PLIEGO DE CONDICIONES ADMINISTRATIVAS Y TÉCNICAS PARTICULARES

ÍNDICE.

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

1. Entidad contratante.

Entidad contratante	Sociedad Estatal Correos y Telégrafos, S.A. S.M.E. (en adelante "Correos")
Órgano de contratación	Comité de Inversiones
Dirección/Subdirección gestora de la necesidad UGC	Dirección de Tecnología y Transformación Digital Subdirección de Explotación de Infraestructuras UGC28
Perfil de contratante	https://www.correos.com/perfil-contratante/
Dirección de contacto	C/Conde de Peñalver,19 Bis. 28006, Madrid.
Responsable del contrato	Dirección de Transformación Digital y Tecnología Subdirección de Explotación e Infraestructuras Área de Gobierno de la Plataforma Híbrida
	Datos de contacto: expdtes.infraestructura-ti@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 contrato tiene por objeto la adquisición e implantación de una solución de ITSM (Gestión de Servicios de TI), que abarque tanto la suscripción de licencias como los servicios necesarios para su puesta en marcha, configuración y adaptación, con el objetivo de evolucionar y transformar la actual herramienta BMC Remedy ITSM. Asimismo, el alcance del contrato incluye los servicios de mantenimiento y evolución del nuevo software de gestión, desde su puesta en producción y durante toda la vigencia contractual.
Código CPV	72268000 - 1 Servicios de suministro de software. 72267000 - 4 Servicios de mantenimiento y reparación de software
Lotes	☒ NO ☐ SI (Anexo III)

	Justificación de la no división en lotes: El presente procedimiento de licitación, no se divide en lotes. La no división en lotes se justifica según se indica en el artículo 52.3 b) Real Decreto-Ley 3/2020: *"El hecho de que, la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución del mismo desde el punto de vista técnico; o bien que el riesgo para la correcta ejecución del contrato proceda de la naturaleza del objeto del mismo, al implicar la necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes."* En este caso, se cumple la justificación del citado supuesto, en la medida en que la realización independiente de las diversas prestaciones comprendidas en el contrato, todas ellas interrelacionadas, dificultaría la correcta ejecución de éste desde el punto de vista técnico. Se solicita un trabajo íntegro, que contempla el mantenimiento y soporte de las suscripciones de la solución ITSM, de tal modo que se permita disponer de los recursos necesarios en cada momento para poder dar respuesta, con los niveles de calidad requeridos, a las necesidades de gestión de las áreas usuarias. Adicionalmente, en caso de que hubiera varias empresas adjudicatarias, la realización independiente de las diversas prestaciones comprendidas dentro del ámbito del contrato por parte de cada adjudicatario, podría ocasionar incidentes y problemas, lo que no es asumible. Por lo tanto, la naturaleza del servicio imposibilita su división en partes y, en consecuencia, su división en lotes.
¿Se admite oferta integradora (lotes)?	☒ NO ☐ SI (Ver condiciones)

3. Duración del contrato.

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

	Cantidad	Unidad de tiempo	Cómputo
Duración inicial	36	☐ días ☒ meses ☐ años	☐ día siguiente a la formalización del contrato

			☒ día siguiente a la comunicación de inicio del contrato por la entidad contratante ☐ la fecha que figure en la resolución de adjudicación
Prorrogable	☐ NO ☒ SI	N.º de prórrogas: 2 prórrogas, 1 de 12 meses y otra de 3 meses	15 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 y siempre que sus características permanezcan inalterables durante el periodo de duración de esta, sin perjuicio de las modificaciones que se puedan introducir de conformidad con lo establecido en los artículos 109 a 112 del RD 3/2020.			

4. Aspectos económicos.

Las cuantías del contrato serán las expresadas a continuación:

Valor estimado del contrato	3.186.650,00 €	Tres millones sesenta y dos mil novecientos sesenta y site euros con cincuenta céntimos, conforme al método de cálculo especificado en Anexo III		
Presupuesto base de licitación	2.721.774,00 €		IVA/impuesto equivalente	472.374,00 €
Anualidades (IVA incluido o impuesto indirecto equivalente)	2026	2027	2028	Total
	1.029.710,00 €	846.032,00€	846.032,00 €	2.721.774,00€

5. Condiciones de participación.

Los licitadores deberán cumplir, en el momento de finalizar el plazo de presentación de ofertas, los siguientes requisitos de participación.

Habilitación Esquema Nacional de Seguridad	Para prestar los servicios objeto de este contrato, el licitador realizará alguna de las siguientes acciones:

<table>
<tr><td></td><td>

Accederá a datos de clientes o empleados de Correos
Proveerá de aplicaciones, Sistemas de información y/o herramientas a Correos
Almacenará o custodiará información de clientes o empleados de Correos

☒ SI
☐ NO
En caso afirmativo, para ser adjudicatario del contrato, el licitador deberá prestar los servicios conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), y aportar certificación acreditativa para la categoría ALTA.
Para la acreditación, se presentará copia del Certificado de Conformidad, o en su caso, Declaración de Conformidad con el ENS, en la categoría indicada y con el alcance que abarque(n) al menos el/los sistemas(s) de información que soporte(n) los servicios prestados.
La criticidad de este expediente implica que el licitador, así como otros servicios de terceros que se incluyan en la oferta, se tienen que prestar y acreditar, para la categoría:
☐ BÁSICA
☐ MEDIA
☒ ALTA
</td></tr>
<tr><td>Solvencia económica o financiera</td><td>
☒ Volumen anual de negocios en el ámbito al que se refiere el contrato, referido al mejor ejercicio de los tres últimos, de al menos 749.800,00 euros.
☐ Otros:
…
Sobre la forma de acreditar estos requisitos, ver Anexo IV
En el caso de licitación por lotes, el requisito de solvencia se circunscribirá a cada lote
<table>
<tr><td></td><td>LOTE 1</td><td>LOTE 2</td><td>LOTE 3</td></tr>
</table>
</td></tr>
</table>

	Porcentaje/Cifra volumen anual negocio.			
	☐ Responsabilidad solidaria de la ejecución del contrato de las entidades que completen la solvencia económica y financiera del licitador			
Solvencia técnica o profesional	☒ Haber realizado 2 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 524.860,00 €. ☐ 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: … ☒ Otros: • Certificados ISO en vigor (aportando copia de este): o Certificación ISO 9001. Sistema de Gestión de la Calidad o equivalente. o Certificación ISO 27001. Sistema de Gestión de Seguridad de la Información o equivalente. o Certificación ISO 20000-1. Sistema de Gestión de Servicio de Tecnologías de la Información o equivalente. • Declaración responsable del proveedor/fabricante que los servidores que presten los servicios en modo SaaS de la herramienta se encuentren alojados en la UE. La localización de los servicios en la Unión Europea se exige con el fin de garantizar el cumplimiento de la normativa aplicable (incluido el RGPD), reforzar la protección de los datos personales y la soberanía digital, reducir riesgos derivados de legislaciones de terceros			

	países y asegurar la supervisión y control efectivo por parte de las autoridades competentes, todo ello en protección del interés público y de la seguridad de la información tratada. 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
Compromiso de adscripción de medios	☒ Sí. Medios a adscribir: Ver detalle en Anexo I.- Características técnicas específicas del contrato., apartado 3. EQUIPO DE TRABAJO ☐ No.

Los candidatos y licitadores no estarán obligados a aportar aquellos documentos justificativos u otra prueba documental de los datos que ya obraran en poder de la entidad contratante o aquellos otros que pudieran obtenerse de forma directa y gratuita, bien a través del Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público o bien a través de una base de datos nacional de un Estado Miembro de la Unión Europea, como un expediente virtual de la empresa, un sistema de almacenamiento electrónico de documentos o un sistema de precalificación.

6. Licitación del contrato.

6.1. Comunicaciones y notificaciones electrónicas.

Sin perjuicio de la publicidad que pueda acordarse de determinadas actuaciones las comunicaciones y notificaciones a los licitadores se realizarán a través de la Plataforma de Contratación del Sector Público utilizando para los avisos la dirección de correo electrónico que el licitador hubiera facilitado para su registro en dicha Plataforma.

6.2. Resolución de consultas relacionadas con la licitación.

Las dudas o consultas relacionadas con la interpretación del contenido de este Pliego se realizarán obligatoriamente a través de la Plataforma de Contratación del Sector Público, 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 seis (6) días 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 contados desde el día siguiente a aquél en que se publique el anuncio de licitación en el perfil de contratante.

Los licitadores, a excepción del Procedimiento Especial con un único licitador, deberán presentar obligatoriamente sus ofertas de forma electrónica a través de la Plataforma de Contratación de Correos (https://pcc.correos.es/licitacion/licitaciones)

utilizando para ello la "Herramienta de Preparación y Presentación de Ofertas" que desde esa plataforma se pone a su disposición (ver instrucciones y recomendaciones en **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. Criterios de adjudicación.

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

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

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.

Tipología	Criterio	Ponderación
Criterios sujetos a un juicio de valor	Técnico	30%
Criterios evaluables mediante formula o automáticamente	Técnico	21%
	Económico	49%

La distribución de la puntuación, con un 49% asignado al precio y un 51% a la calidad, obedece a la necesidad de valorar de forma prioritaria los aspectos técnicos y funcionales de la solución, dado que los servicios objeto del contrato incorporan desarrollos y componentes con *propiedad intelectual*. En este tipo de prestaciones, la calidad no solo determina la adecuación a las necesidades de la Administración, sino también la garantía de continuidad, interoperabilidad, evolución tecnológica y protección de los derechos de uso. Por ello, resulta proporcionado otorgar un peso superior a la calidad frente al precio, asegurando que la adjudicación recaiga en la oferta que aporte la mejor relación coste-eficacia y la mayor seguridad jurídica y técnica para el interés público.

En caso de incurrir en empate entre varias ofertas tras la aplicación de los criterios de adjudicación, se acudirá a lo dispuesto en el artículo 66.11 del Real Decreto Ley 3/2020

de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, relativo a los criterios de desempate.

6.6. Ofertas integradoras.

Cuando así se haya admitido expresamente, en los supuestos en que se permita la adjudicación de varios lotes a un mismo licitador, y sean varios los criterios de adjudicación, podrán estos realizar ofertas que combinen varios lotes por todos o algunos de ellas, siguiendo el modelo contenido en el Anexo de oferta económica, siempre que hayan presentado oferta individualizada a cada uno de los lotes incluidos en su oferta combinada y acrediten su solvencia económica, financiera y técnica o profesional correspondiente al conjunto de lotes.

6.7. Contenido de las ofertas.

6.7.1. Sobre 1: documentación administrativa.

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

b) En su caso, compromiso de adscripción de medios, según lo indicado en el apartado 5.

c) Compromiso de constitución de Unión Temporal de Empresarios (UTE), en su caso. Cuando dos o más empresas acudan a una licitación con el compromiso de constituirse en Unión Temporal, se deberá aportar una declaración indicando los nombres y circunstancias de los empresarios que la suscriban, la participación de cada uno de ellos y que asumen el compromiso de constituirse formalmente en Unión Temporal, caso de resultar adjudicatarios. El citado documento deberá estar firmado por los representantes de cada una de las Empresas componentes de la Unión. En estos casos cada una de las empresas deberá presentar su propio Documento Europeo Único en materia de Contratación (DEUC) a que se refiere el apartado a).

d) En su caso, declaración de que la empresa a la que representa pertenece a un grupo empresarial, con indicación de las sociedades que forman parte de este

e) Las empresas no españolas deberán aportar declaración de que se somete a la Jurisdicción de los Juzgados y Tribunales españoles de cualquier orden, para todas las incidencias que de modo directo o indirecto pudieran surgir del contrato, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponder al licitador.

f) Las empresas de Estados que no sean miembros de la Unión Europea o signatarios del Acuerdo sobre el Espacio Económico Europeo deberán aportar un informe que acredite su capacidad de obrar, expedido por la Misión Diplomática Permanente u Oficina Consular de España del lugar del domicilio de la empresa, en el que se haga constar, previa acreditación por la empresa, que figuran inscritas en el Registro local profesional, comercial o análogo o, en su

defecto que actúan con habitualidad en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.

g) Otra documentación:

….

6.7.2. Sobre 2: oferta técnica y criterios de adjudicación cuya evaluación depende de un juicio de valor.

Los criterios de adjudicación cuya evaluación depende de un juicio de valor serán los establecidos en el ***Anexo VIII.***

La documentación que constituya la oferta técnica y la que incluya los valores de los criterios de adjudicación cuya evaluación depende de un juicio de valor deberá presentarse en archivo electrónico en una o varias carpetas, comprimidas si no es posible por tamaño, con el nombre "SOBRE 2. DOCUMENTACIÓN TÉCNICA", en archivo ejecutable con formatos *.pdf, *.doc, *.docx, *.xls. *.xlsx *.odt *.ods).

Advertencia: La inclusión de cualquier documentación y/o información en el SOBRE 2 que debiera incluirse en el SOBRE 3 supondrá la exclusión del licitador.

6.7.3. Sobre 3: proposición económica y criterios de adjudicación de evaluación automática y/o con arreglo a fórmulas matemáticas.

Los criterios de adjudicación de evaluación automática y/o con arreglo a fórmulas serán los establecidos en el ***Anexo IX.***

La proposición económica se ajustará al modelo que se incluye como ***Anexo X***.

La documentación que incluya los valores de los criterios de adjudicación cuya evaluación puede realizarse de manera automática deberá presentarse en archivo electrónico, en una o varias carpetas, comprimidas si no es posible por tamaño, con el nombre "SOBRE 3. OFERTA ECONÓMICA", en archivo ejecutable con formatos *.pdf, *.doc, *.docx, *.xls. *.xlsx *.odt *.ods).

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

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

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.

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.
☐	Otra…

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

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

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

7.3. Documentación a presentar por el propuesto como adjudicatario.

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

☒	Los que acrediten la personalidad del empresario y su ámbito de actividad.
☒	Los que acrediten la representación.
☒	En el caso de contratos reservados, documentación que acredite oficialmente su condición como entidad que le faculta para resultar adjudicataria del contrato reservado.
☒	Los que acrediten disponer de la habilitación empresarial o profesional para la realización de la prestación objeto de contrato.
☒	Documentos que acrediten su solvencia económica, financiera y técnica o profesional por los medios que se especifiquen en el Anexo IV. La acreditación de la solvencia mediante medios externos exigirá demostrar que para la ejecución del contrato dispone efectivamente de esos medios mediante la exhibición del correspondiente documento de compromiso de disposición,
☒	Acreditación de la inexistencia de deudas tributarias y con la Seguridad Social, mediante la presentación de los correspondientes certificados emitidos por los organismos competentes.
☒	Los que acrediten la efectiva disposición de los medios que se exijan adscribir a la ejecución o, en su caso, se hubiesen comprometido a dedicar a la ejecución del contrato
☒	Cuando se ejerzan actividades sujetas al Impuesto sobre Actividades Económicas: Alta, referida al ejercicio corriente, o último recibo, junto con una declaración responsable de no haberse dado de baja en la matrícula del citado Impuesto o, en su caso, declaración responsable de encontrarse exento.
☒	Declaración relativa al lugar en el que estarán los servidores en los que se almacenan datos personales y desde dónde se van a prestar los servicios asociados a los mismos, (Esta declaración deberá presentarse con carácter previo cada vez que se producen cambios en las anteriores circunstancias).
☒	Contrato de Encargo de Tratamiento de Datos, conforme al modelo consignado en el Anexo XV en caso de resultar de aplicación.
☒	Resguardo de constitución de la garantía definitiva y, en su caso, provisional.
☒	Declaración responsable sobre la implantación del plan de igualdad conforme a lo establecido en el artículo 71 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☐	Otros

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

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

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

7.4. Adjudicación del contrato.

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

7.5. Perfección del contrato.

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

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

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

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

La formalización de los contratos deberá asimismo publicarse en el perfil de contratante y en el Diario Oficial de la Unión Europea.

