PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

ÍNDICE.

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

Correos:

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

Correos Express:

Entidad contratante	Correos Express Paquetería Urgente, S.A., S.M.E.
Órgano de contratación	Comité de Inversiones
Dirección/Subdirección gestora de la necesidad UGC	Dirección de Tecnología y Sistemas. Área de Ciberseguridad
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 Sistemas. Área de Ciberseguridad Responsable: Ermengol Sansa Lago
	Datos de contacto: ciberseguridad@correosexpress.com

Los beneficiarios de este expediente serán la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. (en adelante, Correos) y Correos Express Paquetería Urgente, S.A., S.M.E. (en adelante, Correos Express). Correos firmará un contrato por el 60% del importe de adjudicación y Correos Express otro contrato por el 40% de dicho importe.

A los efectos previstos en el artículo 89 del RDL 3/2020, Correos será la entidad contratante y la responsable de las actuaciones necesarias en lo referente a las actuaciones de preparación y adjudicación del procedimiento de licitación.

Sin perjuicio de lo anterior, cada una de las empresas del Grupo Correos anteriormente mencionadas firmará su propio contrato, gestionará sus propias facturas y la aplicación de penalidades en el caso de que tuviesen lugar dentro del ámbito de su propio contrato.

2. Objeto del contrato

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

Descripción	Contratación del soporte y mantenimiento hardware, así como de las licencias del agente de transferencia de mensajes o MTA (Mail Transfer Agent por sus siglas en inglés) implantado en los CPD para la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. y Correos Express Paquetería Urgente, S.A., S.M.E. (en adelante, Grupo Correos): equipos Cisco ESA C395 y Reporter (Cisco SMA). El hardware requerido ya fue adquirido en contratos anteriores, por lo que este expediente se circunscribe a la provisión de licencias/derechos de uso y al mantenimiento asociado, en el periodo de vigencia del contrato.
Código CPV	Principal: 48730000-4 (Paquetes de software de seguridad). 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 previsto en el artículo 52.3.b) del Real Decreto-ley 3/2020, de 4 de febrero, se justifica la no división en lotes del presente contrato al concurrir razones técnicas que hacen que la ejecución independiente de las prestaciones comprendidas en su objeto pueda dificultar la correcta ejecución del mismo y comprometer la necesaria coordinación de las distintas actuaciones que integran la solución contratada. El objeto del contrato comprende la contratación del soporte y mantenimiento hardware, así como de las licencias y derechos de uso asociados al agente de transferencia de mensajes (MTA) implantado en los centros de procesamiento de datos (CPDs), integrado por los equipos Cisco Email Security Appliance (ESA C395) y la plataforma Cisco Security Management Appliance (SMA o Reporter). Aunque el hardware objeto de mantenimiento fue adquirido en expedientes anteriores, la continuidad operativa de la solución depende de la prestación conjunta e integrada de los servicios de soporte, mantenimiento, actualización y licenciamiento asociados a dicha infraestructura compartida por Correos y CEX. Las licencias de los equipos Cisco ESA y SMA, las actualizaciones de software, el acceso al soporte especializado del fabricante y la cobertura de mantenimiento hardware constituyen elementos

	estrechamente vinculados e indivisibles desde un punto de vista técnico y funcional. La eventual división del contrato en lotes diferenciados, separando las licencias y derechos de uso de los servicios de soporte y mantenimiento, o atribuyendo dichas prestaciones a distintos adjudicatarios, obligaría a coordinar sobre una misma plataforma tecnológica a varios proveedores, aumentando la complejidad de gestión y dificultando la adecuada trazabilidad de incidencias, actualizaciones, parches de seguridad y sustituciones de equipamiento. Asimismo, dicha fragmentación podría generar discrepancias sobre la atribución de responsabilidades ante eventuales incidencias, degradaciones del servicio o problemas de interoperabilidad entre los distintos componentes de la solución. Debe tenerse en cuenta que los equipos Cisco ESA constituyen una infraestructura crítica para la gestión y protección del tráfico de correo electrónico corporativo del Grupo Correos, mientras que la plataforma Cisco SMA centraliza su administración, monitorización, generación de informes y gestión operativa. En consecuencia, ambas tecnologías conforman una única solución de seguridad y gestión del correo electrónico cuya explotación requiere una actuación coordinada y homogénea sobre todos sus componentes. Por otra parte, el soporte y mantenimiento de la plataforma exige una coordinación permanente entre las actuaciones relacionadas con el licenciamiento, las actualizaciones de software, la resolución de incidencias, la sustitución de componentes hardware si fuera necesaria y la interlocución con el fabricante. La intervención de una posible pluralidad de contratistas no solo dificultaría dicha coordinación, sino que además, incrementaría los tiempos de resolución de incidencias y afectaría a la disponibilidad y continuidad de un servicio esencial para la actividad del Grupo Correos. Adicionalmente, las necesidades de Correos y de CEX. quedan cubiertas mediante una única solución tecnológica integrada, por lo que la eventual división en lotes no aportaría ventajas funcionales ni una mayor eficiencia en la contratación, pudiendo incluso generar duplicidades de gestión y costes adicionales derivados de la existencia de múltiples interlocutores y procesos de coordinación. En consecuencia, la contratación mediante lote único garantiza la coherencia técnica de la solución, la continuidad del servicio, la adecuada asignación de responsabilidades, una gestión eficiente de las incidencias y problemas y un control operativo del entorno tecnológico, evitando los riesgos técnicos y los costes adicionales

	que podrían derivarse de una ejecución fragmentada del contrato. Los beneficiarios del contrato serán Correos y Correos Express. No obstante, a los efectos previstos en el artículo 89 del RDL 3/2020, Correos será la entidad contratante y la responsable de las actuaciones necesarias en lo referente a las actuaciones de preparación y adjudicación del procedimiento de licitación. Correos firmará un contrato por el 60% del importe de adjudicación y Correos Express otro contrato por el 40% de dicho importe. Correos y CEX disponen de infraestructura tecnológica común destinada a la prestación de los servicios de mensajería electrónica y seguridad asociada, basada en una plataforma corporativa compartida que da servicio simultáneamente a ambas sociedades en su ámbito de utilización. Dentro de esta infraestructura común se integran los Agentes de Transferencia de Mensajes (MTA) y las capacidades avanzadas de protección, filtrado, inspección y seguridad del correo electrónico proporcionadas mediante las licencias Cisco. Estas funcionalidades constituyen un servicio centralizado que protege y gestiona el tráfico de correo electrónico del conjunto de las empresas del grupo, independientemente de la sociedad concreta desde la que se origine o reciba cada comunicación. Las licencias objeto de la contratación no responden a un modelo de licenciamiento individualizado por usuario, puesto de trabajo o dispositivo perteneciente a cada sociedad. Por el contrario, se trata de licencias asociadas al funcionamiento y capacidad de una infraestructura tecnológica compartida, dimensionada para atender de forma conjunta las necesidades operativas de ambas entidades del Grupo Correos. Su finalidad es habilitar las capacidades de la plataforma corporativa de correo y seguridad, permitiendo que ambas puedan utilizar simultáneamente los servicios prestados por dicha infraestructura. Dado que el licenciamiento se aplica sobre una plataforma compartida y no sobre elementos individuales pertenecientes a cada sociedad, resulta técnicamente inviable establecer una distribución exacta del número de licencias entre las distintas empresas del grupo. La contratación se realiza para garantizar la disponibilidad global de las capacidades de correo electrónico y seguridad requeridas por la infraestructura corporativa común. Por tanto, las licencias

	constituyen un recurso indivisible desde el punto de vista funcional y operativo. Cualquier intento de asignar un número concreto de licencias a cada sociedad tendría un carácter meramente estimativo o artificial, careciendo de base técnica y contractual, ya que el fabricante no define ni gestiona las licencias bajo criterios de reparto entre las empresas del Grupo. La distribución de costes entre Correos y CEX se realiza mediante criterios objetivos de utilización efectiva de la infraestructura, siendo éste el mecanismo adecuado para reflejar el beneficio obtenido por cada entidad sin que ello implique una asignación individual de licencias. Sin perjuicio de lo anterior, cada una de las empresas del Grupo Correos anteriormente mencionadas firmará su propio contrato, gestionará sus propias facturas y la aplicación de penalidades en el caso de que tuviesen lugar dentro del ámbito de su propio contrato
¿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	22	☐ días ☒ meses ☐ años	☐ día siguiente a la formalización del contrato. ☐ día siguiente a la comunicación de inicio del contrato por la entidad contratante. ☒ desde la fecha de inicio que figure en el contrato.
Prorrogable	☒ NO ☐ SI	Nº de prórrogas: Duración máxima de cada prórroga (en meses):	

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Grupo Correos:

Valor estimado del contrato	464.546,13 euros	Cuatrocientos sesenta y cuatro mil quinientos cuarenta y seis euros con trece céntimos, conforme al método de cálculo especificado en Anexo III	
Presupuesto base de licitación	562.100,82 euros	IVA/impuesto equivalente	97.554,69 euros
Anualidades (IVA o impuesto indirecto equivalente incluido)	2027	2028	Total
	304.628,39 euros	257.472,43 euros	562.100,82 euros

Correos:

Valor estimado del contrato	278.727,68 euros	Doscientos setenta y ocho mil setecientos veintisiete euros con sesenta y ocho céntimos, conforme al método de cálculo especificado en Anexo III	
Presupuesto base de licitación	337.260,49 euros	IVA/impuesto equivalente	58.532,81 euros
Anualidades (IVA o impuesto indirecto equivalente incluido)	2027	2028	Total
	182.777,03 euros	154.483,46 euros	337.260,49 euros

Correos Express:

Valor estimado del contrato	185.818,45 euros	Ciento ochenta y cinco mil ochocientos dieciocho euros con cuarenta y cinco céntimos, conforme al método de cálculo especificado en Anexo III	
Presupuesto base de licitación	224.840,33 euros	IVA/impuesto equivalente	39.021,88 euros
Anualidades (IVA o impuesto indirecto equivalente incluido)	2027	2028	Total
	121.851,36 euros	102.988,97 euros	224.840,33 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.

<table>
<tr><td>Solvencia económica o financiera</td><td>☒ Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, de al menos 253.338,79 euros.
En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote
<table>
<tr><td></td><td>LOTE 1</td><td>LOTE 2</td></tr>
<tr><td>Porcentaje/Cifra volumen anual negocio.</td><td></td><td></td></tr>
</table>
Sobre la forma de acreditar estos requisitos, ver Anexo IV
☐ Responsabilidad solidaria de la ejecución del contrato de las entidades que completen la solvencia económica y financiera del licitador</td></tr>
<tr><td>Solvencia técnica o profesional</td><td>☒ 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. (178.322,87 euros)
☐ Disponibilidad de los siguientes perfiles relativos al personal:
☐ Cumplimiento de las medidas de aseguramiento de la calidad durante la ejecución del contrato que a continuación se relacionan:
☐ Acreditación del cumplimiento de las siguientes medidas de gestión medioambiental:
☐ Disponibilidad de la siguiente maquinaria, material y equipo técnico:
☐ Otros
En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote
<table>
<tr><td></td><td>LOTE 1</td><td>LOTE 2</td></tr>
<tr><td>Importe servicios</td><td></td><td></td></tr>
</table>
Sobre la forma de acreditar estos requisitos, ver Anexo IV</td></tr>
<tr><td>Habilitación profesional: Esquema Nacional de Seguridad</td><td>Para prestar los servicios objeto de este contrato, el licitador realizará alguna de las siguientes acciones:
o Accederá a datos de clientes o empleados de Correos.
o Proveerá de aplicaciones, Sistemas de información y/o herramientas a Correos.
o Almacenará o custodiará información de clientes o empleados de Correos.
☒ SI
☐ NO
En caso afirmativo, para ser adjudicatario del contrato, el licitador deberá prestar los servicios conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), y aportar certificación</td></tr>
</table>

	acreditativa para la categoría BÁSICA. Para la acreditación, se presentará copia del Certificado de Conformidad, o en su caso, Declaración de Conformidad con el ENS, en la categoría indicada y con el alcance que abarque(n) al menos el/los sistemas(s) de información que soporte(n) los servicios prestados. La criticidad de este expediente implica que el licitador, así como otros servicios de terceros que se incluyan en la oferta, se tienen que prestar y acreditar, para la categoría: ☐ MEDIA ☐ ALTA Para la acreditación, se presentará copia de Certificado de Conformidad en la categoría indicada y con el alcance que abarque(n) al menos el/los sistemas(s) de información que soporte(n) los servicios prestados.
Adscripción de medios	☐ Sí. Medios a adscribir ☒ No.

