectuoso de la prestación objeto del contrato, según lo indicado en los ANS relativos a este asunto descritos en el Anexo XIV .	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 por ciento de la prestación.
Subcontratación	Incumplimiento de las condiciones de subcontratación	Penalidad de hasta un 50 por ciento del importe del subcontrato.
Reincidencia	La comisión de una tercera infracción de carácter grave en el plazo de un año	Penalidad de hasta el 6 por ciento del precio del contrato, IVA excluido.
ANS	Por el incumplimiento de los acuerdos de nivel de servicio.	Penalidad de hasta el 10 por ciento del precio de adjudicación del contrato (IVA excluido) por cada día de incumplimiento de dicha obligación.

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 ($4.0 \leq CVSS < 7.0$)	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 de ejecución total o parciales establecidos, considerados como muy grave según lo descrito en Anexo XIV .	☐ 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: Penalidad de hasta un 10 por ciento sobre el importe de la

		facturación mensual € IVA excluido
Cumplimiento defectuoso	Por el cumplimiento defectuoso de la prestación objeto del contrato, según lo indicado en los ANS relativos a este asunto descritos en el Anexo XIV .	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 por ciento de la prestación.
Condiciones especiales de ejecución	Por el incumplimiento de condiciones especiales de ejecución	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
Reincidencia	La comisión de una tercera infracción de carácter muy grave en el plazo de un año	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
ANS	Incumplimiento de los acuerdos de nivel de servicio.	Penalidad de hasta el 10 por ciento del precio de adjudicación del contrato (IVA excluido) por cada día de incumplimiento de dicha obligación.
Por incumplimiento del convenio colectivo aplicable	Incumplimiento del convenio colectivo	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 ≥ 9.0)	5% facturación anual 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 Altas ($7.0 \leq \text{CVSS} < 9.0$)	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 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€
---	---	--

Nota: Con carácter general, las penalidades se deducirán de la factura única si estuviera pendiente de pago. Si la factura se hubiera abonado, se compensarán frente a obligaciones de pago futuras con el Grupo o, en su defecto, se harán efectivas contra la garantía definitiva, que el adjudicatario deberá reponer en el plazo de 10 días hábiles desde el requerimiento.

(*) 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 ≥ 9.0)	Muy grave	15 días	2.000 € por día de retraso
Vulnerabilidades Altas ($7.0 \leq \text{CVSS} < 9.0$)	Muy grave	27 días	2.000 € por día de retraso
Vulnerabilidades Medias ($4.0 \leq \text{CVSS} < 7.0$)	Grave	33 días	1.000 € por día de retraso
Vulnerabilidades Bajas (CVSS < 4.0)	Leve	35 días	500 € por día de retraso

Anexo XIV – Evaluación de Proveedores

La ejecución del presente contrato se encuentra sujeta a controles de calidad por parte de Correos, y a un sistema de evaluación continua y final con el fin de garantizar la buena ejecución y la calidad de los servicios contratados.

Los controles de calidad que se aplicarán quedan definidos por el Acuerdo de Nivel de Servicio (ANS) que se detalla a continuación:

ACUERDO DE NIVEL DE SERVICIO (ANS)

Los servicios que son objeto del presente pliego se regularán en su prestación 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) que se definen en el mismo y que se detallan en este anexo.

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, e independientemente de si presta los servicios con medios propios o si los subcontrata parcialmente (estando esta subcontratación autorizada previamente por Correos). No obstante, si de forma puntual en algún mes uno o varios indicadores individuales se ven afectados por los trabajos correspondientes a equipos ajenos a los del adjudicatario, Correos determinará el ámbito y el alcance de la responsabilidad para ese caso concreto.

En el caso en que se detectara un deterioro en el servicio que no quedara reflejado en los indicadores, se realizaría el correspondiente informe que permitiera mostrar el mismo, identificando y cuantificando su impacto, en el mes en el que correos estime oportuno con posterioridad a dicho deterioro. Esta información se incorporaría al acuerdo de nivel de servicio bien como una modificación en el cálculo y definición de los indicadores que se estén utilizando, bien como la incorporación de un nuevo indicador.

Así mismo, el adjudicatario se compromete a realizar una revisión del ANS con una periodicidad no superior a seis meses, pudiendo acordarse entre Correos y el adjudicatario nuevas condiciones en el ANS (p.e. nuevos valores objetivo y/o porcentajes de cumplimiento, nuevos indicadores de servicio) teniendo en cuenta, entre otros, la evolución histórica de los indicadores del ANS.

Los ANS comenzarán a computarse y aplicarse desde el primer día del servicio. En los apartados correspondientes a cada indicador, se define el valor de cumplimiento y/o el porcentaje de cumplimiento con sus valores objetivo. Estos valores se tendrán en cuenta en el sistema de evaluación y en el caso de que no se alcancen los mínimos requeridos, y en función de la gravedad, se establecerá una minoración en la facturación que en su caso corresponda (ver [Anexo XIII](#)).

SISTEMA DE EVALUACIÓN

El sistema de evaluación del cumplimiento del nivel de servicio queda definido por el cumplimiento de los siguientes indicadores, valores objetivo y forma de evaluación:

Hardware.

1. Disponibilidad

- 1.1 Disponibilidad servicio: $\geq 99,9\%$ mensual.
- 1.2 HA entre equipos proxy: 100% operativa.

Evaluación:

$$\text{Disponibilidad (\%)} = \text{Tiempo activo} / \text{Tiempo total} \times 100$$

2. Piezas

- 2.1 Reposición piezas críticas: $\leq 4\text{h}$ (Premium Plus).
- 2.2 Resto hardware: Next Business Day.