7.6. Constitución de garantías.

RÉGIMEN DE GARANTÍAS		
Constitución de garantía provisional	☒ NO ☐ SI	☐ 3% del presupuesto base de licitación, IVA excluido.
Constitución de garantía definitiva	☒ 5% del importe de adjudicación del contrato o el lote o lotes adjudicados, IVA excluido.	Si el licitador la constituye mediante aval, deberá utilizar el modelo incluido como Anexo V. Si utiliza otro medio, consultará las condiciones que

			debe reflejar el documento de constitución con la entidad contratante.
			Además de por la correcta ejecución del contrato, la garantía definitiva responderá de los daños y perjuicios que se ocasionen a la entidad contratante y de los gastos que puedan derivarse de las reclamaciones fehacientes de cumplimiento o ejecución de las garantías.
Constitución de garantía complementaria	☐ NO ☒ SI	Importe	☒ 5% sobre el importe de adjudicación (en caso de oferta temeraria). (IVA excluido) ☐ Otros: ….
Cuando varíe el importe del contrato por cualquier causa, el contratista vendrá obligado a ajustar el importe de las garantías constituidas en la proporción que corresponda en al plazo de 10 días hábiles desde que se le notifique la causa determinante de la variación del importe del contrato. De no cumplirse este requisito por causas imputables al contratista en el plazo establecido, la entidad contratante podrá resolver el contrato, con pérdida de la garantía que tuviera constituida el contratista. En el caso de que se impongan penalidades al contratista y deban hacerse efectivas contra la garantía definitiva constituida, el adjudicatario quedará obligado a reponer esta garantía en los diez días hábiles siguientes a que se comunique la ejecución de la garantía inicial.			

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

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

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

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

8. Ejecución del contrato.

8.1. Obligaciones del adjudicatario.

8.1.1. Obligaciones en materia fiscal, laboral y medioambiental.

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

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

Para la ejecución de este contrato:

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

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 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:

1. Si el desarrollo del servicio objeto de licitación implicase un acceso del adjudicatario a los datos de carácter personal de los que la entidad contratante resulte Responsable del Tratamiento el adjudicatario, en calidad de Encargado del Tratamiento, se compromete a firmar un Contrato de Acceso a Datos por cuenta de 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

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

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

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

2. Si el desarrollo del servicio objeto de licitación implicase una comunicación de datos ya sea de la entidad contratante (como cedente) al adjudicatario (como cesionario), del adjudicatario (como cedente) a la entidad contratante (como cesionario) o recíproca, el adjudicatario se compromete a regular la comunicación de datos a través de una adenda cuyo cumplimiento garantice que la comunicación de datos se realiza bajo las exigencias previstas en la normativa de protección de datos vigente y, entre otras, recoja los siguientes aspectos:

El compromiso por parte del cedente de que:

I. Los datos personales han sido obtenidos conforme con la legislación vigente, siendo lícita su comunicación y posterior tratamiento para las finalidades enumeradas en el Pliego.

II. Los datos personales son tratados de conformidad con la normativa vigente en materia de protección de datos, y en particular, el RGPD y LOPDGDD.

El compromiso por parte del cesionario de:

I. Utilizar los datos personales exclusivamente para las finalidades expuestas en el Pliego y, en caso de querer utilizarlos para otras finalidades, solicitar el previo consentimiento del cedente o de los propios interesados (en caso de ser éste necesario).

II. Tratar los datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular, el RGPD y la LOPDGDD.

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

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

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

La empresa adjudicataria vendrá obligada a contar con una política propia de prevención de imputaciones delictivas similar a la establecida por la entidad contratante, o directamente adherirse a los procedimientos y políticas internas implantados por la misma. A estos efectos, la empresa adjudicataria podrá consultar el Código General de Conducta para el correcto cumplimiento de este que aparece en el documento "programa de prevención de riesgos penales" accesible a través de la web https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf

8.1.5. Evaluación de proveedores.

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

8.1.6. Obligaciones esenciales del contrato.

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

☒	Compromisos 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 recogidas en las letras a) y e) del artículo 122.2 de la LCSP.
☒	Las relativas al tratamiento de dato personales y al sometimiento a la normativa nacional y europea en la materia.
☒	Las relativas al tratamiento de datos personales y el sometimiento a la normativa nacional y europea en la materia.
☐	Otras

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

Condición esencial	Frecuencia	Forma de acreditación del cumplimiento
Aspectos que se hayan considerado como criterio de adjudicación.	Anualmente. Durante el periodo de ejecución del contrato.	A través de la facturación y de la comprobación de que se están ejecutando los aspectos técnicos requeridos.
Porcentaje de trabajadores fijos igual o superior al 20 por 100.	ANUALMENTE. Durante el periodo de ejecución del contrato.	Mediante certificación que acredite el cumplimiento: Informe sobre número anual medio de trabajadores en situación de alta. 2008/8 o informe de plantilla media de trabajadores en alta. 2011/13.

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

8.1.7. Condiciones especiales de ejecución.

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

☐	Cumplimiento del régimen y plazos de pagos a los subcontratistas o suministradores establecido en la normativa sobre lucha contra la morosidad en operaciones comerciales
☐	El cumplimiento de las políticas de prevención de imputaciones delictivas y los códigos de conducta establecidos por el contratista, que en todo caso resultarán similares a los recogidos en el documento "programa de prevención de riesgos penales" accesible a través de la web

	https://cswetwebcorsta01.blob.core.windows.net/uploads/2022/01/CORREOS-Codigo-General-de-Conducta.pdf
☐	La suscripción de un seguro de responsabilidad civil por los daños que pueda causar el contratista, su personal, subcontratistas o proveedores, por un importe mínimo de …..euros.
☐	Establecimiento de un plan de formación para los empleados adscritos a la ejecución del contrato en materias relacionadas con: ☐ Prevención de riesgos laborales específicos en el marco del servicio a prestar ☐ Régimen de protección de datos de carácter personal. ☐ Otro ……
☐	Establecimiento de un sistema de gestión diferenciada para los residuos que pueda generar la prestación del servicio.
☐	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.
☐	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.
☐	Otras:
	-

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

Condición especial	Frecuencia	Forma de acreditación del cumplimiento
Porcentaje de trabajadores fijos igual o superior al 20 por 100.	ANUALMENTE. Durante el periodo de ejecución del contrato.	A través de registro de empleados.

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

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

8.1.8. Régimen de confidencialidad.

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

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

8.2. Modificaciones del contrato.

En el presente contrato

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

Además, se prevé la posibilidad de acudir a lo dispuesto en el artículo 111 del RD, 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

NOTA: Subcontratación de los servicios profesionales del fabricante

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

- El contratista podrá concertar con terceros la realización parcial de la prestación en un mínimo de 250 horas del fabricante a lo largo de los 3 años de contrato. A efectos de cómputo de este porcentaje máximo, no se tendrán en cuenta los subcontratos concluidos con empresas vinculadas al contratista principal, entendiéndose por tales las que se encuentren en algunos de los supuestos previstos en el artículo 42 del Código de Comercio.
- Los licitadores deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial de los subcontratistas a los que se vaya a encomendar su realización.
- El adjudicatario comunicará su intención de celebrar subcontratos, señalando la parte de la prestación que se pretende subcontratar y la identidad, datos de contacto y representante o representantes legales del subcontratista, y justificando suficientemente la aptitud de este para ejecutarla por referencia a los elementos técnicos y humanos de que dispone y a su experiencia, y acreditando que el mismo no se encuentra incurso en causa de prohibición de contratar. Cualquier cambio respecto de los subcontratos que se produzca durante la ejecución del contrato deberá ser comunicado también a la entidad contratante.
- En el caso de que la subcontratación afecte al tratamiento de datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, el subcontratista en su caso, quedará sometido a las mismas obligaciones que el contratista y deberá suscribir un Contrato de encargo de tratamiento de datos personales conforme al modelo consignado en el Anexo XV.

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

☐	…

9. Cumplimiento del contrato.

9.1. Responsable del contrato. Representante del contratista.

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

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

9.2. Régimen de penalidades.

El régimen de penalidades aplicable en caso de incumplimiento de obligaciones establecidas en este pliego será el descrito en el Anexo XIII. Los procedimientos para la imposición de penalidades deberán iniciarse antes de la aprobación del acta de conformidad con el servicio prestado, 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 no podrán ser superiores al 10 por ciento del precio del contrato, IVA excluido, ni el total de las mismas superar el 50 por ciento del precio del contrato.

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

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

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

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

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

9.3. Abonos al contratista. Facturación.

El pago del servicio se efectuará conforme al siguiente plan de facturación, previa presentación de la correspondiente factura:

- **Suscripción de Licencias SaaS:** La facturación se realizará con periodicidad mensual y a periodo vencido, de forma que cada factura refleje los servicios efectivamente prestados durante el mes natural inmediatamente anterior.

Cada factura deberá reflejar claramente:

- El número total de licencias incluidas en el periodo mensual
- El importe unitario por licencia y el importe total mensual
- El periodo de prestación del servicio cubierto.

- **Implantación de la herramienta:** se establece como un componente de carácter variable vinculado al cumplimiento de hitos previamente definidos en el marco del proyecto de migración. La naturaleza, alcance y criterios de ejecución de estos hitos serán definidos y acordados por ambas partes al inicio del contrato. El importe no utilizado correspondiente a los servicios de migración de los años 2026 y 2027 podrá ser redistribuido y aplicado durante el resto del periodo de vigencia del contrato, en caso de ser necesario.

- **Servicio de evolución, innovación y mantenimiento**: La facturación del contrato se realizará tras la puesta en producción del sistema (GoLive) y se organizará en torno al siguiente plan, que incluye desglose por los siguientes conceptos:
  - Importes a facturar bajo demanda para el S1. Los evolutivos serán facturados a la consecución del siguiente hito. o Implantación estable en producción (al menos 20 días de utilización habitual sin incidencias).
  - Importes fijos a facturar de forma mensual vencida, para el S2.

Mensualmente se calculará la cantidad a facturar para cada servicio, esta se corresponderá con la "Facturación base 100".

Si en el periodo, y como consecuencia del Sistema de Evaluación, no se ha generado ninguna penalización, la facturación real se corresponderá con la "Facturación base 100". Si, por el contrario, en el periodo se han generado penalizaciones por incumplimientos en uno o varios indicadores de los previstos en el apartado INDICADORES, OBJETIVOS Y NIVELES DE CUMPLIMIENTO, se aplicará una "CORRECCIÓN DE FACTURACIÓN". El porcentaje de minoración estará determinado por la gravedad de cada incumplimiento y se aplicará a los importes de referencia establecidos. Tanto estos porcentajes como los importes de referencia están recogidos en el apartado Anexo XIII.- Régimen de penalidades.

Así pues, la "CORRECCIÓN DE FACTURACIÓN" se corresponderá con la suma total de los importes resultantes de aplicar las correspondientes penalidades.

Correos calculará el importe a certificar y consiguientemente a facturar de acuerdo con la siguiente fórmula:

Facturación real = "Facturación base 100" – CORRECCIÓN DE FACTURACIÓN

El pago del servicio se efectuará a la realización conforme del mismo previa presentación de la correspondiente factura. Para el pago de facturas giradas por el adjudicatario, la entidad contratante utilizará los siguientes medios de pago:

- Transferencia bancaria. Correos ordenará la transferencia para el pago de la factura en los 60 días naturales siguientes a la fecha de su recepción, coincidente

con el calendario de pagos de la entidad contratante.

- Confirming. La entidad contratante dispone del servicio de confirming con entidades financieras que facilita al adjudicatario el anticipo del importe de sus facturas. En ningún caso se considerará como medio de pago el uso de servicios de factoring, cesiones de crédito o cualquier otro de similar naturaleza, sin perjuicio de la utilización del servicio de confirming de la entidad contratante.

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

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

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

Campo		Facturae 3.2
Expediente		
Lote		
Grupo Gestor		Facturae/Parties/BuyerPart y/AdministrativeCentres/ AdministrativeCentre/Cent reCode
Descripción de la operación		Facturae/Invoices/Invoice/ AdditionalData/InvoiceAd ditionalInformation
Fecha de la operación		Facturae/Invoices/Invoice/ InvoiceIssueData/Operatio nDate
Grupo Gestor		Facturae/Parties/BuyerPart y/AdministrativeCentres/ AdministrativeCentre/Cent reCode (RoleTypeCode 02)
N.º línea del pedido		Facturae/Invoices/Invoice/ Items/InvoiceLine/Sequenc eNumber
Referencia legal		Facturae/Invoices/Invoice/ Items/InvoiceLine/Additio nalLineItemInformation

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

9.4. Recepción y liquidación.

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

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

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

9.5. Plazo de garantía.

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

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

10. Resolución del contrato.

10.1. Causas de resolución.

Serán causa de resolución del contrato:

☒	Las previstas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
☒	El incumplimiento de obligaciones calificadas expresamente como «esenciales» en este Pliego, de acuerdo con lo establecido en el apartado 8.1.6.
☒	Cuando teniendo que llevar a cabo una modificación en el mismo que, no estando prevista en el pliego, no concurrieran las circunstancias establecidas en

	el artículo 111 del Real Decreto Ley 3/2020 de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.
☒	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.
☒	La subcontratación realizada habiendo incumplido la obligación de notificar tal intención de subcontratar al órgano de contratación, en favor de un subcontratista que no cumpla los requisitos de capacidad y ello de conformidad con lo establecido en el artículo 107 RD 3/2020.
☒	Incumplimiento de las condiciones especiales de ejecución, de modo que se frustre el objeto del contrato.
☒	Las recogidas en las letras a) y e) del artículo 122.2 de la LCSP.

10.2. Procedimiento

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

11. Protección de datos.

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

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

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

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

11.2 Información a representantes, trabajadores y personas de contacto

Los datos de carácter personal de las personas de contacto de los licitantes y, en su caso, de sus trabajadores serán tratados por la entidad contratante con la finalidad de gestionar su participación en la presente contratación, y en caso de resultar adjudicatario del contrato, con la finalidad de gestionar la relación contractual que se formalice entre las partes, siendo la base legitimadora del tratamiento la ejecución del contrato y el cumplimiento de la normativa de aplicación. En este sentido, le informamos que los datos facilitados no se cederán a terceros, salvo obligación legal.

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

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

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

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

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

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

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

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

El objeto del contrato tiene carácter mixto, al comprender tanto el suministro de una solución técnica como la prestación de servicios asociados a su utilización y mantenimiento.