Se exime a los licitadores de la obligatoriedad de presentar los medios que acrediten su solvencia en el caso de que presenten su inscripción en el registro oficial de licitadores y empresas clasificadas del Estado.

En dicha inscripción en el registro oficial de licitadores y empresas clasificadas del Estado deben constar todos los datos relativos a su capacidad, solvencia económica- financiera y técnica o profesional, representación y habilitaciones exigidos en este pliego, haciendo constar, además, que no se hallan incursos en prohibición para contratar, comprometiéndose a poner a disposición del órgano de contratación, en cualquier momento, cuando así fuese requerido, la documentación justificativa de las indicadas circunstancias.

6. Licitación del contrato

6.1. Comunicaciones y notificaciones electrónicas

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

6.2. Resolución de consultas relacionadas con la licitación

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

Los licitadores, podrán subir sus preguntas a la plataforma de contratación de Correos hasta seis 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".

El procedimiento abierto es uno de los procedimientos ordinarios de adjudicación de los contratos de las administraciones públicas.

La intención es dar a todos los licitadores un tratamiento igualitario, ajustado a los principios de no discriminación, de reconocimiento mutuo, de proporcionalidad, de igualdad de trato, así como al principio de transparencia y de libre competencia (art. 27 R.D.L. 3/2020).

Este procedimiento se considera el más adecuado para garantizar la máxima concurrencia competitiva, permitiendo que cualquier operador económico interesado que cumpla con los requisitos de estipulados en el Pliego de Condiciones Técnicas y

Particulares presente su mejor oferta en igualdad de condiciones, siendo por tanto el procedimiento que mejor se ajusta a los principios que rigen la contratación del sector público.

El objeto del contrato consiste en el suministro de licencias/derechos de uso y soporte oficial para los dispositivos ESA-C395 y SMA Reporter ya implantados. Las características técnicas, operativas y de prestación del servicio están plenamente definidas por el Grupo Correos, 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, la adjudicación se efectuará utilizando como único criterio de adjudicación el precio, aplicado un planteamiento que atienda a la mejor relación coste-eficacia.

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

☐ Pluralidad de Criterios de Adjudicación: MEJOR RELACIÓN CALIDAD-PRECIO.

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

En este caso, la adjudicación se efectuará utilizando como único criterio de adjudicación la mejor relación coste-eficacia, aplicado un planteamiento que atiende al precio, dado que:

- El objeto contractual está perfectamente definido y estandarizado. Las prestaciones objeto del contrato se encuentran completamente determinadas desde el punto de vista técnico, funcional y de alcance. No se solicita el diseño, desarrollo, implantación, evolución ni mejora de la solución tecnológica existente, sino exclusivamente la continuidad de los servicios de soporte, mantenimiento y licenciamiento asociados a una infraestructura previamente adquirida e implantada. Por tanto, las características del servicio están plenamente definidas y no admiten modificaciones.
- No hay margen para aportar valor técnico diferencial. Dado que los equipos y la tecnología objeto de soporte son productos específicos del fabricante Cisco ya desplegados en la infraestructura corporativa, las prestaciones requeridas están definidas por los propios niveles de servicio, condiciones de mantenimiento y licenciamiento establecidos por el fabricante. En consecuencia, los licitadores no disponen de capacidad real para ofrecer soluciones técnicas alternativas o mejoras funcionales que aporten una calidad superior susceptible de valoración objetiva. Tampoco se admiten variantes en los plazos de entrega ni en la forma de prestación del servicio.
- Cualquier licitador deberá proporcionar el mismo servicio (homogeneidad de las prestaciones): la renovación de los derechos de uso y el acceso a los servicios oficiales de soporte y mantenimiento exigidos para garantizar la continuidad operativa de la plataforma existente. Por tanto, una vez acreditado el

cumplimiento íntegro de las prescripciones técnicas establecidas en el pliego, las ofertas resultan equivalentes desde el punto de vista cualitativo. El alcance funcional se circunscribe a la provisión de licencias/derechos de uso y al soporte asociado, sin posibilidad de introducir mejoras técnicas.

- Una vez garantizado el cumplimiento íntegro de todos los requisitos técnicos exigidos en el pliego, la variable que permite identificar la oferta más ventajosa para el interés público es el menor coste económico para el Grupo Correos. La utilización del precio como único criterio favorece la objetividad, transparencia y simplicidad del procedimiento de adjudicación, asegurando simultáneamente el uso eficiente de los fondos públicos.

Por todo ello, al tratarse de prestaciones homogéneas, estandarizadas, plenamente definidas y sin posibilidad de introducir mejoras técnicas relevantes o elementos cualitativos diferenciales, se considera debidamente justificada la adjudicación del contrato mediante un único criterio de valoración basado en el precio, al ser el mecanismo que mejor permite identificar la oferta con la mejor relación coste-eficacia.

Tipología	Criterio	Ponderación
Criterios evaluables mediante formula o automáticamente	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 A: 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.

g) Declaración responsable en materia de protección de datos (según anexo XXI).

6.7.2. Sobre C: 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 C" en archivo ejecutable con formato *.pdf.

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.

Los importes reflejados deberán indicarse solo con dos decimales y truncados al segundo decimal. No se admite el redondeo de decimales.

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.

Los importes sin impuestos de cada uno de los conceptos en los que se desglosa la oferta, así como el importe total sin impuestos, no puede superar los importes sin

impuestos recogidos en el Anexo III. La superación de dichos importes supondrá la exclusión de la oferta del proceso de la licitación.

Así mismo, deberá desglosarse la oferta total por cada una de las empresas del Grupo Correos que participan en este expediente.

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.

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

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

7.2. Ofertas anormalmente bajas

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

☒	Se considerará que una proposición económica es anormalmente baja cuando incluya un porcentaje de baja que, respecto de la media aritmética de los porcentajes de baja de todas las ofertas admitidas, o del presupuesto de licitación en caso de licitador único, exceda de diez unidades porcentuales.
☐	Otra..

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

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

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

7.3. Documentación a presentar por el propuesto como adjudicatario

Al licitador que haya presentado la mejor oferta se le requerirá para que en el plazo de 10 días hábiles a contar desde el siguiente a aquel en el que haya recibido el requerimiento, presente la siguiente documentación original o copias compulsadas:

☒	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 días hábiles.

De no cumplimentarse adecuadamente el requerimiento en el plazo señalado por causas imputables al contratista, se entenderá que el licitador ha retirado su oferta. En

tal supuesto, se procederá a recabar la misma documentación al licitador siguiente, por el orden en que hayan quedado clasificadas las ofertas.

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

7.4. Adjudicación del contrato

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

7.5. Perfección del contrato

El contrato se perfeccionará con su formalización por escrito, que no podrá realizarse hasta transcurridos quince días hábiles desde que se remita la notificación de la adjudicación al licitador que hubiere realizado la mejor oferta y al resto de licitadores. Transcurrido dicho plazo se requerirá al adjudicatario para que formalice el contrato en plazo no superior a cinco días naturales, a contar desde el siguiente a aquel en que hubiera recibido el requerimiento.

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 indicado, el contrato 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.

7.6. Constitución de garantías.

<table>
<tr><td colspan="3">RÉGIMEN DE GARANTÍAS</td></tr>
<tr><td rowspan="2">Constitución de garantía definitiva</td><td rowspan="2">☒ SI. 5% del importe de adjudicación del contrato o el lote o lotes adjudicados (IVA excluido)</td><td>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.</td></tr>
<tr><td>Además de por la correcta ejecución del contrato, la garantía definitiva responderá de los daños y perjuicios que se ocasionen a la entidad</td></tr>
</table>

			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 al plazo de 10 días hábiles desde que se le notifique la causa determinante de la variación del importe del contrato. De no cumplirse este requisito por causas imputables al contratista en el plazo establecido, la entidad contratante podrá resolver el contrato, con pérdida de la garantía que tuviera constituida el contratista. En el caso de que se impongan penalidades al contratista y deban hacerse efectivas contra la garantía definitiva constituida, el adjudicatario quedará obligado a reponer esta garantía en los diez días hábiles siguientes a que se comunique la ejecución de la garantía inicial.			

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

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

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

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

8. Ejecución del contrato

8.1. Obligaciones del adjudicatario

8.1.1. Obligaciones en materia fiscal, laboral y medioambiental

Serán de cuenta del contratista todos los tributos de cualquier índole que graven las operaciones necesarias para la ejecución del contrato y cualquier otra que resulte de

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

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

Para la ejecución de este contrato:

☒ NO procede subrogación de trabajadores
☐ SI procede la subrogación de trabajadores (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

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

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

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

- Actuar sujeto a las instrucciones que, en cada momento, le indique la entidad contratante y no utilizar los datos con una finalidad distinta a la prestación del Servicio al que se hace referencia en el presente Pliego.
- Adoptar todas aquellas medidas técnicas y organizativas que resulten necesarias para garantizar un nivel de seguridad adecuado, guardar bajo su control y custodia los datos personales suministrados por la entidad contratante y no divulgarlos, transferirlos, o de cualquier otra forma comunicarlos, ni siquiera para su conservación a otras personas.
- No subcontratar ninguna de las prestaciones que formen parte del objeto de este Pliego que comporten el tratamiento de datos personales o realizar Transferencias Internacionales de Datos, salvo previa autorización expresa y otorgada por escrito por parte de la entidad contratante.
- Asistir a la entidad contratante en la realización de los análisis de riesgo, la presentación de consultas previas a la AEPD, en el proceso de notificación de violaciones de seguridad y de respuesta a solicitudes de derechos.
- Mantener secreto y confidencialidad respecto de los datos personales a los que acceda y garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que les informará convenientemente.
- Poner a disposición de la entidad contratante toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como permitir la realización de auditorías con acceso físico directo a sus instalaciones o los subcontratistas autorizados y colaborar activamente en su desarrollo.
- Poner a disposición de la entidad contratante, con carácter previo a la formalización del contrato, una declaración escrita que contenga la información acerca de:
    i. La ubicación de los servidores en los que se almacenarán los datos personales tratados por cuenta de la entidad contratante; y
    ii. Lugar de prestación de servicios objeto la licitación.
- Si fuera necesario subcontratar los servidores o los servicios asociados a los mismos, el adjudicatario reflejará esta circunstancia en su oferta, junto con el nombre completo del subcontratista o, en su defecto, la referencia al perfil empresarial del mismo, definido por referencia a las condiciones de solvencia profesional o técnica del mismo.
- Comunicará a la entidad contratante cualquier cambio que se produzca con respecto a los términos y condiciones en los que accederá y tratará los datos personales por cuenta de la entidad contratante, y especialmente aquellas

relacionadas con la información presentada en la declaración previa recogida en el punto octavo de la presente cláusula.

