Contrato de Suministros (Expediente núm. AI260304) *Contrato sometido a las Instrucciones internas de contratación del grupo Correos*			
☒ Procedimiento general		☐ Procedimiento especial	
☒ Ordinario	☐ Simplificado	☐ Con invitación a un único licitador	☐ Con invitación a varios licitadores

PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

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

1. Entidad contratante.

Entidad contratante	Sociedad Estatal Correos y Telégrafos, S.A. S.M.E.
Órgano de contratación	Comité de Inversiones
Dirección/Subdirección gestora de la necesidad YGC	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/Subdirección/Área: Dirección de Tecnología y Transformación Digital. Subdirección de Ciberseguridad. Área de Seguridad de Inteligencia y Ciberdefensa.
	Datos de contacto: expdtes.ciberseguridad@correos.com

2. Objeto del contrato.

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

Descripción	Contratación de los derechos de uso, en modalidad Software as a Service **(SaaS)**, de una plataforma especializada en **gestión de postura de seguridad en la nube** (*Cloud Security Posture Management - CSPM*), así como las licencias, servicios asociados y funcionalidades precisas, con el fin de cubrir la necesidad de disponer de capacidades avanzadas de supervisión, control y mejora continua de seguridad en los entornos cloud de la Sociedad Estatal Correos y Telégrafos, S.A., SME (en adelante, Correos).
Código CPV	48000000-8 - Paquetes de software y sistemas de información.
Lotes	☒ NO ☐ SI (Ver Anexo II) Justificación de la no división en lotes: El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica en el **artículo 99.3 b) de la Ley 9/2017, de 8 de noviembre**, de Contratos del Sector Público (en adelante LCSP): ***"El hecho de que, la realización independiente de las diversas***

	prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución de este desde el punto de vista técnico". En este caso concreto, la no división del contrato en lotes se justifica por la necesidad de disponer de una solución integral, unificada y plenamente integrada que cubra de forma coordinada tanto la gestión de la postura de seguridad en la nube como la protección de cargas de trabajo. Ambas capacidades están estrechamente relacionadas y deben compartir información de contexto, inventarios de activos, configuraciones y eventos de seguridad para garantizar una detección eficaz de riesgos y una respuesta adecuada ante amenazas en entornos cloud. Una única solución permite una visión centralizada del riesgo, una gestión más eficiente, menor carga operativa y una mayor coherencia técnica, lo que redunda en una protección más eficaz y en una optimización de los recursos.
¿Se admite oferta integradora (lotes)?	☒ NO ☐ SI (Ver condiciones)

3. Duración del contrato.

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

	Cantidad	Unidad de tiempo	Cómputo
Duración inicial	36	☐ días ☒ meses ☐ años	☒ día siguiente a la firma de la aceptación de la adjudicación ☐ día siguiente a la comunicación de inicio del contrato por la entidad contratante ☐ La fecha que figure en la resolución de adjudicación
Prorrogable	☒ NO ☐ SI	Nº de prórrogas: - Duración máxima de la de prórroga cada (meses):	-

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Valor estimado del contrato	270.000,00 EUROS (DOSCIENTOS SETENTA MIL EUROS), conforme al método de cálculo especificado en Anexo III				
Presupuesto base de licitación	326.700,00 €		IVA	56.700,00 €	
Anualidades (IVA incluido o impuesto indirecto equivalente)	2026	2027	2028	2029	Total
	63.525,00 €	108.900,00 €	108.900,00 €	45.375,00 €	326.700,00 €

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 rowspan="2">Dispensa de acreditar aptitud, solvencia y capacidad</td><td>☐ SI</td><td colspan="5">☐ Contratistas que hubiesen resultado adjudicatarios de contratos en los dos últimos años, hubiesen acreditado entonces su aptitud y solvencia, y no hubieran cambiado sus circunstancias.</td></tr>
<tr><td>☒ NO</td><td colspan="5">☐</td></tr>
<tr><td rowspan="4">Solvencia económica o financiera</td><td colspan="6">☒ Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, equivalente a 90.000,00 EUROS.

☐ Otros:
…..

Sobre la forma de acreditar estos requisitos, ver Anexo IV
En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote.</td></tr>
<tr><td></td><td>Lote 1</td><td>Lote 2</td><td>Lote 3</td><td>Lote 4</td></tr>
<tr><td>Porcentaje/Cifra volumen anual negocios.</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">☐ 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 colspan="6">☒ Haber realizado 2 suministros 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</td></tr>
</table>

	superior al 70 por ciento de la anualidad media del contrato (63.000,00 EUROS) ☐ Haber realizado ….. suministros de igual o similar naturaleza que los que constituyen el objeto del contrato en los tres últimos años, cuyo importe anual acumulado en el año de mayor ejecución sea igual o superior a …… €. ☐ Disponibilidad de los siguientes perfiles relativos al personal: … ☐ Muestras, descripciones y fotografías de los productos a suministrar: ☐ 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: Con el objetivo de garantizar la calidad, madurez y fiabilidad de la solución ofertada, **el licitador deberá acreditar los siguientes requisitos mínimos:** • **Experiencia comprobada de al menos 5 años** en el desarrollo, comercialización o implementación de soluciones CSPM en entornos empresariales. Se exige esta experiencia para garantizar la solvencia técnica en la mitigación de riesgos críticos de infraestructura, asegurar la correcta integración de la solución en arquitecturas multicloud complejas y avalar la capacidad del adjudicatario para mantener la continuidad del negocio bajo estándares de cumplimiento. • **Presencia activa de la herramienta en al menos 3 proyectos relevantes** de CSPM en organizaciones de tamaño medio o grande (más de 500 empleados o más de 100 recursos cloud gestionados), preferentemente en sectores regulados como financiero, salud, energía o administración pública. Este requisito garantiza que la herramienta ha sido validada en entornos de alta criticidad y escala, asegurando que posee la robustez técnica necesaria para gestionar volúmenes masivos de datos y cumplir con los estrictos controles de seguridad y cumplimiento que exige Correos. • **Presentación de al menos 2 casos de éxito documentados** (para garantizar que el licitador no solo posee la herramienta,

	sino la capacidad operativa real para implementarla en entornos complejos) que incluyan: ○ Nombre del cliente (o sector si hay confidencialidad). ○ Alcance del proyecto. ○ Resultados obtenidos (reducción de riesgos, cumplimiento normativo, mejora de visibilidad, etc.). ○ Tiempo de implementación. • **Reconocimiento por parte de analistas independientes**, como inclusión en informes, **al menos dos**, de Gartner, Forrester, IDC u otros equivalentes, en la categoría de CSPM, CNAPP o seguridad cloud. Esta exigencia asegura que la solución cuenta con el respaldo técnico y la validación de expertos externos, garantizando que es una tecnología líder, competitiva y con una hoja de ruta estable dentro del mercado global de seguridad cloud. • **Al menos 2 certificaciones técnicas del producto**, tales como: ○ ENS, ISO/IEC 27001, SOC 2 Type II, CSA STAR o equivalente. ○ Certificaciones específicas de los proveedores cloud (AWS Security Competency, Azure Advanced Specialization o equivalente). Estas certificaciones garantizarán que el producto cumple con estándares de seguridad rigurosos, asegurando que la herramienta es técnicamente confiable y capaz de proteger la integridad de los datos en nubes complejas. Sobre la forma de acreditar estos requisitos, ver Anexo IV
Adscripción de medios	☐ Sí. Medios que 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.

Las ofertas se presentarán en un plazo de 30 días naturales desde la publicación del anuncio de licitación publicado 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 los mismos) o datos, de los incluidos en las ofertas, tienen la consideración de «confidenciales», sin que resulten admisibles las declaraciones genéricas de confidencialidad de todos los documentos o datos de la oferta. La condición de confidencial deberá reflejarse claramente (sobreimpresa, al margen, o de cualquier otra forma claramente identificable) en el propio documento que tenga tal condición, señalando además los motivos que justifican tal consideración. No se considerarán confidenciales documentos o datos que no hayan sido expresamente calificados como tales por los licitadores.

