

Contrato de Servicios (Expediente núm. MT270303) <i>Contrato sometido a las Instrucciones internas de contratación del grupo Correos</i>			
☒ Procedimiento general		☐ Procedimiento especial	
☒ Ordinario	☐ Simplificado	☐ Con invitación a un único licitador	☐ Con invitación a varios licitadores

PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

1.	Entidad contratante.....	5
2.	Objeto del contrato.	5
3.	Duración del contrato.....	6
4.	Aspectos económicos.	7
5.	Condiciones de participación.	7
6.	Licitación del contrato.	9
6.1.	Comunicaciones y notificaciones electrónicas.....	9
6.2.	Resolución de consultas relacionadas con la licitación.	9
6.3.	Envío de ofertas por medios electrónicos.....	9
6.4.	Documentación confidencial.	10
6.5.	Adjudicación de los contratos	10
6.5.1.	Procedimiento General.....	10
6.5.1.1.	Procedimiento General Ordinario:.....	10
6.6.	Contenido de las ofertas.....	11
6.6.1.	Sobre A: documentación administrativa.	11
6.6.2.	Sobre C: Criterios de adjudicación de evaluación automática o con arreglo a fórmulas matemáticas y/o proposición económica.	11
7.	Adjudicación y perfección del contrato.	12
7.1.	Procedimiento de apertura de sobres y valoración de ofertas.....	12
7.2.	Ofertas anormalmente bajas.....	13
7.3.	Documentación para presentar por el propuesto como adjudicatario.	13

7.4. Adjudicación del contrato.....	14
7.5. Perfección del contrato.....	14
7.6. Constitución de garantías	14
8. Ejecución del contrato.	15
8.1. Obligaciones del adjudicatario.	15
8.1.1. Obligaciones en materia fiscal, laboral y medioambiental.....	15
8.1.2. Obligaciones relativas a la gestión de permisos, licencias y autorizaciones.....	16
8.1.3. Obligaciones del adjudicatario en materia de protección de datos	16
8.1.4. Aceptación y adhesión a las políticas de prevención de imputaciones delictivas.	17
8.1.5. Evaluación de proveedores.	18
8.1.6. Obligaciones esenciales del contrato.....	18
8.1.7. Condiciones especiales de ejecución.	20
8.1.8. Régimen de confidencialidad.	21
8.2. Modificaciones del contrato.....	22
8.3. Cesión y Subcontratación.	22
8.3.1. Cesión del contrato.....	22
8.3.2. Régimen de subcontratación.....	22
9. Cumplimiento del contrato.	23
9.1. Responsable del contrato. Representante del contratista.....	23
9.2. Régimen de penalidades.....	23
9.3. Abonos al contratista. Facturación.	24
9.4. Recepción y liquidación.	25
9.5. Plazo de garantía.....	25
10. Resolución del contrato.....	25
10.1. Causas de resolución.	25
10.2. Procedimiento.....	26
11. Protección de Datos.....	26
11.1 Cláusula informativa de protección de datos personales recabados a través del Canal Ético.....	26
11.2 Información a representantes, trabajadores y personas de contacto	26
12. Régimen jurídico del contrato y reclamaciones contra este pliego.....	27
Anexo I.- Características técnicas específicas del contrato.....	29

1	ÁMBITO TECNOLÓGICO Y ALCANCE DEL CONTRATO	29
1.1	Componentes integrados y dependencias tecnológicas	29
2	SERVICIO DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN	30
3	DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN	30
3.1	Inventario base del objeto de mantenimiento y volumetrías de referencia. .	31
3.2	Pila tecnológica mínima para cubrir por el servicio.....	33
3.3	Catálogo de Prestaciones.....	35
4	CONDICIONES DE PRESTACIÓN DEL SERVICIO	41
5	REPORTE, SEGUIMIENTO Y ENTREGABLES	43
6	PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS	44
7	FASES DE LA PRESTACIÓN DE LOS SERVICIOS	45
7.1	Fase de lanzamiento o asimilación del servicio	45
7.2	Fase de prestación del servicio	47
7.3	Fase de traspaso o finalización del servicio	48
8	PUESTOS CLIENTES DEL EQUIPO DE TRABAJO	48
9	ECOSISTEMA SOFTWARE	49
	Anexo II.- Descripción y limitaciones a la licitación por lotes.	50
	Anexo III.- Resumen de metodología seguida para el cálculo del valor estimado del contrato.....	51
	Anexo IV.- Forma de acreditación de la solvencia económica y financiera, y técnica o profesional.	53
	Anexo V.- Modelo de aval.	55
	Anexo VI. - Instrucciones y recomendaciones para la presentación electrónica de las ofertas.	56
	Anexo VII.- Instrucciones para cumplimentar el DEUC.	57
	Anexo VIII.- Criterios de adjudicación cuya evaluación depende de un juicio de valor.	60
	Anexo IX.- Criterios de adjudicación de evaluación automática	61
	Anexo X.- Modelo de proposición económica.....	71
	Anexo XI.- Régimen de penalidades.	73
	Anexo XII – Evaluación de Proveedores.....	78
	Anexo XIII.- Declaración responsable del adjudicatario del contrato sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.	86

Anexo XIV. - Adscripción de medios.	87
Anexo XV. Compromiso de adscripción de personal al contrato.....	90
Anexo XVI -Requerimientos Arquitectura	91
Anexo XVII– Requerimientos Ciberseguridad.....	109
Anexo XVIII –Requerimientos Gobierno del Dato	118
Anexo XIX–Requerimientos Calidad	119
Anexo XX–Requerimientos Oficina de Proyectos.....	123
Anexo XXI – Requisitos Formación.....	125
Anexo XXII – Declaración responsable en materia de protección de datos.....	129
Anexo XXIII – Cláusula sobre el uso de IA en contratos con Correos	134
Anexo XXIV.- Modelo de contrato de encargo de tratamiento de datos personales.	139

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

1. Entidad contratante.

Entidad contratante	Sociedad Estatal Correos y Telégrafos, S.A. S.M.E.
Órgano de contratación	Comité de Inversiones
Dirección/Subdirección gestora de la necesidad UGC	Dirección de Tecnología y Transformación Digital Subdirección de Transformación Tecnológica UGC28 – Dirección de Organización, Tecnología e Innovación
Perfil de contratante	https://www.correos.com/perfil-contratante/
Dirección de contacto	C/Conde de Peñalver,19 Bis. 28006, Madrid.
Responsable del contrato	Dirección de Tecnología Subdirección de Transformación Tecnológica Área Inteligencia Artificial y Analítica de Datos Responsable: jefa de Área Inteligencia Artificial y Analítica de Datos.
	Datos de contacto: expdtesit@correos.com

2. Objeto del contrato.

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

Descripción	El presente contrato tiene como objeto la contratación de un servicio especializado de mantenimiento y soporte de RPA/Hiperautomatización para los procesos automatizados que actualmente opera la plataforma UiPath en la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. (en adelante, “Correos”), en el marco de la operación tecnológica de las automatizaciones RPA/Hiperautomatización en Correos.
Código CPV	72261000-2 (Servicios de apoyo al software). 72253000-3 (Servicios de unidad de asistencia y de apoyo). 72260000-5 (Servicios relacionados con el software).
Lotes	☒ NO ☐ SI (Ver Anexo II) El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica en el artículo 99.3 b) LCSP, “ <i>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</i> ”. Esta decisión se fundamenta en los siguientes motivos técnicos y organizativos:

	Unidad técnica y operativa del servicio: el mantenimiento y soporte de RPA/Hiperautomatización exige una gestión integrada (incidencias, operación, monitorización, cambios y soporte) sobre un ecosistema común (automatizaciones, componentes de ejecución y control), lo que requiere responsabilidad única e integral para evitar vacíos de alcance y conflictos de atribución. Riesgo de fragmentación del soporte y degradación del servicio: la división en lotes incrementaría los puntos de coordinación y las dependencias entre adjudicatarios (especialmente en incidentes críticos), elevando el riesgo de dilatación de tiempos, falta de trazabilidad en la resolución “punta a punta” y dificultades para aplicar mecanismos de control de calidad del servicio. Proporcionalidad y concurrencia: la configuración como lote único no restringe indebidamente la competencia, dado que el mercado dispone de operadores con capacidad para prestar el servicio completo; y, además, la agrupación evita una arquitectura contractual artificiosa que encarecería la coordinación sin aportar valor.
¿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	13	☐ días ☒ meses ☐ años	☒ a partir del día que se indique en el documento de aceptación de la Resolución de adjudicación ☐ día siguiente a la comunicación de inicio del contrato por la entidad contratante ☐ la fecha que figure en la resolución de la adjudicación

Prorrogable	☐ NO ☒ SI	N.º de prórrogas: Duración máxima de cada prórroga (en meses)	1 Hasta 3 meses
En caso de acordarse, la prórroga será obligatoria para el contratista, siempre y cuando se le notifique con dos meses de antelación al vencimiento. Se condiciona la prórroga del contrato a que sus características permanezcan inalterables.			

Ver fases de prestación del servicio [Anexo I.](#)

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Valor estimado del contrato	168.125,00 €	Ciento sesenta y ocho mil ciento veinticinco euros con cero céntimos, conforme al método de cálculo especificado en Anexo III		
Presupuesto base de licitación (IVA o impuesto indirecto equivalente incluido)	162.745,00 €	IVA/impuesto equivalente		28.245,00 €
Anualidades (IVA o impuesto indirecto equivalente incluido)	2027	2028	TOTAL	
	156.056,85 €	6.688,15 €	162.745,00 €	

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.

Solvencia económica o financiera	☒ Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, de al menos 168.125,00 €.			
	☐ Otros:			
	... Sobre la forma de acreditar estos requisitos, ver Anexo IV En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote			
		LOTE 1	LOTE 2	LOTE 3

	Porcentaje/Cifra volumen anual negocio.			
	☐ Responsabilidad solidaria de la ejecución del contrato de las entidades que completan la solvencia económica y financiera del licitador			
Solvencia técnica o profesional	☒ La relación de los servicios realizados de igual o similar naturaleza que los que constituyen el objeto del contrato en los tres últimos años, cuyo importe anual acumulado en el año de mayor ejecución sea igual o superior al 70 por ciento de la anualidad media del contrato, esto es 117.687,50 €. ☐ Haber realizado servicios de igual o similar naturaleza que los que constituyen el objeto del contrato en los tres últimos años, cuyo importe anual acumulado en el año de mayor ejecución sea igual o superior a €. ☐ Disponibilidad de los siguientes perfiles relativos al personal: ... ☐ Cumplimiento de las medidas de aseguramiento de la calidad durante la ejecución del contrato que a continuación se relacionan: ... ☐ Acreditación del cumplimiento de las siguientes medidas de gestión medioambiental: ... ☐ Disponibilidad de la siguiente maquinaria, material y equipo técnico: ... 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			
Habilitación Profesional	Para ser adjudicatario del contrato, el licitador, así como otros servicios de terceros que se incluyan en la oferta, deberá prestar los servicios conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), y aportar certificación acreditativa para la categoría BÁSICA. Para la acreditación, se presentará copia del Certificado de Conformidad, o en su caso, Declaración de Conformidad con el ENS, en la categoría indicada y con el alcance que abarquen al menos los sistemas de información que soporten los servicios prestados, ver Anexo IV.			
Compromiso de adscripción de medios	☒ Sí. Medios para adscribir: Los licitadores deberán comprometer la adscripción de los medios personales necesarios para la correcta ejecución del contrato, de acuerdo con el alcance y las características del servicio de mantenimiento y soporte RPA/Hiperautomatización objeto del presente Pliego, ver Anexo XV. Dicho compromiso de adscripción tendrá carácter contractual y será exigible durante toda la vigencia del contrato, incluidas, en su caso, las prórrogas, debiendo garantizarse que los medios adscritos cuentan con la			

	capacitación, experiencia y dedicación adecuadas para asegurar la continuidad operativa y la correcta prestación del servicio, ver Anexo XIV. <table border="1"> <thead> <tr> <th>PERFIL</th><th>FTE</th></tr> </thead> <tbody> <tr> <td>Jefe de Proyecto / Responsable del Servicio</td><td>0,5</td></tr> <tr> <td>Especialistas RPA/Hiperautomatización (perfil mixto funcional-técnico)</td><td>2 al 100%</td></tr> </tbody> </table> El detalle de los perfiles, dedicaciones mínimas y condiciones de adscripción se recogerá en el Anexo correspondiente de Adscripción de Medios, sin perjuicio de las facultades de control y seguimiento que corresponden a Correos durante la ejecución del contrato, ver Anexo XIV. ☐ No. No aplica.	PERFIL	FTE	Jefe de Proyecto / Responsable del Servicio	0,5	Especialistas RPA/Hiperautomatización (perfil mixto funcional-técnico)	2 al 100%
PERFIL	FTE						
Jefe de Proyecto / Responsable del Servicio	0,5						
Especialistas RPA/Hiperautomatización (perfil mixto funcional-técnico)	2 al 100%						

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

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

6. Licitación del contrato.

6.1. Comunicaciones y notificaciones electrónicas.

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

6.2. Resolución de consultas relacionadas con la licitación.

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

Los licitadores, podrán subir sus preguntas a la Plataforma de Contratación del Sector Público hasta días 6 días naturales antes de la finalización del plazo para la presentación de ofertas.

6.3. Envío de ofertas por medios electrónicos.

Las ofertas se presentarán en plazo de 30 días naturales. Dicho plazo será también señalado en el anuncio de licitación publicado en el perfil de contratante o en la invitación remitida.

Los licitadores, a excepción del Procedimiento Especial con un único licitador, deberán presentar obligatoriamente sus ofertas de forma electrónica a través de la Plataforma de

Contratación de Correos (<https://pcc.correos.es/licitacion/licitaciones>) utilizando para ello la “Herramienta de Preparación y Presentación de Ofertas” que desde esa plataforma se pone a su disposición (ver instrucciones y recomendaciones en [Anexo VI](#)).

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

6.4. Documentación confidencial.

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

6.5. Adjudicación de los contratos

6.5.1. Procedimiento General

6.5.1.1. Procedimiento General Ordinario:

A. Sin negociación:

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

La elección del procedimiento general se justifica en los siguientes términos:

- 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).

Por tanto, se elige este procedimiento por entender que es el más adecuado, ya que se pretende que cualquier empresario interesado que cumpla con los requisitos de estipulados en el Pliego de Condiciones Técnicas y Particulares pueda presentar su oferta, siendo por tanto el procedimiento que mejor se ajusta a los principios que rigen la contratación del sector público..

☒ Criterio de Adjudicación: MEJOR RELACIÓN CALIDAD-PRECIO.

La adjudicación se realizará atendiendo a la mejor relación calidad-precio, sobre la base de una pluralidad de criterios objetivos. La puntuación final estará compuesta por la suma de los criterios técnicos (evaluables mediante fórmula automática) y el criterio económico.

La puntuación final estará compuesta por la suma de la puntuación asignada en los criterios sujetos a juicio de valor y los criterios evaluables mediante fórmula o automáticamente.

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

Tipología	Criterio	Ponderación
Criterios sujetos a un juicio de valor	Técnico	0%
Criterios evaluables mediante fórmula o automáticamente (Anexo X)	Técnico	30%
	Económico	70%

6.6. Contenido de las ofertas.

6.6.1. Sobre A: documentación administrativa.

- 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.
- En su caso, compromiso de adscripción de medios, según lo indicado en el Apartado 5 y [Anexo XIV](#) de Compromiso de adscripción de personal del contrato y el [Anexo XV](#) compromiso de adscripción del personal.
- 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).
- 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 de este.
- 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.
- 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.
- Declaración responsable en materia de Protección de Datos (Anexo XVII).

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

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

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

La documentación que incluya los valores de los criterios de adjudicación cuya evaluación puede realizarse de manera automática deberá presentarse en archivo electrónico, varias carpetas, comprimidas si no es posible por tamaño, con el nombre “SOBRE Nº C”, en archivo ejecutable con formatos *.pdf. La documentación que constituya la oferta técnica de evaluación automática deberá presentarse de forma separada a la proposición económica.

Todos los precios e importes deben reflejarse con dos decimales. El importe total sin impuestos ofertado y la suma de su desglose de importes, deberá cuadrar al segundo decimal sin mediar redondeo. No podrán superarse los importes máximos sin impuestos por servicio indicados en el Anexo III.- Resumen de metodología seguida para el cálculo del valor estimado del contrato, en caso de superarse, supondrá la exclusión de la oferta. El importe total ofertado sin impuestos no podrá superar el importe de la base imponible del presupuesto base de licitación, indicado en el Anexo III, en caso de superarse, supondrá la exclusión de la oferta.

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.

La proposición económica deberá excluir cualquier importe, línea, precio hora, hito o concepto de cobro asociado a la fase de asimilación.

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 naturales. Únicamente podrá subsanarse la falta de acreditación de requisitos exigidos, siempre que éstos existan al fin del plazo de presentación de las proposiciones.

Se hace constar la imposibilidad de subsanar la documentación referida a la proposición económica y criterios de adjudicación mediante la aportación de determinada documentación exigida en los Pliegos que no se presentó inicialmente.

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

La evaluación de las ofertas conforme a los criterios cuantificables mediante la mera aplicación de fórmulas se realizará 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.

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

7.2. Ofertas anormalmente bajas.

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

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

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 para 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.
☐	Otros

En los supuestos en que la propuesta de adjudicación de un contrato recaiga sobre una unión de empresarios o sobre una agrupación de estos con el compromiso de constituir una sociedad, el plazo para presentar la documentación será de veinte días hábiles.

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

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

7.4. Adjudicación del contrato.

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

7.5. Perfección del contrato.

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

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

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

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

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

7.6. Constitución de garantías

RÉGIMEN DE GARANTÍAS		
		Si el licitador la constituye mediante aval, deberá utilizar el

Constitución de garantía definitiva	☒ 5% del importe de adjudicación del contrato o el lote o lotes adjudicados (IVA excluido).		modelo incluido como Anexo V . Si utiliza otro medio, consultará las condiciones que debe reflejar el documento de constitución con la entidad contratante.
			Además de por la correcta ejecución del contrato, la garantía definitiva responderá de los daños y perjuicios que se ocasionen a la entidad contratante y de los gastos que puedan derivarse de las reclamaciones fehacientes de cumplimiento o ejecución de las garantías, así como por los restantes conceptos indicados en el artículo 110 de la LCSP.
Constitución de garantía complementaria	☐ NO ☒ SI	Importe	☒ 5% sobre el importe de adjudicación (en caso de oferta temeraria) (IVA excluido).

Cuando varíe el importe del contrato por cualquier causa, el contratista vendrá obligado a ajustar el importe de las garantías constituidas en la proporción que corresponda en el plazo de 10 días hábiles desde que se le notifique la causa determinante de la variación del importe del contrato. De no cumplirse este requisito por causas imputables al contratista en el plazo establecido, la entidad contratante podrá resolver el contrato, con pérdida de la garantía que tuviera constituida el contratista.

En el caso de que se impongan penalidades al contratista y deban hacerse efectivas contra la garantía definitiva constituida, el adjudicatario quedará obligado a reponer esta garantía en los diez días hábiles siguientes a que se comunique la ejecución de la garantía inicial

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

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

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

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

8. Ejecución del contrato.

8.1. Obligaciones del adjudicatario.

8.1.1. Obligaciones en materia fiscal, laboral y medioambiental.

Serán de cuenta del contratista todos los tributos de cualquier índole que graven las

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

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

Para la ejecución de este contrato:

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

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

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

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

8.1.3. Obligaciones del adjudicatario en materia de protección de datos

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

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

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

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

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

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

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

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

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

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

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

Lugar de prestación de servicios objeto la licitación.

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

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

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

Cada una de las partes será responsable del incumplimiento de las obligaciones que le correspondan, según lo previsto en el mismo, respondiendo los daños y perjuicios que pudiesen ocasionarse, y en especial de las sanciones que les pudiera imponer la Agencia Española de Protección de Datos o cualquier otro órgano competente ya sea español o europeo, como consecuencia del incumplimiento de las obligaciones establecidas en el presente Pliego.

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

La empresa adjudicataria vendrá obligada a contar con una política propia de prevención de

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

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

8.1.5. Evaluación de proveedores.

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

8.1.6. Obligaciones esenciales del contrato.

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

☒	Mantenimiento de adscripción de medios personales o materiales
☐	Condiciones especiales de ejecución del contrato
☒	Aspectos que se hayan considerado como criterios de adjudicación
☒	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
☒	El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento “programa de prevención de riesgos penales” accesible a través de la web: https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf
☒	Las relativas al tratamiento de dato personales y al sometimiento a la normativa nacional y europea en la materia.
☒	Deber de confidencialidad sobre los datos o antecedentes que, no siendo públicos o notorios, estén relacionados con el objeto del contrato, o que el contratista conozca con ocasión de su ejecución. Cumplimiento de la normativa de protección de datos

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

Condición esencial	Frecuencia	Forma de acreditación del cumplimiento
Mantenimiento del compromiso de adscripción de medios personales o	Semestralmente.	Acreditación mediante informe emitido por el adjudicatario, en el que se detalle la adscripción

materiales		efectiva de los medios personales y materiales al contrato, acompañado de evidencias documentales que acrediten dicha adscripción (contratos laborales, informes de vida laboral o documentación equivalente, certificaciones y relación de recursos adscritos), que permitan verificar el cumplimiento de los requisitos establecidos en el Pliego.
Criterios de adjudicación	Mensual	Informes de seguimiento, comprobación de entregables, certificados de formación, solicitud de partes de servicio.
El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista	Anual	Un documento que refleje el cumplimiento del programa de prevención de riesgos penales
Tratamiento de datos personales	Anual	Verificación del cumplimiento de las obligaciones en materia de protección de datos conforme a lo establecido en el Apartado 8.1.3 y en el Anexo XXVII (Contrato de Encargo de Tratamiento), mediante la revisión de las evidencias técnicas (protocolos de cifrado, controles de acceso, copias de seguridad) y organizativas (políticas de teletrabajo, acuerdos de confidencialidad de los empleados)., registros que prueben que has respondido a las solicitudes de acceso, rectificación, supresión o portabilidad (Derechos ARCO) dentro de los plazos legales y medidas de seguridad aplicables mediante un registro interno de incidentes que documente cómo se detectó y notificó cualquier

		fuga de datos, tanto a la autoridad competente como a los afectados. [1, 2].
Deber de confidencialidad sobre los datos o antecedentes que, no siendo públicos o notorios, estén relacionados con el objeto del contrato, o que el contratista conozca con ocasión de su ejecución.	Semestralmente	Documento firmado por la empresa adjudicataria que recoja el cumplimiento de la normativa de protección de datos vigente.
Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales	Semestralmente	La relación de subcontratistas y sus condiciones de pago y la relación de facturas abonadas.

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

8.1.7. Condiciones especiales de ejecución.

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

☐	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
☐	El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento “programa de prevención de riesgos penales” accesible a través de la web https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf
☐	La suscripción de un seguro de responsabilidad civil por los daños que pueda causar el contratista, su personal, subcontratistas o proveedores, por un importe mínimo de ...euros.
☐	Establecimiento de un plan de formación para los empleados adscritos a la ejecución del contrato en materias relacionadas con: ☐ Prevención de riesgos laborales específicos en el marco del servicio a prestar ☐ Otro

☐	Establecimiento de un sistema de gestión diferenciada para los residuos que pueda generar la prestación del servicio.
☐	Establecimiento de medidas que garanticen la igualdad de trato y no discriminación, así como la inclusión de miembros de grupos vulnerables.
☒	Condición de carácter social: Emplear en la ejecución del contrato un porcentaje de trabajadores fijos igual o superior al 20 por 100.
☒	Sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos. Destrucción de datos: Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado. No obstante, el adjudicatario encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

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.	Anualmente.	A través de registro de empleados.
Sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.	A la finalización	Informe evaluación

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

8.1.8. Régimen de confidencialidad.

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

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

plazo mayor.

8.2. Modificaciones del contrato.

En el presente contrato

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

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

8.3. Cesión y Subcontratación.

8.3.1. Cesión del contrato

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

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

8.3.2. Régimen de subcontratación.

Subcontratación permitida:

☐ NO ☒ SI

El contratista podrá concertar con terceros la realización 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:

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

No obstante, dicha subcontratación no exime al adjudicatario del cumplimiento íntegro de las condiciones contractuales, incluyendo la obligación de garantizar la adscripción efectiva de

medios, la cobertura del horario de prestación del servicio, los ANS y el resto de los requisitos operativos establecidos. Asimismo, el adjudicatario será responsable de asegurar que cualquier tercero subcontratado cumple dichas condiciones.

En todo caso, la subcontratación no podrá suponer una degradación en las condiciones de prestación del servicio, debiendo garantizarse en todo momento el cumplimiento de los horarios, niveles de servicio, adscripción de medios y requisitos operativos establecidos en el pliego.

9. Cumplimiento del contrato.

9.1. Responsable del contrato. Representante del contratista.

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

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

9.2. Régimen de penalidades.

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

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

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

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

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

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

El pago de las penalizaciones no sustituirá al resarcimiento de daños y perjuicios por incumplimiento del adjudicatario, ni eximirá de cumplir con las obligaciones contractuales,

pudiendo exigirse, conjuntamente el cumplimiento de dichas obligaciones y la satisfacción de las penas pecuniarias estipuladas que se imputarán a factura y/o fianza, sin perjuicio de poder optar por la resolución del contrato y la reclamación de daños y perjuicios al adjudicatario.

9.3. Abonos al contratista. Facturación.

El pago del servicio, al tratarse de suscripciones, se efectuará al comienzo de la contratación previa presentación de la correspondiente factura. Para el pago de facturas giradas por el adjudicatario, la entidad contratante utilizará los siguientes medios de pago:

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

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

Las facturas contendrán la información establecida en la normativa que resulte de aplicación, y se tramitarán por vía electrónica con arreglo a las siguientes especificaciones y formato:

- Se requiere que el proveedor adjudicatario del contrato gestione la facturación de este 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/Item

		ms/InvoiceLine/AdditionalLine ItemInformation
--	--	--

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.

La fase de asimilación constituye un periodo de transferencia de conocimiento y solapamiento de equipos, que no genera devengo ni facturación para el adjudicatario entrante.

9.4. Recepción y liquidación.

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

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

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

La validación de la fase de asimilación se acreditará mediante acta técnica de evaluación y aceptación. Esta recepción no genera liquidación económica ni derecho de cobro, al tratarse de un periodo no facturable para el adjudicatario entrante.

9.5. Plazo de garantía.

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

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

10. Resolución del contrato.

10.1. Causas de resolución.

Serán causa de resolución del contrato:

☒	Las previstas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☒	El incumplimiento de obligaciones calificadas expresamente como «esenciales» en este Pliego, de acuerdo con lo establecido en el Apartado 8.1.6.

☒	Cuando teniendo que llevar a cabo una modificación en el mismo que, no estando prevista en el pliego, no concurrieran las circunstancias establecidas en el artículo 205 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☒	La imposición de penalidades por demora en la ejecución, cada vez que alcancen un múltiplo del 5 por 100 del precio del contrato, IVA excluido,
☒	El cumplimiento defectuoso de la prestación, cuando afecte a más del 20% de dicha prestación.
☒	El incumplimiento por el contratista de los plazos de pago a sus proveedores o subcontratistas
☒	La falta de renovación o prórroga de la Póliza de seguro de responsabilidad civil, en los casos en que fuera exigible o lo hubiera ofrecido el adjudicatario.
☒	El desistimiento de la ejecución del servicio por la entidad contratante por circunstancias sobrevenidas, aun cuando se hubiera comenzado dicha ejecución.
☒	Incumplimiento de las condiciones especiales de ejecución, de modo que se frustre el objeto del contrato.
☒	No superar la fase de asimilación o lanzamiento del contrato, de acuerdo con lo previsto en las cláusulas 7.1 y 7.2 del Anexo I del presente Pliego.