De conformidad con lo establecido en el artículo 15.2.a), párrafo segundo, del RDL 3/2020, se ha realizado el análisis cuantitativo de las distintas prestaciones que integran el objeto contractual, resultando lo siguiente:

- Prestaciones de suministro: 46%
- Prestaciones de servicios: 54%

Al ser superior el valor estimado de las prestaciones de servicios, el contrato se califica como contrato de servicios, aplicándosele el régimen jurídico previsto para este tipo contractual en el RDL 3/2020.

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

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

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

☒	El presente Pliego de condiciones administrativas y técnicas particulares, así como todos sus Anexos
☒	Contrato formalizado entre las partes.
☒	Los proyectos o programas de trabajo que se hubiera presentado el adjudicatario
☒	La totalidad de la oferta presentada por el adjudicatario.

El presente pliego podrá ser objeto de reclamación, conforme a lo dispuesto en los artículos 119 y siguientes del Real Decreto Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, en el plazo de quince días hábiles a contar desde la publicación del anuncio de licitación en el perfil de contratante de la entidad.

En Madrid, a 30 de marzo de 2026

LA JEFA DE ÁREA DE GOBIERNO DE LA PLATAFORMA HÍBRIDA

CRESPO ROMERO VERONICA - 53421611V
Firmado digitalmente por CRESPO ROMERO VERONICA - 53421611V
Fecha: 2026.03.30 12:32:38 +02'00'

FDO. VERÓNICA CRESPO ROMERO

CONFORME:
EL SUBDIRECTOR DE EXPLOTACIÓN E INFRAESTRUCTURAS

LOPEZ LIMON DANIEL - 50728751C
Firmado digitalmente por LOPEZ LIMON DANIEL - 50728751C
Fecha: 2026.04.01 10:43:40 +02'00'

FDO. DANIEL LÓPEZ LIMÓN

VºBº:
LA DIRECTORA DE TECNOLOGÍA Y TRANSFORMACIÓN DIGITAL

Firmado digitalmente por: TARRERO MARTOS, CRISTINA
Fecha: 2026.04.01 11:01:27 +02'00'

FDO.: CRISTINA TARRERO MARTOS

Anexo I.- Características técnicas específicas del contrato.

1. CONTEXTO ACTUAL

A continuación, se detallan las características y principales utilidades de las herramientas actuales, las cuales deben ser ofrecidas y cumplidas por la herramienta propuesta por el adjudicatario.

1.1. Componentes Principales

Correos dispone de un extenso conjunto de aplicaciones, características y funcionalidades en su herramienta de Gestión del Servicio, conocida como PoST en Correos, las cuales se listan de manera abreviada a continuación:

- Remedy Single Sign On (SSO) para autenticación de usuarios
- Gestión de datos fundamentales de la herramienta:
  - Empresas
  - Organizaciones
  - Ubicaciones
  - Personas
  - Grupos de soporte
  - Catálogos de operación
  - Catálogos de productos
  - Reglas de asignación
- Gestión de Incidencias y Problemas
- Gestión de Peticiones
- Gestión de Órdenes de Trabajo
- Gestión de Tareas
- Gestión de Cambios
- Gestión de Versiones
- Gestión del Conocimiento
- Gestión de Niveles de Servicio
- Gestión de Activos
- Gestión de Contratos
- Gestión de Configuración (CMDB)
- Digital Workplace Advanced
  - Portal de Autoservicio
  - Gestión del Catálogo de Servicios
- Smart IT
- Smart Reporting
- BMC Analytics (denominado INFOPoST en Correos)
- Utilidades de desarrollo y gestión de datos
  - IDE Developer Studio
  - AR Data Import
  - ETL - Atrium Integrator Spoon
  - Interfaces para la Gestión de Datos
- Múltiples integraciones por diversas vías (WS SOAP, API REST, API Java ARS, SQL y otras)

Adicionalmente, se dispone también de licenciamiento para los siguientes productos, los cuales se encuentran fuera del alcance de esta renovación tecnológica, pero deberán poder ser integrados con la nueva herramienta:

- BMC Discovery 23.1.00 (prevista su migración a BMC Helix Discovery antes de la adjudicación del presente contrato): denominado ATICo en Correos, se trata de la solución de descubrimiento de centros de datos que automáticamente identifican el inventario, la configuración y las relaciones de los elementos en los CPDs. Actualmente no se encuentra activa la sincronización con la CMDB de Remedy, si bien lo estuvo en pasadas versiones y se espera que en la futura herramienta se realice nuevamente la integración.
- BMC Truesight 11.3.02 (en proceso de migración a BHOM también de BMC): Integrado de forma estándar con BMC ITSM para la generación de incidencias a partir de eventos de monitorización.

1.2. Versiones Instaladas

Las versiones de los productos instalados actualmente son los siguientes:

- BMC Remedy ITSM suite:
  - Versión 20.02.03 en RSSO (Remedy Single Sign On), DWP (Digital Workplace). DWP-C (catalog) y motor de corre
  - Versión 18.08.00 en el resto de los componentes (Midtier, AR Server, Smart Reporting, Smart IT, …).
- BMC Analytics y su universo basado en SAP Business Objetcs 4.1
- BMC Discovery versión 23.1 (prevista su migración a BMC Helix Discovery antes de la adjudicación del presente contrato)
- BMC Truesight 11.3.02 (en proceso de migración a nueva versión SaaS BHOM)

Todo ello apoyándose en versiones de software middleware y bajo nivel alineados con lo establecido para la versión 18.08.00:

- Sistema operativo: Red Hat Enterprise Linux 7.7
- Servidor de aplicaciones: Apache Tomcat 8.5.55
- Base de Datos: Oracle Database 12c Enterprise Edition

Siendo la arquitectura técnica establecida para la plataforma que aloja los componentes de PoST principales la siguiente:

- 5 servidores ARS (3 usuario, 1 administrativo, 1 Smart Reporting)
- 2 servidores DWP Catalog
- 2 servidores DWP
- 2 servidores Smart IT
- 3 servidores Mid-Tier (2 usuario, 1 administrativo)
- 2 servidores de Remedy Single Sign On

- 2 servidores de Smart Reporting

1.3. Configuraciones de la Solución Base

La solución está configurada en modo Multicompañía, existiendo 3 empresas en PoST:

- Correos
- Correos Express y
- Correos Telecom

Estas empresas disponen de un modelo de organizaciones, departamentos y ubicaciones, las cuales incluyen información específica de Correos, que incorporan mediante personalización de atributos propios de Correos, como:

- El CODIRED como elemento de ubicación,
- distribución en 7 zonas geográficas nacionales e internacionales (Internacional y Portugal),
- características y horarios específicos de oficinas,
- así como otros atributos.

Actualmente esta información de ubicación se encuentra integrada con un sistema Maestro de dicha información, que mantiene actualizados los datos de más de 35.000 ubicaciones.

Adicionalmente, el sistema cuenta con un inventario de más de 500 empresas identificadas como fabricantes, proveedores, etc.

Mediante esta estructura se caracterizan todos los usuarios de Correos, dando servicio a más de 20.000 usuarios solicitantes activos en Portal de Autoservicio, y 2.500 usuarios de soporte con un uso activo mensual de más de 1.000 usuarios técnicos/mes.

Para los servicios técnicos que se dan en la solución, la plataforma cuenta con una configuración de más de 400 grupos de soporte.

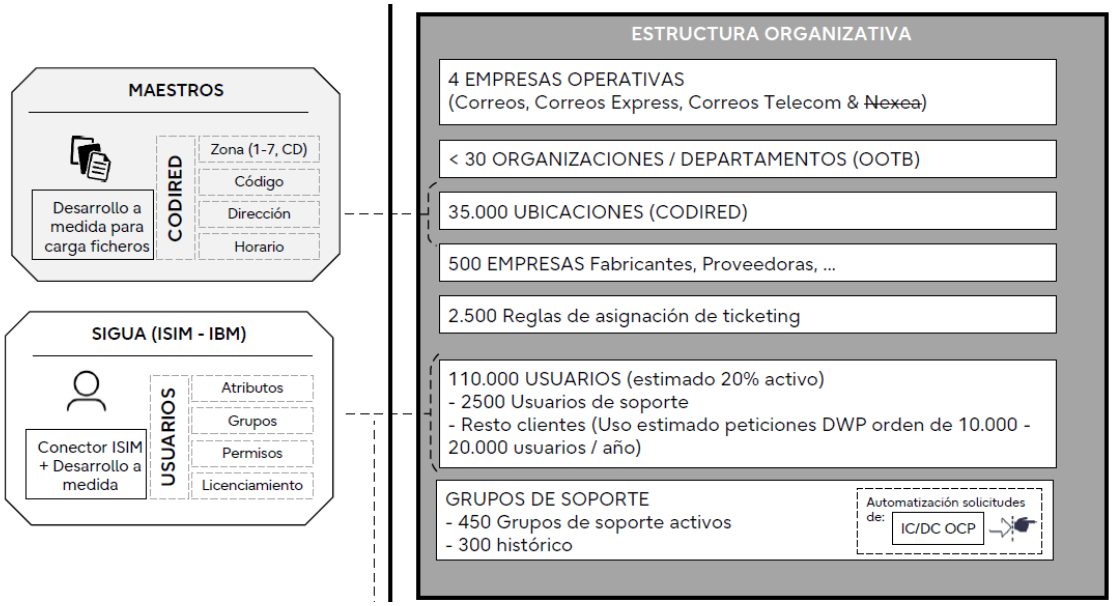


Ilustración 1. Elementos clave de configuración base

1.4. Digital Workplace Advanced

Digital Workplace y su componente Digital Workplace Catalog es la solución sobre la que se construye y publica el actual catálogo de servicios a usuarios de Correos. Desde este portal, los usuarios pueden realizar sus solicitudes de servicio, abrir incidencias, solicitar cambios, consultar artículos de conocimiento u otros recursos de interés

A la fecha existen del orden de 170 servicios publicados en el portal de Digital Workplace. Esas peticiones de servicio se presentan a usuario por las siguientes vías:

- Mediante una estructura de 14 bloques de categorías principales las cuales, mediante una navegación tipo menú, permiten el acceso a subcategorías y grupos de servicios.
- En la pantalla principal, mediante 5 grandes secciones agrupadoras de servicios que alojan los principales servicios, y permiten un acceso ágil a los mismos. Estas secciones son:
    - Destacado
    - Oficina, Distribución & Logística
    - Jefaturas y Unidades Administrativas
    - DTI – Sede Central
    - Correos Express
- Adicionalmente, el buscador global principal del portal permite la localización rápida de cualquier petición de servicio publicada, artículo de conocimiento u otro recurso de interés.

Para gestionar la visibilidad de las peticiones del portal, se utiliza una definición de en torno a 15 agrupaciones de derechos de visibilidad. Estos derechos permiten restringir el acceso a servicios específicos en base a diferentes necesidades y criterios como pueden ser seguridad, necesidades de negocio, de pruebas, etc.

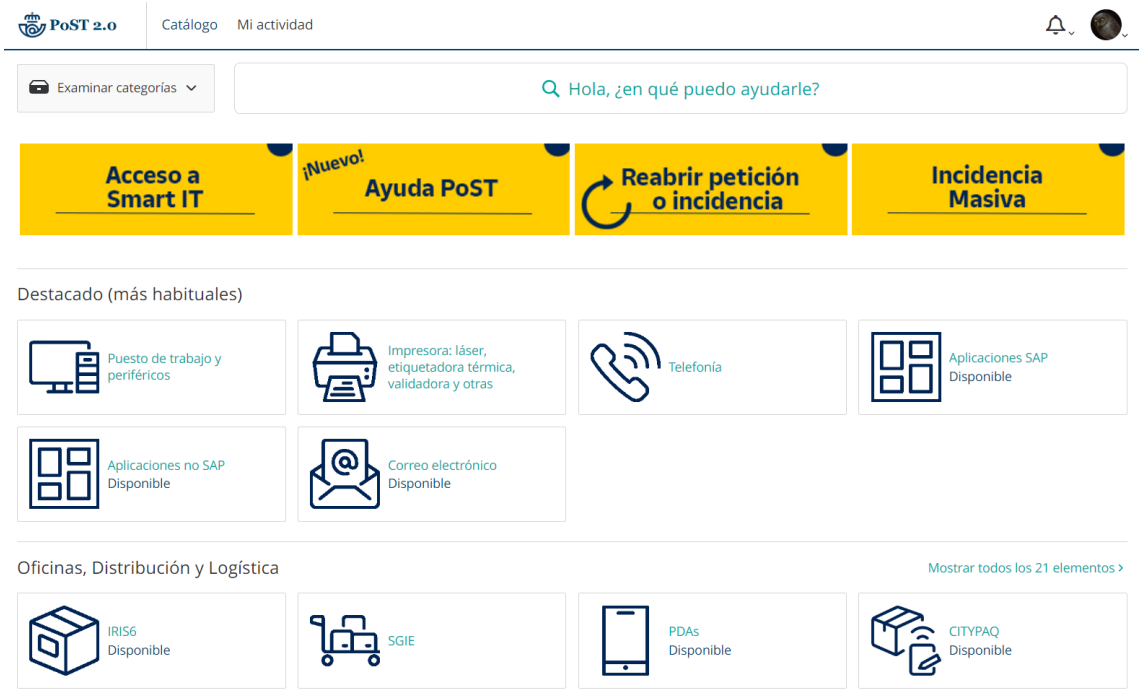


Ilustración 2. Portal Digital Workplace Correos

Volumetría y aspectos principales

En PoST se generan en promedio unas 270.000 peticiones desde Digital Workplace al año. Se calculan unas 1.000 peticiones cada día laboral.

Cada una de estas peticiones puede generar uno o más tickets para el BackOffice de las siguientes tipologías:

- Incidencias (INC),
- Peticiones, que en Correos se tratan como órdenes de trabajo (WO),
- Y Cambios (CRQ)

La siguiente imagen es una representación de las estructuras descritas en este apartado.

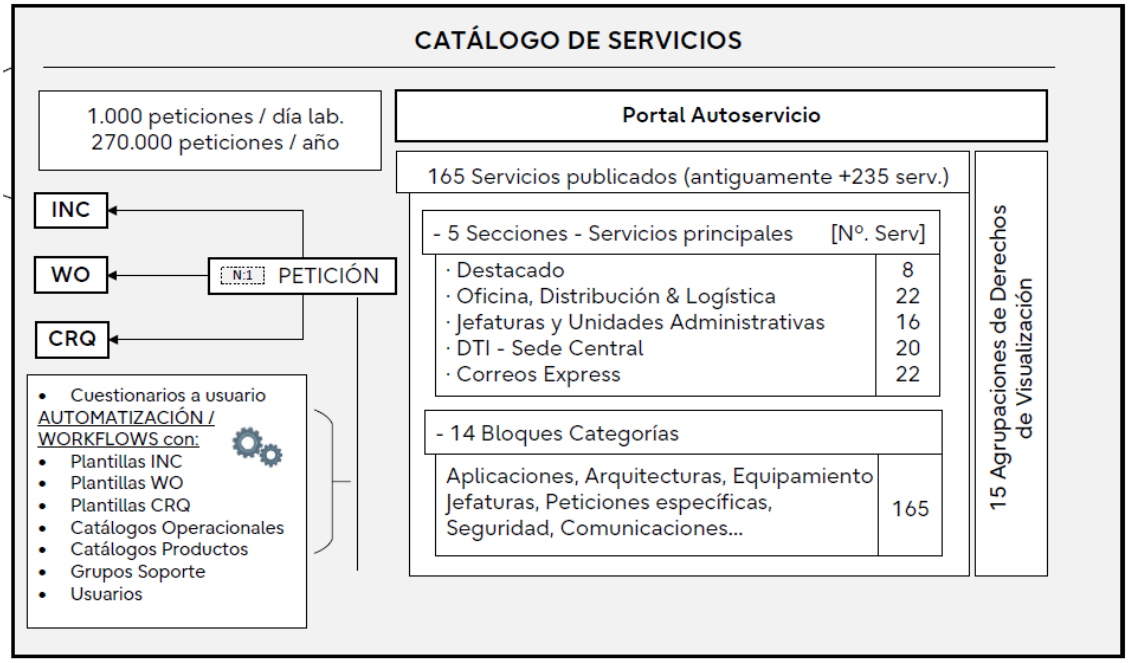


Ilustración 3. Catálogo de servicios Digital Workplace

El diseño de cada petición puede tener distinto grado de complejidad.