6.5. Adjudicación de los contratos.

6.5.1 Procedimiento General.

6.5.1.1 Procedimiento General Ordinario:

Al amparo de las instrucciones aplicables a la contratación de las entidades que forman parte del Grupo Correos se propone como procedimiento de contratación el procedimiento del apartado 11, **Procedimiento General.**

La elección del presente procedimiento obedece a las siguientes razones:

- El Procedimiento General es uno de los procedimientos ordinarios de adjudicación de los contratos de las entidades que forman parte del Grupo Correos.
- La intención es dar a todos los licitadores un tratamiento igualitario, ajustado a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación (art. 1 de la LCSP).

A. Sin negociación:

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

Por tanto, se elige este procedimiento con el objetivo de maximizar la concurrencia, la transparencia y la libre competencia entre proveedores de soluciones CSPM en la nube, garantizando así la igualdad de trato a todas las empresas del sector. Además, este procedimiento permite obtener la **mejor relación calidad-precio (siendo la relación 30%-70% respectivamente),** evaluando diversas características adicionales de la herramienta (gestión y análisis de la postura de seguridad de las aplicaciones creadas por Correos, cumplimiento de seguridad en las SaaS y postura de seguridad a nivel del dato o similares) y asegurando que no se elija solo la opción más barata, sino la que ofrezca mejor retorno en seguridad y operatividad.

La puntuación técnica, mediante criterios automáticos, se obtendrá de la siguiente forma:

- **Se podrán obtener hasta 30 puntos por incluir en la oferta las siguientes características técnicas**:

Característica	Puntuación Máxima
Herramienta de Exposure Management	6
Gestión y análisis de la postura de seguridad de las aplicaciones creadas por Correos	6
Postura de seguridad a nivel del dato	6
Cumplimiento de seguridad en las SaaS	12

Estas características opcionales, se valorarán según lo detallado en el Anexo VIII.- Criterios de adjudicación de evaluación automática.

Distribución de la ponderación:

Tipología	Criterio	Ponderación
Criterios sujetos a un juicio de valor	Técnico	- %
Criterios evaluables mediante formula o automáticamente (Anexo IX)	Técnico	30 %
	Económico	70 %

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

6.6. Contenido de las ofertas.

6.6.1. Sobre 1: documentación administrativa.

a) Documento Europeo Único en materia de Contratación (DEUC). Cumplimentado conforme a las indicaciones contenidas en el Anexo VII, firmado por el licitador o su representante.

b) 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).

c) 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.

d) 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.

e) Las empresas de Estados que no sean miembros de la Unión Europea o signatarios del Acuerdo sobre el Espacio Económico Europeo deberán aportar un informe que acredite su capacidad de obrar, expedido por la Misión Diplomática Permanente u Oficina Consular de España del lugar del domicilio de la empresa, en el que se haga constar, previa acreditación por la empresa, que figuran inscritas en el Registro local profesional, comercial o análogo o, en su defecto que actúan con habitualidad en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.

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

Los criterios de adjudicación de evaluación automática con arreglo a fórmulas serán los establecidos en el ***Anexo VIII.***
La proposición económica se ajustará al modelo que se incluye como ***Anexo IX***.

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

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

7. Adjudicación y perfección del contrato.

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

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

La evaluación de las ofertas conforme a los criterios cuantificables mediante la mera aplicación de fórmulas se realizará tras efectuar previamente la de aquellos otros criterios en que no concurra esta circunstancia.

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, exceda de diez unidades porcentuales.

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 que 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 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.

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 expediente.

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.

La formalización se realizará mediante la firma de aceptación por el contratista del acuerdo de aceptación de la adjudicación donde ha de constar de forma expresa la fecha de inicio del expediente.

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

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

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

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

7.6. Constitución de garantías.

<table>
<tr><td colspan="4">RÉGIMEN DE GARANTÍAS</td></tr>
<tr><td rowspan="2">Constitución de garantía definitiva</td><td colspan="2" rowspan="2">☒ 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 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.</td></tr>
<tr><td>Constitución de garantía complementaria</td><td>☐ NO ☒ SI</td><td>Importe</td><td>☒ 5% sobre el importe de adjudicación (en caso de oferta temeraria). (IVA excluido)
☐ Otros: ….</td></tr>
</table>

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.

En el caso de que, debido a actuaciones u omisiones de la empresa, de sus contratistas o subcontratistas, la entidad contratante fuese sancionada por incumplimientos de las disposiciones vigentes en materia laboral, de seguridad social, de integración social de personas

con discapacidad, de prevención de riesgos laborales, de protección del medio ambiente o cualesquiera otra que resulten de aplicación en ejecución del contrato, bien en exclusiva o con carácter solidario, el adjudicatario abonará a la entidad contratante la cantidad que resulte de dicha sanción, al primer requerimiento, y sin perjuicio de las acciones legales que posteriormente le pudieran corresponder.

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

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

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

El desarrollo del servicio objeto de licitación no requiere ni de una comunicación de datos, ni de un acceso por parte del adjudicatario a los datos de carácter personal bajo la responsabilidad de la entidad contratante, el adjudicatario se compromete a:

- Evitar todo acceso a datos, informando expresamente a sus trabajadores y profesionales de que el mismo se encuentra prohibido.

- En caso de acceso accidental o simple visionado por necesidad de acceso a las instalaciones: i) Guardar la más estricta confidencialidad y secreto sobre los datos accedidos; II) Adoptar las medidas oportunas para evitar su reiteración; III) Proceder a la inmediata destrucción de las copias accidentales que se hayan podido realizar.

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

No obstante, lo anterior, cuando el servicio objeto de licitación sí requiera una comunicación de datos entre las Partes o cualquiera de las Partes debiera tener acceso a los datos de carácter personal titularidad de la entidad contratante o del adjudicatario, éstos se comprometen a la firma de un documento, que cumpla con las exigencias previstas en la normativa de protección de datos vigente.

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:

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 XI.

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 Codigo-General-de-Conducta.pdf

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

Condición esencial	Frecuencia	Forma de acreditación del cumplimiento
Condiciones especiales de ejecución del contrato	Evaluación trimestral.	Auditorías internas y revisiones de cumplimiento.
Aspectos que se hayan considerado como criterio de adjudicación.	Anualmente. Durante el periodo de ejecución del contrato.	A través de la facturación y la certificación del cumplimiento de las características obligatorias y adicionales.

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, cuyo 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 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 suministro a realizar ☐ Otro ……
☐	Establecimiento de un sistema de gestión diferenciada para los residuos que pueda generar la prestación del suministro.
☐	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: Emplear en la ejecución del contrato un porcentaje de trabajadores fijos igual o superior al 20 por 100.

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

Condición especial	Frecuencia	Forma de acreditación del cumplimiento
Emplear en la ejecución del contrato un porcentaje de trabajadores fijos igual o superior al 20 por 100.	Revisiones anuales.	A través de registro de empleados.

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

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

8.1.8. *Régimen de confidencialidad.*

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

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

8.2. Modificaciones del contrato.

En el presente contrato

☒ NO están previstas modificaciones.
☐ SÍ se han previsto la posibilidad de acordar modificaciones en los supuestos descritos

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.*

Cesión permitida:

☐ NO ☒ SI

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

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

8.3.2. *Régimen de subcontratación.*

Subcontratación permitida:

☐ NO ☒ SI

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

- Los licitadores deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial de los subcontratistas a los que se vaya a encomendar su realización.

- El adjudicatario comunicará su intención de celebrar subcontratos, señalando la parte de la prestación que se pretende subcontratar y la identidad, datos de contacto y representante o representantes legales del subcontratista, y justificando suficientemente la aptitud de este para ejecutarla por referencia a los elementos técnicos y humanos de que dispone y a su experiencia, y acreditando que el mismo no se encuentra incurso en causa de prohibición de contratar. Cualquier cambio respecto de los subcontratos que se produzca durante la ejecución del contrato deberá ser comunicado también a la entidad contratante.