10.2. Procedimiento

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

11. Protección de Datos

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

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

Para Correos:

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

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

11.2 Información a representantes, trabajadores y personas de contacto

Los datos de carácter personal de las personas de contacto de los licitantes y, en su caso, de sus trabajadores serán tratados por la entidad contratante con la finalidad de gestionar su participación en la presente contratación, y en caso de resultar adjudicatario del contrato, con la finalidad de gestionar la relación contractual que se formalice entre las partes, siendo la base legitimadora del tratamiento la ejecución del contrato y el cumplimiento de la normativa de

aplicación. En este sentido, le informamos que los datos facilitados no se cederán a terceros, salvo obligación legal.

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

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

Para Correos:

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

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

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

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

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

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

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

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

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos
☒	Aceptación 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

En Madrid, a 22 de julio de 2026

LA RESPONSABLE DE
ÁREA INTELIGENCIA ARTIFICIAL Y ANALÍTICA
DE DATOS

LA SUBDIRECTORA DE
TRANSFORMACIÓN TECNOLÓGICA

Fdo.: Ana Isabel Estévez Maestre

Fdo.: Cristina Cid Gil

VºBº

LA DIRECTORA DE TECNOLOGÍA Y TRANSFORMACIÓN DIGITAL DE CORREOS

Fdo.: Cristina Tarrero Martos

Anexo I.- Características técnicas específicas del contrato.

1 ÁMBITO TECNOLÓGICO Y ALCANCE DEL CONTRATO

El objeto del presente contrato consiste en la prestación de un servicio especializado de mantenimiento y soporte de automatizaciones RPA/Hiperautomatización, actualmente en explotación en Correos, basadas en la plataforma UiPath, desplegada en infraestructura de la organización.

El servicio tiene como finalidad garantizar la continuidad operativa, la estabilidad técnica y el correcto funcionamiento de los procesos automatizados existentes, mediante actuaciones de soporte, operación, monitorización y mantenimiento técnico de las automatizaciones y de los componentes de ejecución, orquestación y supervisión propios de la plataforma UiPath.

El ámbito tecnológico del contrato se circunscribe exclusivamente al entorno RPA/Hiperautomatización de Correos. La operación de la infraestructura tecnológica subyacente (sistemas, servidores, bases de datos y demás elementos de entorno) corresponde a los servicios internos de Explotación de Correos, debiendo el adjudicatario coordinarse con dichos servicios cuando resulte necesario.

1.1 Componentes integrados y dependencias tecnológicas

Sin perjuicio de que la plataforma RPA/Hiperautomatización se basa en UiPath, las automatizaciones RPA/Hiperautomatización en producción pueden depender de otros componentes corporativos (p. ej., capas de integración, aplicaciones de negocio o servicios auxiliares).

A efectos del presente contrato, dichas dependencias se consideran incluidas únicamente en lo necesario para asegurar la continuidad operativa de las automatizaciones RPA/Hiperautomatización y la resolución de incidencias asociadas a su ejecución. El adjudicatario realizará el diagnóstico técnico, aportará evidencias y coordinará/escalará con los equipos responsables cuando proceda, pero no asumirá el mantenimiento general, administración, evolución ni gobierno de plataformas o productos ajenos al ámbito RPA/Hiperautomatización.

La coordinación con Explotación y con los equipos responsables de componentes dependientes se realizará conforme al modelo de gestión de incidencias y cambios definido en el presente Pliego, en particular en el Anexo I – apartados “Mantenimiento permanente de sistemas”, “Resolución de incidencias”, “Gestión de problemas” y “Coordinación, control y seguimiento de los servicios”.

El presente contrato tiene un alcance exclusivamente de servicios, quedando expresamente excluidos:

- el suministro, renovación o gestión de licencias,
- el desarrollo de nuevas automatizaciones,
- la incorporación de nuevas funcionalidades,

- cualquier evolución funcional o tecnológica distinta de las actuaciones estrictamente necesarias para garantizar la continuidad operativa de las automatizaciones existentes y que no esté incluida entre las tareas identificadas dentro del mantenimiento correctivo, preventivo, perfectivo o adaptativo.

El servicio contempla la atención de incidencias en régimen de disponibilidad 24x7 exclusivamente para aquellas que tengan la consideración de críticas, manteniéndose la prestación ordinaria del servicio en horario laboral.

Además, el servicio puede tener que realizar intervenciones planificadas fuera del horario laboral en aquellos casos en los que por necesidades técnicas y/o de negocio no puedan ser realizadas en el horario laboral del servicio (por ejemplos validaciones por upgrades de sistemas operativos, nuevas versiones de aplicaciones de terceros con las que se integran los robots, tareas planificadas requeridas por los equipos de arquitectura, explotación, ciberseguridad, necesarias tanto para regulación, cumplimiento normativo, seguridad o continuidad de la disponibilidad de los sistemas en producción.

2 SERVICIO DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN

El servicio de mantenimiento y soporte RPA comprende el conjunto de prestaciones necesarias para asegurar el correcto funcionamiento de los procesos automatizados en producción, proporcionando una gestión unificada del servicio, con criterios técnicos homogéneos, trazabilidad de actuaciones y coordinación permanente con Correos.

El adjudicatario deberá disponer de los recursos técnicos y humanos necesarios para prestar el servicio de forma ordenada, consistente y continua, garantizando la calidad de la prestación conforme a las condiciones establecidas en el presente Pliego y sus Anexos.

3 DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN

Con objeto de facilitar la correcta comprensión del alcance, el dimensionamiento del servicio y la comparabilidad de ofertas se facilita a los licitadores una estimación del inventario de elementos en explotación objeto de mantenimiento y de la volumetría media de actividad.

Las volumetrías que se indican a continuación tienen carácter informativo y de referencia, al estar sujetas a variaciones propias de un servicio en producción (picos operativos, estacionalidad y evolución de automatizaciones). En todo caso, el adjudicatario deberá garantizar la prestación del servicio y la cobertura de las prestaciones del Anexo I conforme al alcance del contrato.

En el arranque del contrato, Correos facilitará el inventario operativo de referencia y, de mutuo acuerdo con el adjudicatario, se procederá a su validación definitiva (incluyendo identificadores, criticidad, dependencias y contactos), que servirá como base de seguimiento del servicio, sin que ello suponga modificación del objeto ni de las condiciones esenciales del contrato.

Dicha validación tendrá carácter de ajuste operativo inicial, sin que pueda implicar ampliación o reducción del alcance del servicio definido en el Pliego.

Durante la ejecución del contrato, el inventario inicial podrá verse alterado como consecuencia de la evolución del servicio y de la actividad operativa, tanto por la desactivación de automatizaciones que dejen de requerir mantenimiento como por la incorporación a explotación de nuevos robots (desarrollados por los correspondientes equipos de desarrollo), cuya operación y mantenimiento deberá ser asumida dentro del alcance del servicio.

Estas variaciones se entienden incluidas en el modelo de prestación definido en el Anexo I, que contempla la atención de los distintos tipos de mantenimiento (correctivo, adaptativo, preventivo y perfectivo) y la asimilación de automatizaciones en producción, y deberán ser atendidas dentro de la capacidad de servicio contratada.

En ningún caso dichas variaciones podrán suponer una ampliación del objeto contractual ni un incremento automático de las condiciones económicas, ni implicar la exigencia de prestaciones que excedan de la capacidad efectiva del servicio definida en el Pliego.

3.1 Inventario base del objeto de mantenimiento y volumetrías de referencia.

I. Objeto de mantenimiento:

PRODUCTO	Componente	COMPLEJIDAD	Nº OBJETOS
ROBOTS DESATENDIDOS ¹	Robot	Alta	15
	Robot	Media	25
	Robot	Baja	4
SERVICIOS MULESOFT	APIs	Media	6
	Endpoints	Media	150
AWS LAMBDA (Python)	Servicio	Media	1
APLICACIONES APPIAN	Media/Baja	Media/Baja	2
IA GENERATIVA (Azure GPT Open AI)	Prompts	Media	5
IA MODELOS (Azure Document Intelligence)	Clasificación	Media/Alta	2
	Extracción*	Media/Alta	9

¹ ROBOTS DESATENDIDOS - Previsión crecimiento esperado en 2026: Ampliación en torno a 5-8 robots.
MODELOS EXTRACCIÓN – Previsión crecimiento esperado en 2026: Ampliación en torno a 10-15 modelos.

La clasificación de complejidad se emplea a efectos de estimación y priorización de trabajos, pudiendo Correos ajustar la clasificación de un elemento concreto en función de su criticidad, dependencias y efectos en la continuidad operativa.

El inventario y volúmenes indicados tienen carácter orientativo y constituyen una estimación basada en la situación del servicio en el ejercicio 2026, a efectos exclusivamente informativos para el dimensionamiento por parte de los licitadores.

En consecuencia, podrán producirse variaciones durante la ejecución del contrato derivadas de la evolución natural del servicio en producción (altas, bajas, modificaciones o ajustes de automatizaciones y de sus componentes asociados), siempre dentro del alcance funcional definido en el presente Anexo I y sin que ello implique la incorporación de nuevas prestaciones ni una alteración del objeto

II. Volumetría de carga de trabajo:

Tipo trabajo	Descripción Trabajo	Volumen mensual
Incidencias	Errores en producción	70
Peticiones (work order)	Solicitudes de trabajo (cambios de configuración, extracción de información, revisión/seguimiento robots,)	50
Tareas	Trabajos colaterales por impacto en proyectos globales (pruebas de validación tras upgrades tecnológicos, cambios en sistemas de terceros con los que se integran los robots,)	50
Incidencias/Alertas Monitorización	Revisión y resolución de alertas o incidencias generadas por los sistemas de monitorización en producción	150
Acciones transversales	Tareas englobadas en el marco del mantenimiento preventivo, perfectivo y/o adaptativo	8

III. Volumetría específica Appian

De las dos aplicaciones Appian incluidas en el alcance:

- Estación de verificación: ~4.000 instancias de proceso/mes (en torno a 200.000 record type).
- GAO (Gestión Aprovechamiento Oficinas): ~1 instancia de proceso/mes (en torno a 100.000 record type).

Las volumetrías anteriores se facilitan como referencia para el dimensionamiento del servicio y la planificación operativa. No obstante, el adjudicatario deberá mantener la continuidad del servicio y el cumplimiento de las prestaciones del contrato ante variaciones razonables de carga, gestionando picos mediante su modelo operativo y de priorización.

3.2 Pila tecnológica mínima para cubrir por el servicio

Para la ejecución de las prestaciones contempladas en el Pliego resulta necesario disponer de experiencia contrastada en las tecnologías base que se utilizan principalmente para el mantenimiento de los procesos automatizados y servicios objeto del contrato. A tal efecto, el equipo adscrito al servicio deberá cubrir, como mínimo, la pila/torre tecnológica que se detalla a continuación, organizada en torno a tres bloques funcionales:

A. HIPERAUTOMATIZACIÓN

▪ Suite de productos UiPath.

A continuación, se enumeran los principales productos utilizados, sin perjuicio de que puedan incorporarse otros productos del portfolio UiPath en función de necesidades del negocio:

- UiPath Robots (Attended/Unattended).
- UiPath Robotic Enterprise Framework.
- UiPath Studio.
- UiPath Orchestrator.
- UiPath Apps.
- UiPath Maestro.
- UiPath IXP.
- UiPath Document Understanding.
- UiPath Communications Mining.
- UiPath Agentic Automation.

▪ Desarrollo UiPath en lenguajes VB.NET y C#.

B. LÓGICA DE NEGOCIO E INTEGRACIÓN,

▪ MuleSoft.

Plataforma de integración utilizada para conectar aplicaciones, datos y sistemas (on premise y nube) de forma estructurada y reutilizable principalmente mediante APIs.

Uso en Correos: integración de sistemas y aplicaciones, creación y gestión de APIs y automatización de flujos de negocio cuando así se requiera.

Conocimiento detallado en:

- Lenguaje DataWeave.
- Anypoint Platform y Anypoint Code Builder.
- Diseño de APIs (RAML/OAS).
- Protocolos REST/SOAP.
- Arquitectura de tres capas (System, Process, Experience APIs).

- **Appian**

Plataforma low-code de automatización de procesos (BPM), utilizada para diseñar, automatizar y ejecutar procesos empresariales, creando aplicaciones de forma rápida y visual, con poco código.

Uso en Correos: acotado y limitado a dos aplicaciones sin previsión de evolución, al tratarse de una tecnología en vías de decomisado. El volumen de trabajo relativo a Appian se considera residual, sin perjuicio de que el equipo deba estar preparado/capacitado para atender necesidades que puedan surgir.

- **Ecosistema AWS.**

Conocimiento de los servicios más comunes en AWS, incluyendo S3.

- **AWS Lambda.**

Este servicio forma parte del ecosistema AWS, pero se hace mención especial puesto que es de uso crítico en hiperautomatización.

Es un servicio de computación en modo serverless (sin servidores) de Amazon Web Services (AWS) que permite ejecutar código en la nube sin tener que crear/administrar/mantener servidores.

Uso en Correos: Servicios que implementan lógica de negocio e integraciones desarrollados en Python.

- **Integración continua.**

GitHub y Jenkins.

C. INTELIGENCIA ARTIFICIAL.

- **Azure AI.**

Actualmente, el uso de Inteligencia Artificial en hiperautomatización está acotado a servicios de Azure (principalmente GPT). Se requiere que el equipo disponga de conocimiento y experiencia en los siguientes servicios:

- Ingeniería de prompts con Azure OpenAI (LLMs)
- Análisis de confianza
- Azure AI Document Intelligence Studio
- Azure AI Foundry Studio
- Azure AI Services
- Document Intelligence (modelos predefinidos y personalizados)
- Content Understanding
- Procesamiento del Lenguaje Natural (NLP)
- Formateo de datos

Lo expuesto anteriormente sienta las bases del conjunto mínimo obligatorio de conocimientos tecnológicos que deben cubrir los recursos que se oferten para la prestación de los servicios requeridos en el pliego, pero dado que la arquitectura y ecosistema de datos de Correos puede evolucionar durante la vigencia del contrato puede ser necesaria la ampliación del ámbito

tecnológico en cualquiera de las fases de prestación de este. Por tanto, se encuentra dentro del alcance del contrato, la adaptación (siempre con previa antelación y de mutuo acuerdo entre ambas partes) de los perfiles de trabajo a las nuevas plataformas y tecnologías que sean requeridas. En función de las necesidades de cada momento, esto puede implicar, la inclusión de nuevos recursos con nuevos conocimientos, el reciclaje del equipo actual (el coste de reskilling deberá ser asumido al 100% por el adjudicatario) y/o la sustitución de los recursos actuales por otros especializados en las nuevas tecnologías.

3.3 Catálogo de Prestaciones.

Las prestaciones mínimas que se incluyen en el servicio objeto del contrato son las siguientes, todas ellas referidas exclusivamente a las automatizaciones RPA/Hiperautomatización existentes en producción:

a. Continuidad del servicio

Actuaciones necesarias para asegurar la disponibilidad y correcta ejecución de las automatizaciones RPA/Hiperautomatización en producción, incluyendo la documentación necesaria para su operación y soporte.

Si se identifican errores durante la fase de pruebas de aceptación de usuario priorizar su resolución para que no haya esperas de tiempo elevadas por parte de los usuarios y para que no tengan la sensación de que no se les atiende o de que no se tiene el control suficiente sobre el proceso/robot desarrollado como para resolver errores lo más rápidamente posible.

Gestionar la expectativa del usuario comunicándole de manera directa, clara y detallada el trabajo que se va a realizar y el resultado que va a obtener. Acordar desde el inicio del proyecto cómo será la manera exacta de validar el producto desarrollado para evitar malentendidos y retrasos en la fase de pruebas de aceptación y asegurar que estas pruebas se superan con éxito y en el tiempo planificado para ello.

b. Mantenimiento permanente de sistemas

Tareas recurrentes de mantenimiento técnico de las automatizaciones RPA/Hiperautomatización, incluyendo la supervisión diaria, control de ejecuciones y resolución de incidencias.

Entre las tareas incluidas en esta categoría, destacamos las siguientes:

- Resolución de incidencias: Solucionar en el plazo requerido, conforme a los niveles de servicio establecidos en el Anexo XII (Evaluación de Proveedores – ANS), todos aquellos problemas en producción tanto si se trata de incidencias abiertas por usuarios (mediante la correspondiente herramienta de tickets) o de manera interna por equipos de Correos o por el propio equipo del servicio de mantenimiento objeto de la presente licitación.

Incluye la atención al peticionario y seguimiento de resolución de incidencias con los equipos implicados

- Resolución de peticiones: Atender y solucionar en el plazo requerido, conforme a los niveles de servicio establecidos en el Anexo XII (Evaluación de Proveedores – ANS), todas aquellas peticiones abiertas en la herramienta de tickets y que se correspondan con trabajos de mantenimiento (informes, cambios en la planificación de procesos, cambio en la parametrización del sistema, modificación de ficheros de soporte, dudas/consultas de usuarios y/o personal de Correos o relacionado con el mismo dentro del objeto de la presente licitación.)
Incluye la atención al peticionario y seguimiento de resolución de incidencias con los equipos implicados
- Replanificación de procesos en paradas planificadas por motivos técnicos y/o funcionales tanto procedentes de equipos de explotación (actuaciones requeridas tanto a nivel de sistema operativo, software base, redes, requerimientos de seguridad, etc.) como de aplicaciones con las que se integran los procesos de RPA/hiperautomatización (ya sean propios de Correos o de terceros)
- Análisis y seguimiento de la parrilla de licencias para garantizar el mejor uso y aprovechamiento de estas. Implica análisis y seguimiento de ítems encolados en los robots para detectar cuellos de botella, cumplimiento de automatización en el horario requerido/comprometido con el negocio para cada proceso, así como la necesidad de redistribuir las ejecuciones entre las licencias disponibles e identificar cuando es necesario ampliar el conjunto de licencias existente.
- Recibir transferencia de nuevos desarrollos desde el equipo de desarrollo de RPA/Hiperautomatización ya sea relativos a nuevos robots/procesos o a la ampliación/modificación de capacidades/funcionalidades en robots/procesos ya existentes.

Entre las tareas requeridas se encuentran, como mínimo, las siguientes:

- Revisión de documentación técnica previa al desarrollo de los distintos equipos de RPA/Hiperautomatización y seguimiento durante todo el ciclo de desarrollo.
- Revisión de planes de prueba para asegurar que se contemplan todos los casos para asegurar el buen funcionamiento y rendimiento en producción.
- Revisión y validación de código, previamente al despliegue en Producción de cualquier equipo de RPA/Hiperautomatización de cara a garantizar el cumplimiento de la metodología, normativa de calidad, uso de plantillas y buenas prácticas.
- Soporte al equipo de desarrollo de RPA/Hiperautomatización. Entre las tareas requeridas en este soporte, se encuentran las siguientes:
 - Revisión de documentación técnica Resolución de dudas/consultas respecto a la metodología, normativa de calidad, plantillas de desarrollo y buenas prácticas.
 - Soporte para la realización de despliegues en producción (procedimientos y acciones) asegurando que no se afecta a la disponibilidad y rendimiento de los

procesos en producción.

- Administración de la plataforma UiPath (en cualquiera de los componentes de la suite), incluyendo la realización de todas las acciones y actuaciones necesarias para garantizar su correcto funcionamiento, estabilidad y disponibilidad.
 - Asimismo, el adjudicatario deberá velar por el control de costes asociados a su utilización en el caso de servicios bajo modalidad de pago por uso, si los hubiera, así como por el adecuado aprovechamiento de las licencias adquiridas y la optimización del uso de las suscripciones.
 - Las actuaciones sobre la infraestructura tecnológica subyacente (hardware y software base sobre los que se apoya la plataforma UiPath, tales como servidores on-premise, sistemas operativos o sistemas de terceros) serán responsabilidad exclusiva del equipo de Explotación de Correos.
 - No obstante, el adjudicatario deberá colaborar con dichos equipos cuando sea requerido, así como identificar posibles incidencias o riesgos asociados a dicha infraestructura, aportando diagnóstico técnico y gestionando su resolución mediante los equipos responsables.

c. Mantenimiento correctivo

Engloba el conjunto de acciones a realizar para corregir errores o fallos en una solución ya implementada que producen un funcionamiento incorrecto, deficiente o incompleto o que afectan a la calidad de los resultados.

Este tipo de mantenimiento implica llevar a cabo, las siguientes tareas:

- 1) Identificar y diagnosticar el problema
- 2) Aplicar la corrección adecuada

Las acciones correctivas, sobre todo aquellas más críticas o graves, requieren de un tiempo de respuesta muy corto (suelen implicar intervenciones de urgencia justificada) y generalmente se traducen en aplicar un “workaround” que es una solución temporal utilizada para evitar o mitigar un problema sin resolverlo de forma definitiva cuando no es posible implantar una solución más compleja de inmediato, ya sea por limitaciones técnicas, de tiempo, de recursos o de impacto.

Este tipo de soluciones buscan minimizar el impacto en el negocio mientras se trabaja más cuidadosamente en la solución definitiva, así como evitar interrupciones largas en servicios críticos.
- 3) Modificar el proceso/robot afectado para resolver el problema raíz de manera permanente y definitiva (cambio en código, configuración, lógica de negocio.)
- 4) Validar la solución asegurándose que el problema está resuelto y no se han generado nuevos errores como efecto colateral al cambio realizado (pruebas de regresión)
- 5) Documentar la incidencia y la solución aplicada y en caso de tratarse de un error lo suficientemente significativo, informar al resto del equipo de mantenimiento, así como a los compañeros del Servicio de Evolución, Nuevos Desarrollos y Transformación para que lo conozcan y eviten repetirlo.
- 6) Si Correos así lo determina, la resolución de las incidencias puede llevar asociado el seguimiento y reporte con los usuarios, así como el soporte de dudas tanto a nivel funcional como técnico o de las herramientas utilizadas.

- 7) Si la incidencia se identifica como provocada por un desarrollo que está en garantía o por un sistema tercero, de acuerdo con el responsable de Mantenimiento, podrá ser escalada a dichos equipos para su resolución.
- 8) A su vez, se incluyen en este apartado la corrección de aquellos errores de nuevos evolutivos que hayan llegado a producción, a pesar de los trabajos de aseguramiento de la calidad y que ya hayan superado el tiempo de garantía del proveedor que los desarrolló.
- 9) Las incidencias resueltas deben quedar debidamente registrada en un repositorio común (y accesible para Correos) de manera que todo el equipo del contrato disponga de documentación respecto a lecciones aprendidas
- 10) Notificar a los equipos que realizan nuevas evolutivos los problemas acontecidos para que los tengan en cuenta y los subsanen en los desarrollos en curso

d. Mantenimiento adaptativo

Engloba el conjunto de acciones a realizar para modificar una solución ya existente y adaptarla debido a cambios en el entorno sin que necesariamente haya un error que motive el cambio.

Incluye aquellas intervenciones de carácter menor en forma de desarrollo, esto es, que por su naturaleza y alcance no tienen entidad suficiente como para considerarse un proyecto (no hay cambio funcional en requisitos de usuario final) pero que requieren de un desarrollo para adaptar alguna funcionalidad necesaria de la compañía para el mantenimiento de la cadena productiva.

Incluye todos los cambios y ajustes técnicos necesarios para mantener operativas las automatizaciones ante cambios en aplicaciones o entornos con los que interactúan los robots (por ejemplo, incluye los cambios que hubiera que realizar si una aplicación de terceros que es invocada desde un robot cambia su ubicación o modifica ligeramente su interfaz y esto provoca que el proceso que lo invoque deje de funcionar correctamente).

Estas actuaciones no tendrán la consideración de desarrollos evolutivos ni implicarán ampliación funcional.

Quedan incluidas en esta categoría las siguientes actividades:

- Actualización de sistemas y/o plataformas, así como en la infraestructura tecnológica (migraciones a nuevas versiones de las herramientas utilizadas, Upgrade de sistemas operativos, modificación de procesos debido a migración de base de datos, reconfiguración de conexiones y/o credenciales requeridas por cambios de servidores, políticas de ciberseguridad así como las modificaciones necesarias sobre la plataforma UIPath a nivel de administración por cambios de arquitectura como puede ser la migración a cloud de determinados componentes si fuera requerido, acciones conducentes a dimensionamiento para escalabilidad, tolerancia a fallos, ajustes para monitorización, alertado,)
- Cambios en normativas o requisitos legales (como nuevas políticas de privacidad y/o auditoría)

e. Mantenimiento preventivo

Actuaciones planificadas orientadas a prevenir incidencias, reducir recurrencias y mejorar la mantenibilidad y estabilidad técnica de las automatizaciones, limitándose el mantenimiento perfectivo a mejoras técnicas internas sin impacto funcional.

Incluye la monitorización preventiva de procesos y detección temprana de incidencias/posibles incidencias, mediante el uso de Cuadro de Mandos PBI, Alertado en plataforma de tickets y

revisión de Orquestador, así como todas aquellas tareas/acciones que se consideren necesarias y/o adecuadas para prevenir problemas o errores futuros en el corto/medio plazo. Si aplica, incluye tareas de housekeeping como limpieza de directorios de ficheros temporales, historificación BBDD.

Incluye el seguimiento y control de uso de licencias de UIPath, así como mapa de calor/carga y evolución de ítems encolados para detectar con antelación aumento de carga/actividad que permita activar nuevas licencias con tiempo suficiente para no impactar en el negocio.

Contempla todas aquellas acciones destinadas a:

- Evitar o mitigar las consecuencias de posibles fallos técnicos/disfunciones de los servicios y/o sistemas, logrando prevenir las incidencias antes de que estas ocurran, a optimizar su funcionamiento, mejorar su rendimiento y a contribuir a que los usuarios dispongan de mayor autonomía en el uso de estas.
- Optimizar funcionalidades que muestran una degradación (de rendimiento, de calidad, de consumo de recursos, de costes.) progresiva en el tiempo, para evitar que finalmente desencadenen una situación de indisponibilidad de esta.
- Mejora en la gestión de errores para evitar problemas desencadenados por comportamientos incorrectos de los procesos por no estar realizando un tratamiento adecuado de las excepciones en código y similar.

f. Mantenimiento perfectivo

Conjunto de acciones a realizar para mejorar o evolucionar una solución ya existente sin que exista un fallo o error previo. A continuación, se muestran ejemplos de este tipo de mantenimiento que englobaría, entre otras, las siguientes modificaciones proactivas para mejorar rendimiento, refactorizar código para hacerlo más limpio, mantenible, configurable, eficiente y/o escalable, actualizar tecnologías o librerías para mantener la solución vigente.

g. Soporte a usuarios

Soporte técnico especializado a usuarios y áreas de negocio en relación con la operación de las automatizaciones RPA/Hiperautomatización, incluyendo apoyo técnico al CAU y documentación de incidencias.

h. Soporte a solicitudes de negocio y de Tecnología

Atención de peticiones y consultas de carácter operativo, relacionadas con la ejecución y explotación de las automatizaciones RPA/Hiperautomatización, sin desarrollo funcional ni nuevas automatizaciones.