Evaluación:

$$\% \text{ de reposiciones dentro de tiempo objetivo } (\geq 95\%)$$

3. Rendimiento

- 3.1 Latencia adicional: $\leq 50 \text{ ms.}$
- 3.2 Autenticación usuario: $\leq 2 \text{ segundos.}$

Evaluación:

$$\text{Promedio mensual y percentil 95 de las mediciones}$$

Soporte hardware.

4. Soporte

La descripción de los tipos de incidencias, en función de su importancia, es la que sigue a continuación:

- 4.1 Se define una incidencia crítica como aquella que ocasiona que el entorno de producción esté caído o que no funcione en absoluto, y no hay forma de evitarlo. Un número significativo de usuarios se ve afectado, y el entorno empresarial de Correos en producción es inoperable.
- 4.2 Se define como una incidencia alta como aquella que un componente no está funcionando, creando un impacto operativo significativo.
- 4.3 Se define como incidencia media aquella que ocasiona que la plataforma no funcione como está documentado o se espera. Baja el rendimiento, pero se puede operar y posible una solución alternativa. Hay un impacto operativo moderado o menor.
- 4.4 Se define como incidencia baja aquella que ocasiona que la plataforma funcione con normalidad de cara a los usuarios, pero supone un mal

funcionamiento que es necesario corregir. No hay impacto operativo, pero sí técnico.

Tipo incidencia	Respuesta	Resolución	Actualización	Porcentaje de Cumplimiento mínimo (PCm)
4.1 Crítica	≤ 1h	≤ 4h	Diaria	90%
4.2 Alta	≤ 2h	≤ 8h	Diaria	90%
4.3 Media	≤ 4h	≤ 24h	Semanal	90%
4.4 Baja	≤ 8h	≤ 48h	Semanal	90%

Evaluación:

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:

$$PC = \text{Incidencias respondidas y resueltas en tiempo} / \text{Total incidencias} \times 100$$

El grado de cumplimiento (en adelante, GC) señala el porcentaje de incidencias solucionadas dentro del valor objetivo, sobre el total de las solucionadas en el mes más las retrasadas de ese mes o meses anteriores. El GC para valores intermedios de PC se calculará sobre el tiempo de respuesta total de incidencias mensualmente de la siguiente forma:

$$GC = 100 * \frac{PC}{PCm}$$

, en donde:

$$GC = 100, \text{ si } PC \geq PCm$$

$$GC = 0, \text{ para } PC = 0$$

El adjudicatario debe obtener un GC = 100 para que Correos no le aplique corrección a la facturación. Este porcentaje de corrección se aplicará sobre el importe mensual total del servicio de mantenimiento permanente y se calculará mensualmente.

5. Seguridad

- 5.1 Actualización firmas: diaria automática
- 5.2 Detección amenazas: ≥ 99%.
- 5.3 Notificación incidentes: ≤ 24h.
- 5.4 Informe RCA: ≤ 48h.

Evaluación:

Auditoría de eventos de seguridad

Licencias asociadas al hardware.

6. Provisión

- 6.1 Entrega de licencias: ≤ 7 días hábiles.
- 6.2 Entrega del HW, Configuración y migración: ≤ 3 meses.
- 6.3 Activación completa: 100%.

Evaluación:

Informes de seguimiento

7. Cobertura

- 7.1 Usuarios protegidos: 100% (10.000 licencias)
- 7.2 Tráfico inspeccionado: 100% HTTP/HTTPS

Evaluación:

Validación mensual de cobertura real vs contratada y auditoría de tráfico inspeccionado.

SEGUIMIENTO Y GESTIÓN DEL SERVICIO.

El adjudicatario se compromete a poner en marcha el sistema de seguimiento del ANS en un plazo máximo de 1 mes desde la fecha de comienzo del proyecto.

El proveedor se compromete a utilizar el sistema corporativo de seguimiento del ANS – PoST que está basado en ITSM Remedy.

No obstante, lo anterior, el proveedor se compromete a aportar un sistema complementario, si el seguimiento de los indicadores del ANS acordado inicialmente así lo requiere o, en su caso, del que resulte de modificaciones posteriores lo requiera. Este sistema complementario deberá ser autorizado, previa y expresamente por Correos.

El contenido y periodicidad de los informes de seguimiento, así como cualquier otra característica del procedimiento de seguimiento, serán indicados por Correos al inicio de los trabajos. La no entrega de los informes de seguimiento solicitados, así como la entrega incompleta, fuera de plazo o sin respetar las especificaciones de Correos, podrá ser considerada como incumplimiento, con la consiguiente corrección en la facturación de los indicadores a que esa información haga referencia.

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

NO APLICA

Anexo XVI.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la ley 9/2017, de 8 de noviembre, de contratos del sector público

Don/Doña

NIF

Con domicilio en

Calle/Plaza, nº

Telf. contacto nº

Correo electrónico

En caso de actuar en representación

Como apoderado de

CIF

Con domicilio en

Calle/Plaza, nº

Correo electrónico

DECLARA BAJO SU RESPONSABILIDAD:

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

☐ CUMPLE con la obligación de contar con un plan de igualdad.

☐ La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

SUMINISTROS SIN TRATAMIENTO DE DATOS
Procedimiento: ABIERTO
Expediente núm.: AI260016



Anexo XVII Adscripción de medios

NO APLICA

Anexo XVIII. Compromiso de adscripción de personal al contrato

NO APLICA

Don/Doña

NIF

Con domicilio en

Calle/Plaza, nº

Telf. contacto nº

Correo electrónico

En caso de actuar en representación

Como apoderado de

CIF

Con domicilio en

Calle/Plaza, nº

Correo electrónico

DECLARA BAJO SU RESPONSABILIDAD / MANIFIESTA

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

- Medios Humanos

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

Lugar, fecha y firma de licitador

Anexo XIX – Requerimientos Arquitectura

1. Introducción:

En este anexo se especifican los requisitos tecnológicos que deben tenerse en cuenta a la hora de ofertar una solución. Estos requisitos son de obligado cumplimiento por parte del adjudicatario, y aplicarán en función de la naturaleza de la solución, del modo que se explica en los siguientes puntos.