- En caso de incumplimiento: Responder de los daños y perjuicios que pudiesen ocasionarse y, en especial, de las sanciones que les pudiera imponer la agencia española de protección de datos (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
Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia	Mensual	Documento aportado por la empresa adjudicataria, firmado con la aceptación de la persona responsable del proyecto que refleje el cumplimiento de la normativa de protección de datos vigente

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, y en su caso al subcontratista, el cumplimiento de dichas condiciones, conforme al artículo 202.1 de la ley de contratos del sector público (LCSP).

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, cada una de las entidades contratantes utilizará los siguientes medios de pago:

- Transferencia bancaria. Cada empresa el Grupo 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 (Correos o Correos Express) 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:

Correos:

- 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, como mínimo se proporcionarán los siguientes:

Campo		Facturae 3.2
Expediente		MT270001
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

Campo		Facturae 3.2
Referencia legal		Facturae/Invoices/Invoice/Items/InvoiceLine/AdditionalLineItemInformation

Correos Express:

Las facturas emitidas por el adjudicatario deberán ajustarse a lo establecido en el artículo 6 del Reglamento por el que se regulan las obligaciones de facturación, aprobado por Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

La facturación será mensual conforme se realice la ejecución de la presente contratación y en función de los servicios requeridos. Es decir, se facturará bajo la modalidad de pago por uso, condicionando tales abonos al número prestaciones solicitadas por Correos Express y efectivamente ejecutadas atendiendo a lo indicado en el presente Pliego, no estando obligada Correos Express a consumir la totalidad del importe establecido.

A la recepción de conformidad por parte de Correos Express de los servicios prestados, el adjudicatario emitirá la correspondiente factura cuyo pago se efectuará mediante confirming en el plazo de 60 días naturales.

El pago de cualquier importe del precio no implicará que Correos Express considere cumplidas todas las obligaciones derivadas de la presente contratación.

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 Correos Express que figura en el punto anterior.

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 facturae 3.2.x en cualquiera de sus versiones 3.2, 3.2.1 y 3.2.2) y a través de la plataforma que se le indique (actualmente se utiliza la VAN de Telefónica-Indra (Ecosystems B2B), para la recepción de facturas).
- Como campos específicos de Correos Express, además de los obligatorios en el formato Facturae, como mínimo se proporcionarán los siguientes:

Campo	Facturae 3.2
Referencia del expediente	Facturae/Invoices/Invoice/Items/InvoiceLine/FileReference
(opcional pero recomendable)	Facturae/Invoices/Invoice/Items/InvoiceLine/ReceiverTransactionReference
Número de pedido del receptor	Facturae/Parties/BuyerParty/AdministrativeCentres/AdministrativeCentre/CentreCode

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:

Para Correos:

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

Para Correos Express:

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

Puede consultar más información en la Política de Protección de Datos del Canal Ético para Clientes y Proveedores.

11.2. Información a representantes, trabajadores y personas de contacto

Los datos de carácter personal de las personas de contacto de los licitantes y, en su caso, de sus trabajadores serán tratados por la entidad contratante con la finalidad de gestionar su participación en la presente contratación, y en caso de resultar

adjudicatario del contrato, con la finalidad de gestionar la relación contractual que se formalice entre las partes, siendo la base legitimadora del tratamiento la ejecución del contrato y el cumplimiento de la normativa de aplicación. En este sentido, le informamos que los datos facilitados no se cederán a terceros, salvo obligación legal.

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

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

Para Correos Express:

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

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

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

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

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

12. Régimen jurídico del contrato y reclamaciones contra este pliego

El contrato se regirá, en cuanto a su preparación y adjudicación, por lo dispuesto en el presente Pliego y en 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 regirán por lo previsto en la documentación que revista carácter contractual y por el Derecho Privado.

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

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos.
☒	Aceptación del acuerdo de aceptación.
☒	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, 17 de julio de 2026

EL SUBDIRECTOR DE CIBERSEGURIDAD

Firmado Digitalmente por MAYOR SENDRA, JESUS (FIRMA)
Fecha: 2026.07.17 11:58:37 +02'00'

Fdo.: Jesús Mayor Sendra

VºBº
EL DIRECTOR GENERAL DE CORREOS EXPRESS

Y2830232G ANTONIO MANUEL BORGES (R: A28799120)
Firmado digitalmente por Y2830232G ANTONIO MANUEL BORGES (R: A28799120)
Fecha: 2026.07.22 11:44:21 +02'00'

Fdo.: Antonio Manuel Borges Vaz

VºBº
LA DIRECTORA DE TECNOLOGÍA Y TRANSFORMACIÓN DIGITAL DE CORREOS

Firmado digitalmente por: TARRERO MARTOS, CRISTINA
Fecha: 2026.07.23 16:43:18 +02'00'

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 de las licencias de la MTA y el Reporter de las que es titular, a través de la prórroga del contrato específico número 20 del expediente AI230001, dotando así al Grupo Correos, incluido Correos Express, 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.

Correos dispone de 3 máquinas para dar el servicio de MTA: 2 Cisco ESA C395 (MTA) y un Cisco SMA (Reporter), cuyo ciclo de vida termina en octubre de 2028 (fin de soporte para dichos modelos), y que dispone de las siguientes licencias:

CANTIDAD	REFERENCIA	DESCRIPCIÓN
1	EMAIL-TG-2K	Cisco Threat Grid 2K Files/Day
1	SEC-AUTO-PUI-LIC	Cisco Security
20.000	ESA-ESS-LIC	Cisco Secure Email Essential Inbound Malware Defense and ANYL
20.000	SMA-EMGT-LIC	SMA Centralized Email Management Reporting License
1	SVS-EMAIL-SUP-B	Basic Support for Email Security
2	CON-PSRT-ESAC395K	SNTC-8X5XNBD ESA C395 Email Security Appliance
1	CON-SNT-M690	SMARTNET 8X5XNBD SMA M690 Security Ma

- La licencia "Cisco Secure Email Essential Inbound Malware Defense and ANYL" (ESA-ESS-LIC), compuesta por las siguientes funcionalidades principales:
  - ✓ External Threat Feeds: actualizaciones de las fuentes de inteligencia de amenazas de Cisco. Permite detectar y bloquear amenazas conocidas, como correos electrónicos de phishing y archivos adjuntos de malware.
  - ✓ File Reputation Active: permite verificar la reputación de los archivos adjuntos a los correos electrónicos entrantes y bloquear archivos que se sabe que son maliciosos
  - ✓ Outbreak Filters: permite detectar y bloquear correos electrónicos que formen parte de un brote de correo electrónico. Su dispositivo podrá protegerlo de virus transmitidos por correo electrónico y otro malware.
  - ✓ IronPort Anti-Spam: permite filtrar los correos electrónicos no deseados. No recibir spam en su bandeja de entrada.
  - ✓ Sophos Anti-Virus: permite analizar los correos electrónicos entrantes en busca de virus y otro malware. Menor riesgo de infección.
  - ✓ File Analysis: permite analizar los archivos adjuntos a los correos electrónicos entrantes. Podrá determinar si es seguro abrir un archivo

- ✓ Bounce Verification: esta funcionalidad permite evitar la denegación de servicio (DoS) en la infraestructura de correo marcando los mensajes que salen de nuestra infraestructura para identificar si los rebotes son legítimos o fraudulentos.
- ✓ Incoming Mail Handling: esta es la funcionalidad principal que permite el manejo del flujo de correo en la infraestructura.

- La licencia "SVS-EMAIL-SUP-B" de soporte básico de seguridad en el email.
- La licencia "EMAIL-TG-2K" de tratamiento de 2000 archivos por día.
- La licencia "SEC-AUTO-PUI-LIC" de seguridad de Cisco.
- La licencia "SMA Centralized Email Management Reporting License" (SMA-EMGT-LIC), que permite centralizar las funciones de administración y generación de informes de múltiples dispositivos Cisco Email Security Appliances (ESA), y está compuesta por las siguientes funcionalidades principales:
  - ✓ Cisco IronPort Spam Quarentine
  - ✓ Cisco Centralized Email Reporting
  - ✓ Cisco Centralized Web Configuration Manager
  - ✓ Cisco IronPort Centralized Email Message Tracking
  - ✓ Cisco Centralized Web Reporting
  - ✓ Incoming Mail Handling

PRESTACIONES A REALIZAR

El contrato tiene por objeto la contratación del soporte y mantenimiento hardware, así como de las licencias de la MTA (Cisco ESA C395) y el Reporter (Cisco SMA) de las que es titular Correos, sin adquisición de hardware adicional.

El adjudicatario del presente contrato deberá proveer a Correos de:

Licencias de la MTA y Reporter.

- Las licencias mencionadas a continuación, suministrando la suscripción con los derechos de uso, actualizaciones, así como los servicios asociados de mantenimiento y soporte software.

CANTIDAD	REFERENCIA	DESCRIPCIÓN
1	EMAIL-TG-2K	Cisco Threat Grid 2K Files/Day
1	SEC-AUTO-PUI-LIC	Cisco Security
19.900	H-ESA-ESS-LIC	Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL
100	CES-ESS-LIC	Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL

19.900	SMA-EMGT-LIC	SMA Centralized Email Management Reporting License

- 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.

Soporte y mantenimiento hardware.

- El soporte y mantenimiento hardware de los dispositivos Cisco ESA C395 y Cisco SMA:
  - ✓ CON-SSSNT-ESAC395K (SMARTNET 8X5XNBD ESA C395 Email Secur) para los 2 dispositivos Cisco ESA C395.

CANTIDAD	REFERENCIA	DESCRIPCIÓN
1	SVS-EMAIL-SUP-B	BASIC SUPPORT FOR EMAIL SECURITY
2	CON-SSSNT-ESAC395K	SMARTNET-8X5XNBD ESA C395 Email Security Appliance

- El Soporte será en modalidad Smartnet, permitiendo la apertura de casos de soporte directamente desde el portal web del fabricante.

CONDICIONES DE PRESTACIÓN DE LOS SERVICIOS

El plazo de duración será el tiempo que transcurra desde la fecha de inicio que figure en el contrato y el 31 de octubre de 2028, con un plazo de ejecución máximo de 22 meses.

No obstante, lo anterior, el plazo para proporcionar las licencias será como máximo de 7 días hábiles, a contar desde el día siguiente de la fecha que figure en el contrato como fecha de inicio de la ejecución del contrato.

Una vez finalizado el periodo de 7 días para el suministro de licencias, 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.

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 el anexo XIX, y en el anexo XX.

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 a uno de los centros de soporte mundial de SAS, 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 o mala praxis.

Tras la adjudicación y antes del inicio del servicio, Correos, en el caso de que el adjudicatario así lo solicitase, facilitará una descripción de las plataformas software 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 del estudio de los precios de referencia (sin IVA):

Grupo Correos:

SUMINISTRO	UNIDADES	PRECIO ANUAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)	Duración (meses)	PRECIO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day)	1	0,00 €	22	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security)	1	0,00 €	22	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	19.900	232.432,00 €	22	426.125,33 €
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	100	1.616,00 €	22	2.962,67 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.900	17.711,00 €	22	32.470,17 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY)	1	0,00 €	22	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	2	2.987,96 €	12	2.987,96 €
TOTAL		254.746,96 €	100,00%	464.546,13 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias, que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

Cada empresa del Grupo Correos firmará su propio contrato con su facturación asociada tal y como se indica a continuación:

Concepto	Correos (% uso)	Correos Express (% uso)	Correos (% coste total)	Correos Express (% coste total)
Correos recibidos	100%	0%	50%	0%
Correos enviados	20%	80%	10%	40%
Total asignado			60%	40%

Como resultado de la aplicación de este criterio, el reparto final del importe total queda establecido en un 60% para la empresa Correos y un 40% para la empresa Correos Express.