Incluye apoyo y colaboración con otros equipos de Correos (arquitectura, gobierno del dato, ciberseguridad, áreas de negocio y usuarios finales) así como de terceros relacionados en el marco de las prestaciones del presente contrato.

i. Monitorización y operación

Monitorización continua de procesos automatizados, revisión de alertas, análisis de logs y

adopción de medidas técnicas para garantizar la estabilidad del servicio.

j. Ejecución de procesos periódicos

Lanzamiento, supervisión y control de procesos RPA/Hiperautomatización que requieran intervención manual puntual, incluyendo validación de resultados y análisis de incidencias.

k. Tratamiento de información

Actuaciones técnicas de tratamiento de información estrictamente necesarias para la correcta ejecución y recuperación de las automatizaciones (consultas técnicas, verificaciones y ajustes operativos autorizados).

l. Capacitación sobre aplicaciones en producción

Acciones puntuales de transferencia de conocimiento operativo, actualización de documentación y sesiones explicativas orientadas a la explotación y soporte, sin formación funcional avanzada ni capacitación en nuevas soluciones.

m. Coordinación, control y seguimiento de los servicios

Planificación, coordinación y seguimiento del servicio, elaboración de informes y evidencias para evaluación de la calidad de la prestación, así como el seguimiento de cumplimiento de los ANS y aplicación de penalizaciones.

n. Plan de mejora continua

Identificación y propuesta de acciones de mejora orientadas a aumentar la estabilidad, eficiencia y mantenibilidad de las automatizaciones RPA/hiperautomatización existentes, sin implicar evoluciones funcionales.

Se espera del equipo de mantenimiento un plan de automatización de tareas de mantenimiento que sean repetitivas para mejorar su productividad, así como la calidad y reducir errores humanos.

o. Pruebas de aceptación de nueva funcionalidad

Pruebas técnicas de validación para la asimilación operativa de hiperautomatización desarrolladas por otros contratos antes de su entrada en explotación bajo mantenimiento.

p. Asimilación de nuevas automatizaciones en explotación

Asimilación técnica y operativa de automatizaciones RPA/hiperautomatización que pasen a producción durante la vigencia del contrato, a efectos de su monitorización y mantenimiento (tanto en términos de operación como de resolución de problemas/incidencias, o cambios provocados por acciones preventivas/perfectivas/adaptativas).

q. Gestión de problemas

Aplicación de un proceso estructurado de gestión de problemas, orientado a identificar causas raíz de incidencias recurrentes y definir acciones correctivas y preventivas.

Establecimiento de workaround (solución temporal) cuando exista un problema en producción

y la resolución de su causa raíz no pueda realizarse en el corto plazo. Será responsabilidad del equipo de mantenimiento definir, proponer e implantar soluciones temporales en el menor plazo de tiempo posible para paliar los problemas en producción cuya resolución definitiva no pueda ser inmediata o en el corto plazo.

r. Documentación

Actualizar la documentación necesaria para la operación de los procesos tanto en cuanto a metodología, plantillas de desarrollo y buenas prácticas. Para ello, se realizarán sesiones de forma periódica, detectando ineficiencias y proponiendo puntos de mejora.

Incluye la generación de documentación respecto a la operativa en producción de los procesos y el mantenimiento de un repositorio de problemas/soluciones de cara a que quede registrado de forma centralizada y pueda ser compartida con todo el equipo de mantenimiento (o quién determine Correos que pueda necesitar conocer dicha información/documentación).

En relación con las tareas de mantenimiento de tipo correctivo, adaptativo, preventivo y perfectivo es importante recalcar que Correos puede solicitar al adjudicatario llevarlas a cabo en el Servicio de Mantenimiento y Soporte independientemente de su complejidad y del esfuerzo en horas que puedan requerir. Este servicio implica una capacidad fija y dedicada, por lo que Correos se reserva la facultad de organizar, priorizar y asignar dicha capacidad para la realización de las tareas que considere más adecuadas en cada momento.

En todo caso, esta facultad se ejercerá exclusivamente dentro de la capacidad contratada, sin que pueda suponer una ampliación del alcance del contrato ni la exigencia de prestaciones adicionales, y garantizando el cumplimiento de los niveles de servicio (ANS) establecidos.

4 CONDICIONES DE PRESTACIÓN DEL SERVICIO

La prestación del servicio de mantenimiento y soporte RPA/Hiperautomatización objeto del presente contrato se realizará conforme a las condiciones que se detallan a continuación, garantizando en todo momento la continuidad operativa de las automatizaciones en producción y la correcta coordinación con los servicios internos de Correos.

El servicio se prestará con carácter general en modalidad remota, sin perjuicio de que Correos pueda requerir, de forma justificada, actuaciones puntuales que deban realizarse en coordinación directa con los servicios internos, especialmente cuando resulte necesario para la correcta resolución de incidencias o la validación de determinadas actuaciones. La modalidad de prestación no exime al adjudicatario de la obligación de garantizar la correcta ejecución del servicio, la trazabilidad de las actuaciones realizadas y la disponibilidad de los medios comprometidos.

Horario laboral

El horario laboral ordinario de prestación del servicio será de 08:00 a 18:00 horas, en días laborables, durante los cuales se atenderán las incidencias y peticiones de carácter operativo relacionadas con la ejecución y mantenimiento de las automatizaciones

RPA/Hiperautomatización. Dentro de este horario se realizarán las actuaciones habituales de soporte, operación, monitorización y mantenimiento previstas en el presente Pliego.

Actuaciones fuera de horario laboral

Sin perjuicio del horario laboral ordinario, Correos podrá requerir la realización de actuaciones fuera de este horario cuando resulte necesario por motivos operativos o de negocio, o por la existencia de ventanas técnicas que imposibiliten su ejecución en horario laboral, siempre dentro del alcance del contrato. A estos efectos, se considerarán incluidas, entre otras, las actuaciones necesarias para:

- la atención de incidencias críticas (contención, mitigación y recuperación del servicio);
- despliegues, instalaciones, actualizaciones, pruebas, validaciones y actuaciones técnicas equivalentes que, por su impacto, deban ejecutarse fuera del horario ordinario;
- actuaciones derivadas o condicionadas por intervenciones de los equipos de Explotación (por ejemplo, upgrades de sistema operativo o software base) que requieran acciones coordinadas sobre robots y/o componentes de orquestación/supervisión, incluyendo paradas, arranques, reejecuciones controladas y verificaciones posteriores.

Estas actuaciones fuera de horario laboral no implican la prestación continuada del servicio en régimen 24x7 para incidencias no críticas ni la realización sistemática de actividades ordinarias fuera del horario establecido; se limitan a los supuestos anteriores, cuando sean necesarias y se encuentren justificadas por ventanas técnicas o necesidades de negocio.

Las actuaciones fuera de horario laboral descritas en este apartado, cuando se realicen dentro del alcance del contrato, se entienden incluidas en la prestación del servicio conforme al Pliego.

Activación, coordinación y trazabilidad

Las actuaciones fuera de horario laboral se realizarán a requerimiento de Correos y/o en coordinación con Explotación cuando proceda, debiendo planificarse con la antelación razonable posible salvo situaciones de urgencia. En todo caso:

- deberán quedar debidamente registradas y trazadas (ticket/registro de actuación, cronología, evidencias técnicas y cierre);
- deberán documentarse las acciones ejecutadas y las verificaciones realizadas para asegurar la estabilidad tras la intervención;
- deberán respetarse los procedimientos de coordinación, escalado y cierre definidos en el Pliego y en el Anexo I.

Coordinación con Explotación y responsabilidad sobre la infraestructura

Dado que la plataforma RPA/Hiperautomatización se encuentra desplegada en infraestructura de Correos, cuya operación corresponde a los servicios internos de Explotación, el adjudicatario deberá coordinarse con dichos servicios cuando sea necesario para:

- la resolución de incidencias cuya causa raíz se encuentre fuera del ámbito estrictamente

RPA/Hiperautomatización,

- la ejecución de actuaciones que requieran intervención sobre el entorno,
- la planificación de ventanas operativas cuando proceda.

En todo caso, la responsabilidad sobre la operación de la infraestructura subyacente no corresponde al adjudicatario.

Carácter contractual

Las condiciones de prestación del servicio recogidas en el presente apartado tienen carácter contractual y serán exigibles durante toda la vigencia del contrato, incluidas, en su caso, las prórrogas.

5 REPORTE, SEGUIMIENTO Y ENTREGABLES

El adjudicatario deberá proporcionar, como mínimo:

- Plan de prestación del servicio.
- Inventario operativo de automatizaciones cubiertas.
- Procedimientos operativos y runbooks.
- Informes periódicos de seguimiento.
- Evidencias de actuación (tickets, logs, registros de ejecución y documentación de cierre).

Los entregables tendrán carácter contractual y permitirán verificar de forma objetiva y trazable la correcta prestación del servicio.

Tabla resumen líneas de servicio:

Bloque de servicio	Qué se presta	Actividades típicas	Evidencia verificable
Soporte RPA/Hiperautomatización	Diagnóstico y resolución de incidencias RPA/Hiperautomatización	Análisis de error de ejecución, corrección de fallos, restablecimiento del servicio	Ticket cerrado + evidencias de actuación + conformidad de cierre
Operación y monitorización	Supervisión técnica de ejecuciones	Revisión de ejecuciones, análisis de logs, detección de patrones de fallo, contención	Logs/registro de plataforma + ticket + informe de seguimiento
Mantenimiento correctivo	Restauración ante fallos	Correcciones para recuperar la ejecución estable	Ticket + detalle de corrección + evidencia de prueba
Mantenimiento preventivo	Reducción de recurrencias	RCA cuando así lo determine Correos, estabilización, medidas preventivas	RCA/nota técnica + ticket + evidencia de mejora.
Gestión de problemas	Análisis estructurado de causas raíz	Identificación de causa raíz, acciones correctivas y preventivas.	RCA formal + plan de acciones + seguimiento.
Ejecución de procesos periódicos	Ejecución controlada de procesos RPA/Hiperautomatización	Lanzamientos manuales, supervisión, validación de resultados	Registro de ejecución + logs + validación
Tratamiento de información	Actuaciones técnicas sobre datos	Consultas técnicas, verificaciones, ajustes operativos autorizados	Ticket + evidencia de actuación + validación

Asimilación de automatizaciones	Incorporación a explotación	Validación técnica, monitorización inicial, documentación operativa	Acta de asimilación + evidencias
Capacitación operativa	Transferencia de conocimiento	Sesiones operativas, actualización de documentación	Material entregado + acta/sesión
Coordinación con Explotación	Actuación conjunta en on-premise	Escalado a Explotación, ventanas, coordinación de cambios/entorno	Acta/registro de coordinación + ticket enlazado.
Incidencias críticas (24x7)	Incidencias críticas (disponibilidad 24x7)	Activación, escalado, mitigación y recuperación	Registro de activación + cronología + cierre con evidencias.

6 PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS

Para la correcta ejecución del contrato, el adjudicatario deberá disponer de un equipo de trabajo con experiencia tanto en el ámbito funcional de los procesos automatizados como en la plataforma tecnológica RPA/Hiperautomatización (UiPath) y en la operación de entornos productivos, en coherencia con el alcance del contrato.

La estimación mínima de recursos y perfiles es la siguiente:

Servicio	Perfil	Nº Recurso	Experiencia mínima
Servicio de Mantenimiento y Soporte.	JP / Responsable del Servicio	0,5 FTE	3 años
Servicio de Mantenimiento y Soporte	Especialistas Hiperautomatización (perfil mixto funcional-técnico)	2 FTE (1,0 FTE cada uno)	2 años

Condición de dedicación mínima

A efectos de este apartado, la dedicación mínima de los Especialistas RPA/Hiperautomatización se entenderá cumplida exclusivamente mediante la adscripción de dos recursos individuales, cada uno con dedicación efectiva del 100% (1,0 FTE). No será válida su cobertura mediante el fraccionamiento en más de dos personas con dedicaciones parciales (por ejemplo, cuatro recursos al 50% u otras combinaciones equivalentes).

Asimismo, no se considerarán válidos, a efectos de acreditación de capacidades (incluyendo certificaciones y currículums aportados), recursos “potenciales”, de apoyo o con dedicaciones marginales no comprometidas. Únicamente se considerarán los recursos efectivamente adscritos al contrato con la dedicación indicada.

A estos efectos, el adjudicatario deberá garantizar expresamente que los recursos adscritos:

- I. Disponen de experiencia suficiente para cubrir todas las tecnologías incluidas en el Anexo I – Apartado “ÁMBITO TECNOLÓGICO Y ALCANCE DEL CONTRATO”; y
- II. Disponen de conocimientos y experiencia para desempeñar todas las tareas/prestaciones descritas en el Anexo I – Apartado “DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN”.

En esta renovación no resultan de aplicación funciones específicas de arquitectura, debiendo cubrirse la totalidad de las funciones operativas, funcionales y técnicas del servicio con los recursos adscritos.

Los dos recursos técnicos adscritos con dedicación del 100 % (1,0 FTE cada uno) constituyen el equipo mínimo obligatorio para la ejecución del contrato, debiendo garantizar, de forma conjunta, la cobertura íntegra de todas las prestaciones definidas en el Anexo I. – Apartado 3 DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/HIPERAUTOMATIZACIÓN, así como las condiciones de prestación recogidas en el resto del Anexo I, sin que sea necesaria una segregación por denominación de perfiles.

Sin embargo, los licitadores podrán adscribir recursos adicionales si así lo consideran, sin que ello suponga una modificación de la capacidad mínima exigida ni de las condiciones del contrato.

A efectos de cumplimiento, únicamente se considerarán los recursos mínimos adscritos conforme a lo establecido en el presente pliego. Asimismo, a efectos de valoración de criterios de adjudicación, únicamente se tendrán en cuenta aquellos recursos que se encuentren expresamente vinculados a dichos criterios en el Anexo IX y que cumplan las condiciones establecidas en el mismo.

7 FASES DE LA PRESTACIÓN DE LOS SERVICIOS

El plazo de ejecución de este contrato se fija en un máximo de 13 meses, incluyendo las siguientes 3 fases:

7.1 Fase de lanzamiento o asimilación del servicio

Actualmente Correos dispone de un servicio contratado que cubre el objeto de este expediente, por lo que se abrirá un período de asimilación. El objetivo principal de esta fase es adquirir el conocimiento específico necesario para la correcta prestación del servicio, incluyendo las particularidades de las funcionalidades a implementar, las herramientas empleadas, la metodología de trabajo y cualquier otro aspecto relevante. En esta fase, el equipo del Servicio de Mantenimiento debe adquirir todos los conocimientos necesarios sobre los proceso/robot, procesos y operativas realizadas actualmente en los entornos productivos asociados a la oficina del dato del Área de Inteligencia Artificial y Analítica de Datos, y esta capacitación debe ser suficiente para hacerse cargo de todos ellos, resolver incidencias y aplicar pequeños cambios adaptativos que pudieran requerirse para el buen funcionamiento.

Esta adquisición de conocimiento se realizará mediante talleres liderados por el adjudicatario actualmente vigente y técnicos de las distintas áreas de Correos implicadas en el ciclo de vida del Servicio de Diseño, Desarrollo, Evolución y Soporte y Mantenimiento objeto de este contrato.

La duración de la fase de asimilación será de 30 días naturales desde el día siguiente a la de aceptación de la Resolución de adjudicación y será de asistencia obligatoria para todo el equipo completo que vaya a formar parte del Servicio de Mantenimiento y Soporte. Con el objetivo de

que se aproveche al máximo esta fase de transferencia del conocimiento y para garantizar que el equipo que va a prestar el servicio adquiera las habilidades necesarias para asumirlo con garantías de éxito, no se aceptará la asistencia parcial del equipo ni la asistencia de personas que posteriormente no vayan a permanecer de manera continuada y activa en alguno de los servicios del contrato.

Durante este periodo, el equipo de trabajo será mixto, compuesto por integrantes del equipo técnico saliente (adjudicatario actual) y del entrante (nuevo adjudicatario), para garantizar la transferencia completa de conocimiento. A la finalización de esta fase, el adjudicatario entrante deberá haber asumido por completo todos los servicios y prestaciones contratadas y comenzará la fase real de prestación del servicio.

Este periodo de asimilación no computará dentro del plazo de ejecución indicado en el apartado 3 (Duración del contrato), ya que la fase de prestación real se iniciará tras la finalización de la asimilación o transcurrido el plazo máximo de 30 días naturales previsto para esta fase. El adjudicatario deberá tener en cuenta las siguientes implicaciones:

- Los recursos técnicos que vayan a formar parte del Servicio de Mantenimiento y Soporte deberán participar en la totalidad de esta fase y, una vez finalizada, permanecer de manera activa y continuada en el servicio, garantizando la continuidad en la prestación y la correcta transferencia de conocimiento. Cualquier sustitución deberá ajustarse a lo dispuesto en el régimen de adscripción de medios establecido en el Pliego. El incumplimiento de esta condición será considerado incumplimiento del régimen de adscripción de medios y de continuidad del equipo, siendo evaluado conforme a los ANS definidos en el Anexo XII y penalizado según el Anexo XI – Régimen de penalidades.
- Si el adjudicatario quisiera incorporar equipo extra a estas sesiones de transferencia del conocimiento deberá asumir los costes de su personal adicional (no se facturará ningún concepto suplementario) y además deberá garantizar que la participación de estos recursos está justificada porque participarán posteriormente de manera activa y continuada en alguno de los servicios del pliego.
- El adjudicatario se compromete a que el equipo que ha participado en la fase de asimilación se ocupe de la formación y traspaso completo del conocimiento adquirido a todos y cada uno de los recursos que se vayan incorporando a cualquiera de los servicios recogidos en el contrato durante toda la duración de este y que no hayan participado en dicha fase.

Para poder garantizar que la transferencia se realiza con éxito, como resultado de esta fase de asimilación, el adjudicatario deberá presentar a Correos:

- Inventario de todas las operativas, procesos y proceso/robot a mantener (para verificar que se cubren todos y cada uno de los procesos actuales en producción)
- Repositorio de documentación centralizado, completo y bien organizado de todos los procesos y proceso/robot que se van a mantener (incluido el material que haya podido generarse durante la fase de transferencia como puede ser videos, actas de reunión,

presentaciones para la formación.)

- Exposición resumen del conocimiento que ha adquirido (para verificar que se ha entendido la funcionalidad requerida)
- Identificación del código fuente de cada uno de los proceso/robot a mantener (para verificar que se tiene localizado todo el código en el control de versiones correspondiente o fuera de este si se diera el caso de algún producto que estuviera siendo gestionado fuera del repositorio de código oficial)
- Evidencias de que conocen y entienden la manera en la que se despliega en producción cada tipo de proceso/robot (para asegurar que llegado el caso podrán ser capaces de poner en producción nuevas versiones de cada uno de ellos)

En caso de considerar que el equipo del adjudicatario no es apto para asimilar el servicio con garantías, ello conllevará la resolución del contrato.

Para determinar la aptitud del equipo del adjudicatario para asimilar el servicio con garantías, la Dirección de Tecnología y Transformación Digital de Correos elaborará, con carácter previo a la finalización de esta fase, un acta de evaluación, que recogerá evidencias de los siguientes extremos:

- Inventario completo de procesos y proceso/robot.
- Repositorio documental centralizado y accesible.
- Verificación de accesos y conectividad en entornos DEV/TEST/PRE/PROD.
- Baseline de ANS/KPI acordada.
- Participación completa del equipo adscrito.

Si en la citada acta se recoge que el equipo del adjudicatario no es apto en alguna de las categorías anteriores, ello supondrá la resolución del contrato.

La fase de asimilación concluirá con la firma del Acta de Evaluación y Aceptación por el director del Proyecto, que acreditará la correcta transferencia de conocimiento y la disponibilidad del servicio conforme a lo previsto en el pliego.

En caso de que el adjudicatario sea el mismo que actualmente presta el servicio, no será necesaria la ejecución de esta fase y, por tanto, no será facturable.

7.2 Fase de prestación del servicio

Esta es la fase principal en el desarrollo del contrato que se inicia tras la finalización de la fase de lanzamiento (si se ejecuta).

En esta fase se desarrolla por completo la prestación de los servicios descritos en el apartado anterior [DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO](#).

El plazo de ejecución de esta fase consta de 12 meses, incluyendo la fase de traspaso o finalización que se realizará simultáneamente.

En caso de ejecución de la prórroga, esta será la parte del contrato que se prorrogará, trasladándose la fase de traspaso o finalización del servicio a los últimos 40 días naturales de la

prórroga .

7.3 Fase de traspaso o finalización del servicio

Sólo en caso de que Correos haya decidido tramitar un nuevo expediente que será el considerado como sucesor del presente y, además, que la empresa adjudicataria resulte ser distinta a la que resulte de este, se ejecutará esta fase. El objetivo de esta fase es asegurar que el adjudicatario entrante adquiere el conocimiento necesario para prestar el servicio con garantías.

La duración de esta fase será de 40 días naturales y se solapará parcialmente con la fase anterior (prestación real del servicio), realizándose ambas en paralelo durante el periodo final del contrato, o la prórroga del mismo, en su caso.

Durante la fase de finalización, el adjudicatario del contrato (que seguirá prestando plenamente el servicio contratado), actuando ya en calidad de adjudicatario saliente (el que cede el servicio), continuará responsabilizándose de manera íntegra del servicio y prestaciones contratadas. Y si como consecuencia de haber tramitado un nuevo expediente, sucesor del actual, en caso de que Correos determine que se tiene que hacer un traspaso del servicio a otro adjudicatario distinto (nuevo adjudicatario, el que asume los servicios), el adjudicatario saliente deberá prestar activamente su colaboración en todas las actividades que sean necesarias para la transferencia de conocimiento y herramientas al nuevo adjudicatario. Esta fase de finalización para el adjudicatario saliente convivirá con la fase de asimilación del adjudicatario entrante y ambos equipos deberán participar y colaborar tanto en las sesiones de transferencia como en la realización de jornadas en modo “Shadowing” (el adjudicatario entrante observa y aprende las tareas realizadas por el adjudicatario saliente necesarias para prestar el servicio) y “Shadowing inverso” (el adjudicatario entrante realiza las tareas necesarias para prestar el servicio bajo la supervisión del adjudicatario saliente de manera que se pueda ir corrigiendo aquello que no se haya entendido o interiorizado bien durante la etapa de “Shadowing”).

Este periodo se desarrollará bajo el esquema de equipo mixto y tendrá por objeto que el nuevo adjudicatario adquiera los conocimientos particulares y el contexto completo de operación, incluyendo sistemas, herramientas, normativas, estándares y metodología aplicable.

Este periodo no computará dentro del plazo de ejecución para el adjudicatario entrante, conforme a lo indicado en el apartado 3 (Duración del contrato), y la fase de prestación real del servicio se mantendrá hasta la fecha de finalización del contrato o la prórroga del mismo , en su caso.

8 PUESTOS CLIENTES DEL EQUIPO DE TRABAJO

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

9 ECOSISTEMA SOFTWARE

Mediante la aceptación de la presente cláusula, el adjudicatario se compromete a no realizar modificaciones del ecosistema software de Correos, que no se detallen específicamente en el pliego, tales como la activación/modificación/desactivación de opciones, productos y servicios de las licencias ya existentes, o la descarga, instalación, activación y suscripción de cualquier software. Cualquier modificación del ecosistema software no especificada en el contrato debe ser previamente solicitada y autorizada por parte de Correos.

El adjudicatario será responsable de velar por el cumplimiento de esta norma por parte de todo su personal al servicio de Correos durante toda la ejecución del contrato, asumiendo los posibles costes y demás responsabilidades de toda índole que pudieran derivarse de su incumplimiento, independientemente de la causa de este, ya sea por desconocimiento, falta de formación y/o de experiencia, negligencia y mala praxis.

Tras la adjudicación y antes del inicio del servicio Correos, en el caso de que el adjudicatario así lo solicitase, facilitará una descripción de las plataformas software a las que tendrá acceso el personal del adjudicatario encargado de prestar el citado servicio, incluyendo información de las suscripciones de software o, en el caso de solicitarlo. Correos también facilitará al adjudicatario los permisos pertinentes para que, bajo su supervisión, pueda acceder a las citadas plataformas software. Adicionalmente, si el adjudicatario lo estima oportuno, podrá pedir a Correos las aclaraciones y/o información adicional que requiera para conocer la citada configuración del ecosistema software en el que prestará su servicio.

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”**.

Esta decisión se fundamenta en los siguientes motivos técnicos y organizativos:

Unidad técnica y operativa del servicio: el mantenimiento y soporte *de RPA* exige una gestión integrada (incidencias, operación, monitorización, cambios y soporte) sobre un ecosistema común (automatizaciones, componentes de ejecución y control), lo que requiere responsabilidad única e integral para evitar vacíos de alcance y conflictos de atribución.

Riesgo de fragmentación del soporte y degradación del servicio: la división en lotes incrementaría los puntos de coordinación y las dependencias entre adjudicatarios (especialmente en incidentes críticos), elevando el riesgo de dilatación de tiempos, falta de trazabilidad en la resolución “punta a punta” y dificultades para aplicar mecanismos de control de calidad del servicio.

Proporcionalidad y concurrencia: la configuración como lote único no restringe indebidamente la competencia, dado que el mercado dispone de operadores con capacidad para prestar el servicio completo; y, además, la agrupación evita una arquitectura contractual artificiosa que

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

Se establece como Presupuesto base de Licitación (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de **162.745,00 € (CIENTO SESENTA Y DOS MIL SETECIENTOS CUARENTA Y CINCO EUROS CON CERO CÉNTIMOS)**, de acuerdo con la siguiente distribución:

Importe del IVA o cualquier otro impuesto indirecto equivalente: **28.245,00 € (VEINTIOCHO MIL DOSCIENTOS CUARENTA Y CINCO EUROS CON CERO CÉNTIMOS)**

Base Imponible del Presupuesto base de Licitación (excluido IVA o cualquier otro impuesto indirecto equivalente): **134.500,00 € (CIENTO TREINTA Y CUATRO MIL QUINIENTOS EUROS CON CERO CÉNTIMOS)**.

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

Año	Base Imponible de Licitación (IVA no incluido)	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)
2027	128.972,60 €	108.336,99 €	12.897,26 €	7.738,36 €	27.084,25 €	156.056,85 €
2028	5.527,40 €	4.643,01 €	552,74 €	331,64 €	1.160,75 €	6.688,15 €
Total	134.500,00 €	112.980,00 €	13.450,00 €	8.070,00 €	28.245,00 €	162.745,00 €

Respecto a los Costes Directos asumidos por el prestador del servicio, se han estimado unos costes salariales en torno al 80% por considerarse que los costes relativos a recursos técnicos-humanos y a la alta especialización requerida en servicios de diseño, desarrollo, evolución, mantenimiento y soporte suponen la mayor carga económica del conjunto actividades a contratar. En la estimación de este porcentaje se ha tenido en cuenta que, de manera general, los costes directos están conformados por personas y servicios. 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 catálogo de servicios contemplados en la presente contratación.

De esta manera, el desglose de los gastos directos es el siguiente:

Costes recursos técnicos-humanos 80%	Costes servicios 20%
90.384,00 €	22.596,00 €

Se establece como **Valor estimado del contrato** (excluido IVA o impuesto indirecto equivalente y teniendo en cuenta las eventuales prórrogas): **168.125,00 € (CIENTO SESENTA Y OCHO MIL CIENTO VEINTICINCO EUROS CON CERO CÉNTIMOS).**

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

VALOR ESTIMADO DEL CONTRATO		
Importe de Licitación		134.500,00 €
Plazo de Ejecución (meses)	12	
Modificación 20%	NO	0,00 €
Prórroga (meses)	SI 3	33.625,00 €
VALOR ESTIMADO DEL CONTRATO		168.125,00 €

El contrato podrá ser prorrogado por 3 meses, en las mismas condiciones técnicas y económicas. Dicha prórroga será obligatoria para el contratista siempre que se produzca con un preaviso de 2 meses de antelación a la finalización del plazo de duración del contrato. No se contempla la opción de modificación.