Solución SaaS (Software as a Service)

Si la solución propuesta por el adjudicatario es de tipología SaaS, este debe facilitar el uso del software, abstrayendo a Correos sobre aspectos relacionados con el hardware, las comunicaciones y la seguridad necesarias. Además, el adjudicatario debe realizar todos los servicios relacionados con el hosting, mantenimiento, operación, recuperación de datos, incidencias (tanto anticipación como resolución) de la solución propuesta, pagando Correos exclusivamente por el uso de la solución.

2. Requisitos de diseño:

- Los componentes tecnológicos que forman parte de la solución deben estar soportados por los fabricantes durante todo el periodo que Correos use la solución SaaS. Además, estos fabricantes han de tener un reconocido prestigio y reconocimiento global (por ejemplo, AWS, GCP o Azure).
- En el supuesto de que la solución SaaS preste su servicio desde varios centros de datos dispersos geográficamente, estos deben estar en el marco de la Unión Europea. El adjudicatario debe indicar en su oferta si se despliega el servicio en un CPD alternativo, y este CPD debe estar ubicado en la Unión europea.
- El adjudicatario debe garantizar la alta disponibilidad de la solución, preferiblemente disponiendo de varias áreas geográficas desde las cuales se pueda seguir dando servicio en caso de que una de ellas no esté disponible.
- La solución debe garantizar la escalabilidad del servicio, en caso de que Correos necesite usar servicios adicionales de la solución, o incrementar el uso de los mismos.
- La solución debe garantizar su normal funcionamiento ante aumentos en la carga de trabajo, proporcionando un servicio sin degradación en las épocas de mayor actividad y garantizando que la plataforma soporte un incremento de hasta el 100% de la carga. En este caso, Correos debe avisar al adjudicatario con aviso previo de 48 horas. El servicio de soporte asociado a la solución debe estar dimensionado y preparado para estos eventuales aumentos en la carga de trabajo.
- Se deberá disponer de sistemas de protección anti-DDoS, así como de filtrado del tráfico, incorporando características WAF.
- El prestatario debe garantizar la portabilidad de los datos que residen en su solución, así como el código fuente y configuraciones específicas de Correos en la

solución, para facilitar la integración con Correos, o bien en otras plataformas de las que disponga el fabricante

- La solución debe contar con medios de protección que garanticen la mitigación de riesgos asociados a la fuga de información, y deben ser explicados a Correos en la oferta del adjudicatario.

3. Requisitos de integración

- La solución SaaS ofrecida debe albergar la posibilidad de integración con servicios y aplicaciones de Correos, mediante los mecanismos de integración estandarizados en Correos, descritos a continuación:
 - a. API (REST, y SOAP)
 - b. Mensajería asíncrona mediante colas MQ
 - c. Intercambio de ficheros con grandes volúmenes de datos (SFTP)
- Estas integraciones podrán ser en ambos sentidos:
 - a. La solución debe exponer mecanismos de integración para que puedan ser invocados por los sistemas de Correos. Por ejemplo, exponer una API.
 - b. La solución debe ser capaz de invocar a los sistemas de Correos para obtener información o ejecutar procesos. Por ejemplo, invocar a un servicio REST.
- La solución debe tener la capacidad de adaptarse a las necesidades de integración desde un punto de vista volumétrico, en caso de que se requiriera un intercambio de mucha información, que haya que realizar de una forma óptima.
- La solución debe permitir la realización de pruebas de integración en entornos no productivos.
- El servicio SaaS debe integrarse con los proveedores de identidad corporativos de Correos, delegando en ellos la autenticación de los usuarios que trabajen con el producto. Esta autenticación podrá realizarse mediante los siguientes mecanismos:
 - a. Oauth 2: Quedando prohibido usar el *implicit grant type*.
 - b. Servicios LDAP que ofrece *Microsoft Active Directory* usado en Correos

4. Requisitos de mantenimiento, operación y monitorización de los sistemas

- Los cambios en la configuración del servicio, los despliegues de las actualizaciones, los procesos de tuning interno, y resto de acciones de mejora continua del servicio, serán comunicados a Correos con una antelación de:
 - a. 15 días, si el cambio no implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.