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

☒	Tendrán la consideración de funciones críticas no susceptible de subcontratación la definición de la postura de seguridad, la priorización y aceptación del riesgo, la aprobación de excepciones, la gestión de accesos y cualquier decisión que implique actuaciones con impacto potencial en los sistemas o en la continuidad del servicio. La reserva de estas funciones como tareas críticas no subcontratables se fundamenta en la necesidad de garantizar el ejercicio de la autoridad de control por parte del adjudicatario.

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 contrato.

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 X. Los procedimientos para la imposición de penalidades deberán iniciarse antes de la aprobación del acta de conformidad con el suministro 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, o seis meses, en casos de infracciones muy graves.

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

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

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

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

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

9.3. Abonos al contratista. Facturación.

Se realizarán tres pagos anuales anticipados, venciendo el primero en la fecha de firma del contrato, y los dos restantes al inicio de cada anualidad sucesiva, previa presentación de las correspondientes facturas. Para el pago de facturas giradas por el adjudicatario, la entidad contratante utilizará los siguientes medios de pago:

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

En caso de que el adjudicatario no estuviera interesado en el anticipo de sus facturas, el importe de las mismas se abonaría mediante transferencia bancaria en los 60 días naturales siguientes a la fecha de su emisión, coincidente con el calendario de pagos de la entidad contratante.
Las facturas contendrán la información establecida en la normativa que resulte de aplicación, y se tramitarán por vía electrónica con arreglo a las siguientes especificaciones y formato:

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

Campo		**Facturae 3.2**
Expediente		
Lote		
Grupo Gestor		Facturae/Parties/BuyerParty/

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

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

9.4. Recepción y liquidación.

El contratista deberá realizar el suministro 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 última entrega realizada de conformidad.
☐ ESPECÍFICO, de …. meses desde la última entrega realizada de conformidad

Transcurrido dicho plazo sin que la entidad contratante haya formalizado ningún reparo, el contratista quedará relevado de toda responsabilidad por razón de la prestación efectuada,

procediéndose a la devolución o cancelación de la garantía definitiva.

10. Resolución del contrato.

10.1. Causas de resolución.

Serán causa de resolución del contrato:

☒	Las previstas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☒	El incumplimiento de obligaciones calificadas expresamente como «esenciales» en este Pliego, de acuerdo con lo establecido en el Apartado 8.1.5.
☒	Cuando teniendo que llevar a cabo una modificación en el mismo que, no estando prevista en el pliego, no concurrieran las circunstancias establecidas en el artículo 205 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☒	La imposición de penalidades por demora en la ejecución, cada vez que alcancen un múltiplo del 5 por 100 del precio del contrato, IVA excluido,
☒	El cumplimiento defectuoso de la prestación, cuando afecte a más del 20% de dicha prestación.
☒	El incumplimiento por el contratista de los plazos de pago a sus proveedores o subcontratistas.
☒	La falta de renovación o prórroga de la Póliza de seguro de responsabilidad civil, en los casos en que fuera exigible o lo hubiera ofrecido el adjudicatario.
☒	El desistimiento de la ejecución del contrato por la entidad contratante por circunstancias sobrevenidas, aun cuando se hubiera comenzado dicha ejecución.
☒	Incumplimiento de las condiciones especiales de ejecución, de modo que se frustre el objeto del contrato.

10.2. Procedimiento.

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

11. Protección de datos.

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

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

Para Correos:

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

- Correo Electrónico: derechos.protecciondatos.correos@correos.com

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

11.2 Información a representantes, trabajadores y personas de contacto.

Los datos de carácter personal de las personas de contacto de los licitantes y, en su caso, de sus trabajadores serán tratados por la entidad contratante con la finalidad de gestionar su participación en la presente contratación, y en caso de resultar adjudicatario del contrato, con la finalidad de gestionar la relación contractual que se formalice entre las partes, siendo la base legitimadora del tratamiento la ejecución del contrato y el cumplimiento de la normativa de aplicación. En este sentido, le informamos que los datos facilitados no se cederán a terceros, salvo obligación legal.
Estos datos se conservarán hasta que se produzca la adjudicación del contrato y, en caso de resultar adjudicatario, durante la realización del servicio. Transcurrido este período se procederá a su bloqueo y, prescritas las acciones derivadas, a su eliminación.

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

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

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

El licitante se compromete expresamente a informar a sus trabajadores y resto de personas de contacto de los términos de la presente 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 las Instrucciones Internas de Contratación del Grupo Correos. El resto de las cuestiones relativas a los efectos, cumplimiento y extinción del contrato se regirán por lo previsto en la documentación que revista carácter contractual y por el Derecho Privado.

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

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos
☒	Aceptación de la resolución de adjudicación
☒	Los proyectos o programas de trabajo que se hubiera presentado el adjudicatario
☒	La totalidad de la oferta presentada por el adjudicatario

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

Madrid, 20 de abril de 2026

EL SUBDIRECTOR DE CIBERSEGURIDAD

Firmado Digitalmente por MAYOR SENDRA, JESUS (FIRMA)
Fecha: 2026.04.21 11:13:47 +02'00'

FDO.: JESÚS MAYOR SENDRA

VºBº:
LA DIRECTORA DE TECNOLOGÍA Y TRANSFORMACIÓN DIGITAL

Firmado digitalmente por: TARRERO MARTOS, CRISTINA
Fecha: 2026.04.21 11:36:16 +02'00'

FDO.: CRISTINA TARRERO MARTOS

Anexo I.- Características técnicas específicas del contrato.

La solución deberá suministrar un ecosistema integral de licencias diseñado para la protección avanzada de activos en nube, estructurado en módulos especializados que garantizan una visibilidad 360° y una respuesta proactiva ante incidentes.

A. Deberá incluir los siguientes módulos:

1. CSPM (Cloud Security Posture Management)

El módulo CSPM debe actuar como el núcleo de gobernanza y cumplimiento regulatorio para la infraestructura en nube pública de Correos. Sus capacidades principales incluyen:

- Detectar todos los elementos de infraestructura creados en las diferentes suscripciones de Correos
- Comprobar su configuración y detectar los problemas de seguridad que pudieran tener.
- Comprobar el alineamiento con los principios de seguridad más utilizados, así como con frameworks regulatorios o políticas internas de la compañía.
- Proveer de visibilidad de las relaciones entre los distintos elementos creados, permitiendo visualizar como afecta un problema de seguridad a otro elemento sobre el que se tiene dependencia.
- Detección de ataques o problemas de seguridad accediendo a los eventos que generan los fabricantes de nube pública.
- Detección de problemas de seguridad en clusters de contenedores con Openshift, Fargate o alguna solución compatible con Kubernetes.
- Compatibilidad multicloud nativa, con soporte comprobado para al menos tres de los principales proveedores de servicios cloud: Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).
- Integración mediante APIs seguras (REST, GraphQL o similares) que permitan la automatización de tareas, extracción de datos y conexión con sistemas externos.
- Capacidad de descubrimiento automático de recursos cloud sin necesidad de instalación de agentes, mediante integración con los servicios de gestión de identidad y permisos de cada proveedor.
- Soporte para autenticación federada y gestión de identidades, incluyendo compatibilidad con SSO (Single Sign-On) mediante protocolos como SAML 2.0, OAuth 2.0 o OpenID Connect.
- Integración con plataformas de gestión de vulnerabilidades y SIEM, como Splunk, QRadar, Sentinel, Tenable, Rapid7, entre otros.
- Capacidad de exportación de informes y datos en formatos estándar (CSV, JSON, PDF) y mediante conectores nativos a plataformas de BI (Power BI, Tableau, etc.).
- Alta disponibilidad y escalabilidad, con SLA documentado que garantice al menos un 99.9% de disponibilidad mensual.
- Cifrado de datos en tránsito y en reposo, conforme a estándares como TLS 1.2+ y AES-256.

2. **CWPP - Cloud Workload Protection Platform.**

Este componente deberá garantizar la integridad de las cargas de trabajo mediante:

- Seguridad completa en tiempo real.
- Protecciones proactivas.
- Integración Multicloud.
- Completa visibilidad en un dashboard unificado.
- Gestión de vulnerabilidades.