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

- Forma de acreditación de la solvencia económica y financiera:

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

- Forma de acreditación de la solvencia técnica y profesional:

☒	Certificado de correcta ejecución de los servicios o trabajos realizados, expedidos o visados por la entidad para la que hayan sido realizados
☐	Relación y perfil o <i>Curriculum Vitae</i> del personal, integradas o no en la empresa, que participará en el contrato. Se aportará el CV ciego del personal o equipo humano (es decir, sin referencia a datos de carácter personal) disponible para el cumplimiento de este 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.
☐	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.

- Forma de acreditación de adscripción de medios

☒	Relación y perfil o <i>Curriculum Vitae</i> del personal, integradas o no en la empresa, que participará en el contrato. Se aportará el CV ciego del personal o equipo humano disponible para la ejecución del contrato, en el que se recoja la formación y experiencia profesional a efectos de verificación del cumplimiento de los requisitos técnicos establecidos en el Anexo I . La experiencia acreditada deberá ser coherente con el perfil adscrito, sin establecerse umbrales genéricos adicionales distintos de los definidos en el citado Anexo I .
-------------------------------------	--

- Forma de acreditación de la habilitación profesional

☒	Certificación o declaración de conformidad con el ENS (Esquema Nacional de Seguridad) La empresa licitadora deberá presentar, copia del Certificado de Conformidad con el Esquema Nacional de Seguridad (ENS), emitido por entidad acreditada conforme al Real Decreto 311/2022, o en su caso, Declaración de Conformidad, exclusivamente válida para sistemas de categoría básica. El documento deberá: ✓ Estar vigente en el momento de la presentación de la oferta. ✓ Indicar claramente la categoría de seguridad (básica, media o alta).
-------------------------------------	---

	✓ Incluir el alcance funcional, que debe abarcar al menos los sistemas de información que soporten los servicios objeto del contrato: implantación, integración, mantenimiento, soporte, interconexión y detección de amenazas con plataformas de ciberseguridad avanzada (APT). ✓ Estar firmado por el representante legal de la entidad o por persona autorizada. En caso de Declaración de Conformidad (categoría básica), se deberá aportar, además: ✓ Evidencia del Plan de Adecuación al ENS. ✓ Documento de autoevaluación técnica conforme a las guías CCN-STIC[1].
--	--

Anexo V.- Modelo de aval.

LA ENTIDAD
.....

AVALA

Solidariamente a la empresacon domicilio
social en NIF

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

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

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

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

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

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

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

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

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

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

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

- 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 Auto Firma.

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). MT250305: contratación de la herramienta Clarity (CA Project and Portfolio Management) en modalidad Software as a Service (SaaS), así como la adquisición del plugin ITD Advanced Resource Planning en pago por uso, que complementará la herramienta Clarity (CA PPM) proporcionando funcionalidades avanzadas para la planificación de recursos, utilizados en la S.E. Correos y Telégrafos, S.A., S.M.E. Identificación de la entidad contratante: S.E. CORREOS Y TELEGRAFOS, S.A., S.M.E., con CIF A83052407.

☒ 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).

SERVICIOS
INSTRUCCIONES CON
TRATAMIENTO DE DATOS
Procedimiento: GENERAL SIN NEGOCIACIÓN
Expediente núm.: MT270303



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

No se contempla.

Anexo IX.- Criterios de adjudicación de evaluación automática

El presente Anexo regula los criterios de adjudicación evaluables mediante fórmula, aplicables a la oferta presentada por los licitadores para el contrato de servicios de mantenimiento y soporte de automatizaciones RPA (Robotic Process Automation) e Hiperautomatización de Correos.

La puntuación máxima atribuible a los criterios automáticos será de 30 puntos, dentro de la ponderación técnica total establecida en el Pliego. Para continuar en el procedimiento de adjudicación, las ofertas deberán alcanzar una puntuación mínima de 15 puntos sobre 30 en el conjunto de dichos criterios.

	Criterios Técnicos evaluables mediante Fórmula Automática	Rango Puntos
1	Aportaciones técnicas específicas:	0 a 30
1.1	Certificaciones oficiales del personal adscrito al contrato relacionadas con RPA/Hiperautomatización	0 a 15
1.2	Acreditación oficial con el fabricante de la plataforma RPA/Hiperautomatización	0 a 7,5
1.3	Experiencia adicional del equipo sobre el mínimo exigido	0 a 7,5
		Total: 30 puntos

1. Aportaciones técnicas específicas (Con un total de 15 puntos)

Este bloque tiene como objetivo evaluar la cualificación técnica y funcional de los equipos propuestos por el licitador para la prestación de cada uno de los servicios contemplados en el pliego.

Se valorará especialmente la disponibilidad de certificaciones oficiales adicionales a las exigidas en el presente Pliego, en las tecnologías base utilizadas para el mantenimiento y soporte de los servicios objeto del contrato, así como una mayor experiencia específica en la tecnología requerida que exceda de la mínima exigida, todo ello conforme a los criterios establecidos en Criterios de adjudicación de evaluación automática.

Para facilitar el proceso de evaluación de estos criterios se requiere que el documento de oferta técnica cumpla las siguientes premisas:

- Debe contener un apartado específico que haga referencia a la evaluación automática y en dicho apartado el adjudicatario debe describir estos criterios de evaluación automática. Se indicará claramente para cada criterio los datos requeridos en cada una de las fórmulas de cálculo mediante las tablas que se solicitan para cada uno de ellos y que se detallan más adelante (TABLAS DE RECURSOS CERTIFICADOS, TABLA DE CERTIFICACIONES DE MAYOR y MENOR RELEVANCIA, TABLA DE EXPERIENCIA).
- Aquellas ofertas que no aporten esta información de manera clara y completa como para poder aplicar la fórmula de evaluación en cada criterio, contabilizarán 0 puntos en aquellos criterios que no puedan ser evaluados.
- Además de la información necesaria para evaluar la formulación, es imprescindible adjuntar las certificaciones y currículums vitae que acrediten la veracidad de los datos

aportados. Si no se adjunta esa información o no coincide con lo especificado en las tablas de detalle correspondiente, contabilizarán 0 puntos en aquellos criterios para los que no se presenten evidencias documentales y oficiales al respecto o en los que la documentación presentada no coincida con el detalle de la tabla de detalle correspondiente.

1.1 Certificaciones oficiales del personal adscrito al contrato relacionadas con RPA/Hiperautomatización (hasta 15 puntos)

Se valorará la disposición por parte del licitador de certificaciones oficiales, vigentes y verificables, correspondientes al personal adscrito al contrato, directamente relacionadas con tecnologías RPA/Hiperautomatización, como elemento objetivo adicional de garantía de calidad en la prestación del servicio de mantenimiento y soporte RPA.

Este criterio no tiene carácter habilitante ni constituye requisito mínimo de participación, valorándose únicamente como mejora objetiva sobre lo exigido en el Pliego.

Certificaciones valorables

Las condiciones que debe cumplir cada certificación para ser contabilizada a efectos de este criterio son las siguientes:

- Deberán ser certificaciones oficiales emitidas por fabricantes de soluciones RPA (o equivalentes) y/o entidades reconocidas
- Deberán estar directamente relacionados con alguna de las tecnologías base que se requieren en el pliego (Ver Anexo I. – Apartado 3.2 Pila tecnológica mínima para cubrir por el servicio)
- Deberán estar vigentes (no caducadas ni a la presentación de la oferta ni durante la ejecución del contrato). Si en algún caso alguno de los certificados caduca durante la ejecución del contrato, el adjudicatario estará obligado a revalidarlo con el fabricante correspondiente y se comprometerá explícitamente mediante declaración responsable en la presentación de la oferta.
- Deberán estar emitidos a nombre de personas que estén asignadas al servicio licitado en este pliego y que implican adscripción de medios (Ver Anexo XIV. – Adscripción de medios) y NO contabilizarán si se trata de personal del adjudicatario que no esté participando de forma activa y continuada en el contrato con una dedicación del 100%:
 - Si existen recursos con un % de dedicación menor al 100% sus certificaciones NO serán contabilizadas a efectos de este criterio.
 - En todo momento, Correos podrá exigir al adjudicatario que el número y tipo de certificaciones de las personas adscritas al contrato sea el que se ha proporcionado en tiempo de oferta para obtener la puntuación formulada de evaluación automática.
 - A efectos de este criterio, únicamente se tendrán en cuenta las certificaciones correspondientes a los recursos efectivamente adscritos al contrato conforme

al Anexo XIV, con la dedicación exigida, y que participen de forma activa y continuada en la ejecución del servicio. La aportación de recursos adicionales no implicará su valoración automática, salvo que se encuentren expresamente vinculados a los criterios de adjudicación definidos en el Anexo IX.

- Esto será controlado mediante el ANS correspondiente y sujeto a penalización en caso de incumplimiento (Ver [Anexo XII – Evaluación de Proveedores](#)).

Todos los certificados que no cumplan todas y cada una de las condiciones anteriores no serán contabilizados en el cálculo de puntuación de este criterio. Además, al inicio del contrato, Correos solicitará al adjudicatario la relación de los certificados aportados por cada uno de los recursos adscritos al contrato, conforme a lo establecido en el Anexo XIV – Adscripción de medios. No se considerará cerrada la composición final del equipo (ni podrán iniciarse ni facturarse los servicios correspondientes) hasta que no se disponga de la relación y volumen de los certificados que se han declarado en la oferta.

En todo momento se contabilizará en un ANS que el equipo dispone de todos los certificados indicados en tiempo de oferta (en número y tipo de certificados), penalizando en caso de incumplimiento.

En caso de no presentar certificados (o que no cumplan todas las condiciones anteriores), se asignará 0 puntos en este criterio.

Fórmula de valoración

La distribución de la puntuación máxima de 15 puntos se repartirá de la siguiente forma:

- Un máximo de **12 puntos** aplicando la contabilización a las certificaciones que se consideran de **mayor relevancia** para los procesos/robots mantenidos en el objeto del contrato, y que se muestran en la siguiente **tabla de certificaciones de mayor relevancia** (a cada tipo de certificación se le ha asociado un COD.CERTIFICACIÓN que será referenciado posteriormente en las tablas en las que se justifican las certificaciones aportadas para este criterio de valoración):

TECNOLOGÍA	COD. CERTIFICACIÓN	CERTIFICACIÓN ²
UIPATH	C1	Agentic Automation Associate o Agentic Automation Professional
UIPATH	C2	Automation Developer Associate o Automation Developer Professional
UIPATH	C3	Automation Business Analyst Associate o Automation Business Analyst Professional
UIPATH	C4	Specialized AI Associate o Specialized AI Professional
UIPATH	C5	Automation Solution Architect Professional
UIPATH	C6	Software Testing Engineer Professional

² Las certificaciones de tipo “Associate” y “Professional” se consideran relacionadas por lo que, si una misma persona dispone de la misma certificación, pero en ambos niveles contabilizará como una única certificación (por eso se registran dentro del mismo COD. CERTIFICACIÓN).

UIPATH	C7	Infrastructure Engineer Professional – Automation Suite
UIPATH	C8	Infrastructure Engineer Professional – Standalone
AWS	C9	AWS Certified Developer Associate
AWS	C10	AWS Certified Cloud Practitioner
AZURE	C11	Microsoft Certified: Azure AI Fundamentals
AZURE	C12	Microsoft Certified: Azure AI Engineer Associate
AZURE	C13	Microsoft Certified: Azure Data Scientist Associate

- Un máximo de 3 puntos aplicando la contabilización al resto de certificaciones no recogidas en el apartado anterior pero que sí estén relacionadas con las tecnologías base contempladas en el pliego (Ver Anexo I. – Apartado 3.2 Pila tecnológica mínima para cubrir por el servicio) y/o que puedan ser consideradas por Correos de interés para el servicio.

Según todo lo expuesto anteriormente, la fórmula para calcular la puntuación de este criterio en las ofertas que presenten recursos en posesión de certificados oficiales será la siguiente:

- **Cálculo puntuación certificaciones de mayor relevancia (máximo 12 puntos):**

Será calculado teniendo en cuenta únicamente el número de certificaciones presentadas por el licitante y que se encuentren incluidas en la tabla indicada anteriormente consideradas como de mayor relevancia

$$Puntos\ Cert.\ Relevancia = \frac{N^{\circ}_{Cert.\ Relevancia\ Ofertados}}{N^{\circ}_{mayor\ Cert.\ Relevancia\ ofertado}} \times 12$$

- $N^{\circ}_{Cert.\ Relevancia\ Ofertados}$ = número de certificaciones válidas que si estén catalogados en la listas de certificados de mayor relevancia.
- $N^{\circ}_{mayor\ Cert.\ Relevancia\ ofertado}$ = número mayor de certificaciones válidos que sí estén catalogados en la lista de certificados de mayor relevancia de todas las ofertas de diferentes licitantes que hayan sido presentadas y aceptadas en la licitación del pliego.

- **Cálculo puntuación certificaciones de menor relevancia (máximo 3 puntos):**

Será calculado teniendo en cuenta únicamente el número de certificaciones presentadas por el licitante y que **NO** se encuentren incluidas en las consideradas anteriormente como de mayor relevancia pero que estén relacionadas y/o se consideren de interés para el servicio licitado en el presente pliego.

$$Puntos\ Cert.\ Otros = \frac{N^{\circ}_{Cert.\ NR\ Ofertados}}{N^{\circ}_{mayor\ Cert.\ NR\ ofertado}} \times 3$$

- $N^{\circ}_{Cert.\ NR\ Ofertados}$ = número de certificaciones válidas que NO estén catalogados en la listas de certificados de mayor relevancia.

- $N^{\circ}_{\text{mayor Cert. NR ofertado}}$ = número mayor de certificaciones válidos que NO estén catalogados en la lista de certificados de mayor relevancia de todas las ofertas de diferentes licitantes que hayan sido presentadas y aceptadas en la licitación del pliego.

▪ **Cálculo total (máximo 15 puntos):**

La puntuación final asignada a este criterio será calculada como la suma de las dos puntuaciones anteriores.

$$\text{Puntos Total Cert.} = \text{Puntos Cert. Relevancia} + \text{Puntos Cert. Otros}$$

Con el fin de valorar a todos los licitantes que concurran a esta contratación de manera equitativa bajo este criterio, Correos requiere recibir como parte de la oferta las siguientes tablas:

TABLA DE RECURSOS CERTIFICADOS

Recurso	Perfil ofertado (2)	% Dedicación (3)
Recurso 1		
Recurso 2		
....		
Recurso N		

- (1) Los recursos referenciados deben ser integrantes de manera continuada y activa del contrato en función de lo especificado en la adscripción de medios.
- (2) Indicar el tipo de perfil que cubriría el recurso de los referenciados en el epígrafe “Perfiles profesionales adscritos y dedicaciones mínimas” del **Anexo XIV. - Adscripción de medios**.
- (3) Indicar % de dedicación del recurso en el contrato (respecto a la jornada laboral de 40 horas semanales).

TABLA DE CERTIFICACIONES DE MAYOR RELEVANCIA

Recurso (1)	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
Recurso 1																
Recurso 2																
....																
Recurso N																

- (1) La denominación de cada recurso debe coincidir con la **TABLA DE RECURSOS CERTIFICADOS**.
- (2) En cada columna se indicará la certificación aportada y se marcará con una X para el recurso que disponga de ella. Las certificaciones de esta tabla serán las utilizadas para calcular el indicador **Puntos Cert. Relevancia** y cada columna de la tabla hace referencia al COD.CERTIFICACIÓN (CN) indicado para cada una de ellas anteriormente en la **tabla de certificaciones de mayor relevancia**.

TABLA DE CERTIFICACIONES DE MENOR RELEVANCIA

Recurso (1)	Certificación A (2)	Certificación B (2)	...	Certificación Z (2)
Recurso 1				
Recurso 2				
....				
Recurso N				

- (1) La denominación de cada recurso debe coincidir con la **TABLA DE RECURSOS CERTIFICADOS**.
- (2) En cada columna se indicará la certificación aportada y se marcará con una X para el recurso que disponga de ella. Se incluirán tantas columnas como tipos de certificación diferente se presente. Las certificaciones de esta tabla serán las utilizadas para calcular el indicador Puntos Cert. Otros (y **NO** estarán incluidas en la **tabla de certificaciones de mayor relevancia**).

1.2 Acreditación oficial con el fabricante de la plataforma RPA/Hiperautomatización (hasta 7,5 puntos)

Se valorará la acreditación oficial del licitador como partner del fabricante de la plataforma RPA/Hiperautomatización utilizada para la prestación del servicio (UiPath), por ser un indicador objetivo del grado de madurez, capacidad técnica y experiencia del partner en iniciativas de automatización, así como de su vinculación con el fabricante y acceso a recursos de soporte especializados.

Este criterio no tiene carácter habilitante ni constituye requisito mínimo de participación, valorándose únicamente como mejora objetiva sobre lo exigido en el Pliego.

1.2.1. Nivel oficial de partnerships (hasta 6 puntos)

UiPath estructura su ecosistema de partners en distintos niveles. A efectos de valoración se considerarán los siguientes niveles oficiales:

- Authorized (nivel de entrada): Partners en fase inicial, con conocimientos básicos de la plataforma y primeras experiencias en proyectos.
- Gold: Partners con experiencia demostrada, capacidades técnicas sólidas y participación en proyectos y oportunidades comerciales.
- Platinum: Partners con una práctica consolidada, alto nivel técnico y capacidad para ejecutar proyectos complejos de principio a fin.
- Diamond (nivel más alto): Partners estratégicos con máxima madurez, gran volumen de negocio, amplia experiencia y capacidad para liderar iniciativas de transformación a gran escala.

Asignación de puntuación por nivel oficial de partnerships

A cada nivel se le asigna la siguiente puntuación (P_a):

- Sin partnerships acreditado: $P_a = 0$
- Authorized: $P_a = 1$
- Gold: $P_a = 2$
- Platinum: $P_a = 4$
- Diamond: $P_a = 6$

1.2.2. Reconocimientos complementarios (no jerárquicos) (hasta 1,5 punto)

Adicionalmente, UiPath puede otorgar reconocimientos complementarios (no jerárquicos), tales como:

- Certified / UiPath Services Network
- Fast Track Partner
- Award Winner

Regla de valoración (automática):

- Si el licitador acredita documentalmente uno de los reconocimientos anteriores vigente: 1 punto.
- Si el licitador acredita documentalmente más de uno de los reconocimientos anteriores vigente: 1,5 punto.
- Si no acredita ninguno: 0 puntos.

Puntuación total del criterio

$$P_{Total} = P_a + P_b$$

Documentación acreditativa

- Certificado/credencial oficial vigente emitida por UiPath (o entidad expresamente autorizada por este) que identifique el nivel de partnerships del licitador.
- En su caso, credencial oficial vigente del reconocimiento complementario aportado.
- La documentación acreditativa deberá estar vigente (no caducadas ni a la presentación de la oferta ni durante la ejecución del contrato).

1.3 Experiencia adicional del equipo (hasta 7,5 puntos)

Se valorará la experiencia adicional de los recursos (según la experiencia mínima exigida como se indica en el 6. PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS, del Anexo I) en función del número acumulado de meses de los perfiles del equipo ofertado en relación con las tecnologías requeridas en el pliego, entendiendo que un mayor recorrido profesional redunda en la calidad del servicio al disponer los recursos de un periodo mayor de puesta en práctica de sus conocimientos en tareas similares a las que desarrollarán en el contrato.

La experiencia del equipo en trabajos similares a los que se van a desarrollar en el contrato se pondera sobre 7,5 puntos y la fórmula de valoración se describe a continuación.

Experiencia valorable

Las condiciones que debe cumplir la experiencia adicional del equipo para ser contabilizada a efectos de este criterio son las siguientes:

- Se trata de experiencia adicional sobre la mínima exigida en el pliego (3 años para el jefe de proyecto y 2 años para los técnicos especialistas tal y como se recoge en el [Anexo I - PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS](#)). A efectos de este criterio, únicamente se tendrá en cuenta la experiencia correspondiente a los recursos efectivamente adscritos al contrato conforme al Anexo XIV – Adscripción de medios, con la dedicación exigida y que participen de forma activa y continuada en la ejecución del servicio.
- Se tendrá en cuenta un máximo de 72 meses de experiencia adicional para cada uno de los recursos presentados. El número de meses adicional sobre 72 no contabilizará a efectos de obtener una puntuación mayor en este subcriterio.
- Debe tratarse de meses de experiencia demostrable en alguna de las tecnologías base que se requieren en el pliego (Ver [Anexo I. – Apartado 3.2 Pila tecnológica mínima para cubrir por el servicio](#)) y la acreditación de esta experiencia adicional se realizará mediante declaración responsable de la empresa y CV de los recursos ofertados.
- Se le otorgará el máximo de puntos a la oferta que presente al equipo que acumule mayor experiencia adicional, teniendo en cuenta los recursos ofertados y la dedicación propuesta. Para el resto de los proveedores que presenten un acumulado de experiencia menor, se calculará una puntuación lineal entre 0 y el máximo según su puntuación en relación con el proveedor que ha obtenido la puntuación máxima. En caso de no presentar ningún recurso con experiencia superior al número de meses indicado en cada uno de los servicios, se valorará con 0 puntos.

Todos los meses de experiencia que no cumplan todas y cada una de las condiciones anteriores no serán contabilizados en el cálculo de puntuación de este criterio. Además, al inicio del contrato, Correos solicitará al adjudicatario la relación de experiencia de cada persona del equipo y no se considerará cerrada la composición final de los equipos (ni podrán iniciarse ni facturarse los servicios correspondientes) hasta que no se disponga del volumen de experiencia acumulada que se ha declarado en la oferta.

En todo momento, Correos podrá exigir al adjudicatario que los meses de experiencia adicional de las personas adscritas al contrato sea el que se ha proporcionado en tiempo de oferta para obtener la puntuación formulada de evaluación automática y esto será contabilizado mediante un ANS que verificará que el equipo dispone de la experiencia indicada en tiempo de oferta (en número de meses y tecnologías concretas) penalizando en caso de incumplimiento (Ver Anexo XII – Evaluación de Proveedores)

En caso de no presentar CVs (o que no cumplan todas las condiciones anteriores), se asignará 0 puntos en este criterio.

Formula de valoración

Según todo lo expuesto anteriormente, la fórmula para calcular la puntuación de este subcriterio en las ofertas que presenten recursos con experiencia adicional a la mínima exigida será la siguiente:

$$Puntos \text{ Exp. Adicional} = \sum \frac{Rn ((Exp \text{ Rn} - Exp \text{ Min.}) * \% \text{ DED}))}{N^o \text{ Rn}}$$

Donde:

- *Puntos Exp. Adicional* = Puntuación de la experiencia para la oferta n
- *Rn* = Recurso N, cada uno de los recursos ofertados con sus experiencias
- *Exp Rn* = Experiencia en meses del Recurso n en el perfil ofertado. En caso de experiencia superior a 72 meses se aplicará un valor máximo de 72.
- *Exp Min.* = N° de meses de experiencia mínima exigida en el servicio sobre el que se está calculando la puntuación (siendo 60 meses para el Servicio de Liderazgo Técnico y 36 meses para el resto de los servicios)
- *% DED* = Porcentaje total de dedicación del recurso Rn
- *N° Rn* = Número de recursos de la oferta.

Con el fin de valorar a todos los licitantes que concurran a esta contratación de manera equitativa bajo este criterio, Correos requiere recibir como parte de la oferta la siguiente tabla:

Tabla de experiencia

Recurso (1)	Perfil ofertado (2)	% Dedicación (3)	Meses de experiencia (3)
Recurso 1			
Recurso 2			
....			
Recurso N			

- (1) La denominación de cada recurso puede no ser la misma indicada anteriormente en la TABLA DE RECURSOS CERTIFICADOS, pero deben ser integrantes de manera continuada y activa del servicio para el que se presentan.
- (2) Indicar el tipo de perfil que cubriría el recurso de los referenciados en el [Anexo I - PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS](#).
- (3) Indicar % de dedicación anual sobre un máximo de 1.920 horas y cumpliendo que la suma total debe coincidir como mínimo con lo referenciado para cada tipo de perfil en el [Anexo I - PERFILES PROFESIONALES Y ESTIMACIÓN DE RECURSOS](#).
- (4) Número de meses de experiencia en el perfil ofertado que se ha indicado para el recurso.

5. Oferta económica (Con un total de 70 puntos)

Criterios adjudicación económica			
Descripción	Oferta económica	Ponderación	70 puntos
Formula de valoración	$PE = PEm \left(1 - \frac{(Pon - Pse)}{PL} \right)$ Donde: ▪ PE = Puntuación oferta “n” ▪ PEm = Ponderación asignada al criterio económica ▪ Pon = Importe de la Presupuesto oferta “n” ▪ Pse = Importe de la oferta más económica ▪ PL: Presupuesto de Licitación		

Anexo X.- 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 de este. 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:

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

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

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

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

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

Incluir a continuación el desglose de los importes arriba indicados:

SOPORTE Y MANTENIMIENTO SOFTWARE				
DESCRIPCIÓN	Importe 12 meses (Sin IVA o cualquier otro impuesto indirecto equivalente)	Tipo impositivo aplicable %	Impuestos (€)	Importe Total(Con IVA o cualquier otro impuesto indirecto equivalente) (€)

Mantenimiento y soporte de RPA/Hiperautomatización para los procesos automatizados que actualmente opera la plataforma UiPath.				
Total:				

* Todos los precios e importes deben reflejarse con dos decimales. El importe total sin impuestos ofertado y la suma de su desglose de importes, deberá cuadrar al segundo decimal sin mediar redondeo. No podrán superarse los importes máximos sin impuestos por servicio indicados en el Anexo III.- Resumen de metodología seguida para el cálculo del valor estimado del contrato, en caso de superarse, supondrá la exclusión de la oferta. El importe total ofertado sin impuestos no podrá superar el importe de la base imponible del presupuesto base de licitación, indicado en el Anexo III, en caso de superarse, supondrá la exclusión de la oferta.

La facturación del contrato se organizará en torno al siguiente plan, que incluye desglose por los siguientes conceptos:

Facturación fija mensual: Importe fijo a facturar mensualmente por el servicio de Mantenimiento de los procesos, soporte y atención técnica del sistema implantado.

Lugar, fecha, sello del licitador y firma autorizada.

Anexo XI.- Régimen de penalidades.

A continuación, se indica el régimen de penalidades para cada uno de los indicadores (IND) recogidos en el [Anexo XII.- Evaluación de proveedores](#), según la gravedad de su incumplimiento.

Las penalidades asociadas a los indicadores ANS se aplicarán por mes natural y exclusivamente en función de la banda mensual (Cumple/Leve/Grave/Muy grave) determinada conforme al Anexo XII – Evaluación de Proveedores (ANS). Las mediciones quincenales, cuando existan, se considerarán evidencias intermedias y no generarán liquidación por sí mismas. No se duplicarán liquidaciones en cierres de fase si ya se han aplicado mensualmente.

La base de aplicación de las penalidades asociadas a los indicadores ANS será la facturación mensual del Servicio de Mantenimiento y Soporte RPA/Hiperautomatización correspondiente al periodo evaluado (IVA excl.), salvo que el propio indicador establezca expresamente otra base de cálculo.

En el caso de las penalidades recogidas en el apartado de Otras penalizaciones, la base de cálculo será el precio del contrato (IVA excl.), conforme a lo establecido en dicho apartado.