- b. 6 meses, si el cambio implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.
- El adjudicatario debe responsabilizarse de la ejecución de implementaciones, configuraciones y acciones predictivas, que permitan la recuperación del servicio ante cualquier desastre. Correos exige que este tiempo de recuperación de los servicios sea de menos de 4 horas.
- La solución debe dar servicio a Correos, sin perjuicio en el rendimiento o la disponibilidad del servicio, ante un incremento de hasta el 100% de la carga, y con un aviso previo de al menos 48 horas por parte de Correos.
- El servicio debe ser convenientemente monitorizado por el prestatario del servicio, y esta monitorización ha de ser extremo a extremo, es decir, desde el nivel físico (hardware) hasta los procesos de negocio.
- Al detectarse una incidencia en el servicio, el adjudicatario debe solucionarla y enviará un informe que incluya:
 - a. La ventana temporal de afectación del servicio.
 - b. Una explicación de las causas que han producido la incidencia.
 - c. Acciones puestas en marcha para solucionar la incidencia.
 - d. Dentro de las 48 horas posteriores a la resolución de una incidencia, se enviará un análisis de la causa raíz (RCA), para eventos críticos.
- Aquellos eventos que puedan afectar al servicio, incluyendo degradación de rendimiento, actualizaciones críticas o incidentes de seguridad, serán notificados de manera proactiva por parte del prestatario a Correos, indicando el impacto previsto y el plan de mejoras a implementar. El adjudicatario debe indicar el tiempo estimado de resolución de la incidencia.
- La solución, o en su defecto el adjudicatario del servicio, deben proveer a Correos de información respecto a los parámetros del servicio prestado. Correos debe tener disponible tanto datos operativos como las métricas del servicio. Debe proveerse esta información a través de cuadros de mando, y esta información debe poder exportarse en algún formato estándar y consensuado con Correos, como XML, JSON o CSV.
- En caso de que la solución tenga versiones del producto on premises y Cloud, debe facilitar la migración de información entre las versiones del producto. El proceso de migración de datos, procesos y configuraciones específicas que ha implementado Correos en la plataforma, debe ser exportable en la plataforma origen, e importable en la plataforma destino, con algún mecanismo manual o automático que facilite esta migración.

5. Requisitos sobre acuerdos a nivel de servicio

- La disponibilidad del servicio debe ser 99.9% o mayor. En esta métrica deben incluirse fines de semana sólo si Correos va a usar el servicio durante estos días.
- Si el adjudicatario fuera capaz de mejorar los ANS exigidos por Correos, deberá presentar en su oferta dicha propuesta de nuevos ANS específicos para Correos, incluyendo indicadores y métricas del servicio. Una vez que Correos haya validado los indicadores propuestos por el adjudicatario y el cumplimiento de los mínimos requeridos, ambas partes suscribirán el correspondiente Acuerdo de Niveles de Servicio Definitivo, que será de aplicación durante todo el periodo de vigencia del contrato.
- La solución (y el adjudicatario de la misma) deben proponer un modelo de gobierno del servicio, que incluya un modelo de comunicación efectivo para Correos, y defina las funciones y responsabilidades de los distintos actores en el desarrollo del servicio.
- RTO (Return Time Objective) o tiempo máximo de restablecimiento del servicio una vez que ya no se ha cumplido el ANS contratado, y Correos podrá aplicar KPIs incrementales a fin de evitar que la persistencia de una incidencia no se refleje adecuadamente en los indicadores una vez que ya ha contabilizado como tal.
- RPO. (Return Point Objective) o período de tiempo máximo asumible sobre el que se puede perder datos. Desde Correos por defecto, la tendencia debe ser igual a cero.
- Correos será el propietario de cuantos trabajos parciales o finales se deriven de esta colaboración, así como de todos los datos, y el adjudicatario se compromete a la devolución de los mismos, sin que el adjudicatario pueda conservarlos, ni obtener copia de los mismos o facilitarlos a terceros. El adjudicatario sólo podrá consultar o extraer estos datos con la autorización expresa de Correos.
- En la oferta presentada por el adjudicatario, deben especificarse claramente las condiciones sobre las que se registrará la devolución de la información residente en la solución.

Solución PaaS (Platform as a Service)

Dentro de las soluciones de esta tipología, el adjudicatario debe administrar la plataforma a nivel de sistema operativo, almacenamiento, comunicaciones, y demás recursos de bajo nivel, abstrayendo a Correos de esta gestión operativa, y ofreciendo un servicio fácilmente escalable para Correos.

Los requerimientos exigidos para la solución SaaS son aplicables para la solución PaaS, teniendo en cuenta algunos requisitos adicionales que se detallan a continuación.

6. Requisitos específicos de PaaS

- La solución debe permitir la creación de nuevos tenant o mecanismos alternativos que permitan el crecimiento ordenado del servicio. El tiempo de respuesta y los

recursos dedicados al servicio de Correos no se verá afectado por picos en los procesos que sean compartidos con otros clientes.

- La solución debe incorporar políticas de respaldo de información, automatizadas, y el adjudicatario debe realizar pruebas de restauración, de forma periódica, con una retención de al menos 30 días.

Productos comerciales:

Correos puede necesitar adquirir un producto software o hardware, que debe instalar y desplegar en su infraestructura *on premises* normalmente, o también en *cloud* (por ejemplo, instalado en IaaS), sin tratarse de un producto que se consume en modalidad SaaS. Los siguientes requisitos describen la naturaleza del producto que se instalará en la infraestructura de Correos.

7. Requisitos de diseño:

- El producto debe seguir el diseño de arquitectura física en tres capas:
 - a. Capa de presentación. Donde se despliegan artefactos relacionados con la interfaz de usuario.
 - b. Capa de lógica de negocio. Donde se despliegan los componentes de backend de la solución.
 - c. Capa de datos. Donde se alojarán los datos, que sólo serán accesibles desde la capa de lógica de negocio.

En caso de que el producto no disponga de esta arquitectura, la propuesta alternativa debe ser explicada por el adjudicatario a Correos, en la oferta presentada.