3. **Gestión de la seguridad en autorizaciones, accesos, permisos en identidades (IAM).**

El sistema debe proveer de un módulo que ayude a monitorizar de forma continua que los permisos asociados a cualquier elemento se mantienen estables en el tiempo y notificar de desvíos y conjunto de permisos excesivos, aplicando el principio de mínimo privilegio de forma centralizado.

4. **Postura de seguridad de la Inteligencia Artificial:**

El sistema debe proporcionar visibilidad del uso y postura de seguridad de los motores más usados en el momento dentro de las infraestructuras de Correos.

También debe detectar el uso de paquetes de inteligencia artificial dentro de imágenes de contenedores, mapeando las dependencias de los paquetes de software que se usen en el código generado por Correos.

5. **Escaneo de IaC (Infraestructura como Código)**

Este módulo debe integrarse con repositorios de código como GitLab o como plugin en editores de código como VSCode, de forma que de forma proactiva analice código de despliegue de infraestructuras como Terraform o Ansible, detecte y notifique de configuraciones inseguras, accesos y permisos muy laxos y credenciales, secretos no suficientemente securizados y escaneo de vulnerabilidades que resultarían de aplicar el código.

6. **Seguridad en el CI/CD.**

La suite ofertada deberá proveer de elementos que analicen la seguridad de los despliegues automatizados de nuevas versiones de código, de forma que se analicen buscando:

- Código malicioso / librerías maliciosas
- Binarios manipulados.
- Secretos y contraseñas comprometidos.
- Abusos en las infraestructuras de despliegue.
- Vulnerabilidades en el código o en las librerías dependientes.

B. SOPORTE TÉCNICO

- Disponibilidad del servicio mensual mínima: 99,9%.

- **Horario de atención**: de lunes a viernes, de 08:00 a 20:00 (hora local).
- **Canales de soporte**: correo electrónico, portal web o teléfono.
- **Seguimiento de tickets**: acceso a histórico y trazabilidad de cada incidencia.

C. CARACTERÍSTICAS OBLIGATORIAS:

Cualquier incumplimiento de estas características supondrá que la oferta no superará el corte técnico:

- El sistema ofertado debe ser una plataforma **SaaS nativa** cuya operatividad no dependa de la provisión de infraestructura adicional por parte de Correos. La monitorización de la postura de seguridad no podrá degradar el rendimiento de las cargas de trabajo (*workloads*) productivas. Cualquier elemento de software desplegado en el entorno de Correos deberá estar optimizado para una **huella de computación mínima**, garantizando que el análisis de vulnerabilidades y configuración se realice de forma asíncrona o mediante el uso de **snapshots**, evitando así cualquier incremento en los costes operativos de infraestructura por consumo de recursos.
- **Requerimiento de Cumplimiento CPSTIC (CCN-CERT).** El fabricante de la solución propuesta (agentes, portal web y herramientas de gestión entre otras) deberá tener productos incluidos y vigentes en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** del Centro Criptológico Nacional (disponible en www.cpstic.ccn.cni.es y en la Guía CCN-STIC 105). La oferta técnica deberá incluir obligatoriamente los enlaces directos a las fichas de los productos en el catálogo.
- **Evaluación Continua de la Seguridad y Configuración (CSPM):** El sistema deberá proporcionar visibilidad y evaluación continua de la postura de seguridad (Cloud Security Posture Management) en entornos de nube pública multicloud (AWS, Azure y GCP) mediante análisis automatizados de configuración.
- El sistema deberá realizar escaneos bajo demanda y programados para mantener un inventario actualizado y detallado de la infraestructura cloud desplegada.
- **Detección basada en eventos y monitorización en tiempo real.** La solución debe soportar la detección basada en eventos (event-driven) para monitorizar modificaciones en los elementos de infraestructura en tiempo cuasi real.

  Debe activar alertas inmediatas ante los siguientes escenarios:

  - Provisión de nuevos elementos con configuraciones inseguras.
  - Modificaciones en elementos existentes que resulten en configuraciones inseguras.
  - Borrado o eliminación masiva de recursos.
- **Cumplimiento Normativo y Cuadros de Mando (Dashboards):** La plataforma deberá

proveer de cuadros de mando (dashboards) personalizables que reflejen el estado de cumplimiento normativo en tiempo real.

- El sistema deberá **mapear automáticamente las configuraciones de seguridad de la infraestructura contra los marcos normativos exigidos**, incluyendo obligatoriamente: Esquema Nacional de Seguridad (ENS), NIST, ISO/IEC 27001, y otros marcos sectoriales relevantes para Correos.

- **Gestión de Identidades y Autenticación.** El sistema deberá integrarse con el sistema de gestión de identidades corporativo de Correos permitiendo la autenticación de usuarios mediante protocolos modernos y seguros, tales como OAuth v2, SAML o similar.

- **Gestión de Eventos de Seguridad.** La herramienta deberá proveer acceso, exportación y gestión de los eventos de seguridad y logs generados por la actividad de los usuarios en los entornos cloud, facilitando la auditoría y respuesta ante incidentes.

Además, el licitador deberá integrar una **Matriz de Cumplimiento de Requisitos Mínimos**, en la cual se indicará si la herramienta cumple o no cumple con las características obligatorias definidas en este epígrafe. Dicha matriz **se exige para valorar la aptitud de la oferta:**

REQUISITO	CARACTERÍSTICAS OBLIGATORIAS	CUMPLE	NO CUMPLE
1	El sistema ofertado debe ser una plataforma **SaaS nativa.**		
2	**Requerimiento de Cumplimiento CPSTIC (CCN-CERT).** El fabricante de la solución propuesta (agentes, portal web y herramientas de gestión entre otras) deberá tener productos incluidos y vigentes en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** del Centro Criptológico Nacional (disponible en www.cpstic.ccn.cni.es y en la Guía CCN-STIC 105).		
3	**Evaluación Continua de la Seguridad y Configuración (CSPM)**		
4	El sistema deberá realizar escaneos bajo demanda y programados para mantener un inventario actualizado y detallado de la infraestructura cloud desplegada.		
5	**Detección basada en eventos y monitorización en tiempo real.**		
6	**Cumplimiento Normativo y Cuadros de Mando (Dashboards).**		
7	El sistema deberá **mapear automáticamente las configuraciones de seguridad de la infraestructura contra los marcos normativos exigidos**, incluyendo obligatoriamente: Esquema Nacional de Seguridad (ENS), NIST, ISO/IEC 27001, y otros marcos sectoriales relevantes para Correos).		
8	**Gestión de Identidades y Autenticación.**		
9	**Gestión de Eventos de Seguridad.**		

Será necesario cumplir la totalidad de los requisitos para continuar en el proceso. El incumplimiento de cualquiera de ellos implicará la exclusión automática de la oferta.

D. CARACTERÍSTICAS ADICIONALES

Se valorará adicionalmente que se proporcione licenciamiento para los siguientes análisis:

1. **Herramienta de Exposure Management.**

Plataforma de gestión de los assets expuestos y sus vulnerabilidades, gestionando la evolución del riesgo durante todo el ciclo de vida del asset. La herramienta debe proveer un sistema que recomiende soluciones de mitigación a los problemas de configuración dentro de una vista unificada para todos los assets detectados.

2. **Gestión y análisis de la postura de seguridad de las aplicaciones creadas por Correos**

Este módulo deberá proveer de las siguientes características:

- Inventario de aplicaciones.
- Vulnerabilidades.
- Errores de configuración.
- Identificación de datos personales.
- Identificación de usos y practicas inseguras.

3. Postura de seguridad a nivel del dato.

El sistema debe proveer de una solución que permita identificar la tipología de los datos independientemente de dónde se hayan guardado.

El sistema debe proveer de alertas en tiempo real de desviaciones de cumplimiento.

La herramienta deberá ayudar a establecer las medidas de seguridad necesarias del dato en función del sistema regulatorio español.

Este módulo debe establecer una metodología para clasificar los datos encontrados en base a las tipologías habituales de clasificación de datos tal como:

- Información pública.
- Información interna.
- Información confidencial.
- Información restringida

4. Cumplimiento de seguridad en las SaaS

La plataforma puede proveer de características de análisis de seguridad y cumplimiento de Soluciones de SaaS. Los ámbitos en los que se debe actuar son:

- Gestion de configuraciones incorrectas.
- Seguridad del dato.
- Seguridad de la identidad.
- Riesgos de IA.
- Riesgos en accesos y descarga de datos.
- Detección de actividades maliciosas.
- Integraciones de terceros.