Hay peticiones que requieren diseñar múltiples cuestiones y preguntas condicionadas a usuario, otras que generan N tickets en secuencia o en paralelo en función del diseño de la capa de negocio y las respuestas del usuario, y todas en general hacen uso de elementos comunes como pueden ser catálogos operacionales, de producto, plantillas preconfiguradas, etc.

Los diseños más simples pueden manejar un grupo reducido de cuestiones, flujos de proceso y/o plantillas. Un ejemplo podría ser un servicio DWP de: entre 5-10 cuestiones, flujo reutilizable simple con 3 o 4 actividades, y el uso de una plantilla final para la creación del ticket. Pero los servicios complejos son escenarios donde se pueden llegar a tener que gestionar y mantener: decenas de cuestiones anidadas, flujos de proceso complejos con múltiples ramificaciones y decenas de actividades en secuencia o paralelas, creando tickets o no en función de condiciones del cuestionario, el avance de

otros tickets, y usando para ello múltiples plantillas de creación de tickets preconfiguradas en el workflow.

Todo esto se encuentra diseñado en workflows de Digital Workplace Catalog. Este componente ha reemplazado a las peticiones basadas en Service Request Management (SRM) que se usaban hasta las versiones previas de PoST en Correos. Ya no queda ninguna de esas peticiones en uso, siendo todas las peticiones actuales construidas en Digital Workplace Catalog.

Se estima la siguiente distribución en base al grado de complejidad:

- Complejidad alta: 15% de los servicios
- Complejidad media: 30% de los servicios
- Complejidad baja: 55% de los servicios

Por otro lado, los usuarios pueden hacer seguimiento de sus tickets directamente en el Portal, con áreas específicas como "Mi Actividad", donde pueden visualizar, filtrar y localizar sus peticiones. Y desde el mismo Portal pueden realizar acciones como Cancelar, Pedir de nuevo o Reabrir.

El sistema dispone de un completo sistema de notificaciones a peticionarios, lo cuales pueden ser notificados mediante correo electrónico o avisos en la aplicación de los eventos más relevantes de los tickets, tales como: cambios de estados, notas de interés, aprobaciones, etc. e incluso de la denominada "actividad social", de actualizaciones y notificaciones sobre gente a la que sigue.

La activación o desactivación de varios de estos tipos de notificación pueden ser realizados por los propios usuarios directamente en sus preferencias de aplicación.

Personalizaciones

Las principales modificaciones realizadas en el portal de autoservicio son:

- Branding corporativo en el portal, siguiendo el estándar, colores e iconografía específica de Correos.
- Participación en la nueva funcionalidad que permite la identificación de incidencias como "Incidencias Masivas" por parte de técnicos autorizados, haciéndolas seleccionables en el portal de Digital Workplace, y habilitando así a los usuarios del portal a dejar constancia de que tienen el mismo error.
- Funcionalidad de reapertura de peticiones o incidencias mediante una petición que muestra la información filtrada.
- Información ampliada incluida en la bitácora de actividad.
- Envío de información estructurada a formularios a medida para desencadenar automatizaciones de asignación dinámica de tareas a grupos o usuarios.

1.5. Gestión de Incidencias y Problemas

El proceso de gestión de incidencias tiene un uso intensivo en Correos. Prácticamente todos los grupos de soporte que dan servicio en PoST tienen acceso y roles para la gestión de incidentes.

El proceso de gestión de problemas, si bien se encuentra disponible en la herramienta, en la actualidad no se encuentra en uso. Existe un proceso de gestión de problemas en Correos, pero no emplea PoST para su gestión.

Volumetrías

En PoST se generan en promedio unas 400.000 incidencias al año.

Los medios de apertura de incidencias más habituales en la actual plataforma son los siguientes:

- A través del portal de autoservicio "Digital Workplace".
- Mediante contacto directo con el Centro de Atención a Usuarios (CAU) por las vías que éste establece (teléfono, email, …)
- Vía SmartIT directamente por otros usuarios técnicos.
- Vía integraciones (Web Services, API, email entrante…), siendo la integración con el sistema de alertas de BMC (TSIM/TSOM) una de las integraciones con mayor nivel de demanda en el alta de incidencias.

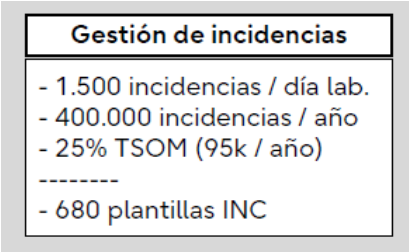


Ilustración 4. Vista volumetrías de incidencias

Plantillas de incidencias y tareas

Para el alta de incidencias, ya sea de forma manual o automatizada, se emplean plantillas preconfiguradas que facilitan la rápida creación de las incidencias, con información normalizada y adecuada al objeto de la apertura.

Actualmente existen cerca de 680 plantillas de incidencias que son usadas por los distintos canales de apertura de incidencias (DWP, SmartIT, integraciones, …)

En el mismo ámbito de las incidencias, existe un uso habitual de Tareas y Grupos de Tareas preconfiguradas que se emplean para estructurar los trabajos necesarios en ciertos escenarios de resolución. Estas tareas son seleccionadas una vez creado el incidente, y constituyen una guía de resolución.

El alto volumen de plantillas de incidencias, de tareas y de grupos de tareas (se estiman unas 3.000 plantillas de tareas, y más de 120 de grupos de tareas), así como la dependencia de ellas y con los distintos puntos o componentes de la plataforma, se considera un aspecto necesario de optimizar y simplificar en la nueva herramienta.

Uso de catálogos

La actual solución permite el uso de catálogos operacionales, de producto y de resolución, los cuales aportan información estructurada con la que tipificar los tickets de incidencias. A la fecha no existe una diferenciación estricta de dicha configuración por proceso ITIL, siendo el total de esta configuración de catálogos:

- 2.600 categorías operacionales,
- 5.000 categorías de producto y
- 2.700 categorías de resolución.

Estos volúmenes y sus características específicas constituyen un alto nivel de deuda tecnológica que se requiere optimizar como parte del proceso de migración.

El flujo actualmente implementado en el proceso de gestión de incidencias exige con carácter obligatorio que al menos el primer nivel de las categorías operacional y de producto sea rellenado en la creación del ticket. En caso de ser atendido por el CAU de Correos, una personalización extiende este comportamiento y requiere obligatoriamente que los 3 niveles de categoría operacional y los 3 niveles principales de categoría de producto sean informados.

Personalizaciones

Las siguientes son algunas características añadidas mediante personalizaciones en la herramienta:

- Para extender la disponibilidad de información empleada en el registro de la incidencia, una nota en la bitácora de trabajo (WorkLog) con el resumen y la descripción del ticket (por ejemplo, con atributos rellenados por el solicitante desde el portal Digital Workplace) es creado en el momento del alta del ticket.
- Nuevos desarrollos permiten identificar directamente y filtrar incidencias duplicadas desde la consola de tickets de Smart IT.
- Implementación de un contador de reclamaciones que se incrementa mediante la creación de un worklog del tipo "Customer Follow-up".
- Desarrollos de prefijado forzoso del grupo propietario habitual a grupos de primer nivel en caso de categorizaciones operacionales específicas para dichos grupos.
- Se muestran campos contadores de “Núm.. Reaperturas” y “Núm.. Reclamaciones” en Smart IT.
- No se permite guardar o crear una incidencia, que tiene una o más tareas relacionadas sin grupo asignado.
- Así mismo, no se permite la creación de tareas cuando una incidencia está en estado resuelto.
- Se visualiza el campo ID Petición en Smart IT correspondiente a Digital Workplace, quedando a su vez también incluido en el buscador del sistema (FTS).
- Mediante una nueva funcionalidad, se permite la identificación de incidencias como “Incidencias Masivas” por parte de técnicos autorizados, haciéndolas seleccionables en el portal de Digital Workplace, y habilitando así a los usuarios del portal a dejar constancia de que tienen el mismo error.
- Nuevos valores de motivo de estado amplían el conjunto de opciones provisto de caja.
- En el trabajo por tareas:
    - No se permite cerrar tareas sin tener un grupo asignado.

  - Tampoco se permite el cierre fallido.
  - Se realiza un cálculo del tiempo que una tarea ha pasado en los estados Pendiente (Asignación) y Pendiente (Error)

- Se ha eliminado la generación de REQ cuando los tickets son creados desde Digital Workplace, para simplificar la identificación por parte de los usuarios.
- Los cambios de grupo en incidencias quedan reflejados en la bitácora de trabajo (WorkLog).
- Se incorpora también la funcionalidad de copiar incidencias con posibilidad de relacionar la original.
- Bajo determinados escenarios (por ejemplo, en caso de que la incidencia sea atendida por el CAU de Correos) una personalización obliga a rellenar los 3 niveles de categoría operacional y los 3 niveles principales de categoría de producto.
- En la resolución de los incidentes por parte de los equipos técnicos, requiere que el texto de resolución contenga un tamaño mínimo de 20 caracteres de forma obligatoria.
- El contenido de la resolución de la incidencia es copiado a la bitácora de trabajo (WorkLog).
- Se permite la confirmación de resolución o reapertura a través del propio aplicativo de las incidencias tratadas, ya sea por el solicitante en Digital Workplace, o en ciertos casos también por los usuarios de SmartIT.
- En la fase de resolución, no se permite la transición al estado final "Cerrado" por parte de usuarios de soporte. Únicamente usuarios de sistema, automatizaciones o grupos especiales autorizados (como CPD) pueden proceder con el cierre final. El resto solo tiene capacidad de pasar a Resuelto.
- En los casos de reaperturas, éstas quedan registradas en un formulario a medida dejando reflejo de los grupos y técnicos con incidencias reabiertas.
- Como medida de mantenimiento del dato, existen procesos de archivado de las incidencias cerradas de más de un año de antigüedad. Para su consulta por parte de los usuarios, se han habilitado mecanismos de acceso en modo lectura esta información histórica a través de vistas clásicas de Remedy.

Notificaciones

El sistema dispone de un completo sistema de notificaciones a grupos/técnicos resolutores, responsables o asignados a los tickets, así como a peticionarios. Este sistema es altamente configurable. Los distintos roles, en función de diferentes criterios, son notificados mediante correo electrónico o avisos en la aplicación de los eventos más relevantes de los tickets, tales como: cambios de estados, de asignación, notas de interés, aprobaciones, etc.

Adicionalmente el sistema cuenta con unos pocos desarrollos y personalizaciones, realizados para potenciar la granularidad de algunos eventos sobre incidencias no contemplados en el out-of-the-box (por ejemplo, notificar a usuario contenido de notas publicas), a la vez que incluir branding o características corporativa en los emails.

1.6. Gestión de Peticiones (Órdenes de Trabajo)

El proceso de gestión de peticiones tiene un uso extendido en Correos.

En Correos, la gestión de peticiones se traduce en gestión de órdenes de trabajo (también conocida como "Work Order"), ya que este tipo de ticket es el usado para tratar las solicitudes de servicio.

Volumetrías

En PoST se generan en promedio unas 100.000 órdenes de trabajo al año.

Los medios de apertura de órdenes de trabajo más habituales en la actual plataforma son los siguientes:

- A través del portal de autoservicio "Digital Workplace".
- Vía SmartIT directamente por otros usuarios técnicos.
- Vía integraciones de tipo Web Service principalmente.

Gestión de peticiones
- 400 peticiones / día lab. - 100.000 peticiones / año -------- - 500 plantillas WO

Ilustración 5. Vista volumetrías de incidencias

Todos los usuarios de Correos tienen acceso a un catálogo de servicios que le permite abrir distintas tipologías de peticiones, en ocasiones restringidas según criterios de visibilidad.

Por otro lado, prácticamente todos los grupos de soporte que dan servicio en PoST tienen acceso y roles para atender esas peticiones de servicio cuando le son directamente asignadas.

Un escenario habitual es la asignación inicial o creación de peticiones centralizada en el grupo de Correos denominado GESTIÓN-PETICIONES, como encargado de modelar y crear las tareas necesarias para los distintos grupos que deban participar en la ejecución de la orden de trabajo.

Las órdenes de trabajo pueden ser tratadas directamente o, lo más habitual, mediante descomposición en tareas secuenciales o paralelas. A la finalización de todas las tareas, la orden de trabajo queda terminada.

Plantillas de órdenes de trabajo y tareas

Para el alta de ordenes de trabajo, ya sea de forma manual o automatizada, se emplean plantillas preconfiguradas que facilitan la rápida creación de la petición, con información normalizada y adecuada al objeto de la apertura. Una de las mayores ventajas de este mecanismo es que permite preconfigurar la lista de tareas que se deben ejecutar para atender dicha petición.

Actualmente existen cerca de 500 plantillas de órdenes de trabajo que son usadas por los distintos canales de apertura (DWP, SmartIT, integraciones, …)

Adicionalmente, también existe un uso habitual de plantillas de Tareas y de Grupos de Tareas preconfiguradas que se emplean para estructurar los trabajos necesarios en ciertos escenarios. Estas tareas son seleccionadas una vez creado el ticket, y constituyen una guía de trabajo para los distintos grupos.

El alto volumen de plantillas de órdenes de trabajo, de tareas y de grupos de tareas (se estiman unas 3.000 plantillas de tareas, y más de 120 de grupos de tareas), así como la dependencia de ellas y con los distintos puntos o componentes de la plataforma, se considera un aspecto necesario de optimizar y simplificar en la nueva herramienta.

Uso de catálogos

La actual solución permite el uso de catálogos operacionales y de producto, los cuales aportan información estructurada con la que tipificar los tickets de órdenes de trabajo. A la fecha no existe una diferenciación estricta de dicha configuración por proceso ITIL, siendo el total de esta configuración de catálogos:

- 2.600 categorías operacionales, y
- 5.000 categorías de producto.

Estos volúmenes y sus características específicas constituyen un alto nivel de deuda tecnológica que se requiere optimizar como parte del proceso de migración.

El flujo actualmente implementado en el proceso de gestión de peticiones exige con carácter obligatorio que al menos el primer nivel de las categorías operacional y de producto sea rellenado en la creación del ticket.