De esta manera, los importes máximos para los suministros demandados y cada empresa del grupo serán:

Correos:

SUMINISTRO	BASE IMPONIBLE DEL PRESUPUESTO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day) **	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security) **	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	255.675,20 €
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.777,60 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.482,10 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY) **	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	1.792,78 €
Total	278.727,68 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que estamos pidiendo el mantenimiento.

Correos Express:

SUMINISTRO	BASE IMPONIBLE DEL PRESUPUESTO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day) **	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security) **	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	170.450,13 €
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.185,07 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	12.988,07 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY) **	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	1.195,18 €
Total	185.818,45 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que estamos pidiendo el mantenimiento.

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

El presente procedimiento de licitación no se divide en lotes. De conformidad con lo previsto en el artículo 52.3.b) del Real Decreto-ley 3/2020, de 4 de febrero, se justifica la no división en lotes del presente contrato al concurrir razones técnicas que hacen que la ejecución independiente de las prestaciones comprendidas en su objeto pueda dificultar la correcta ejecución del mismo y comprometer la necesaria coordinación de las distintas actuaciones que integran la solución contratada. [boe.es]

El objeto del contrato comprende la contratación del soporte y mantenimiento hardware, así como de las licencias y derechos de uso asociados al agente de transferencia de mensajes (MTA) implantado en los centros de procesamiento de datos del Grupo Correos, integrado por los equipos Cisco Email Security Appliance (ESA C395) y la plataforma Cisco Security Management Appliance (SMA o Reporter).

Aunque el hardware objeto de mantenimiento fue adquirido en expedientes anteriores, la continuidad operativa de la solución depende de la prestación conjunta e integrada de los servicios de soporte, mantenimiento, actualización y licenciamiento asociados a dicha infraestructura. Las licencias de los equipos Cisco ESA y SMA, las actualizaciones de software, el acceso al soporte especializado del fabricante y la cobertura de mantenimiento hardware constituyen elementos estrechamente vinculados desde un punto de vista técnico y funcional.

La eventual división del contrato en lotes diferenciados, separando las licencias y derechos de uso de los servicios de soporte y mantenimiento, o atribuyendo dichas prestaciones a distintos adjudicatarios, obligaría a coordinar sobre una misma plataforma tecnológica a varios proveedores, aumentando la complejidad de gestión y dificultando la adecuada trazabilidad de incidencias, actualizaciones, parches de seguridad, sustituciones de equipamiento y procedimientos RMA. Asimismo, dicha fragmentación podría generar discrepancias sobre la atribución de responsabilidades ante eventuales incidencias, degradaciones del servicio o problemas de interoperabilidad entre los distintos componentes de la solución.

Debe tenerse en cuenta que los equipos Cisco ESA constituyen una infraestructura crítica para la gestión y protección del tráfico de correo electrónico corporativo del Grupo Correos, mientras que la plataforma Cisco SMA centraliza su administración, monitorización, generación de informes y gestión operativa. En consecuencia, ambas tecnologías conforman una única solución de seguridad y gestión del correo electrónico cuya explotación requiere una actuación coordinada y homogénea sobre todos sus componentes.

Por otra parte, el soporte y mantenimiento de la plataforma exige una coordinación permanente entre las actuaciones relacionadas con el licenciamiento, las actualizaciones de software, la resolución de incidencias, la sustitución de componentes hardware y la interlocución con el fabricante. La intervención de una pluralidad de contratistas podría dificultar dicha coordinación, incrementar los tiempos de resolución de incidencias y

afectar a la disponibilidad y continuidad de un servicio esencial para la actividad del Grupo Correos.

Adicionalmente, las necesidades de Correos y de CEX. quedan cubiertas mediante una única solución tecnológica integrada, por lo que la eventual división en lotes no aportaría ventajas funcionales ni una mayor eficiencia en la contratación, pudiendo incluso generar duplicidades de gestión y costes adicionales derivados de la existencia de múltiples interlocutores y procesos de coordinación.

En consecuencia, la contratación mediante lote único garantiza la coherencia técnica de la solución, la continuidad del servicio, la adecuada asignación de responsabilidades, una gestión más eficiente de las incidencias y un mejor control operativo del entorno tecnológico, evitando los riesgos técnicos y los costes adicionales que podrían derivarse de una ejecución fragmentada del contrato.

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

Grupo Correos:

Se establece como presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de 562.100,82 euros (QUINIENTOS SESENTA Y DOS MIL CIEN EUROS CON OCHENTA Y DOS CÉNTIMOS), de acuerdo con la siguiente distribución:

- Importe del IVA o cualquier otro impuesto indirecto equivalente: 97.554,69 euros (NOVENTA Y SIETE MIL QUINIENTOS CINCUENTA Y CUATRO EUROS CON SESENTA Y NUEVE CÉNTIMOS).
- Base imponible del presupuesto base de licitación (excluido IVA o cualquier otro impuesto indirecto equivalente): de 464.546,13 euros (CUATROCIENTOS SESENTA Y CUATRO MIL QUINIENTOS CUARENTA Y SEIS EUROS CON TRECE CÉNTIMOS), con el siguiente desglose estimado a partir de los suministros demandados:

SUMINISTRO	UNIDADES	PRECIO MÁXIMO UNITARIO (IVA o cualquier otro impuesto indirecto excluido)	PRECIO ANUAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)	% SOBRE EL TOTAL	PRECIO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day)**	1	0,00 €	0,00 €	0,00%	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security)**	1	0,00 €	0,00 €	0,00%	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	19.900	11,68 €	232.432,00 €	91,73%	426.125,33 €
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	100	16,16 €	1.616,00 €	0,64%	2.962,67 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.900	0,89 €	17.711,00 €	6,99%	32.470,17 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY)**	1	0,00 €	0,00 €	0,00%	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	2	1.493,98 €	2.987,96 €	0,64%	2.987,96 €
TOTAL			254.746,96 €	100,00%	464.546,13 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias, que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el

fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

Este presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) se reparte teniendo en cuenta los costes indicados en la siguiente tabla:

Suministros	Mantenimiento y soporte del catálogo de productos software. Soporte y mantenimiento hardware.					
CPV	Principal:48730000-4 (Paquetes de software de seguridad). Secundario: 48218000-9 (Paquetes de software de gestión de licencias).					
AÑO	Base imponible de licitación	Costes directos (84%)	Costes indirectos (10%)	Beneficio industrial (6%)	IVA o impuesto indirecto equivalente (21%)	Presupuesto base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2027	251.759,00 €	211.477,56 €	25.175,90 €	15.105,54 €	52.869,39 €	304.628,39 €
2028	212.787,13 €	178.741,19 €	21.278,71 €	12.767,23 €	44.685,30 €	257.472,43 €
TOTAL	464.546,13 €	390.218,75 €	46.454,61 €	27.872,77 €	97.554,69 €	562.100,82 €

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

Respecto a los costes directos asumidos por el prestador del servicio, se han estimado unos costes salariales en torno al 5% por considerarse que los costes relativos a las actividades a realizar son los asociados al soporte y mantenimiento del hardware, considerándose que el 95% restante corresponde a los costes del mantenimiento y soporte del catálogo de productos en donde intervienen las actualizaciones necesarias para la ejecución del contrato.

En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes directos están conformados únicamente por el coste salarial del personal adscrito al servicio. El Convenio Colectivo que se ha tenido en cuenta como referencia para el cálculo económico es el XIX Convenio Colectivo Estatal de Empresas de Consultoría, de Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública, publicado el pasado 16 de abril de 2025 en BOE (Disposición 7766 del BOE núm. 92 de 2025), con efectos desde el 01 de enero de 2025, vigente desde el 17 de abril de 2025 hasta el 31 de diciembre de 2027 (prorrogable). Además, se ha tenido en cuenta el grado de especialización y el catálogo de servicios contemplados en la presente contratación.

De esta manera, el desglose de los costes directos es el siguiente: del total de 390.218,75 €, un 5% corresponde a costes salariales y un 95% a costes de servicios, distribuyéndose de la siguiente forma:

Costes salariales (mantenimiento hardware) 5%	Costes licencias/suscripciones 95%
19.510,94 €	370.707,81 €

El valor estimado del contrato (excluido IVA o impuesto indirecto equivalente y teniendo en cuenta las eventuales prórrogas): 464.546,13 euros (CUATROCIENTOS SESENTA Y CUATRO MIL QUINIENTOS CUARENTA Y SEIS EUROS CON TRECE CÉNTIMOS).

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

Presupuesto base de licitación (IVA excluido)	464.546,13€	
Plazo de ejecución (meses)	22	
Modificación 20%	No	
Prórroga (meses)	No	
VALOR ESTIMADO DEL CONTRATO (SUMINISTRO)	464.546,13€	

Se renuncia expresamente a la posibilidad de modificación y/o prórroga.

Para la determinación del reparto de costes asociados al uso de la MTA para cada empresa del grupo, se ha aplicado el siguiente criterio metodológico:

- En primer lugar, se ha dividido el coste total de utilización de la MTA en dos bloques equivalentes:
  - ✓ 50% vinculado al volumen de correos enviados
  - ✓ 50% asociado al volumen de correos recibidos.
- A continuación, se ha calculado el porcentaje de utilización correspondiente a cada empresa (Correos y Correos Express) en cada uno de estos bloques, tomando como referencia las volumetrías registradas. Los datos de uso considerados son los siguientes:
  - ✓ Volumen de correos recibidos: 100% Correos.
  - ✓ Volumen de correos enviados: 20% Correos y 80% Correos Express.

Como resultado de la aplicación de este criterio, el reparto final del importe total queda establecido en un 60% para la empresa Correos y un 40% para la empresa Correos Express:

Concepto	Correos (% uso)	Correos Express (% uso)	Correos (% coste total)	Correos Express (% coste total)
Correos recibidos	100%	0%	50%	0%
Correos enviados	20%	80%	10%	40%
Total asignado			60%	40%

Por lo tanto, en los cuadros de los suministros y servicios que vienen a continuación en donde se detalla el cálculo del valor estimado para los contratos de cada una de las empresas del Grupo, no es posible realizar el calcular por unidades, porque las unidades son para el Grupo, pues no se adquieren licencias individuales, sino en base al porcentaje explicado de la contratacion que cada empresa va a asumir del contrato, sobre las unidades ofertadas para el grupo.

Correos:

Se establece como presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de 337.260,49 euros (TRESCIENTOS TREINTA Y SIETE MIL DOSCIENTOS SESENTA EUROS CON CUARENTA Y NUEVE CÉNTIMOS), de acuerdo con la siguiente distribución:

- Importe del IVA o cualquier otro impuesto indirecto equivalente: 58.532,81 euros (CINCUENTA Y OCHO MIL QUINIENTOS TREINTA Y DOS EUROS CON OCHENTA Y UN CENTIMOS).
- Base imponible del presupuesto base de licitación (excluido IVA o cualquier otro impuesto indirecto equivalente): de 278.727,68 euros (DOSCIENTOS SETENTA Y OCHO MIL SETECIENTOS VEINTISIETE EUROS CON SESENTA Y OCHO CÉNTIMOS), con el siguiente desglose estimado a partir de los suministros demandados:

SUMINISTRO	BASE IMPONIBLE DEL PRESUPUESTO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day) **	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security) **	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	255.675,20 €

SUMINISTRO	BASE IMPONIBLE DEL PRESUPUESTO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.777,60 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.482,10 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY) **	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	1.792,78 €
Total	278.727,68 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

Este presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) se reparte teniendo en cuenta los costes indicados en la siguiente tabla:

Suministros	Mantenimiento y soporte del catálogo de productos software. Soporte y mantenimiento hardware.
CPV	Principal:48730000-4 (Paquetes de software de seguridad). Secundario: 48218000-9 (Paquetes de software de gestión de licencias).