- Los licitadores deberán describir la arquitectura propuesta de manera detallada indicando expresamente cualquier necesidad de servicio horizontal o hardware adicional para el funcionamiento de su solución. Entre los datos de la arquitectura, está la arquitectura del procesador, versionados de sistema operativo, middleware, bases de datos, y en general de todo el software de base y todo elemento que forme parte de la infraestructura, bien sea de hardware o de software. Deberá facilitarse una propuesta de solución.
- En la solución propuesta se admitirá el uso de componentes Hardware (Appliances) sólo en el caso de que no exista la posibilidad de realizarla con el hardware que aprovisiona Correos. Así mismo, todo Servidor que requiera un software base con tecnologías distintas al apartado de Entorno Tecnológico, excluyendo versiones, podría ser tratado también como appliance si el equipo de explotación no tuviera el conocimiento para su administración, teniendo que contemplar el licitante expresamente en la oferta como concepto de administración y mantenimiento por el conjunto de servidores y su software base, excluyendo el de producto o desarrollo que presta el servicio. Una vez adjudicado

se evaluará la compatibilidad con las herramientas de monitorización, logs y de backup, junto los equipos de explotación de Correos.

- El producto será escalable (horizontal y verticalmente), con la posibilidad de extender la plataforma a medida que se incorporan nuevos usuarios o cargas de trabajo, reduciendo el tiempo de provisión de equipamiento que soporte los nuevos servicios.

Entono tecnológico para el producto:

La infraestructura y el software sobre el que se instale la solución debe ajustarse a la matriz de compatibilidad del fabricante, y será Correos quien decida el software base y la torre tecnológica a utilizar.

8. Cloud

Elemento	Versiones
Sistemas Operativos	Red Hat Enterprise Linux 8 o superior (plataforma de 64 bits) Windows 2019 o superior (plataforma de 64 bits) Amazon Linux 2 o superior
Gestor de Base de Datos	<u>Relacional:</u> Amazon RDS (PostgreSQL 16.x) Amazon RDS (MySQL 8.0.39) <u>Clave-valor:</u> DynamoDB <u>No relacional:</u> Atlas MongoDB 8.x
Servidores de aplicaciones	NodeJS (lambda) 20 o superior
Runtimes e Interpretes	OpenJDK (caas)1.17 OpenJDK (lambda)1.17 OpenJDK (onPremise) - SpringBoot1.11 PHP (caas) 8.2 Python (lambda) 3.12 Javascript/Typescript para los frontales ReactJS

Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux. Nginx1.20
Orquestador Contenedores	Openshift Container Platform 4.16 (Docker) para arquitecturas basadas en microservicios.
Imágenes de contenedores	<u>Contenedores:</u> Frontend: Nginx (1.22) / Apache (2.4.x) / Node.js (20 o superior) / Tomcat (9 o superior) Backend: Springboot con tomcat embebido (3.1.4)
Integración	API Gateway (CaaS): Mulesoft (4.3) ETL: Apache Nifi 1.23 y lambdas Intercambio de ficheros: Apache Nifi 1.23
Gestor de Contenidos	Adobe Experience Manager 6.5.20 o superior
Servicios nativos AWS	SQS, SNS, Eventbridge, Step Functions, Lambda, Kinesis, Data firehose, IoT Core, DMS, Glue, Sagemaker
Servicios nativos Azure	Webapp, API Management, OpenAI

9. On premises

Elemento	Versiones
Virtualizadores	IBM Power 8 VMware (versión 5.5 o superior).
Sistemas Operativos	Red Hat Enterprise Linux 8 o superior (plataforma de 64 bits) Windows 2019 R2 o superior (plataforma de 64 bits) IBM AIX 7.3 (plataforma IBM Power) Amazon Linux 2.0 o superior

Gestor de Base de Datos	Oracle 21C PostgreSQL 16 SQLServer 2019
Gestor Documental	Documentum 2023.4
Gestor de Contenidos	Adobe Experience Manager 6.5.0 o superior
Lenguajes de programación corporativos	OpenJDK 11 o superior para arquitectura basadas en Linux. Javascript/Typescript para la para los frontales en ReactJS. IBM SDK 7 o superior para arquitecturas basadas en AIX. .NET v4.8 para arquitectura basadas en Windows.
Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux. IBM HTTP Server 8.5.5 para arquitecturas basadas en AIX. IIS 10
Servidores de aplicaciones	JBossEAP 7.3 para arquitecturas basadas en Linux. WebSphere Application Server Network Deployment 8.5.5 para arquitecturas basadas en AIX. Internet Information Server 10 para arquitecturas basadas en Windows. Tomcat 10 o superior para arquitecturas basadas en Linux.
Integración	Colas: IBM MQ 12 ETL: ACE112 Intercambio ficheros: Spazio 2.9

Tanto el software listado anteriormente como su licenciamiento será proporcionado por Correos, salvo en el caso de *appliances*. En el caso de que el producto requiriera de un software/hardware específico no contemplado en las tablas anteriores, este software/hardware debe ser disponibilizado y asumido su coste por parte del adjudicatario (por ejemplo, *Windows Cal*). La administración y explotación de dicho software recaerá en el adjudicatario del presente expediente.

10. Requisitos de integración

- El producto debe facilitar la integración con servicios y aplicaciones de Correos, mediante los mecanismos de integración estandarizados en Correos, descritos a continuación:
 - a. API (REST, y SOAP)
 - b. Mensajería asíncrona mediante colas MQ
 - c. Intercambio de ficheros con grandes volúmenes de datos (SFTP)
- Estas integraciones podrán ser en ambos sentidos:
 - a. La solución debe exponer mecanismos de integración para que puedan ser invocados por los sistemas de Correos. Por ejemplo, exponer una API.
 - b. La solución debe ser capaz de invocar a los sistemas de Correos para obtener información o ejecutar procesos. Por ejemplo, invocar a un servicio REST.
- El producto comercial debe integrarse con los proveedores de identidad corporativos, delegando en ellos la autenticación de los usuarios que trabajen con el producto. Esta autenticación podrá realizarse mediante los siguientes mecanismos:
 - a. Oauth 2: Quedando prohibido usar el *implicit grant type*.
 - b. Servicios LDAP que ofrece *Microsoft Active Directory* usado en Correos
- La infraestructura de Correos se divide actualmente en tres entornos:
 - a. Entorno de desarrollo Integrado: Utilizado para las pruebas de Aceptación de Usuario, validación de funcionalidad del código, y pruebas integradas con otras aplicaciones. También como entorno para acciones de formación. Por tanto, es importante recalcar que este entorno no está destinado a la construcción de software. El software debe ser construido en las instalaciones del cliente, y ser desplegado en Correos cuando sea el momento de validarlo e integrarlo.
 - b. Entorno de preproducción: Utilizado para el análisis, verificación y validación del proceso de paso a producción.
 - c. Entorno de producción: Entorno productivo, de acceso por parte de los Usuarios de Correos para el desarrollo de su trabajo diario y por parte de empresas externas.