Personalizaciones

Las siguientes son algunas características añadidas mediante personalizaciones en la herramienta:

- Para extender la disponibilidad de información empleada en el registro de la orden de trabajo, una nota en la bitácora de trabajo (WorkLog) con el resumen y la descripción del ticket (por ejemplo, con atributos rellenados por el solicitante desde el portal Digital Workplace) es creado en el momento del alta del ticket.
- Se visualiza el campo ID Petición en Smart IT correspondiente a Digital Workplace, quedando a su vez también incluido en el buscador del sistema (FTS).
- Se ha eliminado la generación de REQ cuando los tickets son creados desde Digital Workplace, para simplificar la identificación por parte de los usuarios.
- Los cambios de grupo en órdenes de trabajo quedan reflejados en la bitácora de trabajo (WorkLog).
- Así mismo, estos escalados entre grupos son registrados con objeto de que puedan ser contabilizados y tratados vía informes.
- Bajo determinados escenarios, una personalización obliga a rellenar los 3 niveles de categoría operacional y los 3 niveles principales de categoría de producto.

- Nuevos valores de motivo de estado amplían el conjunto de opciones provisto de caja.
- En el trabajo por tareas:
    - No se permite cerrar tareas sin tener un grupo asignado.
    - Tampoco se permite el cierre fallido.
    - Se realiza un cálculo del tiempo que una tarea ha pasado en los estados Pendiente (Asignación) y Pendiente (Error)
- En la resolución de las órdenes de trabajo por parte de los equipos técnicos, se requiere de un texto de resolución con carácter obligatorio, y dicho texto debe tener un tamaño mínimo de 20 caracteres.
- El contenido de la resolución de la orden de trabajo es copiado a la bitácora de trabajo (WorkLog).
- Se permite la confirmación de resolución o reapertura a través del propio aplicativo de las incidencias tratadas, ya sea por el solicitante en Digital Workplace, o en ciertos casos también por los usuarios de SmartIT.
- En la fase de resolución, no se permite la transición al estado final "Cerrado" por parte de usuarios de soporte. Únicamente usuarios de sistema o automatizaciones pueden proceder con el cierre final. El resto solo tiene capacidad de pasar a Terminado.
- Como medida de mantenimiento del dato, existen procesos de archivado de las órdenes de trabajo cerradas de más de un año de antigüedad. Para su consulta por parte de los usuarios, se han habilitado mecanismos de acceso en modo lectura esta información histórica a través de vistas clásicas de Remedy.

Notificaciones

El sistema dispone de un completo sistema de notificaciones a grupos/técnicos resolutores, responsables o asignados a los tickets, así como a peticionarios. Este sistema es altamente configurable. Los distintos roles, en función de diferentes criterios, son notificados mediante correo electrónico o avisos en la aplicación de los eventos más relevantes de los tickets, tales como: cambios de estados, de asignación, notas de interés, aprobaciones, etc.

Adicionalmente el sistema cuenta con unos pocos desarrollos y personalizaciones, realizados para potenciar la granularidad de algunos eventos sobre ordenes de trabajo no contemplados en el out-of-the-box (por ejemplo, notificar a usuario contenido de notas publicas), a la vez que incluir branding o características corporativa en los emails.

1.7. Gestión de Cambios y Versiones

El proceso de gestión de cambios tiene un uso extendido en Correos.

El proceso de gestión de versiones, si bien se encuentra disponible en la herramienta, en la actualidad no se encuentra en uso.

Volumetrías

En PoST se generan en promedio unos 11.000 cambios al año.

Los medios de apertura de cambios más habituales son los siguientes:

- A través del portal de autoservicio "Digital Workplace".
- Vía SmartIT directamente por otros usuarios técnicos.
- Vía una integración específica propia del equipo de Gestión de Cambios (cuyo alias es OperatorBot).

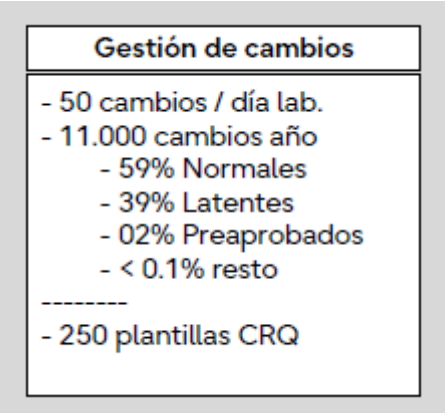


Ilustración 6. Vista volumetrías de cambios

Todos los usuarios de Correos tienen acceso a un catálogo de servicios que le permite abrir distintas tipologías de peticiones, en ocasiones restringidas según criterios de visibilidad. Algunas de estas solicitudes generar peticiones de cambios de infraestructura (CRQ).

Ciertos grupos de soporte que dan servicio en PoST tienen acceso y roles para trabajar como coordinadores o gestores de cambios cuanto las peticiones de cambios le son directamente asignadas.

El escenario más extendido, no obstante, es la asignación inicial o creación de peticiones de cambio por parte de dos grupos de Correos, denominados GESTIÓN-PETICIONES y GESTION-CAMBIOS.

Estos grupos, ya sean como primeros receptores de la solicitud, o como creadores de esta, son los encargados de registrar las tareas necesarias sobre el mismo cambio. En ocasiones será mediante el uso de plantillas con información y tareas preconfiguradas, y en otras ocasiones mediante creación manual. Cada tarea es una unidad de trabajo y es asignada al grupo correspondiente que deba participar en la ejecución del cambio. El cambio será ejecutado mediante la ejecución de cada una de sus tareas por parte de los respectivos grupos resolutores. Una vez se ejecutan todas las tareas, el cambio se considera terminado.

Plantillas de cambios y tareas

Para el alta de cambios, ya sea de forma manual o automatizada, se emplean plantillas preconfiguradas que facilitan la rápida creación de la petición, con información normalizada y adecuada al objeto de la apertura. Una de las mayores ventajas de este mecanismo es que permite preconfigurar la lista de tareas que se deben ejecutar para atender dicha petición.

Actualmente existen cerca de 250 plantillas de órdenes de trabajo que son usadas por los distintos canales de apertura (DWP, SmartIT, integraciones, …)

Adicionalmente, también existe un uso habitual de plantillas de Tareas y de Grupos de Tareas preconfiguradas que se emplean para estructurar los trabajos necesarios en ciertos escenarios. Estas tareas son seleccionadas una vez creado el ticket, y constituyen una guía de trabajo para los distintos grupos.

El alto volumen de plantillas de cambios, de tareas y de grupos de tareas (se estiman unas 3.000 plantillas de tareas, y más de 120 de grupos de tareas), así como la dependencia de ellas y con los distintos puntos o componentes de la plataforma, se considera un aspecto necesario de optimizar y simplificar en la nueva herramienta.

Uso de catálogos

La actual solución permite el uso de catálogos operacionales y de producto, los cuales aportan información estructurada con la que tipificar los tickets de órdenes de trabajo. A la fecha no existe una diferenciación estricta de dicha configuración por proceso ITIL, siendo el total de esta configuración de catálogos:

- 2.600 categorías operacionales, y
- 5.000 categorías de producto.

Estos volúmenes y sus características específicas constituyen un alto nivel de deuda tecnológica que se requiere optimizar como parte del proceso de migración.

El flujo actualmente implementado en el proceso de gestión de cambios exige con carácter obligatorio que al menos el primer nivel de las categorías operacional y de producto sea rellenado en la creación del ticket.

Personalizaciones

Las siguientes son algunas características añadidas mediante personalizaciones en la herramienta:

- Se visualiza el campo ID Petición en Smart IT correspondiente a Digital Workplace, quedando a su vez también incluido en el buscador del sistema (FTS).
- Como mecanismo de agilizar el alta de solicitudes de cambio, existe una funcionalidad customizada de "Copiar cambio".
- Se ha eliminado la generación de REQ cuando los tickets son creados desde Digital Workplace, para simplificar la identificación por parte de los usuarios.
- Bajo determinados escenarios, una personalización obliga a rellenar los 3 niveles de categoría operacional y los 3 niveles principales de categoría de producto
- Nuevos valores de motivo de estado amplían el conjunto de opciones provisto de caja.
- En el trabajo por tareas:
    - No se permite cerrar tareas sin tener un grupo asignado.
    - Tampoco se permite el cierre fallido.

- Se realiza un cálculo del tiempo que una tarea ha pasado en los estados Pendiente (Asignación) y Pendiente (Error)

- Como medida de mantenimiento del dato, existen procesos de archivado de los cambios cerrados de más dos años de antigüedad. Para su consulta por parte de los usuarios, se requiere de una solicitud a los administradores para la extracción de la información necesaria.

Notificaciones

El sistema dispone de un completo sistema de notificaciones a grupos/técnicos resolutores, responsables o asignados a los cambios y las tareas, así como a peticionarios. Este sistema es altamente configurable. Los distintos roles, en función de diferentes criterios, son notificados mediante correo electrónico o avisos en la aplicación de los eventos más relevantes de los tickets, tales como: cambios de estados, de asignación, notas de interés, aprobaciones, etc.

1.8. Gestión de Niveles de Servicio

El módulo de Gestión de niveles de servicio se emplea para realizar el seguimiento de los Niveles de Servicio de los distintos grupos de soporte definidos en la herramienta.

Este módulo puede actuar para el cálculo de métricas sobre incidencias (INC), peticiones (REQ), órdenes de trabajo (WO), cambios (CRQ), tareas (TAS)… El mayor nivel de uso está orientado al uso de Objetivo de Servicios, permitiendo el cálculo de tiempos relativos principalmente a:

- Tiempos de respuesta
- Tiempos de resolución

Mediante la evaluación de los tiempos definidos, se mide el "Cumplimiento" o "Incumplimiento" de una incidencia, petición, cambios, ...

En la actualidad existen del orden de 800 objetivos de servicios activos definidos en la herramienta. Un 50% corresponden a objetivos de servicios sobre incidencias, siendo un 30% correspondientes a órdenes de trabajo, y el 20% restante correspondiente a tareas y cambios principalmente.

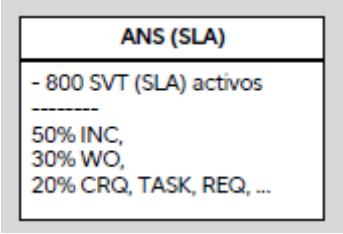


Ilustración 7. Volumetrías definiciones SLA

El alto volumen de objetivos de servicio, con cierta cantidad que se estima que puedan estar obsoletos, es algo que se requiere optimizar como parte del proceso de migración.

Cada objetivo de servicio se registra en el sistema con los siguientes elementos:

- Título y Descripción del contenido del acuerdo
- Tipo de Objetivo: Tiempo de Respuesta / Tiempo de Resolución

- Términos y Condiciones que debe cumplir el ticket para la activación del objetivo de servicio. Estos términos y condiciones se basan en valores específicos de determinados campos informados en el ticket, tales como pudieran ser:
    - El cliente afectado
    - La prioridad
    - La categorización de producto y/o operación
    - La ubicación
- Objetivo de respuesta/resolución medida en horas y minutos.
- Horario laboral que aplica para la medición del tiempo objetivo.
- Condiciones de inicio de contadores
- Condiciones de parada de contadores
- Condiciones de exclusión de tiempos intermedios
- Hitos a considerar asociados al cumplimiento del objetivo de servicio (Por ej.:, 50% de tiempo transcurrido, 75% de tiempo transcurrido, incumplimiento…)
- Acciones a realizar asociadas a los hitos identificados, por ejemplo, el incremento de la prioridad del ticket, el envío de e-mail a técnico asignado o a responsable…

El módulo de acuerdos de nivel de servicio permite gestionar diferentes tipos de acuerdos, no obstante, la gran mayoría de los objetivos definidos en el sistema miden el desempeño de los distintos proveedores de servicios en Correos, y se encuentran dados de alta como tipo SLA.

En el módulo se han configurado también todos los calendarios laborales y horarios acordes a las necesidades de los servicios ofrecidos por los distintos grupos de soporte.

Personalizaciones

- Para configurar objetivos de servicio calculados sobre algunos elementos no incluidos de caja, como las tareas, fue necesario realizar la personalización correspondiente.
- Existe un motor hecho a medida que permite evaluar automáticamente el uso de los distintos objetivos de servicio con el objeto de identificar SLAs en desuso.
- Hay creadas vistas entre SLAs y distintos tipos de tickets, lo que favorece la extracción de reporting habitual relacionado con estas métricas de tiempos.

1.9. Gestión del Conocimiento

El sistema dispone de módulo de gestión del conocimiento que permite, desde una consola, la creación, categorización, revisión, autorización, publicación, búsqueda y consulta de artículos de conocimiento. Este módulo y su contenido se encuentra integrado totalmente con la solución de ITSM y todos sus procesos.

Los artículos de conocimiento, cuando se diseñan y se da visibilidad para usuarios finales, son accesibles desde Digital Workplace.

Se pueden registrar artículos en los que incluir información de diferente naturaleza. Para ello, el sistema dispone de plantillas con información habitual como la siguiente:

- Contenido del artículo, que depende del tipo de este. Por ejemplo:
    - Artículos de conocimiento del tipo "Instrucciones ¿Cómo?" disponen de campos como: "Pregunta", "Respuesta", "Notas técnicas".
    - Artículos de conocimiento del tipo "Errores Conocidos" disponen de: "Error", "Causa raíz", "Solución", "Notas técnicas".
    - Artículos de conocimiento del tipo "Soluciones a problemas" disponen de: "Problema", "Solución", "Notas técnicas"
- Palabras clave
- Categorización de producto y operación
- Visibilidad del artículo: si es visible para usuarios finales, técnicos, o subconjuntos.

Existen diferentes usuarios autorizados para la creación de artículos de conocimiento. Generalmente son usuarios o responsables técnicos pertenecientes a diferentes grupos resolutores de diferentes ámbitos (CAU, Gestión de Usuarios, Seguridad, Tecnologías de Zonas, etc.). Esos usuarios son los encargados de la generación del contenido, que normalmente será relativo a sus propias áreas o ámbitos de trabajo. El conjunto de todos estos artículos constituye la base de datos de conocimiento disponible en la herramienta de ticketing PoST.

A la fecha existen unos 290 artículos publicados. Se trata tanto de artículos de conocimiento para usuarios, como para técnicos, guías y asistencia integradas en la herramienta.

1.10. Gestión de la Configuración (CMDB)

La CMDB de PoST en Correos está constituida principalmente por elementos de configuración (CIs) correspondientes a:

- Diferentes tipos de sistemas informáticos, equipamiento, impresoras y UPS gestionados por el equipo de microinformática (denominado Dotaciones)
- Elementos de configuración integrados por terceros, como es el caso de SCCM
- Elementos de configuración generados internamente por la propia herramienta (como pueden ser los activos de personas)
- Adicionalmente, y aunque a la fecha se encuentra "desconectada", activos correspondientes a la solución de BMC Discovery (denominada ÁTICO en Correos) que realiza el descubrimiento en los centros de datos o CPDs de Correos.

La siguiente imagen ilustra la distribución principal, características y algunos aspectos volumétricos principales de la CMDB de PoST en Correos.