AÑO	Base imponible de licitación	Costes directos (84%)	Costes indirectos (10%)	Beneficio industrial (6%)	IVA o impuesto indirecto equivalente (21%)	Presupuesto base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2027	151.055,40 €	126.886,54 €	15.105,54 €	9.063,32 €	31.721,63 €	182.777,03 €
2028	127.672,28 €	107.244,72 €	12.767,23 €	7.660,34 €	26.811,18 €	154.483,46 €
TOTAL	278.727,68 €	234.131,25 €	27.872,77 €	16.723,66 €	58.532,81 €	337.260,49 €

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

Respecto a los costes directos asumidos por el prestador del servicio, se han estimado unos costes salariales en torno al 5% por considerarse que los costes relativos a las actividades a realizar son los asociados al soporte y mantenimiento del hardware, considerándose que el 95% restante corresponde a los costes del mantenimiento y soporte del catálogo de productos en donde intervienen las actualizaciones necesarias para la ejecución del contrato.

En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes directos están conformados únicamente por el coste salarial del personal adscrito al servicio. El Convenio Colectivo que se ha tenido en cuenta como referencia para el cálculo económico es el XIX Convenio Colectivo Estatal de Empresas de Consultoría, de Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública, publicado el pasado 16 de abril de 2025 en BOE (Disposición 7766 del BOE núm. 92 de 2025), con efectos desde el 01 de enero de 2025, vigente desde el 17 de abril de 2025 hasta el 31 de diciembre de 2027 (prorrogable). Además, se ha tenido en cuenta el grado de especialización y el catálogo de servicios contemplados en la presente contratación.

De esta manera, el desglose de los costes directos es el siguiente: del total de 234.131,25 €, un 5% corresponde a costes salariales y un 95% a costes de servicios, distribuyéndose de la siguiente forma:

Costes salariales (mantenimiento hardware) 5%	Costes licencias/suscripciones 95%
11.706,56 €	222.424,69 €

El valor estimado del contrato (excluido IVA o impuesto indirecto equivalente): 278.727,68 euros (DOSCIENTOS SETENTA Y OCHO MIL SETECIENTOS VEINTISIETE EUROS CON SESENTA Y OCHO CÉNTIMOS).

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

Presupuesto base de licitación (IVA excluido)	278.727,68€	
Plazo de Ejecución (meses)	22	
Modificación 20%	No	
Prórroga (meses)	No	
VALOR ESTIMADO DEL CONTRATO (SUMINISTRO)	278.727,68 €	

Se renuncia expresamente a la posibilidad de modificación y/o prórroga.

Correos Express:

Se establece como presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de 224.840,33 euros (DOSCIENTOS VEINTICUATRO MIL OCHOCIENTOS CUARENTA EUROS CON TREINTA Y TRES CÉNTIMOS), de acuerdo con la siguiente distribución:

- Importe del IVA o cualquier otro impuesto indirecto equivalente: 39.021,88 euros (TREINTA Y NUEVE MIL VEINTIÚN EUROS CON OCHENTA Y OCHO CÉNTIMOS).
- Base imponible del presupuesto base de licitación (excluido IVA o cualquier otro impuesto indirecto equivalente): de 185.818,45 euros (CIENTO OCHENTA Y CINCO MIL OCHOCIENTOS DIECIOCHO EUROS CON CUARENTA Y CINCO CÉNTIMOS), con el siguiente desglose estimado a partir de los suministros demandados:

SUMINISTRO	BASE IMPONIBLE DEL PRESUPUESTO TOTAL LICITACIÓN (IVA o cualquier otro impuesto indirecto excluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day) **	0,00 €
SEC-AUTO-PUI-LIC (Cisco Security) **	0,00 €
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	170.450,13 €
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.185,07 €
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	12.988,07 €
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY) **	0,00 €
CON-SSSNT-ESAC395K (12 Meses) *	1.195,18 €
Total	185.818,45 €

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

Este presupuesto base de licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) se reparte teniendo en cuenta los costes indicados en la siguiente tabla:

Suministros	Mantenimiento y soporte del catálogo de productos software. Soporte y mantenimiento hardware.
CPV	Principal:48730000-4 (Paquetes de software de seguridad). Secundario: 48218000-9 (Paquetes de software de gestión de licencias).

AÑO	Base imponible de licitación	Costes directos (84%)	Costes indirectos (10%)	Beneficio industrial (6%)	IVA o impuesto indirecto equivalente (21%)	Presupuesto base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2027	100.703,60 €	84.591,02 €	10.070,36 €	6.042,22 €	21.147,76 €	121.851,36 €
2028	85.114,85 €	71.496,47 €	8.511,49 €	5.106,89 €	17.874,12 €	102.988,97 €
TOTAL	185.818,45 €	156.087,49 €	18.581,85 €	11.149,11 €	39.021,88 €	224.840,33 €

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

Respecto a los costes directos asumidos por el prestador del servicio, se han estimado unos costes salariales en torno al 5% por considerarse que los costes relativos a las actividades a realizar son los asociados al soporte y mantenimiento del hardware, considerándose que el 95% restante corresponde a los costes del mantenimiento y soporte del catálogo de productos en donde intervienen las actualizaciones necesarias para la ejecución del contrato.

En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes directos están conformados únicamente por el coste salarial del personal adscrito al servicio. El Convenio Colectivo que se ha tenido en cuenta como referencia para el cálculo económico es el XIX Convenio Colectivo Estatal de Empresas de Consultoría, de Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública, publicado el pasado 16 de abril de 2025 en BOE (Disposición 7766 del BOE núm. 92 de 2025), con efectos desde el 01 de enero de 2025, vigente desde el 17 de abril de 2025 hasta el 31 de diciembre de 2027 (prorrogable). Además, se ha tenido en cuenta el grado de especialización y el catálogo de servicios contemplados en la presente contratación.

De esta manera, el desglose de los costes directos es el siguiente: del total de 156.087,49 €, un 5% corresponde a costes salariales y un 95% a costes de servicios, distribuyéndose de la siguiente forma:

Costes salariales (mantenimiento hardware) 5%	Costes licencias/suscripciones 95%
7.804,37 €	148.283,12 €

El valor estimado del contrato (excluido IVA o impuesto indirecto equivalente y teniendo en cuenta las eventuales prórrogas): 185.818,45 euros (CIENTO OCHENTA Y CINCO MIL OCHOCIENTOS DIECIOCHO EUROS CON CUARENTA Y CINCO CÉNTIMOS)

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

Presupuesto base de licitación (IVA excluido)	185.818,45 €	
Plazo de Ejecución (meses)	22	
Modificación 20%	No	
Prórroga (meses)	No	
VALOR ESTIMADO DEL CONTRATO (SUMINISTRO)	185.818,45 €	

Se renuncia expresamente a la posibilidad de modificación y/o prórroga.

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

- Forma de acreditación de la solvencia económica y financiera:

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

- Forma de acreditación de la solvencia técnica y profesional:

☒	Certificado de correcta ejecución de los servicios o trabajos realizados, expedidos o visados por la entidad para la que hayan sido realizados.
☐	Relación y perfil o 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: ENS nivel básico

Anexo V.- Modelo de aval

LA ENTIDAD .....
.....
AVALA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anexo VII.- Instrucciones para cumplimentar el DEUC

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

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

https://visor.registrodelicitadores.gob.es/espd-web/filter#

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

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

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

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

☒ PARTE I: Información sobre el procedimiento de contratación y el poder adjudicador (Identificación del contrato 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

Criterios adjudicación económica			
Descripción	Oferta económica	Ponderación	100 puntos
Formula de valoración	$$\mathrm{PE} = \mathrm{PEm}\left(1 - \frac{(Pon - Pse)}{\mathrm{PL}}\right)$$ 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:

Para el Grupo Correos:

Precio Base (en cifras) ……..€ (sin IVA o cualquier otro impuesto indirecto equivalente)

Precio Base (en letras) …… Euros (sin IVA o cualquier otro impuesto indirecto equivalente)

Tipo Impositivo, IVA (o impuesto indirecto equivalente): …… %

Precio (en cifras) ……./€ (con IVA o cualquier otro impuesto indirecto equivalente)

Precio (en letras): …… Euros (con IVA o cualquier otro impuesto indirecto equivalente).

Los importes arriba indicados se desglosan para cada una de las empresas del Grupo Correos en los siguientes Importes:

Para la S.E. Correos y Telégrafos, S.A., S.M.E.:

Precio Base (en cifras) ……..€ (sin IVA o cualquier otro impuesto indirecto equivalente)

Precio Base (en letras) …… Euros (sin IVA o cualquier otro impuesto indirecto equivalente)

Tipo Impositivo, IVA (o impuesto indirecto equivalente): …… %

Precio (en cifras) ……./€ (con IVA o cualquier otro impuesto indirecto equivalente)

Precio (en letras): …… Euros (con IVA o cualquier otro impuesto indirecto equivalente).

Para la Correos Express Paquetería Urgente, S.A., S.M.E.:

Precio Base (en cifras) .....€ (sin IVA o cualquier otro impuesto indirecto equivalente)

Precio Base (en letras) ..... Euros (sin IVA o cualquier otro impuesto indirecto equivalente)

Tipo Impositivo, IVA (o impuesto indirecto equivalente): ..... %

Precio (en cifras) ...../€ (con IVA o cualquier otro impuesto indirecto equivalente)

Precio (en letras): ..... Euros (con IVA o cualquier otro impuesto indirecto equivalente).

Las ofertas anteriores se desglosan en los siguiente conceptos e importes:

Para el Grupo Correos:

SUMINISTRO GRUPO CORREOS	UNIDADES	PRECIO MÁXIMO UNITARIO (IVA o cualquier otro impuesto indirecto excluido)	Precio máximo de la licitación (excluido el IVA o cualquier otro impuesto indirecto)	Precio (excluido el IVA o cualquier otro impuesto indirecto)	IVA o cualquier otro impuesto indirecto	Precio (con IVA o cualquier otro impuesto indirecto incluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day)**	1	0,00 €	0,00 €			
SEC-AUTO-PUI-LIC (Cisco Security)**	1	0,00 €	0,00 €			
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	19.900	11,68 €	426.125,33 €			
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	100	16,16 €	2.962,67 €			
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.900	0,89 €	32.470,17 €			
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY)**	1	0,00 €	0,00 €			
CON-SSSNT-ESAC395K (12 Meses) *	2	1.493,98 €	2.987,96 €			
TOTAL			464.546,13 €			

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado

en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

En los cuadros de los suministros y servicios que vienen a continuación, en donde se detalla el cálculo del valor estimado para los contratos de cada una de las empresas del Grupo, no es posible realizar el calcular por unidades, porque las unidades son para el Grupo, pues no se adquieren licencias individuales, sino en base al porcentaje de la contratacion que cada empresa va a asumir del contrato, sobre las unidades ofertadas para el grupo:

Concepto	Correos (% uso)	Correos Express (% uso)	Correos (% coste total)	Correos Express (% coste total)
Correos recibidos	100%	0%	50%	0%
Correos enviados	20%	80%	10%	40%
Total asignado			60%	40%

Como resultado de la aplicación de este criterio, el reparto final del importe total queda establecido en un 60% para la empresa Correos y un 40% para la empresa Correos Express.

Para la S.E. Correos y Telegrafos, S.A., S.M.E.