En todo caso, las penalidades deberán ser proporcionales a la gravedad del incumplimiento y su cuantía no podrá superar, para cada penalidad, el 10% del precio del contrato (IVA excl.), ni el total acumulado de penalidades el 50% del precio del contrato (IVA excl.), conforme a lo previsto en el artículo 192 de la LCSP. Las penalidades se impondrán por acuerdo del órgano de contratación y se harán efectivas mediante deducción en los pagos o sobre la garantía cuando proceda, conforme al artículo 194 de la LCSP.

IND1- Resolución de incidencias en plazo

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5 % sobre el importe de la facturación mensual (IVA excl.) de la prestación afectada, por incumplimientos del tiempo objetivo de resolución de incidencias (excluidas causas no imputables y ventanas aprobadas).
Grave	Penalidad de hasta un 7,5 % sobre la facturación mensual (IVA excl.) en caso de desviaciones relevantes o persistentes respecto a los umbrales de SLA definidos para resolución de incidencias.
Muy grave	Penalidad de hasta un 10 % sobre la facturación mensual (IVA excl.) cuando las desviaciones superen el nivel grave o afecten de forma crítica a la disponibilidad del servicio RPA/Hiperautomatización y/o afecten de forma crítica a la disponibilidad del servicio.

IND2- Índice de reapertura de incidencias resueltas

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5 % sobre la facturación mensual (IVA excl.) por incumplimiento de los umbrales de reapertura (ratio de reabiertas sobre resueltas) que evidencien deficiencias en la calidad de resolución..
Grave	Penalidad de hasta un 7,5 % sobre la facturación mensual (IVA excl.) cuando el índice de reapertura exceda el umbral grave, impactando la confianza en la corrección aplicada.

Muy grave	Penalidad de hasta un 10 % sobre la facturación mensual (IVA excl.) por ratios de reapertura persistentes y de alto impacto para negocio, evidencien deficiencias graves y persistentes .
-----------	---

IND3- Resolución de solicitudes en plazo

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5 % sobre la facturación mensual (IVA excl.) por incumplimiento del SLA de cierre de solicitudes (peticiones funcionales/servicio) según prioridad (solo aplica a solicitudes operativas).
Grave	Penalidad de hasta un 7,5 % sobre la facturación mensual (IVA excl.) por desviaciones relevantes y repetidas (solo aplica a solicitudes operativas).
Muy grave	Penalidad de hasta un 10 % sobre la facturación mensual (IVA excl.) por incumplimientos que afecten a la operativa con alto impacto (p.ej., ventanas críticas de planificación) (solo aplica a solicitudes operativas). ³

IND4- Seguimiento de la calidad de los entregables

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 3% sobre la facturación mensual (IVA excl.) cuando el porcentaje de entregables rechazados supere el umbral leve establecido en el Anexo XII.
Grave	Penalidad de hasta un 5% sobre la facturación mensual (IVA excl.) cuando el porcentaje de entregables rechazados supere el umbral grave establecido en el Anexo XII.
Muy grave	Penalidad de hasta un 10% sobre la facturación mensual (IVA excl.) cuando el porcentaje de entregables rechazados supere el umbral muy grave o los defectos comprometan el uso del entregable o impacten gravemente en la operativa.

IND5- Estabilidad y compromiso del equipo de trabajo⁴

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5 % sobre el importe de la facturación mensual (IVA excl.) de la prestación afectada, cuando se produzcan rotaciones no autorizadas de carácter puntual que no comprometan de forma significativa la continuidad del servicio.
Grave	Penalidad de hasta un 7,5 % sobre la facturación mensual (IVA excl.) en caso de rotaciones no autorizadas relevantes o reiteradas que afecten a la estabilidad del equipo, a la adecuada transferencia de conocimiento o a la calidad de la prestación del servicio.

³ Aplicable a los IND, en todo caso, la cuantía resultante de la penalidad quedará limitada a un máximo del 10% del precio del contrato (IVA excl.), conforme al artículo 192 de la LCSP.

⁴ A efectos del presente indicador, se considerará rotación no autorizada cualquier sustitución de personal que no cumpla simultáneamente los requisitos establecidos en el contrato, incluyendo la comunicación previa, el plan formal de traspaso de conocimiento, la equivalencia de certificaciones y experiencia, y los límites máximos de rotación permitidos. Asimismo, se considerará rotación no autorizada el fraccionamiento de la dedicación comprometida mediante recursos con dedicaciones parciales o marginales.

Muy grave	Penalidad de hasta un 10 % sobre la facturación mensual (IVA excl.) cuando el porcentaje de rotaciones no autorizadas supere el umbral del 20 %, o cuando dichas rotaciones afecten de forma crítica a la continuidad operativa del servicio, a la preservación del conocimiento o al cumplimiento de las prestaciones contractuales, la transferencia de conocimiento o la calidad del servicio.
-----------	---

IND6- Incumplir las comunicaciones de incidentes de seguridad

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de 3% facturación anual de la adjudicación o 5.000€, cuando no se entrega del informe forense.
Grave	Penalidad de 5% facturación total de la adjudicación o 10.000€ en caso de ausencia de actualizaciones durante el incidente.
Muy grave	Penalidad de 10% facturación total de la adjudicación o 20.000€ cuando no se comunique el incidente y haya sido detectado por terceros o por Correos.
Muy grave	Penalidad de 10% facturación total de la adjudicación o 20.000€, cuando haya retraso en el primer comunicado.
Muy grave	Penalidad de 10% facturación total de la adjudicación o 10.000€, cuando haya retraso en el segundo comunicado.

IND7- Detección de vulnerabilidades de ciberseguridad en procesos y soluciones de terceros

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de 2% facturación anual de la adjudicación o 5.000€, cuando se detecten 10 o más vulnerabilidades Baja (CVSS < 4.0).
Grave	Penalidad de 3% facturación anual de la adjudicación o 5.000€, cuando se detecten 5 o más vulnerabilidades Media (4.0 ≤ CVSS < 7.0).
Muy grave	Penalidad de 5% facturación anual de la adjudicación o 10.000€, cuando se detecten 1 o más vulnerabilidades Altas (7.0 ≤ CVSS < 9.0).
Muy grave	Penalidad de 5% facturación anual de la adjudicación o 10.000€, cuando se detecten 1 o más vulnerabilidades Críticas (CVSS ≥ 9.0).

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

IND8- Incumplir los requerimientos del servicio de gestión segura de la cadena de suministro

INCUMPLIMIENTO	PENALIZACIÓN
----------------	--------------

Leve	Penalidad de 3% facturación anual de la adjudicación o 5.000€, cuando no se asista a una reunión dentro del plazo de 30 días.
Grave	Penalidad de 5% facturación anual de la adjudicación o 10.000€, cuando no se faciliten las evidencias necesarias para la auditoría o evaluación dentro del plazo de 15 días.
Grave	Penalidad de 5% facturación anual de la adjudicación o 10.000€, cuando no se ejecute una prueba técnica específica o no entregar los resultados de esta dentro del plazo de 30 días.
Muy grave	Penalidad de 10% facturación anual de la adjudicación o 20.000€, cuando no se subsanen las no conformidades o no implementar los controles requeridos dentro del plazo de 90 días.

IND9- Pérdida o caducidad de las certificaciones de seguridad requeridas en la adjudicación

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de 1% facturación anual de la adjudicación o 1.000€, cuando la renovación de la certificación se produzca en más de 30 días naturales.
Grave	Penalidad de 2% facturación anual de la adjudicación o 2.000€, cuando la renovación de la certificación se produzca en más de 60 días naturales.
Grave	Penalidad de 3% facturación anual de la adjudicación o 3.000€, cuando la renovación de la certificación se produzca en más de 90 días naturales.
Muy grave	Penalidad de 5% facturación anual de la adjudicación o 5.000€, cuando se produzcan retrasos en la notificación de la pérdida/caducidad/suspensión de la certificación en el plazo de 72 horas.

IND10- Incumplimiento del mantenimiento del nivel de certificaciones y experiencia del equipo adscrito.

INCUMPLIMIENTO	PENALIZACIÓN
Muy grave	Penalidad fija del 10 % sobre el importe de la facturación mensual (IVA excluido) correspondiente al periodo evaluado, cuando uno o más recursos adscritos al contrato no mantengan el nivel de certificaciones técnicas y/o experiencia profesional comprometido en la oferta y validado al inicio del contrato.

Otras penalizaciones

Reincidencia

Las penalidades asociadas al incumplimiento de los indicadores aplicables por periodos mensuales de evaluación y las penalidades por reincidencia reguladas en este apartado son compatibles entre sí.

En particular:

a) La penalidad mensual se aplicará cuando, en el periodo de evaluación correspondiente, el indicador incurra en la calificación de Leve/Grave/Muy Grave conforme a los umbrales establecidos.

b) La penalidad por reincidencia se aplicará adicionalmente cuando, dentro de la ventana temporal definida para el mismo indicador (p. ej., tres infracciones leves en seis meses; tres infracciones graves o muy graves en doce meses), se alcance el umbral de reiteración, aplicándose una única vez en el momento en que se produzca la infracción que determina la reincidencia.

La aplicación de la penalidad por reincidencia no tiene carácter retroactivo sobre periodos ya penalizados y se entiende referida exclusivamente a la reiteración del incumplimiento del mismo indicador dentro de la ventana temporal establecida.

En todo caso, la imposición y cuantía de las penalidades se ajustará a los límites previstos legalmente (proporcionalidad; cuantía máxima de cada penalidad $\leq 10\%$ del precio del contrato, IVA excluido; límite total acumulado $\leq 50\%$ del precio del contrato, IVA excluido) y se hará efectiva mediante deducción en la factura del periodo o, si no fuera posible, sobre la garantía, conforme a lo previsto en la normativa aplicable.

- Leve: comisión de tres infracciones leves del mismo IND en 6 meses $\rightarrow$ hasta 3.000 € (IVA excl.).
- Grave: comisión de tres infracciones graves del mismo IND en 12 meses $\rightarrow$ hasta 6.000 € (IVA excl.).
- Muy grave: comisión de tres infracciones muy graves del mismo IND en 12 meses $\rightarrow$ hasta 10.000 € (IVA excl.).

Las penalidades por reincidencia computarán a efectos del límite máximo acumulado de penalidades (50% del precio del contrato, IVA excl.), conforme al artículo 192 de la LCSP.

Subcontratación

Incumplimiento del régimen de subcontratación del pliego $\rightarrow$ penalidad de hasta el 50% del importe del subcontrato (IVA excl.), sin que la cuantía resultante pueda superar en ningún caso el 10% del precio del contrato (IVA excl.), conforme al artículo 192 de la LCSP.

Condiciones especiales de ejecución

Incumplimiento de las CEE $\rightarrow$ penalidad hasta el 10 % del precio del contrato (IVA excl.).

Anexo XII – Evaluación de Proveedores.

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

ACUERDO DE NIVEL DE SERVICIO (ANS)

Los servicios que son objeto del presente pliego se regularán en su prestación por el sistema de “Acuerdo de Nivel de Servicio”. En consecuencia, las tareas correspondientes deberán realizarse ajustándose a los “Indicadores de nivel de servicio (INS)” y “valores objetivos” (VO) que se definen en el mismo y que se detallan en este anexo.

El adjudicatario, dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los VO establecidos, con independencia de los recursos que para ello tenga que incorporar en cada momento, e independientemente de si presta los servicios con medios propios o si los subcontrata parcialmente (estando esta subcontratación autorizada previamente por Correos). No obstante, si de forma puntual en algún mes uno o varios indicadores individuales se ven afectados por los trabajos correspondientes a equipos ajenos a los del adjudicatario, Correos determinará el ámbito y el alcance de la responsabilidad para ese caso concreto.

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

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

Los ANS comenzarán a computarse y aplicarse desde el primer día de la fase de prestación real del servicio (ver [Anexo I](#)).

En los apartados correspondientes a cada indicador se define el Valor de Cumplimiento y/o el Porcentaje de Cumplimiento con sus valores objetivo. Estos valores se tendrán en cuenta en el Sistema de Evaluación y en el caso de que no se alcancen los mínimos requeridos, y en función de la gravedad, se establecerá una minoración en la facturación que en su caso corresponda (ver [Anexo XI](#)).

Los ANS comenzarán a computarse y aplicarse desde el primer día de la fase de prestación real del servicio (ver [Anexo I](#)).

Para aquellos proyectos que se gestionen con metodologías ágiles, será imperativa la obtención de métricas de proyecto que permitan monitorizar el avance de este. Para ello, durante todo el proyecto deberá tenerse perfectamente controlado y publicado el nº de historias totales identificadas en el proyecto (“backlog” o pila de producto), las historias comprometidas en cada ciclo (“sprint backlog” o pila del sprint, sólo para el “siguiente ciclo”), las realizadas en el último ciclo, y la deuda técnica/funcional que vaya quedando pendiente de ciclos anteriores. Estas

sencillas métricas, tras un periodo inicial de adopción y ajuste que deberá acordarse al inicio del proyecto, deberán permitir al proyecto dotarse de cierta predictibilidad.

Sistema de evaluación

El sistema de evaluación contempla dos fases:

1. Evaluación continua y periódica durante la ejecución del contrato.
Para este contrato, el periodo de evaluación continua se establece en 1 mes.
2. Evaluación general que se realizará al finalizar un contrato consolidando los resultados de las distintas evaluaciones continuas.

Los puntos que evaluar son los siguientes:

- A. Seguimiento de prestación de servicios.
- B. Calidad.
- C. Seguimiento Equipo de Trabajo

A continuación, se muestran los ANS definidos para cada categoría y serán medidos a cada uno de los servicios objeto del contrato en la medida en que le sean de aplicación.

A. Seguimiento de prestación de servicios

Se controlan los indicadores Tiempo de resolución de incidencias/solicitudes, Reaperturas e Incidencias atrasadas. El primero mide el porcentaje de incidencias y solicitudes cerradas en el periodo dentro del valor objetivo de tiempo de resolución; el segundo, el porcentaje de incidencias reabiertas sobre el total de cerradas; y el tercero, el porcentaje de incidencias que superan el tiempo máximo establecido y permanecen abiertas a fin de periodo. El cómputo se realiza en la ventana L–V, 08:00–18:00.

Tiempo de Resolución de Incidencias/Solicitudes, Reaperturas e Incidencias Atrasadas. Mide, tanto los porcentajes del número de incidencias y solicitudes cerradas en el periodo dentro de unos valores objetivos para el tiempo de resolución, como el número de Incidencias reabiertas sobre el total de Incidencias del período y el volumen de incidencias que quedan sin resolver y superan el tiempo máximo establecido al finalizar cada periodo.

Los indicadores que intervienen

1. Resolución de incidencias en plazo:

Fórmula	Elementos Fórmula	Nivel	Consideraciones	Origen Dato	Valores de Referencia
$PC = \left(\frac{\sum NIC}{\sum TIC} \right) \times 100$	NIC = Nº de incidencias cerradas en el periodo dentro del valor objetivo para el tiempo de resolución TIC= Total de incidencias cerradas en el periodo	Todas las aplicaciones y servicios incluidos en el pliego	Se pueden establecer diferentes valores de referencia en función de la criticidad de la incidencia y del tipo (incidencias de usuario o de monitorización). En su evaluación se tendrá en cuenta el cumplimiento de las condiciones de prestación del servicio.	PoST	PCmin= Porcentaje de cumplimiento mínimo

CÓDIGO	INDICADOR DE SERVICIO	VALORES OBJETIVO	% CUMPLIMIENTO (PCmin)
1.1	Resolución de incidencias de usuario Críticas en plazo en el periodo	<= 4 horas	>= 90 %
1.2	Resolución de incidencias de usuario No Críticas en plazo en el periodo	<= 4 días	>= 90 %
1.3	Resolución de incidencias de tipo "evento de monitorización"	<= 6 horas	>= 90 %

Los valores están expresados en periodos laborables.

Observación al indicador 1.3: Se clasifican como eventos de monitorización las incidencias generadas en POST de forma automática desde las herramientas de monitorización de procesos, que recogen una ejecución fallida de algún proceso programado.

PC	PC ≥ 90,0%	85,0% ≤ PC < 90,0%	75,0% ≤ PC_Pub < 85,0%	PC_Pub < 75,0%
Gravedad	Cumple	Leve	Grave	Muy Grave

2. Índice de reapertura de incidencias resueltas:

Mide el porcentaje de incidencias reabiertas sobre el total de incidencias resueltas en el periodo.

Fórmula	Elementos Fórmula	Nivel	Consideraciones	Origen Dato	Valores de Referencia
$PC = \left(\frac{\sum IR}{\sum TIR} \right) \times 100$	IR: número total de incidencias reabiertas en el periodo TIR: Número total de Incidencias resueltas en el periodo	Todas las aplicaciones y servicios incluidos en el pliego	Se pueden establecer diferentes valores de referencia en función de la criticidad de la incidencia	PoST	PCmin= Porcentaje de cumplimiento mínimo

CÓDIGO	INDICADOR DE SERVICIO	% CUMPLIMIENTO (PCmin)
2.1	Índice de reapertura de incidencias críticas (S1) resueltas en el periodo	<= 5%
2.2	Índice de reapertura de incidencias no críticas resueltas en el periodo	<= 10%

Observaciones al indicador 2.1 y 2.2:

- En caso de que se detecte una nueva incidencia debido a la falsa resolución de una incidencia anterior, esta podrá considerarse como una reapertura.
- Para este indicador no se consideran los eventos de monitorización.

No se consideran, a efectos de este indicador, los eventos de monitorización. La calificación de una nueva incidencia como reapertura deberá quedar documentada en el ticket (enlace a la incidencia original y motivo).

Críticas (S1)	≤ 5,0%	>5,0-8,0 %	> 8,0-12,0 %	> 12,0 %
---------------	--------	------------	--------------	----------

No críticas	≤ 10,0 %	> 10,0–15,0 %	> 15,0–20,0 %	> 20,0 %
Comprobación mensual	Cumple	Leve	Grave	Muy Grave

3. Resolución de solicitudes en plazo:

Mide el % de solicitudes cerradas dentro del valor objetivo de tiempo de resolución en el periodo.

Fórmula	Elementos Fórmula	Nivel	Consideraciones	Origen Dato	Valores de Referencia
$PC = \left(\frac{\sum NSC}{\sum TSC} \right) \times 100$	NSC = nº de solicitudes cerradas en el periodo dentro del valor objetivo para el tiempo de resolución TSC= nº total de solicitudes cerradas en el periodo	Todas las aplicaciones y servicios incluidos en el pliego	Se pueden establecer diferentes valores de referencia en función de la criticidad de la solicitud	PoST	PCmin= Porcentaje de cumplimiento mínimo

Código	Indicador de Servicio	Valores Objetivo	% Cumplimiento (PCmin)
3.1	Resolución de solicitudes críticas en plazo en el periodo	≤ 3 días	≥ 90 %
3.2	Resolución de solicitudes no críticas en plazo en el periodo	≤ 12 días	≥ 90 %

Determinación: mensual (PC del mes).

	PC ≥ 90,0 %	85,0 % ≤ PC < 90,0 %	75,0 % ≤ PC < 85,0 %	PC < 75,0 %
Gravedad	Cumple	Leve	Grave	Muy Grave

B. Seguimiento de Calidad

4. Seguimiento de la calidad de los entregables

Mide el porcentaje de entregables rechazados en el periodo. Se entenderá por entregable cualquier producto generado en el marco del servicio, incluyendo:

- Documentación técnica o funcional.
- Código fuente.
- Informes de pruebas.
- Manuales de usuario o explotación.
- Trazabilidad de las actuaciones realizadas.

- Cualquier otro elemento que forme parte de la entrega formal de un servicio o servicio de mantenimiento y soporte RPA/Hiperautomatización.

Este indicador se medirá:

Fórmula	Elementos Fórmula	Periodo de tiempo	Frecuencia de medición	Valores de Referencia
$PC = \left(\frac{NRech}{NEntre} \right) * 100 \%$	NRech: número de entregables rechazados por correos en el periodo, por no cumplir los requisitos de calidad, formato, contenido o funcionalidad. NEntre: número total de entregables presentados en el periodo	A establecer en el arranque del servicio de mantenimiento y soporte RPA/Hiperautomatización, por defecto, los periodos de facturación.	A establecer en el arranque del servicio de mantenimiento y soporte RPA/Hiperautomatización, por defecto, los periodos de facturación.	VCmin: Valor objetivo mínimo VCmax: Valor máximo aceptable

A partir de este porcentaje calculado de PC, el Grado de Cumplimiento de cada entrega se calculará en base a los parámetros fijados como plazo de desviación máxima y mínima aceptados, de la siguiente forma:

Indicador servicio de mantenimiento y soporte RPA/Hiperautomatización	Indicador Servicio	VCmin	VCmax
4	Porcentaje de entregables rechazados	$VCmin \leq 10\%$	$VCmax \geq 30\%$

Gravedad de incumplimiento

	% de entregables rechazados: $PC \leq 10\%$	% de entregables rechazados $10\% < PC \leq 20\%$	% de entregables rechazados $20\% < PC \leq 30\%$	% de entregables rechazados $PC > 30\%$
Gravedad	N/A	Leve	Grave	Muy grave

C. Seguimiento de prestación de servicios

5. Estabilidad y compromiso del equipo de trabajo

Este indicador tiene como objetivo garantizar la estabilidad y continuidad del equipo técnico adscrito al contrato, así como asegurar una adecuada transferencia de conocimiento en caso de

sustitución de personal y el mantenimiento de la relación de certificaciones técnicas aportadas por los equipos.

Se evaluará el grado de rotación del equipo durante la ejecución del contrato en todas y cada una de las fases de prestación de los servicios, considerando como rotación autorizada aquella que cumpla simultáneamente todas y cada una de las siguientes condiciones:

- Haya sido comunicada a Correos por escrito con al menos 15 días hábiles de antelación.
- Incluya un plan de traspaso formal de conocimiento entre el recurso saliente y el entrante, con una duración mínima de 10 días hábiles y para la que se presentarán evidencias de su realización.
- En caso en que el recurso saliente dispusiera de alguna de las certificaciones técnicas alegadas en tiempo de oferta y comprobada al inicio del contrato solo podrá ser sustituido por un recurso entrante que disponga de la misma certificación o equivalente (que deberá estar vigente y ser acreditada adecuadamente)
- Los meses de experiencia del recurso entrante debe ser de la misma cuantía o superior a los del recurso saliente.
- No supere el límite de una rotación anual por recurso, salvo causa debidamente justificada (por ejemplo, baja voluntaria en la empresa, jubilación, cambio de empresa u otras causas de fuerza mayor).

Cualquier cambio de personal que no cumpla con estos requisitos se considerará rotación no autorizada y será objeto de penalización.

Este indicador busca evitar prácticas como la sustitución de perfiles cualificados por otros con menor experiencia una vez adjudicado el contrato, sin conocimiento ni consentimiento de Correos, así como reducir el riesgo de pérdida de conocimiento en el servicio minimizando el número de cambios realizados en el personal adscrito al mismo.

Formula de evaluación

Fórmula	Elementos Fórmula	Periodo de tiempo	Frecuencia de medición	Valores de Referencia
$PC = \left(\frac{N_{rotac\ no\ autori}}{N_{total\ recursos\ adscri}} \right) 100 \%$	Nrotac no autori: Número de cambios de personal realizados sin cumplir los requisitos establecidos. Ntotal recursos adscri: Número total de personas adscritas al contrato durante el periodo evaluado.	Trimestral	Cambio de personal adscrito al contrato	$VC_{min} = 0\%$ $VC_{max} \geq 20\%$

Indicador Proyecto	Ámbito	Nombre	Descripción
5	Compromiso de proyecto	Rotación del personal	Porcentaje que mide la permanencia y continuidad de los profesionales que el adjudicatario disponga en el contrato.

Gravedad de incumplimiento

	% de rotación no autorizada $PC = 0\%$	Total, de rechazos en PaP $0\% < PC \leq 10\%$	Total, de rechazos en PaP $10\% < PC \leq 20\%$	Total, de rechazos en PaP $PC > 20\%$
Gravedad	N/A	Leve	Grave	Muy grave

A efectos de interpretación del indicador de rotación no autorizada, se entenderá como incumplimiento muy grave aquel caso en el que el porcentaje de rotaciones no autorizadas supere el 20% del total de recursos adscritos al contrato durante el periodo evaluado.

Por ejemplo, en un equipo compuesto por 2,5 personas, se considerará incumplimiento muy grave si se producen 0,5 o más rotaciones no autorizadas en un mismo trimestre.

6. Estabilidad y mantenimiento de certificaciones del equipo de trabajo

Este indicador tiene como objetivo garantizar que, durante toda la vigencia del contrato, el equipo técnico adscrito mantiene de forma permanente el nivel de certificaciones técnicas y experiencia profesional comprometido por el adjudicatario en su oferta y verificado por Correos al inicio del contrato.

El indicador busca asegurar que las capacidades técnicas que han sido objeto de valoración en la fase de adjudicación no se degraden durante la ejecución, evitando prácticas como la adscripción inicial de perfiles altamente cualificados para obtener puntuación y su posterior sustitución, pérdida de certificaciones o reducción efectiva del nivel de experiencia sin conocimiento ni autorización de Correos.

Condiciones de cumplimiento

Se considerará que el indicador se cumple cuando, durante el periodo de evaluación, todos los recursos adscritos al contrato cumplan simultáneamente todas y cada una de las siguientes condiciones:

- Mantienen vigentes las certificaciones técnicas alegadas en la oferta y comprobadas al inicio del contrato, o certificaciones equivalentes que hayan sido expresamente aceptadas por Correos.
- Mantienen un nivel de experiencia profesional igual o superior (en meses) al acreditado en la oferta o al existente en el momento de su incorporación autorizada al contrato.
- Están efectivamente adscritos al contrato conforme a lo establecido en el Anexo XIV (Adscripción de medios), con la dedicación comprometida.
- No han sido sustituidos, apoyados o complementados mediante recursos no adscritos o con dedicaciones marginales a efectos de cubrir capacidades técnicas, certificaciones o experiencia.

El incumplimiento de cualquiera de estas condiciones para uno o más recursos adscritos supondrá el incumplimiento del indicador durante el periodo evaluado.

Formula de evaluación

Fórmula	Elementos Fórmula	Periodo de tiempo	Frecuencia de medición	Valores de Referencia
$IC = \left(\frac{N^{\circ} \text{ recursos no conforme}}{N_{\text{total recursos adscri}} \right) 100 \%$	Nrecursos no conforme: Número de recursos adscritos que, durante el periodo evaluado, no cumplen el nivel de certificaciones y/o experiencia comprometido. Ntotal recursos adscri: Número total de personas adscritas al contrato durante el periodo evaluado.	Mensual	Revisión del equipo adscrito al contrato	$VC_{min} = 0\%$ $0\% IC > 0\%$

Indicador Proyecto	Ámbito	Nombre	Descripción
10	Compromiso de proyecto	Mantenimiento de certificaciones y experiencia del equipo	Indicador que mide el mantenimiento efectivo del nivel de certificaciones técnicas y experiencia profesional comprometido por el adjudicatario durante la ejecución del contrato..

Gravedad de incumplimiento

	IC = 0%	IC > 0%
Gravedad	N/A	Muy grave ⁵

A efectos del presente indicador, se considerará recurso no conforme aquel que, durante el periodo evaluado:

- haya perdido la vigencia de una certificación comprometida sin sustitución autorizada,
- haya sido sustituido por otro recurso con menor nivel de certificación o experiencia,
- no esté efectivamente adscrito al contrato conforme al Anexo XIV,
- requiera el apoyo de recursos no adscritos o con dedicaciones marginales para mantener las capacidades técnicas del servicio.

La evaluación del indicador se realizará con periodicidad mensual, aplicándose la penalización correspondiente por cada mes en el que se detecte la situación de no conformidad, hasta su completa regularización.