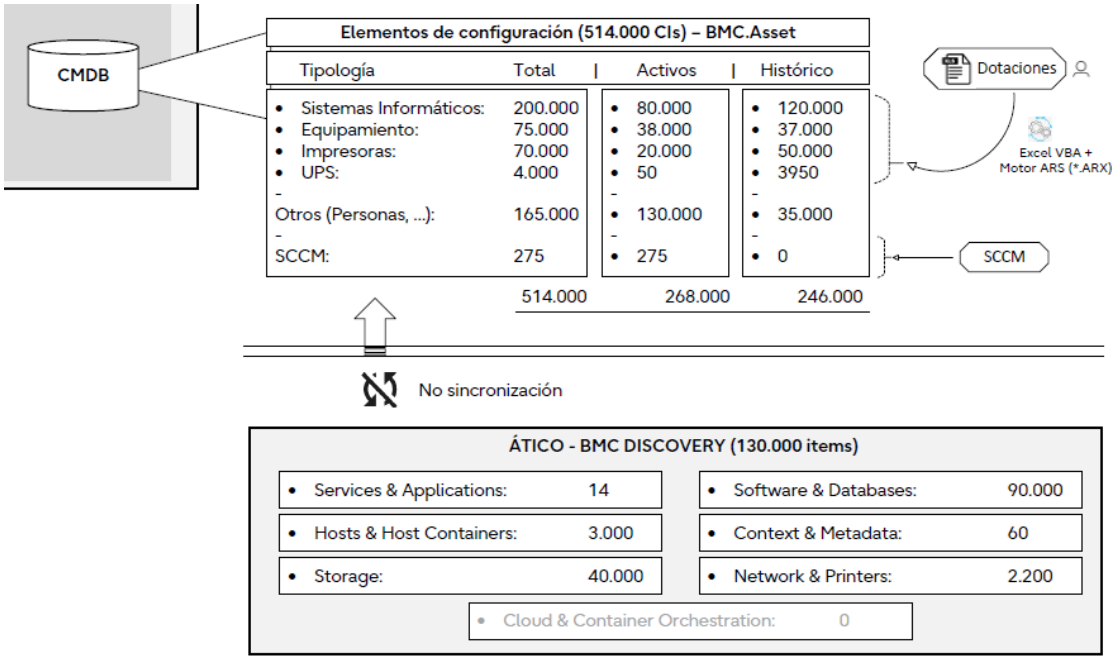


Ilustración 8. CMDB & ATICo (BMC Discovery)

Los actores que participan en la población de la CMDB de Correos a la fecha son los siguientes:

1-. Equipo de microinformática de Correos ("Dotaciones").

Mediante desarrollo a medida usan un Excel de carga para introducir y mantener sistemas informáticos (equipos portátiles, PDAs, …), Impresoras, UPS, y diferente equipamiento de Correos.

Vigentes a la fecha, son en torno a 150.000 activos (más 210.000 activos historificados), para los cuales se usan 5 clases del estándar de CMDB de Remedy con distintos niveles de personalización consistentes principalmente en nuevos atributos de clase.

Si bien estos activos están relacionados con usuarios, grupos y se pueden relacionar con los procesos ITIL, no están relacionados entre ellos.

Los activos están repartidos de la siguiente manera:

- Clase "Sistemas Informáticos": 80.000 activos como portátiles, PDAs, móviles, routers, etc.
- Clase "Equipamiento": 38.000 activos, como lectores ópticos, cámaras, escáneres…
- Clase "Impresoras": 20.000 activos, para distintos tipos de impresoras.
- Clase "UPS": 40 activos correspondientes a equipos SAI.
- Clase "Tarjetas": sin activos a la fecha, pero usado para tarjetas de routers ADSL, RDSI, forwarding, criptográfica…

2-. Herramienta de descubrimiento ÁTICo.

Se trata de la herramienta de BMC Discovery, la cual descubre los sistemas de los centros de datos o CPDs. Esta herramienta se está usando en modalidad stand-alone, empleando las capacidades de configuración, descubrimiento y de generación de informes directamente sobre ella. De esta forma, la información necesaria se explota directamente en ATICo.

Los activos y sus relaciones descubiertos en BMC Discovery no se envían a la CMDB de Remedy. Por distintas necesidades, tras un último upgrade del componente, y la ejecución de limpieza y optimización de datos, la sincronización fue desconectada de Remedy a la espera de incorporarla en el futuro roadmap de actualización/migración de la herramienta. Se espera, por tanto, que esta información sí que sea volcada a la nueva herramienta de ITSM.

Los números aproximados de ATICo son cercanos los 130k activos, siendo estos principalmente:

- Software & Databases: 90.000 activos
- Storage: 40.000 activos
- Hosts & Host Containers: 3.000 activos
- Network & Printers: 2.200
- Context & Metadata: 60
- Services & Applications: 14

3-. Integraciones

Con la CMDB interactúan varias integraciones, destinadas principalmente a leer información mediante SQL de bases de datos específicas de la organización, especialmente en el ámbito de las PDAs, y trasladarla a los atributos de los elementos de configuración existentes en la CMDB. Son integraciones como PDAWEB, Airwatch o MSP. Estas integraciones son tratadas con mayor nivel de detalle en la sección correspondiente a las integraciones.

En el ámbito de la carga de activos, existe una integración que carga activos con SCCM. Se estima que el dataset de esta integración consta de unos 275 elementos de configuración.

Personalizaciones

Las siguientes son algunas características añadidas mediante personalizaciones en la herramienta:

- Herramienta de carga mediante Excel. Para el equipo de Dotaciones existe un desarrollo a medida que incluye plantilla Excel personalizada con código en Visual Basic e integración con Remedy Data Import. El uso de esta plantilla requiere además de formularios y flujos Remedy hechos a medida para el tratamiento de los datos. Esta herramienta en conjunto permite cargar nuevos activos, así como modificar múltiples atributos de los existentes.
- Desarrollo de auditoría de CMDB. Mediante trabajos programados, y desarrollos internos, se genera de forma periódica un informe de auditoría que permite obtener

características relacionadas con el correcto mantenimiento de los datos de CMDB. Son datos relacionados principalmente con la calidad del dato de los activos, sus categorías de producto, empresas, etc.

- Implementación de permisos específicos para limitar el acceso a las consolas clásicas de gestión de activos.
- Ampliación de atributos de clase. Existen varias extensiones de los atributos de las clases estándar de BMC que se han realizado con diferentes objetivos dentro del alcance de proyecto en Correos. Algunos de esos atributos son, por ejemplo:
    - Datos relativos a garantías: Garantía, fecha de expiración de la garantía, empresa que da la garantía.
    - "Descripción Codired", siendo el Codired la denominación de ubicación empleada en Correos.
    - Campo de "Etiqueta" como identificador principal de los activos de equipamientos de Correos
    - Número y Descripción de Expediente.
    - Periodo
    - Asignado a usuario
    - Valor contable
    - Unidad concentradora
    - Campos para integraciones (y otros).

1.11. Gestión de Activos

El módulo de gestión de activos es usado principalmente desde el área de Dotaciones Informáticas para la gestión del diferente equipamiento existente en la organización. Estos usuarios lo emplean tanto desde la nueva consola disponible en SmartIT, como ocasionalmente las vistas clásicas de Remedy para la gestión de activos.

Los activos cuentan con la información cargada y mantenida desde el área de Dotaciones mediante su plantilla de carga, así como mediante la gestión directa en la herramienta. Estos activos pueden ser editados por los usuarios autorizados, así como relacionados con los tickets y/o usuarios correspondientes.

Las volumetrías de activos son equivalentes a las descritas en la sección de Gestión de Configuración (CMDB). Adicionalmente, se contemplan los contratos, como se explica más adelante.

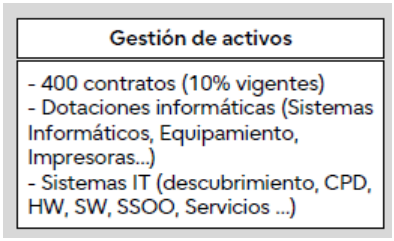


Ilustración 9. Activos y contratos

Contratos

El sistema permite la gestión de contratos de soporte, garantía, mantenimiento…cada uno de los cuales se puede relacionar con uno o varios activos gestionados en el sistema. Mediante el uso de la gestión de contratos se puede realizar un seguimiento de la información de cada contrato y el ciclo de vida de este.

Cada contrato de forma general viene identificado en el sistema con campos como:

- ID
- Resumen
- Términos y Condiciones
- Estado
- Motivo del Estado (complementa el campo Estado)
- Vigencia
- Fecha de inicio
- Fecha de expiración
- Fecha de notificación (al contacto, previo a su expiración)
- Grupo de Soporte/ Persona de contacto asociada
- Proveedor del contrato y datos de contacto del proveedor.
- Coste del contrato y coste por activo asociado
- Se permitirá asociar un contrato con uno o varios CIs existentes en la CMDB

El sistema alberga cerca de unos 400 contratos. En torno al 10% de ellos se encuentran vigentes.

La gestión de estos contratos se realiza desde las consolas clásicas de Remedy.

Personalizaciones

En el ámbito de la gestión de activos existen:

- Personalizaciones de nuevos atributos hechas en CMDB, algunas de las cuales son propagadas a las vistas de usuarios y su correspondiente visualización Smart IT (Descripción Codired, Garantía, …).
- Flujo para impedir que un activo quede sin información de ubicación (Codired)

1.12. Reporting

Existen dos soluciones principales para la obtención de informes de PoST: Smart Reporting e INFOPoST

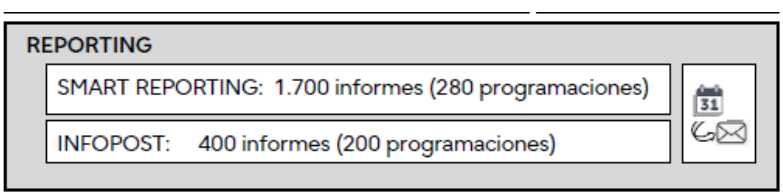


Ilustración 10. Sistemas de informes en PoST

Smart Reporting

Es el componente principal de BMC para la elaboración de informes en la versión de Remedy 18.08 instalada en Correos.

Permite la creación de paneles e informes a partir de la información de PoST en vivo, ya que en la implantación en Correos se alimenta de la información directamente en producción.

Sirve múltiples informes, tanto públicos como privados, generados estos últimos por los propios usuarios en etapas iniciales del uso de la herramienta. No obstante, esta capacidad ha sido discontinuada, para evitar impactos en el rendimiento del operacional, y a fecha de hoy todo nuevo informe es gestionado íntegramente por los administradores del sistema.

Además de permitir la extracción de información ejecutando un informe, este componente permite la programación de envíos a usuarios y direcciones de correo electrónico.

Actualmente, y tras varias limpiezas, existen en el sistema:

- Unos 1.700 informes, públicos y privados. No obstante, se estima que muchos de ellos, principalmente privados, no son útiles, y por tanto es una importante área de mejora para la siguiente herramienta.
- Cerca de 280 informes se encuentran configurados con programaciones en la herramienta, que permiten extraer listados e informes operativos que son enviados por correo electrónico en formato Excel.

BMC Analytics (denominado INFOPoST en Correos)

Módulo analítico de generación de informes basado en BO, a partir de la información proveniente de una copia diaria de la Base de Datos de PoST. Permite la obtención de informes pesados sin afectar a la producción.

Se trata de un componente que se encuentra fuera de soporte, pero que ha seguido siendo usando con el objetivo de limitar la carga de trabajo que pudiera afectar al rendimiento del sistema productivo.

Facilita la obtención de grandes volúmenes de información, o información que involucra a tablas con grandes volumetrías. Prácticamente todo el personal técnico de Correos y proveedores obtiene de este sistema los informes para el análisis de cumplimiento de SLAs, puesto que es uno de los ámbitos más exigentes para la extracción de información del sistema.

Actualmente existen en el sistema:

- Cerca de 400 informes,
- de los cuales en torno a 200 incluyen programaciones para envío por email.

La gestión de los informes en INFOPoST es realizada por los administradores de POST. No existe capacidad por el resto de los usuarios para la gestión o creación de informes.

El nivel de personalización del componente afecta principalmente a múltiples extensiones realizadas del Universo de datos. Estas extensiones se han llevado a cabo para permitir la obtención de datos que no estaban en el out of the box del producto.

Otros sistemas externos conectados para la obtención de información

- Cuadro de Mandos – CEO: sistema de informes para gestión principalmente de informes de SLAs. El objetivo principal es el control de los contratos con proveedores. El mecanismo de extracción de datos actual es mediante SQL. Dichas SQL las ejecuta un extractor de Java que saca los datos a CSV, para que posteriormente se importen en CEO.
- Teradata – BI - Cuadro de mando SSN (Subdirección de Sistemas de Negocio): Cuadro de mandos para Subdirección de Sistemas de Negocio. Los objetivos del reporting de este sistema son tiempos, cumplimientos y SLAs.
- COAP: sistema de informes para el seguimiento de SLA. Como método de extracción, se lanzan una serie de Scripts (PHP) para ejecutar queries, que generan ficheros CSV que luego se cargan en COAP.
- Cuadro de Mandos del CAU: El cuadro de mandos del CAU presenta información de SLAs. El método de extracción para la elaboración del cuadro de mandos CAU es Infopost. Desde Infopost se general ficheros Excel que se importan en el cuadro de mandos mediante un desarrollo a medida. Adicionalmente se recogen datos de textos planos y otras fuentes datos.

1.13. Integraciones

El sistema actual de PoST dispone de un variado conjunto de integraciones con otros sistemas. Estas integraciones se presentan desglosadas de la siguiente manera:

- Integraciones de plataforma: como pueden ser la integración con LDAP, el Gestor de Identidades, el maestro de ubicaciones, los extractores de información del transaccional, o el correo saliente.
- Integraciones de ticketing: aquellas mediante las cuales determinados sistemas externos llevan a cabo creación/consulta/modificación de incidencias, órdenes de trabajo, cambios o tareas.
- Integraciones para población de CMDB**:** destinadas a la carga y actualización masiva o automática de la CMDB de PoST.

Integraciones de plataforma

Se consideran como integraciones de plataforma las siguientes.

- Remedy SSO, LDAP & AD

Remedy Single Sign-On (SSO) es la solución de autenticación usada para PoST que permite a los usuarios acceder a sus múltiples aplicaciones de forma segura utilizando una única credencial de inicio de sesión. Esto permite autenticarse una vez, y navegar entre componentes de PoST sin tener que introducir nuevamente la credencial al cambiar de uno a otro.

El actual Remedy SSO integra y unifica la autenticación los componentes de PoST siguientes:

- SmartIT
- Digital Workplace (Portal de Autoservicio)
- Digital Workplace Catalog

- Smart Reporting
- Capa web clásica (Remedy MidTier)
- BHOM (BMC Helix Operations Management)

En el Remedy SSO de Correos existe integración con LDAP (Lightweight Directory Access Protocol) y el correspondiente Active Directory de Correos para autenticar a los usuarios. Esto significa que los usuarios pueden iniciar sesión en las aplicaciones de Remedy utilizando las credenciales almacenadas en el directorio LDAP, lo que centraliza la gestión de usuarios y simplifica el proceso de autenticación.

Adicionalmente, el Remedy SSO dispone también de configuración de usuarios locales para cubrir las necesidades de gestión interna de componentes y administración del sistema.