Ejemplos de soluciones SaaS que se deberían analizar: Microsoft 365, Okta, Teams, Salesforce, Teams, Active Directory, Jira y PowerApps entre otras.

E. INVENTARIO DE EQUIPAMIENTO A ANALIZAR

Listado de elementos que se encontrarán creados y que deberá cubrir el licenciamiento ofertado, sirviendo a su vez como guía de volumetría para establecer la cantidad de licencias necesarias:

Característica	Valor
Almacenamiento bloques (TB)	600
Azure SQL	10
Azure Storage Account	35
Azure Virtual Machine	10
Buckets S3	700
Clústeres Contenedores	4
EC2	600
ECR Image	75000
ECR repository	2400
Lambda function	900
RDS	600
Desarrolladores de IaC	10

F. SEGUIMIENTO Y GESTIÓN DEL SERVICIO

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

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

No obstante, el proveedor se compromete a aportar un sistema complementario, si el seguimiento de los indicadores de los acuerdos de nivel de servicio acordados inicialmente o, en su caso, del que resulte de modificaciones posteriores lo requiera. Este sistema complementario deberá ser autorizado, de manera previa y expresamente por Correos.

G. ACUERDOS DE NIVEL DE SERVICIO (ANS)

El proveedor adjudicatario deberá garantizar el cumplimiento de los siguientes niveles mínimos de servicio para la herramienta CSPM:

1. **DISPONIBILIDAD DEL SERVICIO**
   - **Disponibilidad mensual mínima**: 99.9%
   - **Medición**: Se calculará sobre el total de minutos del mes, excluyendo mantenimientos programados previamente notificados con al menos 48 horas de antelación.
2. **TIEMPO DE RESPUESTA ANTE INCIDENCIAS**
   - Respuesta en menos de 24 horas.
3. **ACTUALIZACIONES Y MANTENIMIENTO**

- **Actualizaciones de seguridad**: deben aplicarse en un plazo máximo de 7 días desde su publicación por el fabricante.
- **Mantenimientos programados**: deben ser comunicados con al menos 48 horas de antelación y no podrán superar las 4 horas consecutivas.

4. SOPORTE TÉCNICO

- **Horario de atención**: de lunes a viernes, de 08:00 a 20:00 (hora local).
- **Canales de soporte**: correo electrónico, portal web o teléfono.
- **Seguimiento de tickets**: acceso a histórico y trazabilidad de cada incidencia.

5. RENDIMIENTO DE LA HERRAMIENTA

- **Tiempo de detección de cambios en configuración cloud:** máximo 60 minutos.
- **Generación de informes de postura de seguridad:** en menos de 15 minutos para entornos de hasta 1.000 recursos.

H. PENALIZACIONES POR INCUMPLIMIENTO DE ANS

1. DISPONIBILIDAD DEL SERVICIO

- **Entre 99.0% y 99.89%**: penalización del **0.5% del importe mensual**.
- **Entre 98.0% y 98.99%**: penalización del **1% del importe mensual**.
- **Inferior al 98.0%**: penalización del **2% del importe mensual** y revisión contractual.
- **Dos meses consecutivos por debajo del 99.0%**: posibilidad de **resolución anticipada del contrato**.

2. TIEMPO DE RESPUESTA ANTE INCIDENCIAS

- **Retraso en respuesta a incidencias**: penalización de **300 € por cada día de retraso**, hasta un máximo de 3.000 € por incidencia.

3. ACTUALIZACIONES Y MANTENIMIENTO

- **Retraso en aplicación de actualizaciones de seguridad:** penalización de **1% del importe mensual por cada día de retraso, hasta un máximo de 5%.**
- **Mantenimientos no comunicados o fuera de horario acordado:** penalización de **500 € por evento.**

4. SOPORTE TÉCNICO

- **Falta de respuesta dentro del horario establecido**: penalización de **200 € por cada ticket sin respuesta en plazo**.
- **Falta de trazabilidad o seguimiento de tickets**: penalización de **500 € por cada incumplimiento documentado**.

6. RENDIMIENTO DE LA HERRAMIENTA

- **Superación de los tiempos máximos de detección o generación de informes**: penalización de **0.5% del importe mensual por cada métrica incumplida**, hasta un máximo de 2%.

I. Penalizaciones de ciberseguridad

Se impondrán penalizaciones al adjudicatario cuando incurra en alguna de las causas previstas a continuación.

Anexo definiciones

- Incidente de seguridad: Evento que tenga impacto en la confidencialidad e integridad de la información propiedad de Correos y/o sus partes interesadas, así como en la disponibilidad de los servicios, sistemas o recursos tecnológicos relacionados, ya sea de forma accidental o ilícita.
- Vulnerabilidad: Debilidad o fallo de un sistema, aplicación o solución que puede ser explotado por un atacante para causar un incidente de seguridad.
- CVSS: Estándar internacional empleado para calcular y clasificar la severidad de las vulnerabilidades de seguridad en sistemas de información mediante un modelo matemático basado en métricas definidas, que genera una puntuación numérica normalizada.
- CVE: Sistema estandarizado internacionalmente que permite identificar, definir y catalogar vulnerabilidades de seguridad en software y hardware, asignando un identificador único a cada vulnerabilidad.

1. Por incumplir las comunicaciones de incidentes de seguridad.

El adjudicatario deberá notificarle a Correos cualquier incidente de seguridad en el momento en el que sea detectado a través de los métodos que se establezcan con el adjudicatario al inicio del contrato. A estos efectos, el adjudicatario deberá cumplir con las siguientes obligaciones de comunicación:

- Primer comunicado: deberá enviarse de manera inmediata y como máximo dentro de la primera hora desde la detección del incidente, incluyendo la información esencial disponible en ese momento.
- Segundo comunicado: deberá remitirse en un plazo máximo de 1 hora desde el primer comunicado, incorporando la información adicional requerida por Correos.
- Tercer comunicado: deberá enviarse en un plazo máximo de 24 horas desde el segundo comunicado, ampliando el detalle técnico del incidente.
- Comunicaciones posteriores: mientras el incidente permanezca activo, será obligatorio remitir actualizaciones periódicas cada 3 horas, informando del progreso, los riesgos emergentes y el estado de la contención.

Todas las comunicaciones deberán realizarse obligatoriamente utilizando el formato oficial que Correos proporcionará tras la formalización del contrato, y siempre a través de los canales oficiales de comunicación designados para tal fin.
Una vez resuelto el incidente, el adjudicatario deberá entregar un informe forense en un plazo razonable, que incluya la información necesaria, como la descripción del incidente, su causa, alcance, medidas aplicadas y consecuencias, para que Correos pueda evaluar adecuadamente el incidente y verificar las medidas correctivas implementadas.
El incumplimiento de los plazos de comunicación, de la obligación de colaboración o de la entrega del informe final permitirá a Correos aplicar las penalizaciones correspondientes. En los casos de impacto grave o reiteración, dicho incumplimiento podrá considerarse causa suficiente para la resolución del contrato, sin perjuicio de la reclamación de daños y perjuicios y de la posible ejecución del aval de garantía.

Supuesto	Gravedad	Penalización (a criterio de Correos)
Incidente no comunicado y detectado por terceros o por Correos	Muy grave	10% facturación total de la adjudicación o 20.000€
Retraso en el primer comunicado	Muy grave	10% facturación total de la adjudicación o 20.000€
Retraso en el segundo comunicado	Muy grave	10% facturación total de la adjudicación o 10.000€
Ausencia de actualizaciones durante el incidente	Grave	5% facturación total de la adjudicación o 10.000€
No entrega del informe forense	Leve	3 facturación total de la adjudicación o 5.000€

2. **Por la detección de vulnerabilidades de ciberseguridad en procesos y soluciones internas de Correos**

No se admitirán productos, soluciones o desarrollos del adjudicatario que contengan vulnerabilidades conocidas y publicadas con un identificador CVE. En caso de detectarse cualquier vulnerabilidad publicada y catalogada en el CVE, Correos podrá considerarla como un incumplimiento, aplicándose las penalizaciones que correspondan en función de su severidad, evaluada conforme al estándar CVSS.