SUMINISTRO S.E. CORREOS Y TELEGRAFOS, S.A., S.M.E.	Precio máximo de la licitación (excluido el IVA o cualquier otro impuesto indirecto)	Precio (excluido el IVA o cualquier otro impuesto indirecto)	IVA o cualquier otro impuesto indirecto	Precio (con IVA o cualquier otro impuesto indirecto incluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day)**	0,00 €			
SEC-AUTO-PUI-LIC (Cisco Security)**	0,00 €			
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	255.675,20 €			
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.777,60 €			
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	19.482,10 €			

SUMINISTRO S.E. CORREOS Y TELEGRAFOS, S.A., S.M.E.	Precio máximo de la licitación (excluido el IVA o cualquier otro impuesto indirecto)	Precio (excluido el IVA o cualquier otro impuesto indirecto)	IVA o cualquier otro impuesto indirecto	Precio (con IVA o cualquier otro impuesto indirecto incluido)
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY)**	0,00 €			
CON-SSSNT-ESAC395K (12 Meses) *	1.792,78 €			
TOTAL	278.727,68 €			

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el mantenimiento.

Para Correos Express Paquetería Urgente S.A., S.M.E.

SUMINISTRO CORREOS EXPRESS PAQUETERÍA URGENTE S.A., S.M.E.	Precio máximo de la licitación (excluido el IVA o cualquier otro impuesto indirecto)	Precio (excluido el IVA o cualquier otro impuesto indirecto)	IVA o cualquier otro impuesto indirecto	Precio (con IVA o cualquier otro impuesto indirecto incluido)
EMAIL-TG-2K (Cisco Threat Grid 2K Files/Day)**	0,00 €			
SEC-AUTO-PUI-LIC (Cisco Security)**	0,00 €			
H-ESA-ESS-LIC (Cisco Secure Email Hybrid ESS Inbound + Malware Defense & ANYL)	170.450,13 €			
CES-ESS-LIC (Ciso Secure Email Cloud ESS Inbound + Malware Defense & ANYL)	1.185,07 €			
SMA-EMGT-LIC (SMA Centralized Email Management Reporting License)	12.988,07 €			
SVS-EMAIL-SUP-B (BASIC SUPPORT FOR EMAIL SECURITY)**	0,00 €			
CON-SSSNT-ESAC395K (12 Meses) *	1.195,18 €			
TOTAL	185.818,45 €			

(*) En el caso del soporte y mantenimiento HW (CON-SSSNT-ESAC395K), es para los últimos 12 meses porque ya está cubiertos los otros 10 meses con el soporte contratado

actualmente en el expediente AI230001-20-P01 (prórroga CE20) - PR12MCE20 LICENCIAS Y MANTENIMIENTO MTA Y REPORTER - CISCO ESA Y CISCO MSA).

(**) Se indican en la tabla estas licencias que son las características básicas del funcionamiento del producto, y que están incluidas por defecto con el hardware pagado en su momento, porque es necesario indicarlo ya que es así como el fabricante identifica los conceptos de las licencias incluidas en el hardware sobre el que se solicita el

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

Se deberá incluir en la oferta tanto el importe total ofertado como los importes de cada uno de los conceptos en los que se desglosa la misma, desglosándose los precios ofertados por cada concepto, así como el importe de la oferta total en: precio ofertado sin impuestos y precio ofertado con impuestos, e importe de los impuestos.

Los importes ofertados sin impuestos por cada concepto, así como el importe total sin impuestos de la oferta, no podrán superar los precios fijados como "Precio máximo de la licitación (excluido el IVA o cualquier otro impuesto indirecto)" en este anexo (estos importes también están fijados como base del presupuesto base de licitación y su desglose en el anexo III del pliego). La superación de dichos importes supondrá la exclusión de la oferta del proceso de la licitación.

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:

Licencias, con su mantenimiento y soporte (software)

- Importes fijos anualmente al inicio del periodo (2 anualidades).

Mantenimiento y soporte hardware

- Importe fijo a la finalización del periodo (1 anualidad).

Cada una de las empresas del Grupo Correos anteriormente mencionadas firmará su propio contrato, gestionará sus propias facturas y la aplicación de penalidades en el caso de que tuviesen lugar.

Siguiendo el plan de facturación indicado, en cada ocasión, el adjudicatario emitirá dos facturas separadas y simultáneas, una para cada empresa del grupo:

- Correos (SE Correos y Telégrafos, S.A., S.M.E.): 60% del importe total ofertado (base imponible), con su IVA correspondiente.

- Correos Express Paquetería Urgente, S.A.: 40% del importe total ofertado (base imponible), con su IVA correspondiente.

Este reparto se aplica sobre cada uno de los conceptos objeto de la facturación según la oferta presentada.

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

Anexo XII.- Modificaciones previstas del contrato

NO APLICA

Anexo XIII.- Régimen de penalidades

A).- INCUMPLIMIENTOS LEVES

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Obligaciones generales	Incumplimiento de las obligaciones establecidas en este pliego y que no hayan sido tipificados como incumplimientos graves o muy graves	Hasta 1.000 euros
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, según lo indicado en los ANS relativos a cumplimiento de la planificación para la realización de los servicios conforme se explica en el 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 1.000,00 € IVA excluido. Para cada incumplimiento
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 XI.	penalidad de hasta el 5 por ciento del precio del contrato, IVA excluido, siempre y cuando el cumplimiento defectuoso no afectase a más del 20% de la prestación.
Reincidencia	La comisión de una tercera infracción de carácter leve en el plazo de un año	Penalidad de hasta el 3 por ciento del precio del contrato, IVA excluido.
Incumplir las comunicaciones de incidentes de seguridad	No entrega del informe forense en 3 meses tras la detección del incidente (apartado 11 de anexo XX).	3% facturación total de la adjudicación o 5.000€
Detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 10 o más vulnerabilidades Baja (CVSS < 4.0)	2% facturación anual de la adjudicación o 5.000€
Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro	No asistir a una reunión dentro del plazo de 30 días (apartado 12 de anexo XX).	3% facturación anual de la adjudicación o 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 o 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% 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, según se indican en el Anexo XI.	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 o 10.000€
Detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 5 o más vulnerabilidades Media (4.0 ≤ CVSS < 7.0)	3% facturación anual de la adjudicación o 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 o 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 o 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 o 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 o 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.

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 o 20.000€
Incumplir las comunicaciones de incidentes de seguridad	Retraso en el primer comunicado	10% facturación total de la adjudicación o 20.000€
Incumplir las comunicaciones de incidentes de seguridad	Retraso en el segundo comunicado	10% facturación total de la adjudicación o 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 o 10.000€
Detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros*	Detectar 1 o más vulnerabilidades Altas (7.0 ≤ CVSS < 9.0)	5% facturación anual de la adjudicación o 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 o 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 o 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 ≤ CVSS < 9.0)	Muy grave	27 días	2.000€ por día de retraso
Vulnerabilidades Medias (4.0 ≤ 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

Licencias, con su mantenimiento y soporte (software).

El servicio de mantenimiento y soporte de las licencias (software) estará sometido a los siguientes niveles de cumplimiento:

1-Resolución de incidencias en plazo:

Tiempo de resolución de incidencias con el software. – Mide el tiempo de resolución de incidencias con el software dentro de unos valores objetivos para el tiempo de resolución, así como el número de incidencias reabiertas sobre el total de incidencias del período medido y que supere el tiempo máximo de resolución establecido en el periodo.

Fórmula	Elementos Fórmula	Nivel	Consideraciones	Origen Dato	Valores de Referencia
$PC = \left(\frac{\sum NIC}{\sum TIC}\right) x100$	NIC = Nº de incidencias cerradas en el periodo dentro del valor objetivo para el tiempo de resolución TIC= Total de incidencias cerradas en el periodo	Todas las aplicaciones de la plataforma	Se pueden establecer diferentes valores de referencia en función de la criticidad de la incidencia y del tipo. En su evaluación se tendrá en cuenta el cumplimiento de las condiciones de prestación del servicio.	PoST (herramienta de ticketing)	PCmin= Porcentaje de cumplimiento mínimo

Los indicadores que interviene en el cálculo son los siguientes:

CÓDIGO	INDICADOR DE SERVICIO	VALORES OBJETIVO	% CUMPLIMIENTO (PCmin)
1.1	Resolución de incidencias de usuario muy grave en plazo en el periodo	<= 2 horas	>= 90 %

1.2	Resolución de incidencias de usuario grave en plazo en el periodo	<= 4 horas	>= 90 %
1.3	Resolución de incidencias de usuario leve en plazo en el periodo	<= 1 día	>= 90 %

Se define una incidencia muy grave 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.

Se define como una incidencia grave como aquella que un componente no está funcionando, creando un impacto operativo significativo.

Se define como incidencia leve 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.

Los valores están expresados en periodos laborables.

Será el Grupo Correos quien decidirá, en función de la urgencia y de la gravedad de cada caso, si una incidencia es muy grave, grave o leve.

Al final del periodo se medirán, para todos los niveles de severidad, los porcentajes de cumplimiento (PC). Si, para un nivel de severidad, el PC es inferior al porcentaje de cumplimiento mínimo (PCmin) se considerará como 1 incumplimiento. Se acumularán todos los incumplimientos para el contrato y periodo, asignándose una puntuación y gravedad según la siguiente tabla:

	Número de Incumplimientos = 0	Número de Incumplimientos >0 y <=2	Número de Incumplimientos >2 y <=4	Número de Incumplimientos >4
Gravedad	N/A	Leve	Grave	Muy grave

La Puntuación/Gravedad será tenida en cuenta a la hora de aplicar penalizaciones sobre la facturación (ver Anexo XIII).

Mantenimiento y soporte hardware.

El servicio de mantenimiento y soporte hardware estará sometido a los siguientes niveles de cumplimiento:

1- Resolución de incidencias en plazo:

Por “resolución” se entiende el restablecimiento del servicio a niveles operativos aceptables (p. ej., aplicación de workaround temporal, actualización, rollback controlado, aislamiento de tráfico, sustitución temporal de equipo, reconfiguración)

que elimina o mitiga el impacto de la incidencia hasta su corrección definitiva por el fabricante si fuera necesaria.

Alcance y método:

- Se incluyen incidencias Críticas (afectación severa a seguridad/servicio) y Graves relacionadas con los equipos y licencias objeto del contrato.
- Ventana de atención: 24×7 para ambas severidades.
- Se excluyen incidencias sin severidad o sin sellos fehacientes (no medibles).

Fórmula:

$$\text{Cumplimiento\_resol (\%)} = \frac{\text{Incidencias Servicio reestablecido en el tiempo objetivo}}{\text{Incidencias medibles}^{1}} \text{ x } 100$$

Umbrales/objetivos:

- Críticas: resolución < 4 horas para restablecimiento del servicio.
- Graves: resolución < 8 horas para restablecimiento del servicio.
- Objetivo mensual global2 (Crítica + Grave): ≥ 95%; umbral de alerta 90–95%. (La gradación evita "todo/nada" y permite corrección antes de penalidad mayor).

Evidencias:

- Extractos de portales del fabricante: apertura, hitos y timestamps.
- Export del sistema de tickets utilizado por el adjudicatario (herramienta propia o de terceros), con ID, severidad, apertura/cierre, hitos intermedios.
- Bitácora de intervención y/o correo con sellos de fecha/hora (inicio, medidas aplicadas, restablecimiento).
- Actas del comité e Informe ANS mensual con trazabilidad y enlace a evidencias.

Graduación de incumplimientos:

- Leve: 93%–<95%.
- Grave: 90%–<93%.
- Muy grave: <90%.