Otros componentes del ecosistema, tales como ATICo (BMC Discovery) o INFOPoST (BMC Analytics), disponen también de integración con LDAP para la autenticación, pero no lo realizan a través del Remedy Single-Sign On. En estas aplicaciones es necesario introducir las credenciales cuando se intenta acceder, aunque se provenga de otros componentes de la solución PoST.

- Gestor de Identidades (SIGUA / ISIM / IIQ)

Actualmente todos los usuarios de PoST son creados y mantenidos desde un sistema Gestor de Identidades corporativo de Correos. Este sistema centraliza todas las necesidades de gestión de usuarios y accesos de Correos. Esto aplica a múltiples sistemas, herramientas y aplicaciones.

El Gestor de Identidades está compuesto por un aplicativo de interfaz web hecho a medida, denominado SIGUA, y el uso de conectores como el ISIM (IBM Security Identity Manager) para el envío de información a PoST.

Este sistema es el encargado y maestro de la gestión de usuarios, encargándose de enviar a PoST:

- La creación, modificación y baja de usuarios, con todos sus atributos relevantes (nombre, apellidos, email, teléfono, ubicación, …)
- La gestión de permisos de usuarios (del sistema, de las aplicaciones ITSM, etc.)
- La gestión de pertenencia a grupos de soporte

Este sistema externo es quien realmente gestiona el gran volumen de usuarios del sistema, no siendo necesaria la participación de los administradores de Remedy salvo ante casos de error de sincronización.

Adicionalmente, también existe una pequeña gestión local de usuarios, como pueden ser determinados usuarios administradores o de integraciones, los cuales pueden ser gobernados por los administradores de Remedy sin participación de SIGUA.

Para esta integración existen desarrollos hechos a medida específicamente sobre Remedy. Son customizaciones hechas para agregar automáticamente algún permiso (por ejemplo, se otorgan por desarrollo los permisos/roles para órdenes de trabajo), o paliar alguna deficiencia de la integración.

Actualmente se está llevando a cabo la migración a un nuevo sistema Gestor de Identidades, el cual hará uso de otro tipo de conector IdentityIQ (IIQ) y sustituirá al actual conector de ISIM, que presenta múltiples deficiencias. No obstante, desde la perspectiva funcional y el enfoque de PoST el comportamiento aquí descrito seguirá siendo el mismo, ya que se ha planteado como una migración transparente para PoST.

- Maestros (ubicaciones)

En PoST, la configuración de ubicaciones es uno de los datos fundamentales y transversales a la herramienta. Las ubicaciones son las que permiten, por ejemplo: identificar la localización de un usuario, una oficina, un activo de la CMDB, un ticket generado en el sistema, etc.

Esta configuración de ubicaciones (Sites) del sistema se basa en el concepto de CODIRED (o código de red) usado en Correos.

Se trata de un código numérico que representa cada ubicación posible de la organización. Estos CODIRED disponen también de atributos adicionales, tales como: dirección postal, provincia, municipio, zona, código postal, tipología, horario, inmueble, …

Para la gestión de esta información, Correos dispone de un sistema central gestor de ubicaciones, denominado "Maestros", que actúa como fuente original de estos datos para otros sistemas.

PoST se integra manualmente con este sistema mediante ficheros. Esta integración tiene las siguientes características principales:

- Maestros genera varios ficheros "*.txt" los días 1 y 15 de cada mes.
- Estos ficheros tienen un formato de salida constituido por filas de datos secuenciales en espacios de columna de tamaño fijo (fixed-width format) incluyendo todos los datos de un CODIRED.
- Los ficheros son descargados y cargados en el sistema para que sean procesados por desarrollos personalizados, los cuales procesan y cargan la información en PoST de forma estructurada.

Mediante este sistema, +35.000 ubicaciones son creadas y mantenidas regularmente en el sistema.

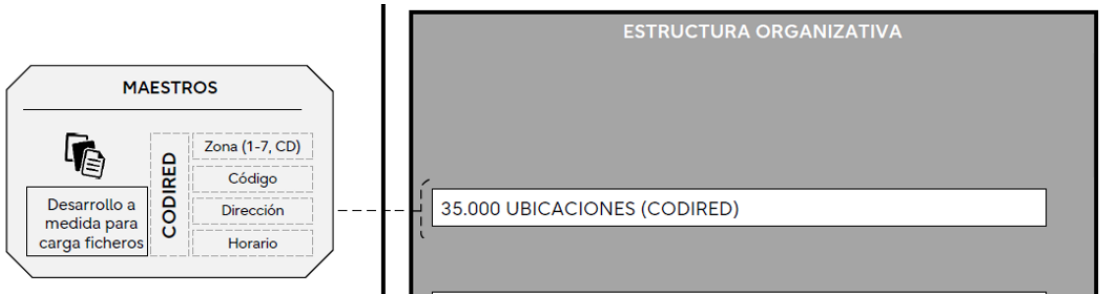


Ilustración 11. Integración con MAESTROS para ubicaciones

Existen algunas excepciones configuradas de forma manual en el sistema, pero son una muy pequeña parte del sistema de localización de la herramienta.

- Cuadro de Mandos (CEO)

Se trata de un sistema de informes para gestión principalmente de informes de SLAs. El objetivo principal es el control de los contratos con proveedores.

Desde este sistema se proceden con extracciones del sistema PoST.

El mecanismo de extracción de datos actual es mediante SQL. Dichas SQL las ejecuta un extractor de Java mediante una integración con el motor ARS, sacando los datos a CSV para su posterior importación en CEO.

Las extracciones para este cuadro de mando se consideran actividades pesadas, puesto que consultan partes del modelo de datos de BMC Remedy que contienen altas volumetrías, como pueden ser: incidencias, registros de auditoría de campos y asignaciones, métricas del motor SLM, etc.

A la fecha, este tipo de extracciones están limitados por configuración Remedy, la cual limita la extracción a 3.000 registros por consulta. Los sistemas externos han de gestionar las consultas necesarias.

- Extractor CdM Gest. Sol Terceros

Se trata de un extractor de comportamiento similar al descrito en "Cuadro de Mandos (CEO)", pero aplicado al área de "Soluciones a Terceros." Surge a raíz del proyecto ID00013112.- CdM Gest. Sol Terceros.

Este Cuadro de Mandos consume datos de POST y se realizado un proceso ETL para extraer datos de PoST a Teradata. El mecanismo de integración es similar al de CEO, vía conector Java a través del ARS.

A la fecha, este tipo de extracciones están limitados por configuración Remedy, la cual limita la extracción a 3.000 registros por consulta. Los sistemas externos han de gestionar las consultas necesarias.

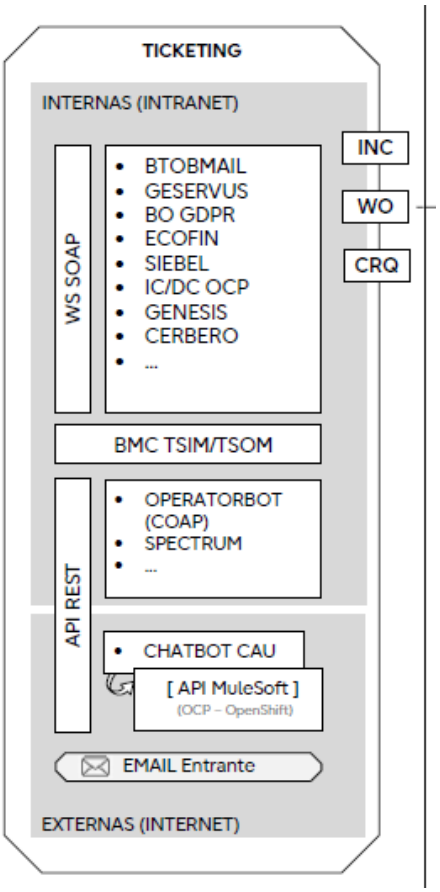
- Servidor Correo Saliente

Se emplea para el envío de emails salientes de PoST. El servicio de correo electrónico es propio de Correos, denominado "mailforapp".

Integraciones de ticketing

Se agrupan bajo esta sección el conjunto de integraciones denominadas de ticketing, que son aquellas mediante las cuales determinados sistemas externos llevan a cabo actividades en PoST relativas a:

- Creación de incidencias, órdenes de trabajo, cambios o tareas.
- Consulta de esos tipos de tickets.
- Modificación de esos tipos de tickets



Los mecanismos de integración empleados por estas integraciones son uno de los tres disponibles en PoST:

- Por Web Services SOAP
- Por API REST
- Por correo entrante

La práctica totalidad de ellas tienen el carácter de "interna", en cuanto a que se realizan desde sistemas alojados en la red interna de Correos, sin exposición con el exterior (internet). Los casos en los cuales hay acceso desde internet, tienen la consideración de "externas".

Como personalización del sistema, existen un desarrollo a medida que monitoriza las creaciones de tickets por parte de sistemas terceros vía Web Service SOAP o API REST, y permite el bloqueo de integraciones de ticketing concretas, con posibilidad de mostrarles un mensaje particularizado con el motivo del bloqueo.

- Integración con BHOM (BMC Helix Operations Manager):

Actualmente existe una integración entre la consola de eventos de BHOM y PoST para la creación de incidencias.

Cuando un agente que opera en la consola de BHOM identifica que debe crear una incidencia en PoST como consecuencia de una alerta, dispone de un botón "Enviar a PoST" mediante el cual se genera automáticamente una nueva incidencia en PoST.

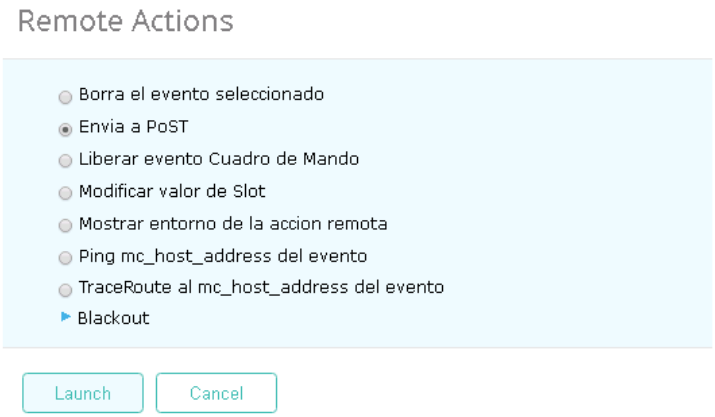


Ilustración 12. Acción remota para creación de incidencia

Esta incidencia es tratada en PoST, y una vez el ticket es cerrado en PoST, también queda cerrado en TrueSight.

Esta integración se lleva a cabo mediante los conectores estándar, ya que ambos productos son de BMC, y usan una interlocución de caja basada en Web Services SOAP e interfaces específicos para el tratamiento de eventos.

Se estima que en torno al 25% de las incidencias generadas en el sistema diariamente provienen de esta integración. Esto supone unas 95.000 incidencias al año.

Gestión de incidencias
- 1.500 incidencias / día lab. - 400.000 incidencias / año - 25% TSOM (95k / año) -------- - 680 plantillas INC

Ilustración 13. Volumetrías integración BHOM

- DXNetops – Spectrum

Se trata de una integración mediante el API REST de PoST.

Consiste en la integración de un sistema de monitorización de red de Correos Telecom. En este sistema hay operadores que revisan alarmas y mediante acción manual lanzan creaciones o actualizaciones de tickets.

Los operadores utilizan un aplicativo de consola Java (Spectrum), desde el cual cuando le dan al botón Crear Incidencia, Crear Petición o similar, invocan a scripts Python que mediante el API REST de PoST hacen las creaciones o modificaciones de incidencias.

A través del API REST pueden llevar a cabo las lecturas y modificaciones necesarias para mantener su sistema integrado.

Todas las actividades parten del sistema externo, no siendo PoST encargado de iniciar ninguna comunicación hacia el sistema externo.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 120 peticiones (órdenes trabajo)
- 2.153 incidencias

• Operatorbot (Gestión de Cambios y Tareas)

Se trata de una integración mediante el API REST de PoST.

Consiste en la integración de un sistema externo de ayuda a la Gestión de Cambios y Tareas.

Este sistema externo se ha desarrollado a medida, y dispone de un interfaz de gestión que permite a usuarios del grupo de Gestión de Cambios:

- Crear Cambios (CRQ).
- Crear/modificar tareas de un cambio

Esto lo llevan a cabo haciendo uso de un sistema de carga de ficheros Excel en los que previamente han preparado la información a cargar.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 196 cambios
- 11.540 tareas

• Btobmail

Se trata de una integración mediante Web Service SOAP de PoST.

Cuando el sistema B2BMail detecta un incumplimiento de umbrales de control de emails en su sistema, crean incidencias en PoST asignadas al grupo de soporte BTOBMAIL.

Este sistema externo emplea los Web Services de PoST para la creación de tickets de incidencia.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 88 incidencias

• Geservus

Se trata de una integración mediante Web Service SOAP de PoST.

Estos Web Services permiten la creación, consulta y modificación de tickets de incidencias y de órdenes de trabajo. Los Web Services de órdenes de trabajo son una implementación a medida, los cuales emplean los interfaces y formularios out of the box de PoST. Permiten, así mismo, el envío de ficheros adjuntos, ya que es una de las necesidades del sistema externo Geservus.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 1.333 incidencias
- 9.338 peticiones (órdenes trabajo)

• OCP: Plataforma de contenedores y sistemas de IC/DC

Se trata de una integración mediante Web Service SOAP de PoST.

Estos Web Services permiten la creación, consulta y modificación de tickets de incidencias, de órdenes de trabajo y de peticiones de cambio. Los Web Services de órdenes de trabajo son una implementación a medida, los cuales emplean los interfaces y formularios out of the box de PoST.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 11.740 cambios
- 986 incidencias
- 444 peticiones (órdenes trabajo)
    - INT Moni.Inter ECOFIN

Se trata de una integración mediante Web Service SOAP de PoST.

Estos Web Services permiten la creación, consulta y modificación de tickets de incidencia.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 4.028 incidencias
    - Cerbero

Se trata de una integración mediante Web Service SOAP de PoST.

Estos Web Services permiten la creación, consulta y modificación de tickets de incidencia.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 1.448 incidencias
    - Quorum Quejas y Reclamaciones (SIEBEL)

Se trata de una integración mediante Web Service SOAP de PoST.

Estos Web Services permiten la creación, consulta y modificación de tickets de incidencia.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante esta integración:

- 53 incidencias
    - Creación de tickets por correo entrante

Existen tres integraciones por correo entrante:

- CITYPAQ
- TamTam Services (servicio informático de control horario)
- Punto Correos

Este mecanismo permite a determinados sistemas externos, con capacidades o contextos limitados, dar de alta incidencias mediante el envío de un correo electrónico al sistema PoST.

Las características principales de este tipo de integración son:

- El envío del correo se realiza desde un conjunto acotado de cuentas de email. Cada caso de uso tiene sus cuentas previamente identificadas.
- El email enviado tiene unas características concretas respecto al formato de su asunto.
- A la recepción del email por PoST, una nueva incidencia es creada en el sistema, y asignada a un grupo concreto en base a información preconfigurada.