Supuesto	Gravedad	Penalización (a criterio de Correos)
Detectar 1 o más vulnerabilidades Críticas (CVSS ≥ 9.0)	Muy grave	5% facturación anual de la adjudicación o 10.000€
Detectar 1 o más vulnerabilidades Altas (7.0 ≤ CVSS < 9.0)	Muy grave	5% facturación anual de la adjudicación o 10.000€

Supuesto	Gravedad	Penalización (a criterio de Correos)
Detectar 5 o más vulnerabilidades Media (4.0 ≤ CVSS < 7.0)	Grave	3% facturación anual de la adjudicación o 5.000€
Detectar 10 o más vulnerabilidades Baja (CVSS < 4.0)	Leve	2% facturación anual de la adjudicación o 5.000€

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

Supuesto	Gravedad	Tiempo de resolución	Penalización
Vulnerabilidades Críticas (CVSS ≥ 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 Baja (CVSS < 4.0)	Leve	35 días	500€ por día de retraso

3. **Por la detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros.**

El adjudicatario deberá colaborar en la ejecución de las auditorías y pruebas técnicas de seguridad que Correos determine realizar sobre los sistemas, soluciones, desarrollos o servicios incluidos en el alcance del contrato. Estas auditorías y pruebas podrán comprender tests de vulnerabilidades, pruebas de intrusión, revisiones de bastionado seguro o cualquier otra actividad técnica que Correos necesite para verificar el cumplimiento de los requisitos de seguridad establecidos. En caso de que en el resultado de estas auditorías se detecten vulnerabilidades que superen los umbrales de la organización, Correos podrá aplicar las siguientes penalizaciones:

Supuesto	Gravedad	Penalización (a criterio de Correos)
Detectar 1 o más vulnerabilidades Críticas (CVSS ≥ 9.0)	Muy grave	5% facturación anual de la adjudicación o 10.000€
Detectar 1 o más vulnerabilidades Altas (7.0 ≤ CVSS < 9.0)	Muy grave	5% facturación anual de la adjudicación o 10.000€

Supuesto	Gravedad	Penalización (a criterio de Correos)
Detectar 5 o más vulnerabilidades Media (4.0 ≤ CVSS < 7.0)	Grave	3% facturación anual de la adjudicación o 5.000€
Detectar 10 o más vulnerabilidades Baja (CVSS < 4.0)	Leve	2% facturación anual de la adjudicación o 5.000€

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

Supuesto	Gravedad	Tiempo de resolución	Penalización
Vulnerabilidades Críticas (CVSS ≥ 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

4. **Por incumplir los requerimientos del servicio de gestión segura de la cadena de suministro.**

El adjudicatario estará obligado a atender las solicitudes de reuniones comunicadas por Correos en relación con la gestión segura de la cadena de suministro y con las auditorías de seguridad de la información, en un plazo máximo de 30 días naturales desde la fecha oficial de comunicación.
Cuando Correos requiera evidencias relativas a los procesos, medidas o controles de ciberseguridad implementados por el adjudicatario, incluyendo políticas internas, informes de auditoría, análisis de vulnerabilidades o cualquier otra documentación técnica, dichas evidencias deberán ser entregadas en un plazo máximo de 15 días naturales desde la solicitud. En aquellos casos en los que Correos solicite la realización de pruebas técnicas específicas, el adjudicatario deberá ejecutarlas y remitir las evidencias de sus resultados en un plazo máximo de 30 días naturales desde la solicitud.
Cuando en las evaluaciones o auditorías realizadas por Correos se detecten incumplimientos, controles insuficientes o desviaciones respecto a los requisitos de seguridad regulatorios o definidos en el contrato, el adjudicatario estará a obligado a corregir las no conformidades e implementar los controles necesarios en un plazo máximo de 90 días naturales desde la notificación oficial. No obstante, en el caso de no conformidades críticas, clasificadas con criterios objetivos y que puedan tener un impacto grave en la operativa de Correos, podrá exigirse un plazo de subsanación más reducido.

Supuesto	Gravedad	Penalización (a criterio de Correos)
No subsanar las no conformidades o no implementar los controles requeridos dentro del plazo de 90 días	Muy grave	10% facturación anual de la adjudicación o 20.000€
No ejecutar una prueba técnica específica o no entregar los resultados de esta dentro del plazo de 30 días	Grave	5% facturación anual de la adjudicación o 10.000€
No facilitar las evidencias necesarias para la auditoría o evaluación dentro del plazo de 15 días	Grave	5% facturación anual de la adjudicación o 10.000€
No asistir a una reunión dentro del plazo de 30 días	Leve	3% facturación anual de la adjudicación o 5.000€

5. **Por pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación.**

El adjudicatario estará obligado a mantener en vigor, durante toda la vigencia del contrato, todas las certificaciones de seguridad exigidas para su contratación por parte de Correos. En caso de producirse la pérdida, expiración o cualquier circunstancia que afecte a la validez de dichas certificaciones, el adjudicatario deberá comunicarlo formalmente a Correos en un plazo máximo de 72 horas desde el momento en que tenga conocimiento de ello. Junto a la comunicación, se deberá aportar un plan de remediación, detallando las acciones previstas y el calendario estimado para la recuperación o renovación de la certificación afectada.
La pérdida, caducidad o falta de renovación en plazo de cualquiera de las certificaciones obligatorias se considerará un incumplimiento de las condiciones contractuales, pudiendo dar lugar a la aplicación de las penalizaciones correspondientes en función de su gravedad.

Supuesto	Gravedad	Penalización (a criterio de Correos)
Retraso en la notificación de la pérdida/caducidad/suspensión de la certificación en el plazo de 72 horas	Muy grave	5% facturación anual de la adjudicación o 5.000€
Renovación de la certificación en más de 90 días naturales	Grave	3% facturación anual de la adjudicación o 3.000€
Renovación de la certificación en más de 60 días naturales	Grave	2% facturación anual de la adjudicación o 2.000€
Renovación de la certificación en más de 30 días naturales	Leve	1% facturación anual de la adjudicación o 1.000€

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

El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica en el **artículo 99.3 b) de la Ley 9/2017, de 8 de noviembre**, de Contratos del Sector Público (en adelante LCSP): ***"El hecho de que, la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución de este desde el punto de vista técnico"***

En este caso concreto, la no división del contrato en lotes se justifica por la necesidad de disponer de una solución integral, unificada y plenamente integrada que cubra de forma coordinada tanto la gestión de la postura de seguridad en la nube como la protección de cargas de trabajo. Ambas capacidades están estrechamente relacionadas y deben compartir información de contexto, inventarios de activos, configuraciones y eventos de seguridad para garantizar una detección eficaz de riesgos y una respuesta adecuada ante amenazas en entornos cloud. Una única solución permite una visión centralizada del riesgo, una gestión más eficiente, menor carga operativa y una mayor coherencia técnica, lo que redunda en una protección más eficaz y en una optimización de los recursos.

Se establece como **Presupuesto base de Licitación** (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de **326.700,00 EUROS (TRESCIENTOS VEINTISEIS MIL SETECIENTOS EUROS)**, de acuerdo con la siguiente distribución:

- **Base Imponible del Presupuesto base de Licitación** (excluido IVA o cualquier otro impuesto indirecto equivalente): de **270.000,00 EUROS (DOSCIENTOS SETENTA MIL EUROS).**
- **Importe del IVA** o cualquier otro impuesto indirecto equivalente: **56.700,00 EUROS (CINCUENTA Y SEIS MIL SETECIENTOS EUROS)**.