Notas operativas:

En incidencias donde el restablecimiento dependa de RMA o firma de seguridad del fabricante, el adjudicatario deberá abrir y escalar el caso de forma inmediata y aplicar medidas de contención hasta el reemplazo o actualización. La trazabilidad se acreditará con el TAC del fabricante y los albaranes/POD cuando proceda.

Los tiempos objetivo se refieren al restablecimiento de servicio; la corrección definitiva podrá requerir acciones ulteriores del fabricante sin penalización adicional si el servicio permanece.

[1] Incidencias "medibles" = con severidad catalogada y sellos de fecha/hora de apertura/cierres verificables.
[2] El cierre definitivo del caso del fabricante puede producirse con posterioridad; no computa contra el tiempo objetivo si el servicio está restablecido

2- Cobertura activa de suscripciones y soporte:

Porcentaje de números de serie objeto del contrato con entitlement vigente (suscripción/soportes activos) en el mes de referencia.
Fórmula:

$$\text{C\_COB (\%)} = \frac{\text{Series con cobertura activa}}{\text{Series del inventario}} \text{ x } 100$$

Objetivo mensual:

- 100%.

Evidencias:

- Extracto de portales de fabricante (listado de series y vigencias), certificados y "License/Entitlement report".
- Cuadre con el detalle de los suministros objeto del contrato Anexo I.

Graduación de incumplimientos:

- Muy grave: C_COB < 100%.
- Si afecta a dispositivo crítico (FG de borde), la penalidad se agrava por riesgo elevado. (Remisión a Anexo XIII).

3- Cumplimiento del soporte 24×7 y del reemplazo RMA NBD[3]/PRMA[4]:

Definición:

- C_24×7: atención de incidencias críticas fuera de horario en ventana 24×7.
- C_RMA: ejecución de RMA de reemplazo dentro de NBD.

Fórmula:

$$\text{C\_RMA (\%)} = \frac{\text{RMA entregados NBD}}{\text{RMA solicitados y aprobados}} \text{ x } 100$$

$$\text{C\_24x7 (\%)} = \frac{\text{Incidencias críticas fuera de horario atendidas en ventana } 24 \times 7}{\text{Incidencias críticas fuera de horario}} \text{ x } 100$$

Umbrales/objetivos:

- C_24×7: 100%.
- C_RMA: 100% en NBD.

Evidencias:

- Registro de guardias/intervenciones (fuera de horario), tickets, aprobación TAC y albaranes/ POD de entrega NBD.

Graduación de incumplimientos:

- Muy grave: C_24×7 < 100% o C_RMA < 100%. (Por impacto directo en continuidad/seguridad)

[3] NBD (Next Business Day): entrega al siguiente día laborable del repuesto/ hardware de reemplazo, con envío avanzado por el fabricante tras aprobación del caso.
[4] RMA (Return Merchandise Authorization): trámite de sustitución de equipo autorizado por el fabricante tras diagnóstico (incluye número/ticket, logística, devolución de defectuoso y reemplazo avanzado).

4- Evidencias de activación de licencias/derechos de uso y certificados (por evento):

Definición:

- Para cada adjudicación/alta/baja/reemplazo (RMA), entrega de evidencia de activación y certificado/entitlement dentro de ≤ 7 días hábiles.

Periodicidad "por evento": interpretación operativa.

- Gatillos: (I) Adjudicación (activación masiva); (II) Alta (nueva serie, p.ej., tras RMA); (III) Baja (cierre ordenado); (IV) Reemplazo (RMA).
- Ventana de cumplimiento: ≤ 7 días hábiles desde el evento.

Fórmula.

$$\text{C\_ACT}\ (\%) = \frac{\text{Eventos con evidencia completa dentro de plazo}}{\text{Total de eventos del mes}}\ \text{x}\ 100$$

Contenido mínimo de la evidencia:

- Serie, fecha de activación/entrada en vigor y captura/descarga del portal del fabricante o certificado formal.

Umbrales/objetivos:

- C_ACT objetivo: 100% dentro de plazo.
- Alerta: 95–<100% (para corrección inmediata).

Graduación de incumplimientos:

- Grave: C_ACT 95–<98% o retrasos puntuales con evidencia completa posterior.
- Muy grave: C_ACT <95% o ausencia de evidencia con brecha de cobertura (se enlaza con punto 2).

5- Activación inicial del contrato en plazo:

Definición:

- Activación completa de todas las licencias/derechos de uso y coberturas de soporte del inventario en el arranque del contrato, con evidencias. Hito crítico para evitar riesgo residual.

Fórmula:

$$\text{C\_ACT0}\ (\%) = \frac{\text{Series activadas con evidencia dentro de}\ \leq\ \text{7 días hábiles}}{\text{Series inventario}}\ \text{x}\ 100$$

Objetivo:

- 100%.

Incumplimiento:

- Muy grave si C_ACT0 < 100% (vínculo con punto 2).

6- Informe mensual de servicio:

Definición:

- Suministro de fichero estructurado (CSV/XLSX) con los campos necesarios para recalcular los indicadores 1 y 6 y las evidencias soporte (enlace a portal/certificado, POD RMA, export de tickets).

Métricas:

- Puntualidad

$$\text{Puntualidad (\%)} = \frac{\text{Meses con entrega } \leq \text{ día 5}}{\text{Meses del periodo}} \text{ x } 100$$

- Completitud

$$\text{Comp\_INF (\%)} = \frac{\text{Apartados obligatorios completos}}{\text{Apartados obligatorios totales}} \text{ x } 100$$

Objetivo:

- Puntualidad: 100%.
- Completitud ≥ 98%.

Incumplimiento:

- Leve: entrega tardía aislada o Comp_INF 95–<98%.
- Grave: reiteración de retrasos (≥2/6 meses) o Comp_INF 90–<95%.
- Muy grave: omisión de apartados críticos (RMA, coberturas) o Comp_INF <90%.

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

En _____, a __ de _____de 20__.

REUNIDOS

DE UNA PARTE,

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

Y DE OTRA,

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

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

EXPONEN

I. Que la prestación de los servicios objeto de licitación exigen el acceso del adjudicatario a los datos de carácter personal de los que resulta responsable del tratamiento correos

II. que con el fin de dar cumplimiento a la normativa de protección de datos personales ambas partes convienen en firmar el presente contrato de encargo del tratamiento, el cual comprende las siguientes:

CLÁUSULAS

1. Posición de las partes

Correos ostenta la posición de responsable del tratamiento con las funciones, derechos y obligaciones que le son propias. Y de otro lado, el adjudicatario ostenta la posición de encargado del tratamiento con las funciones, derechos y obligaciones que le son propias.

DATOS OBJETO DE TRATAMIENTO

OBJETO DEL CONTRATO	Contratación del soporte y mantenimiento hardware, así como de las licencias del agente de transferencia de mensajes o MTA (Mail Transfer Agent por sus siglas en inglés) implantado en los CPD del Grupo Correos: equipos Cisco ESA C395 y Reporter (Cisco SMA). El hardware requerido ya fue adquirido en contratos anteriores, por lo que este expediente se

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

2. Obligaciones del adjudicatario

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

- Llevar a cabo del tratamiento de datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).
- Tratar los datos de acuerdo con las instrucciones de Correos y no destinarlos para ninguna otra finalidad.
- En el supuesto de que el adjudicatario, como Encargado del Tratamiento, reciba una solicitud legalmente vinculante mediante la cual deba comunicar datos personales dentro del alcance del presente encargo, con carácter previo, se lo notificará a Correos sin dilación indebida. No obstante, no existirá obligación de comunicar este tipo de notificaciones a Correos en caso de que el adjudicatario deba tratar esta información como confidencial (por ejemplo y entre otras, para preservar la confidencialidad de una investigación policial). El adjudicatario rechazará aquellas solicitudes que impliquen comunicar datos personales del responsable del tratamiento y que no sean legalmente vinculantes.
- Mantener actualizado un registro de todas las actividades de tratamiento efectuadas por cuenta de Correos, que contenga al menos: identificación de autorizados; categorías de tratamientos y una descripción general de las medidas técnicas y organizativas de seguridad adoptadas.
- Guardar secreto y la más estricta confidencialidad con respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo.
- Garantizar que las personas autorizadas para tratar datos personales observan las instrucciones y protocolos remitidos por Correos, así como las medidas de seguridad legales, técnicas y organizativas establecidas y asegurar que se comprometen, de forma expresa y por escrito, a respetar la confidencialidad de los datos y a cumplir con las instrucciones de Correos.
- Comprometerse a guardar bajo su control y custodia los datos personales accedidos y a no comunicarlos en modo alguno a terceros.
- Poner a disposición de Correos toda la información necesaria para demostrar el cumplimiento de sus obligaciones, según el proceso establecido en el punto 5.

- Asistir a Correos en la realización de los análisis de riesgo, la presentación de consultas previas a la AEPD, en el proceso de notificación de violaciones de seguridad y de respuesta a solicitudes de derechos.
- Gestión de derechos: Dar traslado de las solicitudes de derechos de protección de datos o quejas o reclamaciones por esta materia que puedan formular los interesados de forma inmediata a Correos y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción.
- El deber de secreto y confidencialidad obliga al adjudicatario durante su vigencia y perdurará indefinidamente en el tiempo una vez finalizada la relación.
- En el caso de que el adjudicatario recabe datos personales por cuenta de Correos se obliga a realizarlo conforme las instrucciones de Correos, siguiendo la redacción y formato indicado y custodiando o dando traslado a Correos (según proceda) de las evidencias recogidas para acreditar el cumplimiento del deber de información y, en su caso, de obtención del consentimiento.

3. Declaración previa

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

(i) Ubicación de los servidores en los que se almacenarán los datos personales tratados por cuenta de Correos; y

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

4. Obligaciones de Correos

Corresponden a Correos las siguientes obligaciones:

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

dieran estos supuestos en la prestación del servicio. El adjudicatario deberá solicitar a Correos dicho texto con carácter previo a dirigirse a los interesados.

5. Medidas de seguridad

El adjudicatario implantará las medidas de seguridad y mecanismos establecidos en el artículo 32 del RGPD y deberá adoptar todas aquellas medidas técnicas y organizativas que, a tenor del análisis de riesgo efectuado por Correos, éste considere que resultan necesarias para garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

6. Derecho de auditoría

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

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

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

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

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

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

7. Notificación de violaciones de seguridad

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

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

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

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

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

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

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

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

9. Subcontratación

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

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

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

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

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

10. Cláusulas de buenas prácticas

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

11. Responsabilidad

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

12. Notificación de cambios

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

13. Tratamiento de datos de representantes y trabajadores

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

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

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

Para Correos:

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

Para Correos Express:

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

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

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

14. Actuación como subencargado

El contenido del presente contrato se aplicará, mutatis mutandis, en aquellos casos supuestos en los que Correos actúe como encargado del tratamiento y el adjudicatario como subencargado del tratamiento, comprometiéndose con carácter adicional a las obligaciones previstas anteriormente a:

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

15. Ley aplicable

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

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

MEDIDAS DE SEGURIDAD

I. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES

- Disponer de un organigrama de asignaciones en materia de seguridad de la información, incluyendo cargos y funciones atribuidas a cada puesto.
- Contar con un procedimiento de control de accesos que incluya, entre otros:
    - Gestión de altas/bajas en el registro de usuarios de repositorios de información asegurando que se asigna un identificador único a cada cuenta de usuario. Excepcionalmente, podrán permitirse identificadores de usuario (IDs) genéricos para ser utilizados por un individuo, en el caso de que las funciones accesibles o las acciones llevadas a cabo por ese identificador o necesiten ser detallada seguidas (por ejemplo, acceso de sólo lectura), o cuando están implantados otros controles (por ejemplo, si la contraseña para un ID genérico sólo se utiliza por una persona al mismo tiempo y se registra tal caso).
    - Gestión de derechos y credenciales de acceso asignados a los usuarios.
    - Gestión de privilegios especiales de acceso según el impacto que puede derivar de un uso inadecuado de los datos de carácter personal.
    - Gestión de información confidencial de autenticación de usuarios.
    - Política de retirada de cancelación de accesos y credenciales.