⁵ No se establecen niveles de gravedad progresivos. La existencia de uno o más recursos no conformes durante el periodo evaluado implicará directamente la aplicación de la penalización correspondiente a dicho periodo.

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

Don/Doña

NIF

Con domicilio en

Calle/Plaza, nº

Telf. contacto nº

Correo electrónico

En caso de actuar en representación

Como apoderado de

CIF

Con domicilio en

Calle/Plaza, nº

Correo electrónico

DECLARA BAJO SU RESPONSABILIDAD:

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

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

☐ La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

Anexo XIV. - Adscripción de medios.

El presente Anexo tiene por objeto regular el compromiso de adscripción de medios personales por parte del adjudicatario para la correcta ejecución del contrato de mantenimiento y soporte de automatizaciones RPA/Hiperautomatización en Correos, en los términos definidos en el Pliego y sus Anexos.

La adscripción de medios constituye un elemento esencial del contrato, siendo exigible durante toda su vigencia, incluidas, en su caso, las prórrogas.

El adjudicatario deberá garantizar la adscripción efectiva de los medios personales necesarios para prestar el servicio conforme al alcance y condiciones establecidas en el Pliego, respetando los siguientes principios:

- El adjudicatario deberá garantizar que el personal adscrito al contrato dispone de un nivel adecuado de conocimiento del idioma español, suficiente para el correcto desempeño de las funciones encomendadas, la comprensión de la documentación técnica y la interacción fluida con los responsables del contrato, los equipos de Correos y, en su caso, los usuarios del servicio.
- La adscripción se realizará por dedicación (FTE) y cobertura funcional, no siendo obligatoria la identificación nominal de las personas en fase de licitación, salvo que Correos lo requiera expresamente.
- Los medios adscritos deberán contar con la capacitación, experiencia y conocimientos adecuados para la prestación de un servicio especializado de mantenimiento y soporte RPA/Hiperautomatización en entorno productivo.
- El adjudicatario será responsable de asegurar la continuidad del servicio, independientemente de incidencias internas de su organización (bajas, rotaciones, vacaciones u otras).
- La adscripción de medios deberá cubrir tanto el horario ordinario del servicio como la disponibilidad para incidencias críticas fuera de horario, conforme a lo previsto en el Pliego.
- El personal adscrito al contrato deberá prestar el servicio conforme al horario de atención y a los regímenes de disponibilidad establecidos, garantizando su alineación con el huso horario peninsular de España, a efectos de asegurar una adecuada coordinación operativa y capacidad de respuesta durante el horario ordinario y en las actuaciones fuera de horario previstas.

Perfiles profesionales adscritos y dedicaciones mínimas

Para la ejecución del contrato, el adjudicatario deberá comprometer la adscripción de, al menos, los siguientes perfiles profesionales, con las dedicaciones mínimas indicadas:

Servicio	Perfil	Nº Recurso
Servicio de Mantenimiento y Soporte.	JP / Responsable del Servicio	0,5 FTE
Servicio de Mantenimiento y Soporte	Especialistas Hiperautomatización (perfil mixto funcional-técnico)	2 FTE (1,0 FTE cada uno)

A efectos de ejecución del contrato, el adjudicatario deberá garantizar expresamente que los recursos adscritos:

1. Disponen de experiencia suficiente para cubrir todas las tecnologías incluidas en el Anexo I – Apartado “ÁMBITO TECNOLÓGICO Y ALCANCE DEL CONTRATO”; y
2. Disponen de conocimientos y experiencia para desempeñar todas las tareas/prestaciones descritas en el Anexo I – Apartado “DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/Hiperautomatización”.

Jefe de Proyecto / Responsable del Servicio RPA/Hiperautomatización

Dedicación mínima: 0,5 FTE

Coordinación general del servicio, interlocución con Correos, seguimiento de la prestación, supervisión de incidencias relevantes, control del reporting y aseguramiento del cumplimiento de las condiciones contractuales.

Especialistas Hiperautomatización (perfil mixto funcional-técnico)

Dedicación mínima: 2 recursos con dedicación del 100% (1,0 FTE cada uno)

Los dos recursos técnicos adscritos deberán tener dedicación efectiva del 100% al contrato durante el horario ordinario del servicio y la disponibilidad prevista para incidencias críticas, conforme al Pliego.

A efectos del presente Anexo, la dedicación mínima de 2,0 FTE no podrá cumplirse mediante el fraccionamiento en más de dos personas con dedicaciones parciales (por ejemplo, cuatro recursos al 50% u otras combinaciones equivalentes). En consecuencia, el adjudicatario deberá adscribir dos recursos individuales, cada uno con dedicación 1,0 FTE.

Los 2 recursos adscritos con dedicación del 100% deberán garantizar, de forma conjunta, la cobertura integral de las funciones necesarias para prestar el servicio conforme al Pliego y, en particular, la cobertura completa de todas las prestaciones descritas en:

- Anexo I – Apartado “DETALLE DE LAS PRESTACIONES DE MANTENIMIENTO Y SOPORTE RPA/Hiperautomatización”, y
- el resto de las condiciones de prestación y exigencias operativas definidas en el Anexo I.

En particular, deberán cubrir, de forma conjunta, tanto el análisis funcional-operativo y validación de resoluciones como la resolución técnica, operación diaria y mantenimiento correctivo, preventivo y adaptativo de las automatizaciones RPA/Hiperautomatización, incluyendo coordinación con Explotación cuando proceda.

Requisitos mínimos de experiencia y acreditación

Los medios adscritos deberán cumplir, como mínimo, los requisitos de experiencia establecidos en el Anexo I – Perfiles profesionales y requisitos mínimos del equipo, entendiéndose que dicha experiencia deberá estar directamente relacionada con servicios de mantenimiento y soporte RPA/Hiperautomatización en entornos productivos.

La experiencia y capacitación se acreditará mediante currículum vitae y/o acreditaciones equivalentes, que deberán aportarse en los términos y momentos que establezca Correos durante la ejecución del contrato o cuando así se requiera para verificar el cumplimiento de la adscripción comprometida.

A efectos de acreditación documental (incluyendo certificaciones y currículums aportados en la oferta para justificar capacidades), Correos considerará únicamente los recursos efectivamente adscritos conforme a este Anexo, sin que puedan computarse recursos adicionales con

dedicaciones marginales o no comprometidos para acreditar capacidades, certificaciones o cobertura del servicio.

Régimen de sustituciones

En caso de que resulte necesario sustituir a alguno de los medios adscritos, el adjudicatario deberá:

- Comunicar previamente la sustitución a Correos.
- Garantizar que el perfil sustituto cumple requisitos de experiencia y capacitación equivalentes o superiores a los del perfil sustituido.
- He de asegurar que la sustitución no afecta negativamente a la continuidad ni a la calidad del servicio.

Correos podrá rechazar motivadamente aquellas sustituciones que no cumplan los requisitos establecidos en el Pliego y sus Anexos.

Adicionalmente, toda sustitución deberá mantener la capacidad efectiva de cubrir:

- las tecnologías del Anexo I – Ámbito Tecnológico y Alcance, y
- las prestaciones del Anexo I – Detalle de Prestaciones.

En el caso de sustitución de cualquiera de los dos recursos técnicos adscritos (1,0 FTE), el recurso sustituto deberá incorporarse con la misma dedicación del 100% (1,0 FTE) y con experiencia/capacitación equivalentes o superiores, manteniéndose en todo momento la adscripción mínima de dos recursos técnicos al 100%.

Los medios adscritos que vayan a prestar los servicios deberán participar en la fase de asimilación para asegurar la transferencia de conocimiento y la continuidad operativa. Esta participación no genera devengo ni facturación, y se considera condición de ejecución alineada con lo previsto en el Anexo I (7.1).

Anexo XV. Compromiso de adscripción de personal al contrato.

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

En caso de actuar en representación

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

DECLARA BAJO SU RESPONSABILIDAD / MANIFIESTA

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

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

Lugar, fecha y firma de licitador

Anexo XVI -Requerimientos Arquitectura

La empresa adjudicataria quedará obligada a cumplir las especificaciones detalladas a continuación que sean aplicables:

1. Soluciones EN MODO PAGO POR USO / SaaS ("software as a service"):

1.1. Requerimientos Generales: Servicios de la solución Global

El adjudicatario deberá proporcionar el servicio de la solución global en la modalidad "Software as a Service" (SaaS), es decir, dispondrá del software, del hardware, de las comunicaciones y seguridad necesarias y realizará todos los servicios de hosting, mantenimiento, operación, recuperación de datos, anticipación a incidencias, resolución de incidencias, dar la máxima disponibilidad posible del Servicio y cualquier otro para la prestación de un pago por Servicio de la manera más óptima y de máxima disponibilidad.

- Como base de lo aquí descrito, el adjudicatario deberá diseñar, instalar, implantar y mantener la solución bajo las siguientes consideraciones:
- En el supuesto de que el Servicio SaaS, sea montado por el adjudicatario en un IaaS propio, cada componente de la solución deberá estar soportada por un fabricante, con reconocimiento global (por ejemplo, AWS, Microsoft Azure, Google Cloud) durante el inicio y el ciclo de vida del contrato con el mantenimiento del versionado evitando la obsolescencia.
- Se debe aportar, si existiera, la necesidad de integración con Servicios Horizontales y con Aplicaciones, así como sus opciones de integralidad técnica del servicio ofrecido con los sistemas corporativos de Correos.
- En el caso de requerirse integraciones con aplicaciones de Correos, el servicio SaaS deberá permitir el éxito de esta respetando los estándares tecnológicos fijados por Correos:
 - Servicios web (SOAP o REST) que exponen un API de negocio.
 - Intercambio de mensajería mediante el uso de colas.
 - Intercambio de ficheros, vía SFTP/FTPS
 - Otros
- Se debe proveer de un servicio para la realización de pruebas integradas con los Entornos no productivos.
- Los cambios en la configuración de la plataforma SaaS, que se deban realizar como parte de procesos de "tuning" o mejora continua del servicio, serán comunicados a Correos con una antelación mínima de 15 días a fin de que el personal de Correos disponga del tiempo mínimo necesario para seguir los procedimientos internos para programar las intervenciones pertinentes y poder realizar los cambios de configuración.
- En el supuesto de soluciones híbridas que requiera recursos en el CPD de Correos, se deberá especificar las características y necesidades de los recursos que debe aportar Correos.

- Arquitectura que posibilite una alta disponibilidad tanto en una o varias zonas de disponibilidad geográfica de los sistemas que soporten el/los servicios contratados, asegurando que estará por encima de 99,9% anual.
- El adjudicatario deberá tener:
 - Configuraciones y acciones predictivas que permitan reducir el tiempo de recuperación de los servicios en menos de 4 horas, para garantizar la continuidad de estos.
 - Implementación de políticas automatizadas de respaldo con pruebas periódicas de restauración con retención de al menos 30 días
 - Salvaguarda de la información, que permitan establecer un tiempo de recuperación de datos (RPO) igual o con tendencia a cero.
 - En el supuesto de dotar el servicio desde varios centros de datos dispersos geográficamente, estos deben estar en el marco de la Unión Europea y deberá indicarse en la oferta, si se despliega el servicio en un CPD alternativo en una configuración activo-activo, activo-pasivo o simplemente como solución contingencia.
 - Escalabilidad a medida que se incorporan nuevos servicios, nuevos tenant, o mayor consumo del servicio que reduzca el tiempo de provisión de equipamiento que soporte los nuevos servicios. El servicio contratado deberá asegurar los picos de trabajo, proporcionando un servicio sin degradación en las épocas de mayor actividad y garantizando que la plataforma soporte un incremento de hasta el 100% de la carga con aviso previo de 48 horas.
- El tiempo de respuesta y los recursos dedicados al servicio de Correos no se verá afectado por picos en los procesos que sean compartidos con otros clientes.
- Se deberá disponer con sistemas de protección antiDDoS, así como filtrado con características WAF.
- La solución deberá contemplar la posibilidad de una migración (aunque no sea automática) desde modelo en la nube o “SaaS” (on Demand) a un modelo “in house” (On-Premise) y viceversa. Para ello, el prestatario deberá garantizar la portabilidad de datos mediante APIs documentadas y soporte técnico para la transición a otras plataformas, si fuera necesario. Los datos serán eliminados de manera completa y certificada por parte del adjudicatario, en este caso.
- El dato y la información que se guarde en la solución SaaS pertenece a Correos y sólo bajo autorización expresa se permitirá al adjudicatario, extraer datos o información de sus clientes o propios. Especificar los medios de protección que mitigue en este sentido la fuga de información.

1.2. Mantenimiento, operación y monitorización de los sistemas

Las actuaciones necesarias para la operación, el mantenimiento y la evolución del servicio se realizarán preferentemente sin la parada del servicio. Sin embargo, para aquellas situaciones donde sea requisito, se podrán realizar paradas del servicio planificadas:

- Las paradas se realizarán preferentemente en una ventana de menor impacto para Negocio.
- Todas las paradas deberán ser notificadas con anterioridad a Correos, indicando el nivel de afectación esperado y el tiempo previsto sin servicio.
- Las paradas que se lleven a cabo fuera de la ventana de menor impacto deberán ser consensuadas por Correos.

Adicionalmente, Correos podrá definir periodos de congelación de cambios en los sistemas con motivo de la realización de “campañas” que evite afectar a sus clientes por su elevado impacto económico para la compañía y durante las cuales no se podrá realizar intervención alguna sobre los sistemas para no impactar el servicio que ofrece a sus clientes. Así mismo, en caso de prestarse un Servicio de soporte, debe estar perfectamente dimensionado ante cualquier eventualidad en dichas fechas.

El servicio debe ser convenientemente monitorizado por el prestatario desde el nivel físico hasta el negocio (funcionamiento extremo a extremo del servicio). En cuanto se detecte una incidencia, se enviará un informe que incluya tanto los tiempos de indisponibilidad del servicio como una breve explicación de las causas y de las acciones puestas en marcha para solucionar la incidencia. Asimismo, y dentro de las 48 horas posteriores a la resolución, se enviará un análisis de la causa raíz (RCA), para eventos críticos.

Además del mantenimiento y la operación de la totalidad de las infraestructuras sobre las que se presta el servicio, el proveedor deberá administrar de forma proactiva anticipándose a las incidencias y planificando las mejoras necesarias para ofrecer un servicio de calidad. Aquellos eventos que puedan afectar al servicio, incluyendo degradación de rendimiento, actualizaciones críticas o incidentes de seguridad, serán notificados de manera proactiva por parte del prestatario a Correos, indicando el impacto previsto y el plan de mejoras a implementar.

En caso de que Correos solicitara algún tipo de información respecto a los parámetros del servicio prestado, el adjudicatario facilitará a Correos soporte para exportar datos operativos y métricas en formatos estándar para su uso en sistemas internos.

1.3. Acuerdos de Nivel de Servicio

Sobre la base de los Niveles de Servicio incluidos en su propuesta técnica, el adjudicatario del contrato deberá presentar una Propuesta formal de Acuerdo de Nivel de Servicio (ANS), en la que, como mínimo, se contemplen los siguientes requisitos y de acuerdo con las especificaciones indicadas en el presente pliego:

- Alcance sobre cada uno de los servicios.

- Disponibilidad del servicio, en al menos el 99,9% incluyendo fines de semana sólo en el caso de que se use por Correos los fines de semana.
- Modelo de gobierno:
- Modelo de Comunicación.
- Funciones y responsabilidades.
- Tablas de indicadores de nivel de servicio.
- RTO (Return Time Objective) o tiempo máximo de restablecimiento del servicio una vez que ya no se ha cumplido el ANS contratado, y Correos podrá aplicar KPIs incrementales a fin de evitar que la persistencia de una incidencia no se refleje adecuadamente en los indicadores una vez que ya ha contabilizado como tal.
- RPO. (Return Point Objective) o período de tiempo máximo asumible sobre el que se puede perder datos. Desde Correos por defecto, la tendencia debe ser igual a cero.

A la vista de dicha propuesta, y una vez que Correos haya validado los indicadores propuestos por el adjudicatario y el cumplimiento de los mínimos requeridos, ambas partes suscribirán el correspondiente Acuerdo de Niveles de Servicio Definitivo, que será de aplicación durante todo el periodo de vigencia del contrato.

1.4. Propiedad de los datos

Correos será el propietario de cuantos trabajos parciales o finales se deriven de esta colaboración, así como de todos los datos, el adjudicatario se compromete a la devolución de estos siempre que Correos lo considere oportuno sin que el adjudicatario pueda conservarlos, ni obtener copia de estos o facilitarlos a terceros.

Deberá venir especificado en la oferta las condiciones sobre las que se regirá la devolución de la información.

2. Solución “ON-PREMISE” para productos o desarrollo a medida

2.1. Arquitectura basada en capas

La solución, salvo requerimientos de un producto, deberá modelarse siguiendo una arquitectura de N capas:

- Capa de presentación, se corresponde con la interfaz de usuario.
- Capa de lógica o negocio, se corresponde con objetos de negocio perfectamente definidos y completos, es decir, que expongan las funciones de todos los procesos de negocio.
- Capa de datos, se corresponde con la capa específica de acceso a datos según el patrón DAO.

Los licitadores deberán describir la arquitectura propuesta de manera detallada indicando expresamente cualquier necesidad de servicio horizontal o hardware adicional para ofrecer su solución.

Entre los datos de la arquitectura, está la arquitectura del procesador, versionados de sistema operativo, middleware, bases de datos, y en general de todo el software de base y todo elemento que forme parte de la infraestructura, bien sea de hardware o de software. Deberá facilitarse una propuesta de solución.

2.2. Entornos de Servicio disponibles

El CPD (Centro de Proceso de Datos), en adelante CPD, de Correos se divide actualmente en cuatro entornos:

- *Entorno de Desarrollo:* Utilizado para las pruebas de Aceptación de Usuario, validación de funcionalidad del código, y pruebas integradas con otras aplicaciones. También como entorno para acciones de formación. Por tanto, es importante recalcar que este entorno no está destinado a la construcción de software. El software debe ser construido en las instalaciones del cliente, y ser desplegado en Correos cuando sea el momento de validarlo e integrarlo.
- *Entorno de Preproducción:* Utilizado para el análisis, verificación y validación del proceso de paso a producción.
- *Entorno de Producción:* Entorno productivo, de acceso por parte de los Usuarios de Correos para el desarrollo de su trabajo diario y por parte de empresas externas.
- *Entorno de Contingencia:* Dependerá de la criticidad y grado de afectación al negocio de Correos, se decidirá montar una réplica exacta del entorno de Producción que entrará en servicio cuando no es posible reestablecer el sistema de producción y, en un corto periodo de tiempo, se normalizará el funcionamiento del proceso de negocio.

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

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

2.3. Entorno Tecnológico

La solución deberá ajustarse, en la medida de lo posible, a los estándares arquitectónicos de Correos vigentes en el momento de licitación y que se detallarán a continuación.

La infraestructura software sobre la que se instale la solución deberá ajustarse a la matriz de compatibilidad del fabricante cuando sea un producto y será Correos quien decidirá el software base, así mismo, todo desarrollo a medida deberá en la medida de lo posible, ajustarse los siguientes requerimientos y que igualmente será decisión de Correos la Torre Tecnológica a utilizar:

Elemento	Versiones
----------	-----------

Virtualizadores	IBM Power 8 VMware (versión 5.5 o superior).
Sistemas Operativos	Red Hat Enterprise Linux 8 o superior (plataforma de 64 bits) Windows 2019 R2 o superior (plataforma de 64 bits) IBM AIX 7.2 TL4 (plataforma IBM Power) Amazon Linux 2.0
Gestor de Base de Datos	Relacional: - Oracle 19C - PostgreSQL 13 - SQL Server 2019 Documento - MongoDB 4.x
Servidores de aplicaciones	JBossEAP 7.3 para arquitecturas basadas en Linux. WebSphere Application Server Network Deployment 9.0.5 para arquitecturas basadas en AIX. Internet Information Server 10 para arquitecturas basadas en Windows.
Lenguajes de programación corporativos	OpenJDK 11 o superior para arquitectura basadas en Linux. JavaScript/Typescript para la para los frontales en ReactJS. IBM SDK 7 o superior para arquitecturas basadas en AIX. .NET v4.8 para arquitectura basadas en Windows.
Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux. IBM HTTP Server 9.0.5 para arquitecturas basadas en AIX.
Orquestador Contenedores	Open shift Container Platforms 3.11 (Docker) para arquitecturas basadas en microservicios.
Imágenes de Contenedores	Frontend: NGinx (1.x) / Apache (2.4.x) / Node.js (x) Backend: Springboot (XXX) ETL: Nifi (1.x) API: Mulesoft (4.x)

El control de acceso de los usuarios a las aplicaciones se basa en los servicios LDAP que ofrece Microsoft Active Directory montado en Correos. En concreto, las aplicaciones deben usar OAuth 2.0 para interactuar con los IDP corporativos.

Si el Software de Base asociado al producto/desarrollo no estuviera entre el especificado en los puntos anteriores, no se considerará un punto excluyente, si bien es cierto aumentará los costes de la solución global al suponer mayores costes de desarrollo y esfuerzo en la explotación para Correos. Arquitectura de Correos provee de arquetipos que facilitan y aceleran la construcción de aplicaciones corporativas.

Tanto el software listado anteriormente como su licenciamiento será proporcionado por Correos salvo en el caso de los Appliances y si la solución requiere de software específico no

contemplado (Ej.: Windows Cal). la administración y explotación de dicho software recaerá en el adjudicatario.

2.4. Requerimientos Generales

El adjudicatario deberá diseñar, instalar, implantar y mantener, salvo que no se disponga dentro del pliego, la solución bajo las siguientes consideraciones:

- La solución deberá estar soportada por un fabricante. El adjudicatario deberá aportar certificación al respecto de dicho fabricante.
- Correos garantizará la matriz de compatibilidad de fabricantes.
- Correos dotará toda la infraestructura, software base, middleware y BBDD especificada en el punto de Entorno Tecnológico, así como su mantenimiento y explotación, salvo que el producto o servicio contratado lo disponga.
- Dentro del ámbito del mantenimiento de una solución desarrollada a medida, el adjudicatario debe participar activamente en adaptar el código, pruebas, despliegues o cualquiera que haga falta para la actualización del parque tecnológico.
- Se debe aportar, si existiera la necesidad de integración con Servicios Horizontales y con Aplicaciones, así como sus opciones de integración técnica del servicio ofrecido con los sistemas corporativos de Correos.
- Será requisito que la solución se ajuste a las tecnologías, estándares y normativas establecidas en Correos. En el caso de requerirse integraciones con aplicaciones de Correos, la solución deberá permitir el éxito de esta respetando los estándares tecnológicos fijados por Correos:
 - Servicios web (SOAP o REST) que exponen un API de negocio.
 - Intercambio de mensajería mediante el uso de colas.
 - Intercambio de ficheros, vía SFTP/FTPS
 - Otros
- Se debe proveer de un servicio para la realización de pruebas integradas con los Entornos no productivos.
- El licitador debe garantizar la total compatibilidad e integración de la solución (infraestructura y servicios) que ofrezca con los elementos y aplicaciones existentes en los CPD de Correos, así como con sus plataformas de gestión operativas, cumpliendo los requisitos de integración anteriormente expuestos.
- Se deberán definir e implantar configuraciones que permitan reducir el tiempo de recuperación de los servicios.
- Se deberán definir e implantar configuraciones de los sistemas de almacenamiento y de salvaguarda de la información, que permitan establecer un tiempo de recuperación de datos (RPO) igual a cero.
- El servicio será escalable, con la posibilidad de extender la plataforma a medida que se incorporan nuevos servicios, reduciendo el tiempo de provisión de equipamiento que soporte los nuevos servicios.

- La solución deberá contemplar la posibilidad de una migración (aunque no sea automática) desde modelo un modelo “in house” (on premise) a un modelo en la nube o “SaaS” (on Demand), y viceversa.
- En la solución propuesta se admitirá el uso de componentes Hardware (Appliances) sólo en el caso de que no exista la posibilidad de realizarla con el hardware que aprovisiona Correos. Así mismo, todo Servidor que requiera un software base con tecnologías distintas al apartado de Entorno Tecnológico, excluyendo versiones, podría ser tratado también como appliance si el equipo de explotación no tuviera el conocimiento para su administración, teniendo que contemplar el licitante expresamente en la oferta como concepto de administración y mantenimiento por el conjunto de servidores y su software base, excluyendo el de producto o desarrollo que presta el servicio. Una vez adjudicado se evaluará la compatibilidad con las herramientas de monitorización, logs, de backup., junto los equipos de explotación de Correos.
- En el caso de que la solución propuesta por el adjudicatario suponga agregar, modificar, sustituir o realizar cualquier acción adicional sobre la plataforma existente (ya sea de hardware, software, licenciamiento o cualquier otro tipo), será su responsabilidad realizar todas las tareas oportunas, incluyendo capacitación específica al personal técnico correspondiente, para conseguir el correcto funcionamiento del entorno final requerido, sin que esto suponga ningún coste añadido para la entidad ni para el organismo destinatario, sin pérdida de la continuidad del servicio que se presta, y sin perjuicio de los plazos establecidos en el presente Pliego.
- La solución ofertada por el licitador se ajustará a los siguientes requerimientos:
 - Roadmap del producto: el fabricante deberá ofrecer un compromiso de evolución del producto que asegure la continuidad de este como mínimo durante un plazo de CINCO (5) AÑOS o especificar en el caso de no cumplimiento.
 - Consolidación del producto: la fecha de lanzamiento de la primera versión del producto ofertado deberá ser como mínimo TRES (3) AÑOS anterior a la fecha de presentación de la oferta por parte del licitador o especificar en el caso de no cumplimiento.
 - Última versión liberada: la fecha de última versión/actualización del producto ofertado deberá ser como máximo SEIS (6) MESES anterior a la fecha de presentación de la oferta por parte del licitador.
 - Perdurabilidad de las versiones y versión más antigua operativa soportada: la fecha de la versión operativa más antigua que es soportada por el fabricante debe ser como mínimo DIECIOCHO (18) MESES anterior a la fecha de presentación de la oferta por parte del licitador, De manera que Correos pueda evaluar el impacto que supondría la no continuidad del producto sobre la futura evolución de sus sistemas, tanto a nivel de sistema operativo, base

de datos, software de base en general, como de middleware, aplicación, o cualquier otro que pueda imponer dependencias con respecto al servicio a contratar.

2.5. Integración con herramientas corporativas

El proveedor debe asumir que los proceso/robot/desarrollo soporta su integración con las herramientas de backup, monitorización y gestión corporativas que utiliza Correos.

Correos aportará la solución de monitorización, backup y gestión siempre y cuando no se requiriera un Software específico para la misma, en cuyo caso será el adjudicatario quién la proporcionará acorde a los criterios que exige Correos (debe ser centralizada y se debe facilitar la misma información que la herramienta corporativa a sustituir).

Correos dispondrá de acceso remoto al software que permita la gestión y monitorización de los equipos.

Entre las herramientas, que utiliza actualmente Correos en este ámbito, destacan:

- BMC Patrol: sistema de monitorización que permiten gestionar las posibles incidencias que se produzcan en las infraestructuras instaladas para proporcionar servicio a Correos.
- BMC Control-M: sistema para la planificación de procesos batch, quedando prohibida la utilización de crons.
- Tivoli Storage Manager (TSM): Este software gestiona toda la operativa de copias de seguridad de los servidores corporativos con arquitectura abierta existentes en los CPD corporativos.