Año	Base Imponible de Licitación	Costes directos (84%)	Costes indirectos (10%)	Beneficio Industrial (6%)	IVA o impuesto indirecto equivalente	Presupuesto Base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2026	52.500,00 €	44.100,00 €	5.250,00 €	3.150,00 €	11.025,00 €	63.525,00 €
2027	90.000,00 €	75.600,00 €	9.000,00 €	5.400,00 €	18.900,00 €	108.900,00 €
2028	90.000,00 €	75.600,00 €	9.000,00 €	5.400,00 €	18.900,00 €	108.900,00 €
2029	37.500,00 €	31.500,00 €	3.750,00 €	2.250,00 €	7.875,00 €	45.375,00 €
TOTAL	**270.000,00 €**	**226.800,00 €**	**27.000,00 €**	**16.200,00 €**	**56.700,00 €**	**326.700,00 €**

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

Respecto a los Costes Directos que asumirá el prestador del servicio, se han estimado unos Costes Salariales del 0% por considerarse que los costes de las suscripciones suponen la totalidad de la carga económica del conjunto del suministro a contratar. En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes salariales están conformados únicamente por el gasto en personal. En la estimación de porcentaje se ha tenido en cuenta que, de manera general, los costes salariales están conformados únicamente por el gasto en personal. El Convenio Colectivo que se ha tenido en cuenta como referencia para el

cálculo económico es el XIX Convenio Colectivo Estatal de Empresas de Consultoría, de Tecnologías de la Información y Estudios de Mercado y de la Opinión Pública, publicado el pasado 16 de abril de 2025 en BOE (Disposición 7766 del BOE núm. 92 de 2025), con efectos desde el 01 de enero de 2025, vigente desde el 17 de abril de 2025 hasta el 31 de diciembre de 2027 (prorrogable). Además, se ha tenido en cuenta el grado de especialización y el catálogo de servicios contemplados en la presente contratación.

Además, se ha tenido en cuenta los servicios contemplados en la presente contratación.

Costes salariales (0%)	Costes servicios (100%)
- €	226.800,00 €

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

El Valor estimado del contrato (excluido IVA o impuesto indirecto equivalente): **270.000,00 EUROS (DOSCIENTOS SETENTA MIL EUROS).**

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

Valor Estimado del Contrato		
Importe de Licitación	36 MESES	270.000,00 €
Modificación 20%	NO	-
Prórrogas totales	NO	-
VALOR ESTIMADO DEL CONTRATO		**270.000,00 €**

No se contempla la opción de prorrogar o modificar la contratación.

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 suministros 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.
☐	Muestras, descripciones y fotografías de los productos a suministrar:
☐	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.
☒	Con el objetivo de garantizar la calidad, madurez y fiabilidad de la solución ofertada, **el licitador deberá presentan una declaración responsable** para acreditar esta solvencia y posteriormente, solo el propuesto como adjudicatario, acreditar documentalmente lo siguiente: 1. **Experiencia comprobada de al menos 5 años** en el desarrollo, comercialización o implementación de soluciones CSPM en entornos empresariales. Se deben acreditar mediante **2 Certificados de Buena Ejecución o declaraciones responsables firmadas**: • Documentos firmados por los responsables de IT/Seguridad de los clientes donde conste: fecha de inicio/fin, objeto del contrato y tamaño de la infraestructura gestionada (>500 empleados o >100 recursos). • Copia de contratos previos o facturas (omitir importes si es necesario) que demuestren que la solución se comercializa hace más de 5 años.

2. **Presencia activa de la herramienta en al menos 3 proyectos relevantes** de CSPM en organizaciones de tamaño medio o grande (más de 500 empleados o más de 100 recursos cloud gestionados), preferentemente en sectores regulados como financiero, salud, energía o administración pública.

3. **Presentación de al menos 2 casos de éxito documentados**, que incluyan:

   - Nombre del cliente (o sector si hay confidencialidad).
   - Alcance del proyecto.
   - Resultados obtenidos (reducción de riesgos, cumplimiento normativo, mejora de visibilidad, etc.).
   - Tiempo de implementación.

4. **Al menos 2 reconocimientos por parte de analistas independientes,** como inclusión en informes, de Gartner, Forrester, IDC u otros equivalentes, en la categoría de CSPM, CNAPP o seguridad cloud.

   - **Copia de los Informes:** El proveedor debe adjuntar el extracto o el gráfico (ej. el **Cuadrante Mágico de Gartner** o la **Forrester Wave**) donde la herramienta aparezca mencionada explícitamente en el periodo actual o los últimos 24 meses.
   - **Enlace de Verificación:** Enlaces directos a las notas de prensa de las consultoras o portales oficiales de los analistas.

5. **Al menos 2 certificaciones técnicas del producto**, tales como:

   - Copia en PDF de los certificados ENS, ISO/IEC 27001, SOC 2 Type II, CSA STAR o equivalente (los certificados deben estar en vigor).
   - Certificaciones específicas de los proveedores cloud (AWS Security Competency, Azure Advanced Specialization o equivalente). Se deberá adjuntar Captura de pantalla o diploma del portal de partners.

Se deberá incluir una **Matriz de Cumplimiento** donde el licitador indique cada punto y referencie el número de página del documento donde se encuentra la prueba.

Requisito Solicitado	**Documento de Respaldo (Evidencia)**	**Referencia (Pág/Anexo)**
Ejemplo: Experiencia > 5 años en desarrollo/implementación CSPM.	Certificado de Buena Ejecución / Contratos históricos.	Anexo I, Pág. 4

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 VIII.- Criterios de adjudicación de evaluación automática

Criterio de adjudicación 1			
Descripción	**Oferta económica**	Ponderación	**70 puntos**
Fórmula de valoración	PE= PEm (1 – ((Pon – Pse)/PL)) Donde: PE = Puntuación oferta "n" PEm = Ponderación asignada al criterio económica Pon = Presupuesto oferta "n" PSe = Presupuesto oferta más económica PL: Presupuesto de Licitación		

Criterio de adjudicación 2			
Descripción	**Características adicionales**	Ponderación	**30 puntos**
Fórmula de valoración	Se podrán obtener hasta 30 puntos adicionales por incluir en la oferta las siguientes características, descritas en el Anexo I punto D, con el siguiente reparto de puntos:		

Característica	Puntuación Máxima
Herramienta de Exposure Management	6
Gestión y análisis de la postura de seguridad de las aplicaciones creadas por Correos	6
Postura de seguridad a nivel del dato	6
Cumplimiento de seguridad en las SaaS	12

Herramienta de Exposure Management
Se podrán obtener hasta 6 puntos si se proporciona en la suscripción el análisis de assets de Correos expuestos a internet mostrando sus vulnerabilidades.

- Se recibirán 3 puntos si la herramienta contine capacidades de detección automática, configuración manual y proporciona recomendaciones mitigadoras, evaluándose mediante un criterio binario de presencia o ausencia.
- Se recibirán 3 puntos adicionales si este alcance es posible extenderlo a proveedores de Correos, según este reparto:
  - Entre 3 y 10 proveedores: 1 punto
  - Entre 11 y 20 proveedores: 2 puntos
  - 21 proveedores o más: 3 puntos

	Gestión y análisis de la postura de seguridad de las aplicaciones creadas por Correos Se podrán obtener hasta 6 puntos si se proporciona análisis de postura de seguridad de aplicaciones creadas de forma interna en Correos, con el siguiente reparto: • Análisis de repositorios de código en GIT: 2 puntos • Análisis de registro de contenedores: 2 puntos • Análisis de binarios mediante tecnología de Sandbox: 2 puntos. **Postura de seguridad a nivel del dato** Se podrán obtener hasta 6 puntos si se proporciona análisis de postura de seguridad en el dato con el siguiente reparto: • Análisis de BBDD relacionales: 1 punto. • Análisis de datos en almacenamiento de objetos: 1 punto. • Licencia para hasta el 50% de la capacidad de almacenamiento: 1 punto. • Licencia para hasta el 75% de la capacidad de almacenamiento: 2 puntos. • Licencia para hasta el 110% de la capacidad de almacenamiento: 3 puntos. • Licencia ilimitada: 4 puntos. **Cumplimiento de seguridad en las SaaS** Se podrán obtener hasta 12 puntos si se proporciona análisis de cumplimiento de seguridad en las siguientes SaaS: • Microsoft 365: 2 puntos. • Okta: 1 punto. • Teams: 0,5 puntos. • Salesforce: 2 puntos. • Jira: 1 punto. • Powerapps: 0,5 puntos. • Adobe Experience Manager: 2 puntos. • Red Hat OpenShift Container Platform: 1 punto. • Snowflake: 2 puntos.