- Haber establecido un procedimiento de accesos a sistemas y aplicaciones que incluya:
    - La restricción de acceso a la información.
    - Procedimientos seguros de inicio de sesión en el que, como mínimo:
        - Se registre los intentos de entrada no satisfactorios.
        - Se limite el número máximo de intentos fallidos, de forma que La revisión de los privilegios de acceso de forma recurrente y después de cualquier cambio, tal como promoción, degradación o terminación del empleo.
    - Procedimiento de uso de herramientas de administración de sistemas de información, tanto propias como externas.
- La revisión de los privilegios de acceso de forma recurrente y después de cualquier cambio, tal como promoción, degradación o terminación del empleo.

II. PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

- Contar con un procedimiento de gestión de contraseñas de usuario que incluya los siguientes aspectos:
    - Forzar el uso de los identificadores de usuario (IDs) individuales y de las contraseñas para mantener la responsabilidad.
    - Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada.
    - Forzar la elección de contraseñas de calidad.
        - Ser fáciles de recordar.
        - No se basen en algo que alguien más pueda fácilmente adivinar u obtener usando la información relativa a la persona, por ejemplo, nombres, números de teléfono, y fechas de nacimiento.
        - No sean vulnerables a ataques de diccionario (por ejemplo, que no consistan en palabras incluidas en diccionario).
        - No contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos
    - Forzar el cambio de contraseñas, por lo menos, cada 6 meses y siempre que existan indicios de que su confidencialidad ha podido verse comprometida.
    - Forzar a los usuarios el cambio de las contraseñas temporales después de la primera entrada.

- Mantener un registro de las contraseñas de usuarios anteriores y prevenir su reutilización.
- No mostrar las contraseñas en la pantalla cuando se están introduciendo.
- No incluir contraseñas en ningún proceso de registro automático, por ejemplo, almacenamiento en una macro o en una función clave.
- Almacenar los ficheros de contraseñas por separado de los datos de la aplicación del sistema.
- Almacenar y transmitir las contraseñas de forma que se garantice su integridad y confidencialidad.

- Plantear el uso de contraseñas basadas sistemas de autenticación fuerte (p.ej. mediante el uso de tarjetas inteligentes combinado con una contraseña).

III. GESTIÓN DE SOPORTES

- Llevar a cabo un inventariado de soportes y gestión de activos, incluyendo:
  - Un registro de propiedad de los activos.
  - Una política interna de usos aceptables de los activos.
  - Una política de devolución/sustitución de activo.
  - Un registro de asignación de activos al personal al cargo.
- Disponer de una política seguridad de equipos y de control de acceso a los repositorios físicos de información, garantizando que los mismos cuenten con las debidas garantías de seguridad respecto a:
  - El acceso a los repositorios de la información, incluyendo un registro de entradas y salidas.
  - Un procedimiento de salida de activos fuera del entorno de la entidad.
  - Un procedimiento de puesto de trabajo despejado y bloqueos de equipo
  - Un procedimiento de mantenimiento de activos.
- Contar con una política de mesas limpias que exija que:
  - El puesto de trabajo esté limpio y ordenado.
  - La documentación que no se esté utilizando se encuentre guardada correctamente (armario bajo llave para documentos en soporte papel y carpetas de red para soportes informáticos), especialmente en el momento en que se abandona temporalmente el puesto de trabajo y al finalizar la jornada.
  - Prohibir expresamente que haya usuarios o contraseñas apuntadas en post-it o similares o que se comparta esta información.

- Disponer de una serie de normas y procedimientos de control para los puestos de trabajo desatendidos que incluya:
    - El bloqueo automático de la pantalla transcurrido un cierto período de tiempo sin que se utilice.

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

IV. ACCESO FÍSICO AL LOCAL

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

V. MONITORIZACIÓN DE EQUIPOS Y REGISTRO DE LOGS

- Disponer de un procedimiento de monitorización de equipos que incluya:
    - Identificación de las medidas de seguridad.
    - Campos de eventos que deberían ser registrados.
    - Tipología de eventos a registrar.
    - Procesos de recogida y protección de logs.
- Los registros de los logs del administrador y operador de sistemas deben ser revisados regularmente.
- Resulta recomendable contar con sistemas de detección de intrusión gestionados fuera del sistema de control y de los administradores de red, para controlar el cumplimiento de las actividades del sistema y de administración de la red.

VI. FICHEROS TEMPORALES

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

VII. COPIAS DE SEGURIDAD Y RESPALDO Y RESILENCIA

- Disponer de un procedimiento de copias de seguridad y respaldo que, incluya, como mínimo los siguientes aspectos:
    - La realización de una copia de seguridad con una periodicidad mínima semanal en un segundo soporte distinto del destinado a los usos habituales.

- Las pruebas con datos reales deberán evitarse, salvo en aquellos supuestos en que sea inevitable su uso o suponga un esfuerzo desproporcionado atendiendo al nivel de riesgo que implica el tratamiento. En estos casos con carácter previo al desarrollo de pruebas con datos reales se procederá a la realización de una copia de seguridad.

- Disponer de un Plan de continuidad de servicios TI que abarque todos los sistemas y componentes TI que procesan datos personales, incluyendo otras ubicaciones y centros de procesamiento de datos.

VIII. DESTRUCCIÓN DE LA DOCUMENTACIÓN

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

IX. AMENAZAS INFORMÁTICAS

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

información, herramientas de monitorización de actividades de usuarios en los sistemas de información.

X. CIFRADO DE DATOS

- Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá contar con un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- Todo tratamiento de datos sensibles u otros cuya pérdida de integridad, confidencialidad y/o disponibilidad puedan tener un importante impacto en los derechos y libertades de las personas se realizará en base a una política de seudonimización de los mismo frente al acceso de terceros o para la realización de pruebas con datos reales, de manera que garanticen la integridad y confidencialidad de los mismos. Dicha política debe incluir:
    - La gestión de claves para la encriptación/desencriptación.
    - Un sistema de etiquetado/cifrado que garantice el anonimato de los titulares de los datos.
    - Un cifrado de información de dispositivos de almacenamiento (como pendrive, equipos informáticos o almacenamientos remotos).
    - Una política de envío seguro de información a través de documentación cifrada.

XI. CONTROL DE CAMBIOS EN T.I

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

equipos, en el software o en los procedimientos. Cuando los cambios son realizados, se debería conservar un registro de auditoría que contenga toda la información importante.

XII. CONTROL DE CAMBIOS EN APLICATIVOS

- Los procedimientos de control de cambios deberían estar documentados y aplicarse para minimizar la corrupción de los sistemas de información.
- La introducción de nuevos sistemas o de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad e implementación gestionada. Este proceso debería incluir:
    - Una evaluación de riesgos
    - Un análisis de los efectos de los cambios
    - Una especificación de los controles de seguridad necesarios.
    - Las medidas necesarias para garantizar que los procedimientos existentes de seguridad y control no se vean en peligro y que los programadores de la asistencia técnica sólo tengan acceso a aquellas partes del sistema necesarias para su trabajo requiriendo de consentimiento y aprobación formal para cualquier cambio.

XIII. GESTIÓN DE INCIDENCIAS Y BRECHAS DE SEGURIDAD

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

XIV. VIDEOVIGILANCIA

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

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

Don/Doña _____

NIF _____

Con domicilio en _____

Calle/Plaza, nº _____

Telf. contacto nº _____

Correo electrónico _____

En caso de actuar en representación

Como apoderado de _____

CIF _____

Con domicilio en _____

Calle/Plaza, nº _____

Correo electrónico _____

DECLARA BAJO SU RESPONSABILIDAD:

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

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

☐ La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

Anexo XVII Adscripción de medios

NO APLICA

Anexo XVIII. Compromiso de adscripción de personal al contrato

NO APLICA

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 regirá la devolución de la información residente en la solución.

Solución PaaS (Plantform 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	Relacional: Amazon RDS (PostgreSQL 16.x) Amazon RDS (MySQL 8.0.39) Clave-valor: DynamoDB No relacional: 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 Contendores	Openshift Container Platform 4.16 (Docker) para arquitecturas basadas en microservicios.
Imágenes de contenedores	Contenedores: 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 Funtions, 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. E*n 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 traves 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 solucione 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 Auditoria, 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).

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

Para aquellos contratos ya adjudicados y en vigor a la fecha de recibir el presente cuestionario, en caso de obtener una puntuación de cero (0) en alguna de su preguntas, la empresa adjudicataria deberá presentar a la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E un compromiso de adaptación al reglamento 2016/679/UE, de 27 de abril, de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) en el plazo máximo de un mes a contar desde la recepción del mismo. Dicho documento (se adjunta modelo) deberá presentarse junto con el presente cuestionario de privacidad.

*AVISO PARA PEQUEÑAS Y MEDIANAS EMPRESAS:

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

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

El enlace a esta herramienta es el siguiente:

https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIwNTAwMDkxNTQ5NjEyMTMxMDMz?updated=true

Cuestionario para la Privacidad de Proveedores:

Marque y cumplimente lo que corresponda:

D. [ ] con NIF , actuando en

su propio nombre y derecho, como profesional autónomo,

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

DECLARA lo siguiente:

1. Cuestiones generales

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

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

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

5= dispone del registro de actividades actualizado y completado.

A continuación, os facilitamos el enlace del Registro de Actividades de la AEPD a fin de que pueda informarse en relación a qué debe contener un registro de actividades del tratamiento conforme a las exigencias establecidasen el RGPD: https://www.aepd.es/agencia/transparencia/registro-actividades-tratamiento/index.html

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

0= no dispone de DPO siendo obligatorio.

3= no dispone de DPO siendo voluntario.

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

2. Medidas de seguridad

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

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

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

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

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

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

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

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

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

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

A continuación, os facilitamos el enlace de la guía para la gestión y notificación de brechas de seguridad que facilita la AEPD:

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

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

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

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

3. Confidencialidad

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

0= no

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

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

4. Accountability y rendición de cuentas

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

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

0= no tiene implantados controles periódicos.

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

5= tiene definidos e implantados controles periódicos.

5. Subcontratación

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

0= se va a subcontratar el servicio contratado sin cumplir con las obligaciones de autorización previa.

5= se va a subcontratar el servicio y estará debidamente regulado.

6. Transferencias internacionales

¿Se realiza un tratamiento de datos fuera del Espacio Económico Europeo? Artículos 44 a 49 RGPD

0= se realiza Transferencias Internacionales de Datos a un país sin nivel adecuado de protección y sin ninguna garantía habilitante.

3= se realiza Transferencias Internacionales de Datos a un país con nivel adecuado de protección y utilizando alguna de las garantías habilitantes (cláusulas contractuales tipo, BCR´s, etc.). Indique cuál/cuáles: [ ]

5= no se realiza Transferencias Internacionales de Datos.

7. Sanciones y procedimientos inspectores

7.1 ¿Ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años?

1= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos idénticos a los prestados en este caso. Aportar documentación justificativa de haber corregido el motivo de la infracción.

3= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos distintos a los prestados en este caso.

5= no ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años.

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

1= tiene abierto procedimiento sancionador por tratamientos idénticos a los prestados en este caso.

3= tiene abierto procedimiento sancionador por tratamientos distintos a los prestados en este caso.

5= no tiene abiertos procedimientos sancionadores por infracciones de la normativa de protección de datos.

Fdo.:

Anexo XXII. 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.