La solución se instalará y configurará al menos en los entornos de Producción y Preproducción, pero si en el marco de este pliego se realizaran desarrollos a medida para Correos, será obligatorio la instalación y configuración de la solución además en el entorno de Desarrollo Integrado.

Cualquier entorno adicional a los mencionados anteriormente, deberá ser provisto por el adjudicatario en caso de considerarlo necesario, y en todo caso, con el consentimiento de Correos.

11. Requisitos de mantenimiento, operación y monitorización de los sistemas

- El producto debe poder integrarse con las herramientas de gestión operativas. Debe proporcionar mecanismos (como API o webhook) para consultar métricas clave de rendimiento (al menos CPU, memoria, tiempo de respuesta, disponibilidad), así como integración nativa con protocolos como SNMP, y debe ser capaz de integrarse con herramientas como Prometheus o Grafana.
- Correos dispondrá de acceso remoto al software que permita la gestión y monitorización del sistema. Entre las herramientas, que utiliza actualmente Correos en este ámbito, destacan:
 - a. BMC Patrol: sistema de monitorización que permiten gestionar las posibles incidencias que se produzcan en las infraestructuras instaladas para proporcionar servicio a Correos.
 - b. BMC Control-M: sistema para la planificación y ejecución de procesos, quedando prohibida la utilización de cron.
 - c. Tivoli Storage Manager (TSM): Este software gestiona toda la operativa de copias de seguridad de los servidores corporativos con arquitectura abierta existentes en los CPD corporativos.

Se proporcionará documentación completa y actualizada para facilitar la integración y el monitoreo.

- En el caso de que la solución propuesta por el adjudicatario suponga agregar, modificar, sustituir o realizar cualquier acción adicional sobre la plataforma existente (ya sea de hardware, software, licenciamiento o cualquier otro tipo), será su responsabilidad realizar todas las tareas oportunas, incluyendo capacitación específica al personal técnico correspondiente, para conseguir el correcto funcionamiento del entorno final requerido, sin que esto suponga ningún coste añadido para Correos, sin pérdida de la continuidad del servicio que se presta, y sin perjuicio de los plazos establecidos en el presente Pliego.

12. Requisitos sobre acuerdos a nivel de servicio

El producto debe estar soportada por el fabricante de la misma. El adjudicatario deberá aportar certificación al respecto que lo acredite.

Roadmap de producto: el fabricante debe ofrecer un compromiso de evolución del producto que asegure la continuidad del mismo como mínimo durante un plazo de cinco años, o especificar en el caso de no cumplimiento.

Consolidación de producto: la fecha de lanzamiento de la primera versión del producto ofertado deberá ser como mínimo tres años anterior a la fecha de presentación de la oferta por parte del licitador o especificar en el caso de no cumplimiento.

Última versión liberada: la fecha de última versión/actualización del producto ofertado deberá ser como máximo seis meses anteriores a la fecha de presentación de la oferta por parte del licitador.

Perdurabilidad de las versiones y versión más antigua operativa soportada: la fecha de la versión operativa más antigua que es soportada por el fabricante debe ser como mínimo DIECIOCHO (18) MESES anterior a la fecha de presentación de la oferta por parte del licitador, De manera que Correos pueda evaluar el impacto que supondría la no continuidad del producto sobre la futura evolución de sus sistemas, tanto a nivel de sistema operativo, base de datos, software de base en general, como de middleware, aplicación, o cualquier otro que pueda imponer dependencias con respecto al servicio a contratar.

El adjudicatario debe informar a Correos en su oferta de los modos de licenciamiento y su coste asociado, así como aquellos aspectos que puedan ser determinantes en el coste del producto (por ejemplo, tramos de número de usuarios o el número de procesadores necesarios en el servicio a Correos). Deben también especificarse requerimientos de licenciamiento específicos en un Entorno Virtualizado La propuesta del adjudicatario debe estar desglosada por tipo de entorno (productivo o no productivo).

El adjudicatario debe proveer las licencias correspondientes para prestar de forma completa el servicio demandado por Correos. En su oferta debe proponer una solución que garantice la correcta custodia, uso y aprovechamiento de las licencias facilitadas. Una vez implantada la solución, Correos revisará estas condiciones para asegurar que se estén aprovechando correctamente las licencias ofertadas.

Correos podrá definir periodos de congelación de cambios y actualizaciones en el sistema, es decir, periodos en los que no debe alterarse la implementación ni la configuración del servicio por parte del fabricante o del adjudicatario, para minimizar posibles impactos en el negocio de Correos.

Desarrollo a medida

La solución propuesta por el adjudicatario consiste en un sistema construido expresamente para Correos. Este desarrollo software ha de hacerse bajo los estándares tecnológicos de Correos (arquitecturas de referencia), y debe desplegarse en las infraestructuras de Correos (on premises o cloud) a través de los mecanismos de integración continua disponibles en Correos, y su ecosistema de herramientas.