2.6. Licencias

El licitador debe aportar la forma de licenciar de los productos, así como su coste dado que puede afectar de manera significativa a los precios propuestos (Ej.: número de usuarios concurrentes, número de usuarios nombrados, número de servidores, número de procesadores o cualquier otro concepto)

De igual modo, deben especificarse requerimientos de licenciamiento específicos en un Entorno Virtualizado.

Adicionalmente, para aquellos casos en los que sea necesario licenciar Entornos No Productivos, debe indicar el porcentaje de coste de licencia con respecto a un Entorno de Producción.

El adjudicatario deberá proveer las licencias correspondientes para prestar el servicio necesario. Deberá así mismo en su oferta proponer una solución que garantice la correcta custodia, uso y aprovechamiento de las licencias facilitadas. Una vez implantada la solución, Correos revisará estas condiciones para asegurar que se estén aprovechando correctamente las licencias ofertadas.

3. Solución “CLOUD CORPORATIVA” para productos o desarrollo a medida

3.1. Suscripciones/Cuentas

La solución deberá poder construirse en cualquiera de los clouds adoptados por Correos, bajo suscripciones o cuentas facilitadas por Correos.

Si la solución permitiera el uso de diferentes servicios propios del cloud correspondiente, y dado que en el “Cloud” existen distintos modelos de servicio (IaaS, PaaS SaaS, CaaS, FaaS e iPaaS), dichos servicios de cloud deberán ajustarse a los criterios de preferencia de Correos en cuanto a:

- El nivel de abstracción de la solución respecto a la administración, y mantenimiento de la infraestructura.
- La agilidad en la escalabilidad de la solución.
- La optimización de los recursos que ofrezca.

Si, además la solución ofreciera la posibilidad de contenerización, se deberán tener en cuenta lo indicado en la sección “Entorno Tecnológico”

3.2. Arquitectura basada en capas

La solución, salvo requerimientos de un producto, deberá modelarse siguiendo una arquitectura de N capas:

- Capa de presentación, se corresponde con la interfaz de usuario.
- Capa de lógica o negocio, se corresponde con objetos de negocio perfectamente definidos y completos, es decir, que expongan las funciones de todos los procesos de negocio.
- Capa de datos, se corresponde con la capa específica de acceso a datos según el patrón DAO.

Los licitadores deberán describir la arquitectura propuesta de manera detallada indicando expresamente cualquier necesidad de servicio horizontal o hardware adicional para ofrecer su solución.

Entre los datos de la arquitectura, está la arquitectura del procesador, versionados de sistema operativo, middleware, bases de datos, y en general de todo el software de base y todo elemento que forme parte de la infraestructura, bien sea de hardware o de software. Deberá facilitarse una propuesta de solución.

3.3. Entornos de Servicio disponibles

El Cloud de Correos se divide actualmente en tres entornos:

- Entorno de Desarrollo: Utilizado para las pruebas de Aceptación de Usuario, validación de funcionalidad del código, y pruebas integradas con otras aplicaciones, así como acciones de formación. Por tanto, es importante recalcar que este entorno no está

destinado a la construcción de software. El software debe ser construido en las instalaciones del cliente, y ser desplegado en Correos cuando sea el momento de validarlo e integrarlo.

- Entorno de Preproducción: Utilizado para el análisis, verificación y validación del proceso de paso a producción.
- Entorno de Producción: Entorno productivo, de acceso por parte de los Usuarios de Correos para el desarrollo de su trabajo diario y por parte de empresas externas.

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

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

3.4. Entorno Tecnológico

La solución deberá ajustarse, en la medida de lo posible, a los estándares arquitectónicos de Correos vigentes en el momento de licitación y que se detallarán a continuación.

La infraestructura software sobre la que se instale la solución deberá ajustarse a la matriz de compatibilidad del fabricante cuando sea un producto y será CORREOS quien decidirá dicho software base. Así mismo, todo desarrollo a medida deberá en la medida de lo posible, ajustarse los siguientes requerimientos y que igualmente será decisión de Correos la Torre Tecnológica a utilizar:

Elemento	Versiones
Sistemas Operativos	Red Hat Enterprise Linux 7 o superior (plataforma de 64 bits) Windows 2016 R2 o superior (plataforma de 64 bits)
Gestor de Base de Datos	Relacional: ▪ Amazon RDS (PostgreSQL) ▪ Amazon Aurora (motor PostgreSQL) Clave-valor ▪ DynamoDB Documento ▪ Atlas MongoDB 4.x
Servidores de aplicaciones	JBossEAP 7 o superior para arquitecturas basadas en Linux. Internet Information Server 10 para arquitecturas basadas en Windows.
Lenguajes de programación corporativos	OpenJDK 11 o superior para arquitectura basadas en Linux. JavaScript/Typescript para los frontales ReactJS .NET v4.5 o superior para arquitectura basadas en Windows.

Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux.
Orquestador Contenedores (Plataforma Contenedores)	Open shift Container Platforms 3.11 (Docker) para arquitecturas basadas en microservicios.
Imágenes de Contenedores	Frontend: NGinx (1.x) / Apache (2.4.x) / Node.js (x) Backend: Springboot (XXX) ETL: Nifi (1.x) API: Mulesoft (4.x)
IaC	Terraform

El control de acceso de los usuarios a las aplicaciones se basa en los servicios LDAP que ofrece Microsoft Active Directory montado en Correos. En concreto, las aplicaciones deben usar Oauth 2.0 para interactuar con los IDP corporativos.

Si el Software de Base asociado al producto/desarrollo no estuviera entre el especificado en los puntos anteriores, no se considerará un punto excluyente, si bien es cierto aumentará los costes de la solución global al suponer mayores costes y esfuerzo en la explotación para Correos.

Tanto el software listado anteriormente como su licenciamiento será proporcionado por Correos salvo en el caso de los Appliances y si la solución requiriere de software específico no contemplado (Ej.: Windows Cal). La administración y explotación de dicho software recaerá en el adjudicatario.

3.5. Requerimientos Generales

El adjudicatario deberá diseñar, instalar, implantar y mantener, salvo que no se disponga dentro del pliego, la solución bajo las siguientes consideraciones:

- La solución deberá estar soportada por un fabricante. El adjudicatario deberá aportar certificación al respecto de dicho fabricante.
- Correos garantizará la matriz de compatibilidad de fabricantes.
- Correos dotará toda la infraestructura, software base, middleware y BBDD especificada en el punto de Entorno Tecnológico, así como su mantenimiento y explotación, salvo que el producto o servicio contratado lo disponga.
- Dentro del ámbito del mantenimiento de una solución desarrollada a medida, el adjudicatario debe participar activamente en adaptar el código, pruebas, despliegues o cualquiera que haga falta para la actualización del parque tecnológico.
- Se debe aportar, si existiera la necesidad de integración con Servicios Horizontales y con Aplicaciones, así como sus opciones de integración técnica del servicio ofrecido con los sistemas corporativos de Correos.

- Será requisito que la solución se ajuste a las tecnologías, estándares y normativas establecidas en Correos. En el caso de requerirse integraciones con aplicaciones de Correos, la solución deberá permitir el éxito de esta respetando los estándares tecnológicos fijados por Correos:
 - Servicios web (SOAP o REST) que exponen un API de negocio.
 - Intercambio de mensajería mediante el uso de colas.
 - Intercambio de ficheros, vía SFTP/FTPS
 - Otros
- Se debe proveer de un servicio para la realización de pruebas integradas con los Entornos no productivos.
- El licitador debe garantizar la total compatibilidad e integración de la solución (infraestructura y servicios) que ofrezca con los elementos y aplicaciones existentes en Correos, así como con sus plataformas de gestión operativas, cumpliendo los requisitos de integración anteriormente expuestos.
- Se deberán definir e implantar configuraciones que permitan reducir el tiempo de recuperación de los servicios.
- Se deberán definir e implantar configuraciones de los sistemas de almacenamiento y de salvaguarda de la información, que permitan establecer un tiempo de recuperación de datos (RPO) igual a cero.
- El servicio será escalable, con la posibilidad de extender la plataforma a medida que se incorporan nuevos servicios, reduciendo el tiempo de provisión de equipamiento que soporte los nuevos servicios.
- La solución deberá contemplar la posibilidad de una migración (aunque no sea automática) desde modelo un modelo “cloud” a un modelo en la nube o “in house” (on premise), y viceversa.
- En la solución propuesta se admitirá el uso de componentes Hardware (Appliances) sólo en el caso de que no exista la posibilidad de realizarla con el hardware que aprovisiona Correos. Así mismo, todo Servidor que requiera un software base con tecnologías distintas al apartado de Entorno Tecnológico, excluyendo versiones, podría ser tratado también como appliance si el equipo de explotación no tuviera el conocimiento para su administración, teniendo que contemplar el licitante expresamente en la oferta como concepto de administración y mantenimiento por el conjunto de servidores y su software base, excluyendo el de producto o desarrollo que presta el servicio. Una vez adjudicado se evaluará la compatibilidad con las herramientas de monitorización, logs, de backup., junto los equipos de explotación de Correos.
- En el caso de que la solución propuesta por el adjudicatario suponga agregar, modificar, sustituir o realizar cualquier acción adicional sobre la plataforma existente (ya sea de hardware, software, licenciamiento o cualquier otro tipo), será su responsabilidad realizar todas las tareas oportunas, incluyendo capacitación específica al personal técnico correspondiente, para conseguir el correcto funcionamiento del entorno final

requerido, sin que esto suponga ningún coste añadido para la entidad ni para el organismo destinatario, sin pérdida de la continuidad del servicio que se presta, y sin perjuicio de los plazos establecidos en el presente Pliego.

- La solución ofertada por el licitador se ajustará a los siguientes requerimientos:
 - Roadmap del producto: el fabricante deberá ofrecer un compromiso de evolución del producto que asegure la continuidad de este como mínimo durante un plazo de CINCO (5) AÑOS o especificar en el caso de no cumplimiento.
 - Consolidación del producto: la fecha de lanzamiento de la primera versión del producto ofertado deberá ser como mínimo TRES (3) AÑOS anterior a la fecha de presentación de la oferta por parte del licitador o especificar en el caso de no cumplimiento.
 - Última versión liberada: la fecha de última versión/actualización del producto ofertado deberá ser como máximo SEIS (6) MESES anterior a la fecha de presentación de la oferta por parte del licitador.
 - Perdurabilidad de las versiones y versión más antigua operativa soportada: la fecha de la versión operativa más antigua que es soportada por el fabricante debe ser como mínimo DIECIOCHO (18) MESES anterior a la fecha de presentación de la oferta por parte del licitador, de manera que Correos pueda evaluar el impacto que supondría la no continuidad del producto sobre la futura evolución de sus sistemas, tanto a nivel de sistema operativo, base de datos, software de base en general, como de middleware, aplicación, o cualquier otro que pueda imponer dependencias con respecto al servicio a contratar.

3.6. Integración con herramientas corporativas

Si el proveedor no manifiesta en oferta lo contrario, se asume que el producto/desarrollo soporta su integración con las herramientas de backup, monitorización y gestión corporativas que utiliza Correos.

Correos aportará la solución de monitorización, backup y gestión siempre y cuando no se requiriera un Software específico para la misma, en cuyo caso será el adjudicatario quién la proporcionará acorde a los criterios que exige Correos (debe ser centralizada y se debe facilitar la misma información que la herramienta corporativa a sustituir).

Correos dispondrá de acceso remoto al software que permita la gestión y monitorización de los equipos y se proporcionará documentación completa y actualizada para facilitar la integración y el monitoreo.

Entre las herramientas, que utiliza actualmente Correos en este ámbito, destacan:

- BMC Patrol: sistema de monitorización que permiten gestionar las posibles incidencias que se produzcan en las infraestructuras instaladas para proporcionar servicio a Correos.
- BMC Control-M: sistema para la planificación de procesos batch, quedando prohibida la utilización de crons.
- Tivoli Storage Manager (TSM): Este software gestiona toda la operativa de copias de seguridad de los servidores corporativos con arquitectura abierta existentes en los CPD corporativos.

La plataforma debe proporcionar APIs RESTful y Webhook para consultar métricas clave de rendimiento (CPU, memoria, tiempo de respuesta, disponibilidad), así como integración nativa con protocolos como SNMP o exportadores para herramientas como Prometheus o Grafana.

3.7. Licencias

El licitador debe aportar la forma de licenciar de los productos, así como su coste dado que puede afectar de manera significativa a los precios propuestos (Ej.: número de usuarios concurrentes, número de usuarios nombrados, número de servidores, número de procesadores o cualquier otro concepto)

De igual modo, deben especificarse requerimientos de licenciamiento específicos en un Entorno Virtualizado.

Adicionalmente, para aquellos casos en los que sea necesario licenciar Entornos No Productivos, debe indicar el porcentaje de coste de licencia con respecto a un Entorno de Producción.

El adjudicatario deberá proveer las licencias correspondientes para prestar el servicio necesario. Deberá así mismo en su oferta proponer una solución que garantice la correcta custodia, uso y aprovechamiento de las licencias facilitadas. Una vez implantada la solución, Correos revisará estas condiciones para asegurar que se estén aprovechando correctamente las licencias ofertadas.

4. Desarrollos a medida

4.1. Arquitectura de Microservicios

Sistemas en los que las funcionalidades se encuentran divididas en distintos artefactos, independientes entre sí, y de tamaño reducido. Cada uno de estos artefactos expone un API de servicios REST, que permite a los demás servicios interactuar con él para cumplir con la funcionalidad global del aplicativo.

4.1.1. Backend

Estos microservicios deben ser diseñados e implementados teniendo en cuenta que serán desplegados en una plataforma de contenedores, normalmente en infraestructura Cloud. Por tanto, el diseño y la construcción deben estar optimizados, empleando los patrones de diseño oportunos, y empleando buenas prácticas de programación, que optimicen los recursos y los

costes de explotación de la aplicación. La seguridad de estos servicios se basa en el estándar OAuth2, y los mecanismos para la validación de los tokens de seguridad serán provistos por Correos.

Pila tecnológica:

- Java Springboot
- Spring Data JPA
- Feign
- Hystrix
- Docker
- Open shift Container Platforms sobre AWS
- Spring MVC
- Springboot Admin
- Lombok
- MapStrut
- JaCoCo
- Mockito
- Swagger
- Maven
- Mule SDK
- YAML
- JWT

Los arquetipos para desarrollar bajo estas arquitecturas de referencia se encuentran disponibles en el repositorio de código y artifactories de Correos.

4.1.2. Frontend

Para facilitar, acelerar, y estandarizar la labor de construir aplicaciones frontales, Correos ha creado un “boilerplate” (basado en las librerías de ReactJS) que incorpora las dependencias, configuraciones, y elementos necesarios de UI corporativos (Storybook de Correos).

Pila tecnológica:

- ReactJS
- React Router
- Ant Design
- Bootstrap 4
- OAuth2
- npm

Deben emplearse estos arquetipos y boilerplates corporativos de forma obligatoria, ya que incluyen de caja todas las dependencias y configuraciones necesarias para el “compliance” de la nueva aplicación en los ecosistemas de Correos (a nivel de arquitectura, seguridad,

comunicaciones.). Además, el uso de estos arquetipos permite acelerar la construcción de aplicaciones para Correos, permitiendo al programador centrarse exclusivamente en la lógica de negocio.

4.2. UX, UI, Accesibilidad

La interfaz de usuario de las aplicaciones o productos licitados deberá cumplir con todas las especificaciones, normativa y requisitos establecidos por el departamento de UX/Usabilidad presentes y futuras, así como ser aprobado por dicho departamento de UX/Usabilidad de Correos.

Para el Diseño de la interfaz se seguirán las guías de estilos y normativa de usabilidad según las versiones que apliquen en cada momento al tipo de desarrollo realizado. Cuando algún elemento gráfico, visual de interacción, sea novedoso o no recogido en la última versión de estas guías, se tendrán que poner de acuerdo con el departamento de UX/Usabilidad para su desarrollo e implantación.

En cuanto a la Accesibilidad, las aplicaciones y portales de Correos han de cumplir la norma europea de Accesibilidad EN 301 549 para productos y servicios de tecnología de la información y comunicación, transpuesta en el Real Decreto 1112/2018, así como con cualquier otra actualización, o transposición futura sobre accesibilidad que afecta a Correos en los tipos de servicios o productos y los niveles de accesibilidad exigidos. Por tanto, cualquier desarrollo que se realice ha de cumplir de base y en sus mantenimientos con los niveles de accesibilidad necesarios para cumplir con dichas normas, presentes y futuras.

Las aplicaciones en Correos deben segregar su lógica de negocio de la lógica específica de presentación de la información. Por ello, las empresas licitantes deben tener en cuenta en sus diseños, que los frontales web serán artefactos independientes, que preferiblemente se renderizarán en el navegador del usuario final.

4.3. IC/CD

Las aplicaciones que se desarrollen para Correos deben incluirse dentro del ciclo de integración y despliegue continuo definido en Correos.

El proveedor licitante no deberá implementar estos mecanismos, sino que Correos proveerá de la infraestructura y procesos necesarios para que la nueva aplicación se integre en este ciclo. Sin embargo, será responsabilidad de la empresa licitante asegurar que la aplicación desarrollada se integre en este ciclo, y cumplen con los requisitos necesarios para la promoción de su código fuente:

- El código fuente de las aplicaciones estará en GitLab de Correos
- La promoción de este código generará artefactos en Nexus
- El despliegue de estos artefactos se realizará automáticamente al promocionar el código entre ramas.

- La aplicación tiene un grado de cobertura de pruebas unitarias adecuado para Correos, y dichas pruebas pueden ser ejecutadas con éxito.
- La aplicación cumple con los estándares de calidad de código definido en la casa, a través de la herramienta Kiuwan.

La creación de entornos, repositorios, bases de datos y despliegues se realizará con scripts de Jenkins que Correos pondrá a disposición del proveedor licitante.

Anexo XVII– Requerimientos Ciberseguridad

1. Normativa y Conformidad

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

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

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

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

2. Control de Acceso y SSO

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

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

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

reducir riesgos, el número de usuarios administradores no federados debe ser limitado a un máximo de tres (3) cuentas activas.

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

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

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

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

3. Respaldo y recuperación

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

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

4. Comunicaciones

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

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

El adjudicatario debe facilitar a Correos un diagrama de componentes (físicos y lógicos) de comunicaciones y seguridad, en el cual se ubiquen todos los elementos de la aplicación en sus

distintas capas y los flujos de información necesarios para la comunicación entre componentes la misma.

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

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

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

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

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

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

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

5. Integridad y confidencialidad

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

- A. Para datos en tránsito se debe utilizar la capa TLS, en su versión 1.3 o superior, para asegurar la integridad y confidencialidad de los datos transmitidos, siendo obligatorio

su uso para todas las operaciones de administración y aquellas otras, que lo requiera el nivel de confidencialidad de la información transmitida.

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

6. Tratamiento de datos

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

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

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

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

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

7. Desarrollo Seguro

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

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

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

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

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

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

8. Uso de Inteligencia Artificial

No se debe compartir información confidencial o sensible de Correos a través de ninguna herramienta de Inteligencia Artificial Generativa, 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.

Tiene que existir un procedimiento de comunicación de brechas de datos provenientes de un modelo IA a través de los canales oficiales determinados por Correos. Entendiéndose como brecha de seguridad una fuga de datos con un origen accidental o intencionado que afecte a datos de carácter personal.

Se deberán de llevar a cabo auditorías o controles de calidad en la precisión de las respuestas u output de la IA, con el objetivo de evitar errores de precisión que pueden suponer posibles riesgos reputacionales y de disponibilidad en Correos.

Todos los modelos aprendizaje de la IA deben basarse en la recopilación de información acotada exclusivamente al alcance y desarrollo de cada proyecto, cumpliendo con el principio de minimización de recopilación de datos. El entrenamiento de modelos IA con datos reales que puedan ser considerados de carácter personal, deben anonimizarse previamente antes ser utilizados para el entrenamiento.

En caso necesario, deberá existir una segregación de funciones que evite que distintos procesos con distintas IAs crucen información.

Completo cumplimiento de todas las regulaciones que establezca el legislador competente en la materia de IA, así como las políticas, normativas y procedimientos de Correos.

Analizar los riesgos de uso de IA y presentar un documento de análisis de riesgos e impacto para la privacidad específico para la necesidad existente que identifique vulnerabilidades y amenazas a las que se encuentra expuesto, así como su probabilidad de ocurrencia e impacto.

9. **Sistemas operativos y software base**

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

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

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

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

10. **Eventos de auditoría**

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

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

- Autenticación en el sistema
- Accesos a los datos del sistema
- Cambios en las cuentas y grupos de usuarios y contraseñas
- Cambios de accesos y modificaciones del sistema de log o auditoría
- Acciones realizadas con privilegios de administración
- Accesos a los Servicios de integración e intercambio de datos con sistemas internos y externos.

En general toda la actividad de sobre la información catalogada como CONFIDENCIAL. En especial en este caso se deberá generar un evento por cada actividad concreta (lectura, modificación).

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...).
- 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) se definirán con la Subdirección de Ciberseguridad de Correos.

11. Respuesta ante incidentes

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

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

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

12. Auditabilidad

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

exigencias de auditoría sobre el nivel de cumplimiento de estos de acuerdo con 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 de una auditoría interna cuyo informe deberá ser firmado por una persona autorizada y con poder de representación de la empresa prestadora del servicio. En el caso de que en alguno de estos supuestos se detecte una, no conformidad y no se haya visto resuelta, el proveedor deberá realizar una auditoría, a su costa, y proporcionar un informe de auditoría (test de penetración o hacking ético) realizado por un tercero en el último año, junto con el compromiso, en su caso, de solucionar las vulnerabilidades encontradas antes del arranque del servicio.

13. Formación y concienciación

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

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

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

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

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

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

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

Asimismo, en el caso de producirse un incidente de seguridad que tenga origen en un dispositivo ajeno a Correos, la Subdirección de Ciberseguridad podrá solicitar toda la información necesaria para controlar y mitigar los efectos de este y el titular/es del dispositivo se obliga a prestar apoyo

en la resolución del incidente, así como entregar la información registrada en el dispositivo afectado que permita la investigación y resolución del incidente.

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

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

15. Ubicación de los datos

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

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

Anexo XVIII –Requerimientos Gobierno del Dato

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

Desarrollo de integraciones de datos

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

Gestión y gobernanza

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

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

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

Calidad de datos

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

Seguridad y privacidad

El adjudicatario será el responsable de proteger los datos contra accesos no autorizados y garantizar el cumplimiento de las normativas de privacidad tal y como se determinan en los requisitos de **Seguridad de la Información** (confidencialidad, integridad y disponibilidad) (ver [Anexo XX – Requerimientos Ciberseguridad](#))

Anexo XIX–Requerimientos Calidad

Los desarrollos realizados por el adjudicatario en el marco del presente contrato deberán adaptarse a la normativa vigente en cada momento en Correos en cuanto a nomenclaturas, buenas prácticas y controles de aseguramiento de la calidad.

Con este objetivo, por parte de Correos y sobre cada producto que el adjudicatario entregue, como requisito para la aceptación del producto y condición necesaria para su implantación en un entorno de producción, se abordarán las actividades previstas en los procesos de calidad internos para cubrir los siguientes aspectos de la calidad: Control del proceso, Calidad del producto y Calidad del uso.

Estos controles constarán de revisiones documentales, pruebas de producto y auditorías periódicas sobre los sistemas desarrollados. Asimismo, estarán orientados a comprobar que el adjudicatario ha desarrollado conforme a las buenas prácticas, ha seguido la normativa vigente en Correos y ha llevado a cabo los controles de calidad necesarios antes de su puesta en producción.

En este marco, los desarrollos realizados por el adjudicatario deberán superar todas las pruebas necesarias antes de su entrega a Correos (código, unitarias, funcionales, de regresión, de aceptación, de rendimiento, de seguridad.).

Las entregas a Correos de los desarrollos deben cumplir los requisitos mínimos preestablecidos antes de su paso al entorno de producción:

- **Pruebas de código:** todas las entregas deben de cumplir con una serie de reglas de buenas prácticas ligadas al lenguaje en el que estén desarrollados. Estas buenas prácticas suelen ser estándares de facto y se suelen revisar a través de herramientas automáticas (por ejemplo, Sonar, Kiuwan, Code Inspector.) y el resultado de los análisis no deben mostrar errores de tipo “grave” o “muy grave”.
- **Pruebas unitarias:** el nivel de cobertura y de alcance debe cubrir como mínimo el 80% del código desarrollado con resultado OK.
- **Pruebas funcionales:** se debe demostrar que los desarrollos realizados cumplen con todos los requisitos funcionales, historias de usuario, así como poder constatar que el Plan de Pruebas Funcionales propuesto esta pasado y es OK.
- **Pruebas regresión:** deben realizar pruebas funcionales de carácter regresivo para constatar que nuevas funcionalidades no tienen impacto alguno sobre desarrollos ya implantados en Producción.
- **Pruebas de Seguridad:** deben realizar pruebas en las cuales pueda constatar que los desarrollos no tienen errores ni vulnerabilidades de Seguridad.
- **Pruebas de Rendimiento:** deben realizarse las pruebas oportunas de carga para asegurar que el rendimiento de las aplicaciones es el adecuado.

Los desarrollos realizados deberían pasar por unas **Pruebas de Aceptación** (en el caso de desarrollos agile) o bien **Pruebas UAT** (en desarrollos en cascada).

Durante la fase de desarrollo del software, y a la entrega del producto terminado a Correos, se deberá aportar la documentación necesaria para demostrar que se han pasado todos los controles anteriormente descritos y se realizarán a través de la Oficina de Calidad de Correos como mínimo una serie de controles como pueden ser los siguientes:

- **Estrategia de Pruebas:** reuniones, previas a la entrega del producto terminado, con los equipos de desarrollo para determinar el tratamiento que deben recibir por parte de la Oficina de Calidad, así como para obtener una planificación que recoja la entrega del producto, las pruebas a realizar por la Oficina de Calidad y la fecha de Paso a Producción. Esta actividad concluye con la aceptación documental de dicha Estrategia de Pruebas y la fijación de una planificación.
- **Control Documental:** Durante el proceso de desarrollo se realizarán revisiones y verificaciones de documentación referente a Análisis funcionales y Planes de Prueba del Proveedor de desarrollo y Control de Evidencias de Pruebas. Consisten al menos en revisar la existencia y validación de estos por parte de los distintos responsables.
- **Calidad de Código:**
 - Hay que asegurar que el código posee los niveles de calidad mínimos exigibles y sigue el proceso de Integración Continua establecido en Correos.
 - Todo el código que se entregue debe pasar por este proceso, independientemente del lenguaje en el que se haya construido.
 - Los análisis tendrán que **superar la auditoría** que consiste en **no tener defectos nuevos de tipo “Very High”** (desde la última versión que se haya subido a Producción).
- **Pruebas Funcionales:**
 - Previo a la entrega y despliegue en el entorno de test (PRE-producción), se deberán entregar las evidencias de pruebas unitarias y de integración realizadas por el equipo de desarrollo.
 - Es necesario que el equipo de desarrollo proporcione los siguientes entregables:
 - Análisis funcional.
 - Análisis técnico que deberá contener al menos:
 - Definición detallada de flujos de información
 - Definición detallada de servicios y microservicios.
 - Guías de despliegue y marcha atrás.
 - Documento de Plan de Pruebas funcional que incluya trazabilidad con cada uno de los requisitos o HU Funcionales. No se validarán PdP que contengan Requisitos/HU no trazados.
 - Documento de Plan de Pruebas Funcional de Regresión acumulativo con trazabilidad a requisitos/HU.