Anexo IX.- Modelo de proposición económica.

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

En caso de actuar en representación

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

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

SERVICIO	IMPORTE (IMPUESTOS NO INCLUIDO) 3 años	IMPUESTOS	IMPORTE (IMPUESTOS INCLUIDOS) 3 años
Derechos de uso , en modalidad SaaS, de una plataforma especializada en gestión de postura de seguridad en la nube (CSPM) , de los servicos asociados y funcionalidades precisas durante 3 años.			
TOTAL			

* Todos los precios e importes deben reflejarse en euros y con dos decimales. El importe total ofertado y su desglose de importes deberá cuadrar al segundo decimal sin mediar redondeo. En caso de reflejar cualquier importe con más de dos decimales, o de que el desglose de importes no cuadre al segundo decimal al realizar las multiplicaciones y sumas, supondrá la exclusión de la oferta. No podrán superarse los importes máximos sin impuestos por servicio y anualidad indicados en el Anexo II- **Descripción y limitaciones a la licitación por lotes**, para cada uno de ellos, en caso de superarse ello supondrá la exclusión de la oferta. Esto mismo sucederá en caso de que la oferta total supere el importe máximo. El pago del servicio se efectuará conforme al epígrafe 9.3 Abonos al contratista. Facturación del presente pliego.

Lugar, fecha, sello del licitador y firma autorizada.

Anexo X.- Régimen de penalidades.

A). - INCUMPLIMIENTOS LEVES.

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Obligaciones generales	Incumplimiento de las obligaciones establecidas en este pliego y que no hayan sido tipificados como incumplimientos graves o muy graves	Hasta 1.000 euros
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, cuando no exceda del 3 por ciento del plazo.	☐ 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

B). - INCUMPLIMIENTOS GRAVES.

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, cuando no exceda del 5 por ciento del plazo.	☒ 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
Reincidencia	La comisión de una tercera infracción de carácter leve en el plazo de un año	Penalidad de hasta el 2 por ciento del precio del contrato, IVA excluido.
ANS	Incumplimiento de cualquiera de los ANS.	Lo indicado en el Anexo I del presente pliego

C). - INCUMPLIMIENTOS MUY GRAVES.

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

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Plazos	Por el incumplimiento de los plazos de ejecución total o parciales establecidos, o cuando la demora en el cumplimiento de aquellos haga presumir razonablemente la imposibilidad de cumplir el plazo total, o cuando superen el 5 por ciento del plazo.	☒ 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
cumplimiento defectuoso	Por el cumplimiento defectuoso de la prestación objeto del contrato	penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido, siempre y cuando el cumplimiento defectuoso no afectase a más del 20% de la prestación.
condiciones especiales de ejecución	Por el incumplimiento de condiciones especiales de ejecución	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.
Reincidencia	La comisión de una tercera infracción de carácter grave en el plazo de un año	Penalidad de hasta el 10 por ciento del precio del contrato, IVA excluido.

Anexo XI. Evaluación de proveedores.

Parámetro a Evaluar	Indicador	Valor objetivo	Nivel de cumplimiento
Penalizaciones	Incumplimientos que resultan en sanciones económicas u otras medidas	Evitar incumplimientos contractuales para mantener el rendimiento	100% - Cumple totalmente. 75% - Cumple parcialmente con observaciones menores. 50% - Cumple parcialmente con observaciones críticas. 0% - No cumple
ANS	Disponibilidad Operativa	Garantizar Grado de cumplimiento: Disponibilidad del 99.9%.	100% - Cumple totalmente. 75% - Cumple, con observaciones menores. 50% - Cumple, con observaciones críticas. 0% - No cumple

Anexo XII.- Declaración responsable del adjudicatario del contrato sobre la implantación e inscripción 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 inscrito.

☐ La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

Anexo XIII.- Requisitos de seguridad

1.1. Normativa y Conformidad.

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

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

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

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

Adicionalmente, para la adquisición de productos tecnológicos (de seguridad y comunicaciones), se deberá priorizar el uso de soluciones incluidas en la Guía CCN-STIC 105 o en el Catálogo de Productos y Servicios de Seguridad de las TIC (CPSTIC) con la finalidad de cumplir con el Esquema Nacional de Seguridad (ENS).

En caso de adquisición de productos no contemplados en dicho catálogo, podrán admitirse excepciones conforme a lo previsto en los artículos 16 y 19 del ENS, siempre que se justifique el cumplimiento de certificaciones de seguridad reconocidas (Common Criteria European Cybersecurity Certification Scheme (EUCC), Cyber Resilience Act (CRA), ISO15408, etc.) o disponer de unos niveles adecuados de madurez en materia de ciberseguridad, que deberán ser, como mínimo, los indicados en el anexo del pliego correspondiente a los Requisitos de seguridad exigidos por el Servicio de Ciclo de Vida de la Subdirección de Ciberseguridad.

1.2. Control de Acceso y SSO.

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

En el caso de que las aplicaciones tengan un modelo de arquitectura en la nube, el mecanismo de autenticación y autorización debe basarse en la federación de identidades. La infraestructura

de federación de identidades de Correos se fundamenta en el uso de protocolos OAuth 2.0 + OIDC o SAML2.0, integrados en una herramienta de mercado que garantiza el uso de estándares.

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

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

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

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

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

1.3. Respaldo y recuperación.

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

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

1.4. Comunicaciones.

Se deben definir protocolos ligeros, que no sobrecarguen las líneas de comunicaciones, que intercambien solo y exclusivamente la información necesaria para el fin que es recabada, que

posean mecanismos de cifrado de la información en tránsito, y que sean fácilmente procesables en un entorno de tiempo real como el que nos ocupa.

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

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

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

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

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

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

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

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

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

1.5. Integridad y confidencialidad

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

- Para datos en tránsito se debe utilizar la capa SSL/TLS, en su versión 1.3 o superior, para asegurar la integridad y confidencialidad de los datos transmitidos, siendo obligatorio su uso para todas las operaciones de administración y aquellas otras, que lo requiera el nivel de confidencialidad de la información transmitida.
- Para datos almacenados de carácter confidencial o secreto así como para las contraseñas y claves de cifrado nunca se deben almacenar en claro, debiendo aplicar mecanismos de cifrado robustos (AES 256, XML Encryption), y de integridad (RSA, SHA-2, XML Signature), se 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.
- Las operaciones necesiten Firma o Sello de tiempo usarán el Sistema Criptográfico Corporativo de Correos (S3C) para su ejecución.

1.6. Tratamiento de datos.

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

Se debe identificar un responsable de tratamiento, así como el tipo de datos que se tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.

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

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

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

1.7. Desarrollo Seguro.

El adjudicatario debe poder evidenciar el uso de estándares y recomendaciones de seguridad, sobre todo aquellos destinados a evitar ataques conocidos en aplicaciones expuestas a internet

(SQL Injection, XSS, etc.), garantizando así un nivel mínimo de seguridad en el desarrollo de la aplicación y el código utilizado, y cumpliendo así con las buenas prácticas vigentes en Correos. Se debe confirmar la realización de pruebas de seguridad periódicas en la solución ofertada.

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

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

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

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

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

1.8. 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.

1.9. Respuesta ante incidentes.

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

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

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

1.10. Auditabilidad.

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

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

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

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

1.11. Formación y concienciación.

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

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

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

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

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

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

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

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

Todo responsable de equipos de personas y de usuarios debe gestionar de forma activa el alta/baja de las personas de las que es responsable y de sus permisos asociados, así como de verificar y controlar un uso adecuado de las credenciales de acceso a los sistemas, personales e

intransferibles, debiendo velar por que el desarrollo del servicio se realice en todo momento conforme a unas buenas prácticas de seguridad de la información.

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

1.13. 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).

1.14. Uso de tecnología IA.

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

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

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

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

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