13. Requisitos de arquitectura

El desarrollo de la solución debe ajustarse a alguna de las arquitecturas de referencia de Correos, y utilizar las piezas de su pila tecnológica para ser construida. Si la implementación necesitara de una nueva arquitectura de referencia (o una nueva pieza tecnológica) que no exista en Correos y que no se disponga de solución alternativa, esta nueva arquitectura deberá ser consensuada, industrializada y estandarizada en un trabajo conjunto con el equipo de arquitectura de Correos. En este caso, el adjudicatario

debe facilitar arquitectos que colaboren con el equipo de arquitectos de Correos para disponibilizar la solución, sin alterar las planificaciones del proyecto:

Arquitectura de Referencia	Infraestructura	Pila tecnológica
Microservicios	cloud	Openshift CP SpringBoot Python ReactJs Mulesoft API Amazon Aurora PostgreSQL
B2B	cloud/on premises	IBM App Connect IBM Integration BUS Spazio Apache NIFI
Fast Data	cloud native	AWS Lambda AWS Kinesis AWS S3 AWS DynamoDB MongoDB
Sensorización	cloud native	AWS EMR AWS lambda AWS Kinesis AWS IoT
Experiencia Digital	on premises	Adobe EM ReactJS Storybook
Lake House	cloud native	AWS Glue AWS DMS AWS s3 SnowFlake
Arquitectura para IA	cloud	AWS Sagemaker AWS Bedrock Azure OpenAI Azure AI Services
Tradicional	cloud/on premises	Spring Jboss Websphere AS Oracle

La construcción del software debe ceñirse al ciclo de vida del software definido en Correos, cumpliendo con los procesos de ingeniería del software definidos por la metodología que Correos establezca durante las fases de análisis, diseño, implementación y pruebas, generando los entregables y documentación que se estipule necesaria.

La infraestructura de Correos se divide actualmente en tres entornos:

- Entorno de desarrollo Integrado: Utilizado para las pruebas de Aceptación de Usuario, validación de funcionalidad del código, y pruebas integradas con otras aplicaciones. También como entorno para acciones de formación. Por tanto, es importante recalcar que este entorno no está destinado a la construcción de software. El software debe ser construido en las instalaciones del cliente, y ser desplegado en Correos cuando sea el momento de validarlo e integrarlo.
- Entorno de preproducción: Utilizado para el análisis, verificación y validación del proceso de paso a producción.
- Entorno de producción: Entorno productivo, de acceso por parte de los Usuarios de Correos para el desarrollo de su trabajo diario y por parte de empresas externas.

La solución se instalará y configurará al menos en los entornos de Producción y Preproducción, pero si en el marco de este pliego se realizaran desarrollos a medida para Correos, será obligatorio la instalación y configuración de la solución además en el entorno de Desarrollo Integrado.

Cualquier entorno adicional a los mencionados anteriormente, deberá ser provisto por el adjudicatario en caso de considerarlo necesario, y en todo caso, con el consentimiento de Correos.

La construcción de software debe ser realizada utilizando los arquetipos de desarrollo que provee Correos, a través de las herramientas de integración continua. Estos arquetipos facilitan la construcción, implementando algunos aspectos comunes a las aplicaciones, y permitiendo la integración y despliegue continuo en las plataformas de Correos.

El adjudicatario de la solución debe responsabilizarse de realizar las tareas que le sean requeridas de cara a que su aplicación cumpla con los requerimientos de obsolescencia establecidos en Correos.

La aplicación construida debe albergar la posibilidad de integración con servicios y aplicaciones de Correos, mediante los mecanismos de integración estandarizados en Correos, descritos a continuación:

- API (REST y SOAP)
- Mensajería asíncrona mediante colas MQ
- Intercambio de ficheros con grandes volúmenes de datos (SFTP, FTPS).

Los desarrollos que se realicen no cumpliendo estos requisitos, con otras pilas tecnológicas o sin seguir las buenas prácticas de desarrollo en Correos, tendrán que ser adaptados por el adjudicatario y adecuados a la arquitectura de Correos, antes de ser desplegados en las plataformas corporativas.

Requisitos de ICDC. El proveedor debe utilizar el sistema de control de versiones basado en Git para la gestión del ciclo de vida del código fuente y los artefactos, garantizando:

- Repositorio Centralizado. - El código deberá alojarse en el repositorio Git corporativo designado por Correos.
- Estrategia de Branching. - Se deberá seguir una estrategia de ramas adecuada y alineada a la utilizada en Correos (GitFlow)

Debe colaborar con los equipos internos de Correos para adaptar, en caso de existir, o crear, en caso de no existir, un circuito de integración y entrega continua (CI/CD) que sea compatible con la infraestructura y los procesos de Correos, asegurando:

- Despliegues Automatizados
 - a. Se deben definir pipelines para entornos de desarrollo, pruebas y producción con controles de calidad.
 - b. Los despliegues en producción deberán planificarse en el Comité de Implantaciones y aprobarse la fecha de implantación por parte de Correos.
 - c. Los despliegues se podrán hacer:
 - I. Sin interrupción.
 - II. Gradualmente activando de manera controlada una funcionalidad para ciertos usuarios.
 - d. Se deberán establecer mecanismos de rollback automatizados para revertir cambios en caso de fallos de manera:
 - I. Completa.
 - II. O desactivando funciones problemáticas en producción sin necesidad de hacer un despliegue nuevo.
 - e. Gestión de configuración y secretos:
 - I. La configuración debe manejarse a través de archivos versionados y parámetros de entorno.
 - II. No se deben almacenar credenciales en el código fuente; se deberá usar el sistema de gestión de secretos que Correos determine.
 - III. Se debe garantizar la trazabilidad de los cambios en la configuración.
 - f. Control de calidad. - El código deberá pasar las reglas de certificación de código a través de la herramienta corporativa, Kiuwan.