- Documento de Plan de Pruebas de regresión funcional identificando los casos a automatizar por parte de la Oficina de Calidad señalando el tipo de automatización GUI/API prevaleciendo las pruebas API.
- La gestión de pruebas y defectos se hará mediante la herramienta ALM de Microfocus o la que Correos determine y no será posible obtener el GO por parte de la oficina de Calidad con Defectos en estado Abierto o Bloqueado.
- **Pruebas de Seguridad:**
 - Análisis de vulnerabilidades para detectar los incumplimientos de las buenas prácticas del mercado.
 - Estas pruebas pueden tener un carácter estático (SAST), dinámico (DAST) o mixto.
 - Es necesario que el equipo de desarrollo facilite URLs de acceso del entorno de Preproducción y usuario con permisos para navegar por todo el aplicativo.

▪ **Pruebas de Rendimiento:**

Asegurar el correcto rendimiento de los sistemas antes de su explotación en los entornos productivos.

Es necesario que el equipo de desarrollo proporcione el documento del Plan de Pruebas de Rendimiento que deberá contener la siguiente información:

- Especificación de Requisitos No Funcionales
- Diagrama Técnico Arquitectura
- Integración con sistemas externos (Servicios y microservicios)
- Dependencias con otros sistemas (Servicios y microservicios)
- Configuraciones previas
- Flujos por evaluar
- Tareas previas a la ejecución
- URLs de acceso
- Permisos y usuarios de acceso a las mismas
- Datos de entrada
- Datos esperados de salida
- Procedimiento de generación de datos o ficheros necesarios
- Tareas posteriores a la ejecución
- Criterios de aceptación
- Volumetrías
- Tiempos de respuesta
- Matriz Racional
- **Prueba Producción:**

Controles funcionales que aseguren la disponibilidad de las aplicaciones de Correos en Producción.

Es necesario que el equipo de desarrollo proporcione el Documento de Plan de Pruebas funcional no intrusivo para la automatización de casos en Producción.

Tanto la tipología y el alcance de las pruebas, como las herramientas a utilizar en las mismas, deberán ser consensuados con Correos. Correos revisará la documentación de las pruebas realizadas por el adjudicatario tanto antes como después de la entrega, así como las evidencias de estas ejecuciones.

El adjudicatario deberá prestar el apoyo necesario para que Correos pueda verificar la ejecución de todas las pruebas realizadas. Una vez realizada la entrega del desarrollo, Correos realizará las pruebas de producto que considere necesarias para asegurar su calidad antes de su puesta en producción. Asimismo, realizará revisiones y auditorias para asegurar la calidad del uso de las aplicaciones en su fase de explotación.

Anexo XX–Requerimientos Oficina de Proyectos

En este anexo, se refleja los cumplimientos de estándares y metodología de la Dirección de Tecnología y Transformación Digital a los que quedará sujeta la empresa que resulte adjudicataria.

El adjudicatario del presente expediente se compromete a llevar a cabo todas sus iniciativas en conformidad con las directrices establecidas por la Oficina de Proyectos TI de Correos (PMO) y vigentes en cada momento. Esto implica adherirse a los estándares, procedimientos, directrices, prácticas recomendadas y modelos de gobierno con los requisitos de informes especificados por Correos para la ejecución de proyectos dentro del ámbito de la Dirección de Tecnología y Transformación Digital.

La empresa adjudicataria reconoce que cualquier desviación o propuesta de cambio respecto a los estándares y metodologías establecidos requerirá una aceptación y autorización por escrito por parte de Correos. Así, la PMO de Correos se reserva el derecho de evaluar y aprobar cualquier modificación propuesta por el proveedor en relación con los estándares y metodologías aplicables y a actualizar la metodología vigente en el momento de la firma del contrato, en virtud del proceso de mejora continua en el que se halla inmerso. Cualquier modificación será formalmente comunicada estableciendo los periodos de adaptación que se estimen oportunos.

El incumplimiento de esta cláusula por parte del proveedor puede ser considerado como una violación significativa del acuerdo, lo que podría resultar en acciones correctivas y penalizaciones, incluida la terminación del contrato y la exigencia de compensación por cualquier daño o pérdida resultante. El grado de cumplimiento o incumplimiento de esta quedará vinculada al ANS de “Calidad de entregables” referido en el pliego (Ver [Anexo XIV – Evaluación de Proveedores](#), y apartado [Seguimiento de Calidad](#)), estando generalizados en la metodología los entregables por hito, la catalogación de los defectos y los criterios genéricos para la identificación de fallos en la evaluación de la calidad. Las definiciones generales recogidas en la metodología podrán ser ampliadas o modificadas durante la ejecución del contrato.

Esta cláusula será vinculante durante la duración del contrato y cualquier extensión de este.

Una vez pasada la fase de solvencia se facilitará a los licitantes información detallada de la metodología vigente en ese momento.

La empresa adjudicataria será la **responsable de la gestión de los proyectos** tecnológicos durante todo su ciclo de vida, asegurando su ejecución dentro de los **plazos y presupuesto** establecidos y el alineamiento con los **objetivos estratégicos de la compañía**. Requiere de gran capacidad de liderazgo, ya que gestiona las **dependencias** entre todos los participantes del proyecto, entre los cuales se pueden encontrar equipos de desarrollo de Correos (gestores de las iniciativas de los Dominios Funcionales impactados junto con sus proveedores asociados), áreas transversales de Correos (como Arquitectura, Infraestructura, Exploración, Ciberseguridad, Calidad y Oficina del Dato), áreas de Negocio de Correos y equipos terceros de

proveedor, asegurando que trabajan de manera coordinada cumpliendo con la **Metodología de gestión de Proyectos** definida por la Dirección de Tecnología y Transformación Digital.

Será la responsable de realizar un seguimiento continuo de la **planificación**, verificando los hitos establecidos, la disponibilidad de **recursos** y el control del **presupuesto** global. También es la responsable de llevar a cabo la gestión de los **riesgos**, problemas y desviaciones, anticipándose a posibles inconvenientes y estableciendo planes de contingencia adecuados.

Durante la ejecución del proyecto, será responsable de **reportar** el estado coordinando los correspondientes **comités** de acuerdo con el **modelo de gobierno** establecido. Asimismo, será responsable de gestionar el proyecto en las **herramientas** corporativas de forma coordinada con el responsable de proyecto de Correos.

Realizará la **gestión documental** del proyecto garantizando que los documentos de gestión y entregables del proyecto están actualizados en los repositorios documentales definidos de acuerdo con el marco **metodológico vigente en Correos**.

Durante la fase de ideación, colaborará en el aterrizaje de los **requisitos** del proyecto, sus impactos en los procesos actuales y detectará las **necesidades** para la ejecución de este. Además, **coordina** a todos los participantes del proyecto para elaborar la **planificación y alcance global** además de liderar el lanzamiento del proyecto a través del Kick-Off.

Adicionalmente analizará y asegurará que el diseño funcional y técnico de la solución cubre la necesidad global asegurando consistencia en la solución propuesta.

Lidera el desarrollo del proyecto hasta su despliegue y estabilización, siendo responsable de la **coordinación de todas las actividades** necesarias para garantizar el éxito de éste. Entre otras actividades, coordinará la realización de pruebas, despliegues en los distintos entornos, necesidades de infraestructura, elaboración de un plan de contingencia, y todas aquellas actividades que se requieran para garantizar el éxito del proyecto.

Durante la fase de estabilización, establecerá y verificará los **criterios mínimos** que se deben cumplir para el cierre del proyecto, garantizando la **transferencia de conocimiento** y que se cumplen los **objetivos establecidos**.

Anexo XXI – Requisitos Formación

1. Capacitación técnica y funcional

La capacitación tiene por objeto proporcionar formación especializada a los diferentes perfiles de usuarios de Correos, según su rol, para asegurar la correcta implementación y uso de los diferentes sistemas creados o adaptados en el ámbito del contrato. El proveedor deberá garantizar que tanto los usuarios finales como los equipos técnicos reciban la formación necesaria para utilizar y administrar los sistemas de manera eficiente.

1.1. Alcance de los servicios de formación

El proveedor deberá proporcionar un programa de formación completo, detallado y personalizado para cada área y perfil de usuario afectado por la implantación o adaptación de los sistemas. Esto incluirá tanto la formación inicial, los materiales necesarios para la capacitación de todos los perfiles como sesiones adicionales y soporte tras la implantación. La formación abarcará tanto aspectos técnicos como funcionales.

1.1.1. Requisitos de la Formación – Capacitación de Roles

Dentro de cada área, habrá diferentes roles que requerirán distintos niveles de formación por lo que el proveedor deberá capacitarlos diferenciados según la complejidad del uso de las herramientas.

En el ámbito de cada sistema y/o proyecto se identificarán todos los roles, susceptibles de ser formados en cada uno de los siguientes ámbitos:

- Administradores y Técnicos.
- Funcionales por ámbito y nivel de responsabilidad.
- Analíticos y de reporte.
- Formadores internos
- Usuarios finales
- CAU y soporte técnico.

Por cada uno de los roles se concretarán:

- Los contenidos en función de los temas o aspectos a incluir.
- El formato de la formación más idóneo en cada caso.
- Los materiales y recurso para utilizar en la formación,
- La documentación resultante de la formación

1.1.2. Soporte Post-Formación

El proveedor deberá garantizar un servicio de soporte post formación tras la implantación del sistema, que incluirá:

- Acceso a una base de conocimientos: El proveedor deberá proporcionar guiones instruccionales, documentación, manuales, preguntas frecuentes (FAQs), y videos tutoriales.
- Sesiones de refresco: Se deberán ofrecer sesiones de seguimiento para aclarar dudas y ajustar el uso del sistema a las necesidades reales de Correos una vez que haya sido implantado.
- Seguimiento: Realizar un seguimiento para identificar si hay áreas en las que se necesite refuerzo, y ajustar la formación según sea necesario.
- Recoge retroalimentación de los usuarios después de cada etapa de formación para identificar áreas de mejora tanto en el contenido como en la metodología.
- Evalúa la efectividad de la formación a través del rendimiento del usuario en el sistema y su impacto en los procesos.

1.2. Plan de formación

El proveedor deberá presentar un **Plan de Formación** detallado, que deberá ser aprobado por el **Área de Desarrollo y Formación** de Correos antes de la ejecución.

El plan debe incluir:

- **Cronograma de formación:** Fechas de las sesiones, duración, y modalidad (presencial, virtual.).
- **Materiales formativos:** Manuales, guías, vídeos tutoriales, y documentación específica para cada área.
- **Evaluación de la formación:** Mecanismos para evaluar el aprendizaje de los participantes, como pruebas prácticas, encuestas de satisfacción, o ejercicios de simulación.
- **Plan de contingencia:** Acciones a realizar en caso de que surjan problemas durante la formación, ya sea por razones técnicas o por dificultades de comprensión de los usuarios.

1.2.1. Diseño de contenido personalizado

El contenido debe responder a las necesidades de:

- **Capacitación básica:** Introducción general a la nueva herramienta, navegación básica y uso general del sistema. Esta formación será común a todos los perfiles de Recursos Humanos.
- **Capacitación específica por módulo:** Sesiones formativas que se ajusten a las funciones que cada rol va a utilizar.
- **Capacitación en procesos clave:** Analistas de datos, generación de reportes o auditoría de procesos.

1.2.2. Metodología de Formación

La formación se orientará por niveles:

- **Iniciación:** Navegación básica y funciones generales del sistema.
- **Intermedio:** Funcionalidades específicas del rol (por ejemplo, procesos de contratación, administración de personal).
- **Avanzado:** Optimización de procesos, análisis de datos, generación de reportes personalizados.

La metodología se apoyará en alguno de los siguientes soportes:

- **Sesiones presenciales o virtuales:** Interactivas para roles clave como administradores y gestores de procesos.
- **Vídeos tutoriales:** Para formación bajo demanda.
- **Guías y manuales personalizados:** Adaptados a cada perfil.
- **Guías específicas por área:** manuales de uso adaptados a cada área, que contengan ejemplos prácticos y pasos a seguir en los procesos clave que se gestionarán.
- **Capacitación práctica:** Simulaciones y uso de casos reales para que cada perfil practique con el sistema.
- **Guiones instruccionales:** para diseñar formación on line.

1.2.3. Formación continua.

Se contemplará una estrategia para asegurar los refuerzos periódicos y actualizaciones según se vayan agregando nuevas funcionalidades o módulos a la herramienta o se vayan incorporando nuevos perfiles.

1.2.4. Evaluación y Certificación

- **Evaluaciones posteriores:** A medida que los empleados avanzan en los módulos de formación, implementa evaluaciones de conocimiento para asegurar que han comprendido cómo utilizar la nueva herramienta en sus funciones diarias.
- **Certificación por rol:** Los empleados pueden obtener una certificación oficial una vez que completen su formación, a través de un Programa de certificación en la tecnología ganadora según distintos perfiles: RR.HH., Tecnología (desarrollo/funcional, Arquitectura) (Detalle TI)

1.3. Requisitos de proveedor

El proveedor deberá cumplir con los siguientes requisitos en relación con los servicios de formación:

- Proveer un equipo de formadores cualificados con experiencia en la nueva herramienta y en formaciones en empresas similares a Correos.
- Entregar todos los materiales de formación y documentación en formato digital, accesible a todos los participantes.

- Garantizar que las sesiones formativas cuenten con el personal y recursos necesarios para asegurar el éxito del aprendizaje.
- Ofrecer flexibilidad en la personalización de los contenidos de la formación según las necesidades específicas de la empresa.
- Capacidad para la correlación automatizada del servicio formativo ejecutado, en relación con el consumo presupuestario asociado. Modelo de contabilidad analítica, por el que se muestre como se asocian los servicios formativos con el área funcional o departamento que establece la necesidad, mostrando diferentes indicadores para la medición de resultados.

1.4. Condiciones de entrega

El proveedor deberá coordinar con la empresa la programación de las sesiones formativas y realizar los ajustes necesarios para adaptarse a las operaciones diarias de Correos.

Todas las sesiones de formación deberán ser completadas antes de la fecha límite acordada, con un período adicional para soporte post-implantación.

El proveedor deberá entregar un informe final de la formación, que incluya:

- Participación y evaluación de cada usuario.
- Resultados de las evaluaciones de aprendizaje.
- Recomendaciones para formación futura o necesidades adicionales detectadas.

[] de su protocolo, inscrita en el Registro Mercantil de [] en el Tomo [], Folio [], Hoja []; Inscripción [],

DECLARA lo siguiente:

1. Cuestiones generales

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

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

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

5= dispone del registro de actividades actualizado y completado.

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

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

0= no dispone de DPO siendo obligatorio.

3= no dispone de DPO siendo voluntario.

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

2. Medidas de seguridad

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Confidencialidad

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

0= no

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

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

4. Accountability y rendición de cuentas

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

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

0= no tiene implantados controles periódicos.

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

5= tiene definidos e implantados controles periódicos.

5. Subcontratación

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

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

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

6. Transferencias internacionales

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

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

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

5= no se realiza Transferencias Internacionales de Datos.

7. Sanciones y procedimientos inspectores

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

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

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

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

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

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

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

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

Fdo.: []

Anexo XXIII – Cláusula sobre el uso de IA en contratos con Correos

Condiciones en materia de inteligencia artificial

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

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

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

confidencial de CORREOS o datos personales por su cuenta. Dicha comunicación deberá incluir, al menos:

- identificación del sistema o modelo de inteligencia artificial;
- identificación del proveedor o desarrollador del sistema o modelo;
- documentación técnica relevante;
- finalidad prevista del sistema o modelo;
- clasificación o nivel de riesgo del sistema o modelo conforme al RIA u otra normativa aplicable.

(VI) No podrá utilizar, ni permitir que terceros utilicen, la información confidencial de CORREOS —incluidos los datos personales tratados por su cuenta— con fines de entrenamiento, desarrollo, ajuste o mejora de modelos de inteligencia artificial de uso general o de sistemas de inteligencia artificial, ya sean propios o de terceros, salvo autorización previa, expresa y por escrito de CORREOS, y únicamente cuando dicho uso resulte estrictamente necesario para la correcta ejecución de las instrucciones de CORREOS.

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

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

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

Medidas de seguridad en el uso de Inteligencia Artificial

Cumplimiento Normativo y Estándares

El Adjudicatario/Proveedor garantiza el cumplimiento de la normativa aplicable, incluyendo (sin carácter limitativo) el Reglamento (UE) 2016/679 (RGPD), incluyendo el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los

derechos digitales (LOPDGDD), el Esquema Nacional de Seguridad (ENS), la normativa sectorial que resulte de aplicación y el Reglamento Europeo de Inteligencia Artificial (AI Act), en su versión vigente y aplicable al caso concreto.

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

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

Directrices generales de seguridad

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

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

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

CORREOS tendrá derecho a auditar, directamente o mediante un tercero independiente, los procesos y controles del Adjudicatario/Proveedor relacionados con el sistema de IA, incluyendo datos de entrenamiento, validación, seguridad y cumplimiento, con preaviso razonable y sin acceso a secretos industriales no estrictamente necesarios.

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

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

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

Otras consideraciones de seguridad:

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

Control de acceso, uso adecuado y limitaciones

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

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

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

Los siguientes usos para la IA se consideran prohibidos:

- Manipulación subliminal del comportamiento de una persona que tenga por objeto o efecto causar daños físicos o psicológicos a dicha persona o a terceros.
- Explotación de las vulnerabilidades de grupos sociales o personas en situación de especial vulnerabilidad, con el fin de manipular su comportamiento de manera que pueda causarles perjuicios a ellos mismos o a terceros.
- Evaluación, clasificación o puntuación de individuos o grupos (social scoring) basada en su comportamiento social o en características personales, ya sean conocidas, inferidas o predichas.

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

Anexo XXIV.- Modelo de contrato de encargo de tratamiento de datos personales.

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

En _____, a ____ de _____ de 20__.

REUNIDOS

DE UNA PARTE,

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

Y DE OTRA,

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

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

EXPONEN

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

CLÁUSULAS

1. Posición de las partes

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

DATOS OBJETO DE TRATAMIENTO

OBJETO DEL CONTRATO	Se debe incluir el objeto del contrato
TRATAMIENTO QUE REALIZAR	☐ Recogida ☐ Registro ☐ Estructuración ☐ Modificación ☐ Conservación ☐ Extracción ☐ Consulta ☐ Comunicación por transmisión ☐ Difusión ☐ Interconexión ☐ Cotejo ☐ Limitación ☐ Supresión ☐ Destrucción ☐ Comunicación ☒ Gestión operativa de servicios analíticos y resolución de incidencias técnicas.
FINALIDAD DEL TRATAMIENTO	☐ Gestión de clientes, contable, fiscal y administrativa ☐ Gestión de nóminas ☐ Servicios económico-financieros y de seguros ☐ Publicidad y prospección comercial ☐ Videovigilancia ☐ Recursos humanos ☐ Prevención de riesgos laborales ☐ Prestación de servicios de comunicaciones electrónicas ☐ Comercio electrónico ☐ Seguridad y control de acceso a edificios ☒ Gestión de incidencias, soporte técnico y mantenimiento de servicios analíticos.
TIPO DE DATOS	☒ Datos de carácter identificativo ☐ Características personales ☐ Académicos y profesionales ☐ Información comercial ☐ Circunstancias sociales ☐ Detalles del empleo ☐ Transacciones de bienes o servicios ☐ Categorías especiales de datos

	X Datos operacionales y técnicos generados en el uso de los servicios analíticos de Correos
CATEGORÍAS DE INTERESADOS	X Empleados X Clientes y usuarios X Proveedores ☐ Personas de contacto ☐ Beneficiarios ☐ Cargos públicos X Personal técnico y usuarios internos de los servicios analíticos de Correos

2. Obligaciones del adjudicatario

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

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

- Garantizar que las personas autorizadas para tratar datos personales observan las instrucciones y protocolos remitidos por CORREOS, así como las medidas de seguridad legales, técnicas y organizativas establecidas y asegurar que se comprometen, de forma expresa y por escrito, a respetar la confidencialidad de los datos y a cumplir con las instrucciones de CORREOS.
- Comprometerse a guardar bajo su control y custodia los datos personales accedidos y a no comunicarlos en modo alguno a terceros.
- Poner a disposición de CORREOS toda la información necesaria para demostrar el cumplimiento de sus obligaciones, según el proceso establecido en el punto 5.
- Asistir a CORREOS en la realización de los análisis de riesgo, la presentación de consultas previas a la AEPD, en el proceso de notificación de violaciones de seguridad y de respuesta a solicitudes de derechos.
- Gestión de derechos: Dar traslado de las solicitudes de derechos de protección de datos o quejas o reclamaciones por esta materia que puedan formular los interesados de forma inmediata a CORREOS y, a no más tardar, dentro del plazo de tres días naturales a contar desde su recepción.
- El deber de secreto y confidencialidad obliga al adjudicatario durante su vigencia y perdurará indefinidamente en el tiempo una vez finalizada la relación.
- En el caso de que el adjudicatario recabe datos personales por cuenta de CORREOS se obliga a realizarlo conforme las instrucciones de CORREOS, siguiendo la redacción y formato indicado y custodiando o dando traslado a CORREOS (según proceda) de las evidencias recogidas para acreditar el cumplimiento del deber de información y, en su caso, de obtención del consentimiento.

3. Declaración previa

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

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

4. Obligaciones de CORREOS

Corresponden a CORREOS las siguientes obligaciones:

- Permitir al adjudicatario el acceso a los datos objeto de tratamiento de conformidad con lo establecido en la presente cláusula.
- Realizar el análisis de riesgos que puedan derivar de la actividad de tratamiento que va a ser objeto de encargo y, en base a tal análisis, indicar al adjudicatario las medidas

técnicas y organizativas que deberá implementar para la prestación del servicio que conlleva el encargo de tratamiento.

- Realizar, si fuese necesario, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el adjudicatario.
- Realizar a la autoridad de control las consultas previas que correspondan.
- Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del adjudicatario.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- Facilitar el derecho de información en el momento de la recogida de los datos personales y/o en el momento de dirigirse a los interesados, en caso de que se dieran estos supuestos en la prestación del servicio. El adjudicatario deberá solicitar a CORREOS dicho texto con carácter previo a dirigirse a los interesados.

5. Medidas de seguridad

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

6. Derecho de auditoría

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

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

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

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

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

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

7. Notificación de violaciones de seguridad

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

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

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

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

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

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

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

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

9. Subcontratación

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

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

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

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

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

10. Cláusulas de buenas prácticas

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

11. Responsabilidad

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

12. Notificación de cambios

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

13. Tratamiento de datos de representantes y trabajadores

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

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

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

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

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

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

14. Actuación como subencargado

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

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

15. Ley aplicable

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

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

MEDIDAS DE SEGURIDAD

I. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES

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

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

II. PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

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

- Forzar el cambio de contraseñas, por lo menos, cada 6 meses y siempre que existan indicios de que su confidencialidad ha podido verse comprometida.
- Forzar a los usuarios el cambio de las contraseñas temporales después de la primera entrada.
- Mantener un registro de las contraseñas de usuarios anteriores y prevenir su reutilización.
- No mostrar las contraseñas en la pantalla cuando se están introduciendo.
- No incluir contraseñas en ningún proceso de registro automático, por ejemplo, almacenamiento en una macro o en una función clave.
- Almacenar los ficheros de contraseñas por separado de los datos de la aplicación del sistema.
- Almacenar y transmitir las contraseñas de forma que se garantice su integridad y confidencialidad.
- Plantear el uso de contraseñas basadas sistemas de autenticación fuerte (p.ej. mediante el uso de tarjetas inteligentes combinado con una contraseña).

III. GESTIÓN DE SOPORTES

- Llevar a cabo un inventariado de soportes y gestión de activos, incluyendo:
 - Un registro de propiedad de los activos.
 - Una política interna de usos aceptables de los activos.
 - Una política de devolución/sustitución de activo.
 - Un registro de asignación de activos al personal al cargo.
- Disponer de una política seguridad de equipos y de control de acceso a los repositorios físicos de información, garantizando que los mismos cuenten con las debidas garantías de seguridad respecto a:
 - El acceso a los repositorios de la información, incluyendo un registro de entradas y salidas.
 - Un procedimiento de salida de activos fuera del entorno de la entidad.
 - Un procedimiento de puesto de trabajo despejado y bloqueos de equipo
 - Un procedimiento de mantenimiento de activos.
- Contar con una política de mesas limpias que exija que:
 - El puesto de trabajo esté limpio y ordenado.
 - La documentación que no se esté utilizando se encuentre guardada correctamente (armario bajo llave para documentos en soporte papel y

carpetas de red para soportes informáticos), especialmente en el momento en que se abandona temporalmente el puesto de trabajo y al finalizar la jornada.

- Prohibir expresamente que haya usuarios o contraseñas apuntadas en post-it o similares o que se comparta esta información.
- Disponer de una serie de normas y procedimientos de control para los puestos de trabajo desatendidos que incluya:
 - El bloqueo automático de la pantalla transcurrido un cierto período de tiempo sin que se utilice.

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

IV. ACCESO FÍSICO AL LOCAL

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

V. MONITORIZACIÓN DE EQUIPOS Y REGISTRO DE LOGS

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

VI. FICHEROS TEMPORALES

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

VII. COPIAS DE SEGURIDAD Y RESPALDO Y RESILENCIA

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

VIII. DESTRUCCIÓN DE LA DOCUMENTACIÓN

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

IX. AMENAZAS INFORMÁTICAS

- **SEGURIDAD DE REDES:** Deberá contar con una política de gestión de seguridad en las redes que:
 - Proponga mecanismos de seguridad asociados a servicios en red.
 - Disponga de controles de red y políticas de segregación de redes.
- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS:** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida posible.
- **MALWARE:** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL:** Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales. El sistema de cortafuegos deberá ser actualizado de forma periódica.

- FUGA O SALIDA DE INFORMACIÓN: Introducir medidas técnicas en los sistemas de información que restrinjan la posibilidad que datos personales puedan ser exportados de forma no autorizada (p.ej. Restricción de las funcionalidades de descarga, impresión y almacenamiento de datos en los sistemas de información que procesan los datos personales) e implementar medidas técnicas que permitan detectar transmisiones no autorizadas de datos personales dentro de la organización y hacia fuera de la misma (p.ej. Sistemas de prevención de fugas de información, herramientas de monitorización de actividades de usuarios en los sistemas de información).

X. CIFRADO DE DATOS

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

XI. CONTROL DE CAMBIOS EN T.I

- Los sistemas operacionales y las aplicaciones de software deberían estar sometidas a un estricto control de la gestión del cambio. En particular, se deberían considerar los siguientes puntos:
 - La identificación y registro de los cambios significativos.
 - La planificación y pruebas de los cambios.
 - La evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de dichos cambios. d) el procedimiento de aprobación formal de los cambios propuestos.
 - La comunicación de los detalles de los cambios a las personas correspondientes.

- Los procedimientos de colchón, incluyendo los procedimientos y responsabilidades de abortar y recuperar los cambios infructuosos y los eventos imprevistos.
- Los procedimientos y las responsabilidades formales de la Dirección deberían asegurar de una manera satisfactoria el control de todos los cambios en los equipos, en el software o en los procedimientos. Cuando los cambios son realizados, se debería conservar un registro de auditoría que contenga toda la información importante.

XII. CONTROL DE CAMBIOS EN APLICATIVOS

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

XIII. GESTIÓN DE INCIDENCIAS Y BRECHAS DE SEGURIDAD

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

XIV. VIDEOVIGILANCIA

- En caso de contar con sistemas de captación de imágenes con fines de seguridad:
 - Se deberá contar con un registro de ubicaciones de las cámaras y monitores de observación.

Se deberá conservar las imágenes por el plazo máximo de 1 mes, salvo que su conservación resulte necesaria para investigar un hecho que haya afectado a la seguridad de las personas, bienes e instalaciones.