- g. Automatización de Builds y Tests:
 - I. La compilación del código deberá ejecutarse automáticamente en cada commit a ramas principales o de integración.
 - II. Se deberán ejecutar pruebas unitarias, de integración y funcionales como parte del pipeline.
 - III. Se deberán hacer pruebas de performance y escalabilidad, con cargas variables.
- h. Seguridad:
 - I. El código deberá pasar las reglas de seguridad estática (SAST) para detectar errores de seguridad y bloquear la promoción de código con vulnerabilidades críticas.
 - II. En los casos que aplique, las aplicaciones deberán ser sometidas a pruebas de seguridad en entornos controlados antes de su despliegue en producción mediante el análisis dinámico de seguridad (DAST) para detectar vulnerabilidades en la aplicación y su configuración.
 - III. Se deberán integrar herramientas de análisis de seguridad en el pipeline (SAST/DAST), asegurando la generación de informes con trazabilidad de vulnerabilidades y acciones correctivas.
 - IV. Se deberá validar configuraciones de seguridad en la nube a través de CSPM (Cloud Security Posture Management)
 - V. El proveedor será responsable de corregir cualquier vulnerabilidad detectada antes de la aprobación del despliegue en producción.
- i. Monitorización y observabilidad
 - I. Los pipelines deben incluir mecanismos de logging y monitorización de ejecución.
 - II. En caso de fallo, se deberá generar alertas en tiempo real y mantener un registro accesible con los eventos relevantes.
 - III. Se debe realizar, en la medida de lo posible, la integración con las herramientas de monitorización de Correos que permitan detectar anomalías en la ejecución o rendimiento anómalo en la ejecución de las aplicaciones.
 - IV. En caso de que la integración con las herramientas de monitorización de Correos no sea posible, el proveedor deberá proporcionar e integrar alguna herramienta APM (Application Performance Monitoring) compatible que ofrezca visibilidad y seguimiento detallado del rendimiento de las aplicaciones y la infraestructura.
- j. Trazabilidad y Auditoría

- I. Los despliegues deben generar registros accesibles con información de quién ejecutó qué cambios y cuándo.
- II. Se deberá asegurar el almacenamiento de logs de auditoría con retención mínima conforme a las normativas de Correos.

Anexo XX – Requerimientos Ciberseguridad

1. Normativa y conformidad.

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

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

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

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

2. Control de Acceso y SSO.

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

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

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

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

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

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

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

3. Respaldo y recuperación.

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

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

4. Comunicaciones.

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

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

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

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

El acceso de forma remota a los recursos corporativos a través de una red pública, sea realizado con la finalidad de realizar un soporte o por teletrabajo, deberá cumplir los

requerimientos sobre autenticación, cifrado, filtrado de redes y puestos de usuario que establezca la normativa de seguridad de Correos, así como cualquier otro requerimiento que pudiera establecer la Subdirección de Ciberseguridad.

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

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

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

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

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

5. Integridad y confidencialidad.

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

- Para datos en tránsito se debe utilizar la capa SSL/TLS, en su versión 1.2 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 deberá usar la herramienta corporativa S3C para el cifrado en reposo.

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

6. Tratamiento de 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.

7. Desarrollo Seguro

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

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

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

Adicionalmente, el adjudicatario debe restringir el acceso al código fuente del programa. El soporte de la aplicación y las actualizaciones de la aplicación debe garantizar la compatibilidad con la versión de los sistemas usados en Correos.

8. Desarrollo de APIs

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

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

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

9. Sistemas operativos y software base

Se debe conocer las versiones del sistema operativo y del software de la aplicación que va a estar instalado. El software de la aplicación debe estar actualizado con los últimos parches de seguridad recomendados por el suministrador, por lo que debe existir un procedimiento de actualización. Dicho procedimiento debe ser remitido a Correos y acordar el tiempo máximo de actualización entre la publicación de un parche de seguridad y la puesta en producción, en función de la criticidad del mismo.

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.

10. Eventos de auditoría.

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

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

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

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

- Identificador de la aplicación.
- Identificador del usuario (usuario del login, sea o no del dominio).
- Fecha y hora en la que se generó el evento.
- Tipo de acción realizada (modificación, consulta, login..)
- Objeto o datos sobre el que se realiza la acción (acceso a.., ejecución de.., modificación de.., lectura de.., borrado de.., etc.).
- Resultado de la acción (éxito / fallo).
- Identificación del terminal desde el que se ha realizado la acción (dirección IP de origen, MAC, nombre DNS/NetBIOS ..).

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

- Registro de accesos

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

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

11. Respuesta ante incidentes

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

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

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

12. Auditabilidad

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

Correos podrá auditar, por sí misma o a través de un tercero, con el único requisito de preavisar con una antelación de un mes y, de forma presencial o en remoto, todas aquellas medidas y controles que considere necesarios para verificar la seguridad de la información. Además, Correos podrá exigir al proveedor del servicio afectado la aportación de ciertas evidencias de cumplimiento o, en su defecto, la realización una auditoría interna cuyo informe deberá ser firmado por una persona autorizada y con poder de representación de la empresa prestadora del servicio.

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

13. Formación y concienciación

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

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

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

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

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

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

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

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).

16. Uso de Tecnología IA

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.

Anexo XXI. Cláusula sobre el uso de IA en contratos con Correos.

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 subencargados 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.