Desde diciembre de 2022 a febrero de 2025 se han generado mediante este tipo de integración:

- 299 incidencias

Integraciones para población de CMDB

Se trata de integraciones destinadas a la carga y actualización masiva o automática de la CMDB de PoST

- Plantilla de carga de Dotaciones Informáticas

"Dotaciones informáticas" es el área responsable del mantenimiento de todo el equipamiento de microinformática que existe en la CMDB de PoST.

Esto incluye equipamiento de: ordenadores, portátiles, telefonía, escáner, impresoras, fax, PDA, tarjetas, módems, periféricos, etc.

Estos activos se encuentran alojados en cinco clases estándar de CMDB (sistemas informáticos, equipamiento, impresoras, ups y tarjetas), y suponen unas volumetrías en torno a:

- 140.000 activos habilitados,
- y 210.000 historificados.

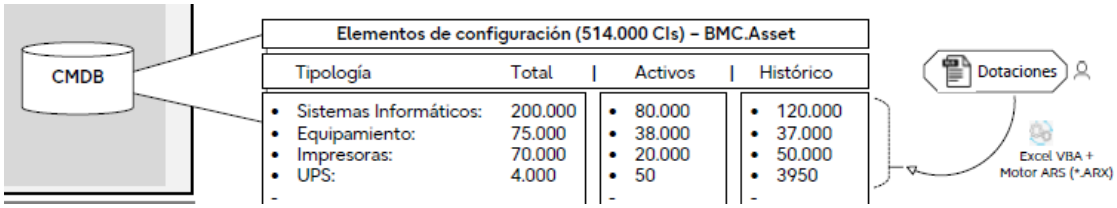


Ilustración 14. Volumetrías CMDB Dotaciones

Desde el equipo de Dotaciones se llevan a cabo cargas y modificaciones masivas de estos activos en CMDB, así como mantenimiento sobre la propia aplicación. Esto permite tener la información de los activos actualizada (su estado, atributos, propietarios, asignados, etc.)

Para las cargas y actualizaciones masiva existe un sistema de custom de carga mediante una plantilla Excel ad-hoc. El proceso es el mostrado en la imagen siguiente, donde:

1. El usuario completa el fichero Excel de carga.
2. Desde el fichero Excel se genera automáticamente mediante código VBA un fichero de datos con la información de los activos.

3. El fichero generado con los activos es procesado por la herramienta de importación de datos de BMC (BMC Remedy Import Data)
4. Los datos quedan cargados y accesibles a través de formularios web de la CMDB.

- PDAWEB

Esta integración está diseñada para mantener los datos de los CODIRED de la CMDB de PoST actualizados con los datos que hay en el aplicativo interno de Correos denominado PDAWEB.

De esta manera la actualización de estos datos de la CMDB es automática, y no se requiere de mantenimiento replicado, puesto que el mantenimiento se realiza en PDAWEB.

Los dos sistemas se integran de la siguiente forma:

- Mediante una implementación en BMC Atrium Integrator Spoon se conecta con la base de datos de PDAWEB, se extrae con SQL los datos necesarios de las PDAs, y se inyectan a PoST en formularios custom.
- En PoST, mediante desarrollos a medida, se procesa la información recibida y se actualizan los activos de CMDB afectados.

- AIRWATCH

Esta integración está diseñada para mantener los datos de determinados activos de la CMDB de PoST actualizados con los datos que hay en el aplicativo interno de Correos denominado AIRWATCH.

De esta manera la actualización de estos datos de la CMDB es automática, y no se requiere de mantenimiento replicado, puesto que el mantenimiento se realiza en AIRWATCH.

Los dos sistemas se integran de la siguiente forma:

- Mediante una implementación en BMC Atrium Integrator Spoon se conecta con la base de datos de AIRWATCH, se extrae con SQL los datos necesarios de los equipos involucrados, y se inyectan a PoST directamente a CMDB.

- Los datos recopilados son relativos a números de serie, identificadores, direcciones MAC, fechas de accesos, … Muchos de estos atributos son una personalización específica como extensión de la CMDB de Correos.

- MSP

Esta integración está diseñada para mantener los datos de determinados activos de la CMDB de PoST actualizados con los datos que hay en el aplicativo interno de Correos denominado MSP.

De esta manera la actualización de estos datos de la CMDB es automática, y no se requiere de mantenimiento replicado, puesto que el mantenimiento se realiza en MSP.

Los dos sistemas se integran de la siguiente forma:

- Mediante una implementación en BMC Atrium Integrator Spoon se conecta con la base de datos de MSP, se extrae con SQL los datos necesarios de los equipos involucrados, y se inyectan a PoST directamente a CMDB.
- Los datos recopilados son relativos a números de serie, identificadores, direcciones MAC, fechas de accesos, … Muchos de estos atributos son una personalización específica como extensión de la CMDB de Correos.

- SCCM

Esta integración está diseñada para mantener los datos de determinados activos de la CMDB de PoST actualizados con los datos hay en el aplicativo SCCM de Correos.

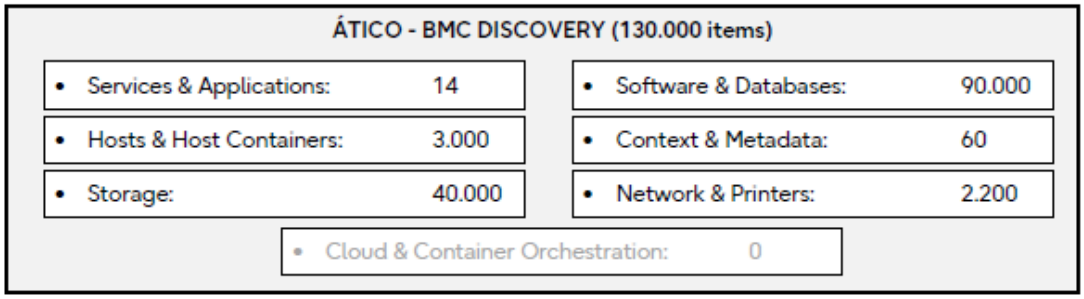
De esta manera la actualización de estos datos de la CMDB es automática, y no se requiere de mantenimiento replicado, puesto que el mantenimiento se realiza en SCCM.

Los dos sistemas se integran de la siguiente forma:

- Mediante la implementación de una ETL en BMC Atrium Integrator Spoon:
  - Se conecta con la base de datos de SCCM,
  - Se extrae con varias SQL los datos necesarios. Por ejemplo, de ámbitos como GS_Computer_System, GS_SYSTEM_ENCLOSURE_UNIQUE, GS_Operating_System, GS_X86_PC_Memory, GS_PC_BIOS
  - Se recopila, procesa y transforma toda la información obtenida.
  - Se inyecta en la CMDB de PoST.
- En PoST, mediante Jobs de reconciliación se terminan de procesar los datos incorporados, fusionándolos con la información del dataset productivo.

- Discovery (ATICo)

BMC Discovery, denominado ATICo en Correos, es la solución de descubrimiento de BMC. En ATICo se lleva a cabo el descubrimiento de los sistemas alojados en los CPDs y centros de datos de Correos. Esto incluye servidores físicos, virtuales, software, sistemas de bases de datos, de alojamiento, comunicaciones, etc.



Este sistema ha estado tradicionalmente integrado y reconciliado con la CMDB de Remedy, con la que además dispone de integración nativa por ser ambos productos de BMC.

No obstante, el escaso uso de estos datos de CMDB, y la falta de mantenimiento, condujeron a aprovechar la última actualización de BMC Discovery para proceder con

la limpieza de la CMDB y desconexión de la sincronización, con el objetivo de sanear el sistema y volver a conectarlo con posterioridad.

A la fecha continúa desconectado, funcionando Discovery en modo stand-alone, y se ha planificado su reconexión directamente con la nueva herramienta a la que se migre el actual PoST.

Así pues, la nueva herramienta deberá ser receptor de los datos de descubrimiento de ATICo.

2. PRESTACIONES A REALIZAR

En el presente apartado se exponen todos los servicios y prestaciones incluidos dentro del alcance del presente contrato.

Dichas prestaciones se dividen en tres bloques:

- Derechos de Uso de la Herramienta ITSM: En este apartado se detallarán los términos y condiciones bajo los cuales se otorgarán los derechos de uso de la nueva herramienta ITSM propuesta por el licitador, y que deben dar acceso a la funcionalidad relacionada en los apartados de requisitos del presente pliego.
- Servicios de Implantación y Puesta en Marcha: Este bloque abordará los servicios necesarios para la correcta implantación y puesta en marcha de la herramienta ITSM, incluyendo la configuración e integración de la solución con el resto de los sistemas del grupo Correos.
- Mantenimiento y Evolución Posterior: Aquí se expondrán los servicios de mantenimiento y evolución que garantizarán el funcionamiento continuo y la mejora de la herramienta ITSM. Se incluirán detalles sobre soporte técnico, actualizaciones, y mejoras futuras.

Actualmente, el grupo Correos dispone de BMC ITSM Remedy implantada en Correos en modo On Premise.

El grupo Correos necesita disponer de una solución que le permita reducir los costes de mantenimiento y de adaptación de las funcionalidades necesarias para reaccionar con agilidad a las necesidades de un mercado cambiante como el actual.

Así, se proporcionará un marco para la automatización y mejora de procesos como la gestión de incidentes, problemas, cambios, solicitudes de servicio y activos, con el fin de asegurar que los servicios de TI sean eficientes, alineados con las necesidades del negocio y con una experiencia de usuario de alta calidad.

Se requiere la implementación de una solución ITSM que cubra los requerimientos demandados por el grupo Correos.

- Diseño de la estrategia de implantación teniendo en cuenta las circunstancias y dimensión del proyecto.
- Provisión de derechos de uso.
- Provisión de 3 entornos (2 no productivos y 1 productivo) y activación del producto en los mismos
- Análisis de los procesos actuales y recogida de cualquier tipo de información relevante para el proyecto: usuarios, roles, plantillas y tipos de comunicaciones, etc.

- Configuración y desarrollos necesarios para adaptar la herramienta ITSM a las necesidades del Grupo Correos.
- Integración de la herramienta con los sistemas que intervienen en el proceso ITSM.
- Soporte a la puesta en producción.

En los siguientes subapartados se detallan cada una de las actividades solicitadas dentro del alcance del servicio

2.1. Capacidades de la Herramienta ITSM

2.1.1. Requisitos Generales

La nueva herramienta se basará en un producto ITSM que contemplará obligatoriamente los siguientes requisitos:

- Modalidad SaaS: La arquitectura propuesta estará basada en el modelo SaaS (Software as a Service), garantizando así la accesibilidad, flexibilidad y escalabilidad necesarias para el adecuado funcionamiento del sistema. La herramienta propuesta cumplirá con los estándares y mejores prácticas asociadas a este modelo.

  El grupo Correos será el titular del servicio de subscripción teniendo, de este modo, la titularidad y gestión de las instancias productivas y no productivas de las que se componga el servicio, así como la gestión del servicio de soporte técnico prestado por el fabricante del software ofertado.

  La solución deberá implementar una arquitectura multi-instancia de alta disponibilidad, donde cada cliente disponga de una instancia independiente de la plataforma. Cada instancia deberá contar con su propia base de datos, lógica de negocio y recursos dedicados, garantizando el aislamiento de datos, la seguridad y la personalización sin afectar a otros clientes. Además, el sistema deberá gestionar automáticamente el rendimiento, las actualizaciones y la escalabilidad de cada instancia a través de su infraestructura en la nube, permitiendo integraciones flexibles y un control total sobre la configuración.

  Adicionalmente, deberá disponer de una arquitectura única con un único modelo de datos, generando eficiencias ya que los módulos de la plataforma no se deberán integrar entre sí, vendrán nativamente conectados.

  Correos debe tener autonomía para controlar los procesos de subidas de versión de la nueva plataforma, una vez ésta haya entrado en funcionamiento. Por tanto, el adjudicatario no podrá realizar ningún cambio en las versiones utilizadas del software que forma parte de la plataforma sin la autorización previa, por escrito, de Correos. El adjudicatario deberá informar a Correos al menos con 1 mes de antelación de su intención de realizar una subida de versión de la plataforma mediante un informe motivado donde se indiquen los motivos de la actualización y las mejoras que se esperan conseguir con la actualización propuesta.

Los requerimientos en detalle para plataformas SaaS se encuentran definidos en el **Anexo XVII.- Declaración responsable en materia de protección de datos**

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

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

*AVISO PARA PEQUEÑAS Y MEDIANAS EMPRESAS:

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

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

El enlace a esta herramienta es el siguiente:
https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIwNTAwMDkxNTQ5NjEyMTMxMDMz?updated=true

Cuestionario para la Privacidad de Proveedores:

Marque y cumplimente lo que corresponda:

D. [ ] con NIF , actuando en
su propio nombre y derecho, como profesional autónomo,

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

DECLARA lo siguiente:

1. Cuestiones generales

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

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

0= no dispone del registro de actividades a pesar de ser obligatorio
5= dispone del registro de actividades actualizado y completado

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

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

0= no dispone de DPO siendo obligatorio.
3= no dispone de DPO siendo voluntario.
5= dispone de DPO siendo obligatorio. Identifíquelo: [ ]

2. Medidas de seguridad

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

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

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

A continuación, os facilitamos el enlace de la Guía de Análisis de Riesgos que facilita la AEPD:
https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

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

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

A continuación, os facilitamos el enlace de la Guía para la Gestión y Notificación de Brechas de Seguridad que facilita la AEPD:
https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

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

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

3. Confidencialidad

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

0= no
3= sí, disponen de código de conducta, o están sujetos a una obligación de naturaleza estatutaria.
5= sí, los empleados que van a realizar actividades en el marco del contrato a suscribir con [ ], han firmado un compromiso de confidencialidad.

4. Accountability y rendición de cuentas

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

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

0= no tiene implantados controles periódicos.
3=definidos no aplicados. Presentar planificación de aplicación con plazo determinado.
5= tiene definidos e implantados controles periódicos.

5. Subcontratación

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

0= se va a subcontratar el servicio contratado sin cumplir con las obligaciones de autorización previa.
5= se va a subcontratar el servicio y estará debidamente regulado.

6. Transferencias internacionales

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

0= se realiza Transferencias Internacionales de Datos a un país sin nivel adecuado de protección y sin ninguna garantía habilitante.
3= se realiza Transferencias Internacionales de Datos a un país con nivel adecuado de protección y utilizando alguna de las garantías habilitantes (cláusulas contractuales tipo, BCR´s, etc.). Indique cuál/cuáles: []
5= no se realiza Transferencias Internacionales de Datos.

7. Sanciones y procedimientos inspectores

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

1= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos idénticos a los prestados en este caso. Aportar documentación justificativa de haber corregido el motivo de la infracción.
3= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos distintos a los prestados en este caso.
5= no ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años.

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

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

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

Fdo.:

Anexo XVIII.- Requerimientos de Seguridad

1. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES

Desde el punto de vista organizativo, el adjudicatario deberá asignar un responsable de seguridad para el servicio prestado a la Sociedad Estatal de Correos y Telégrafos, S.A, que será el interlocutor único en dicha materia con la Subdirección de Ciberseguridad de Correos. Este rol se encargará de revisar y auditar los procesos de seguridad delegados en él, así como de notificar cualquier incidente o aspecto relevante en el ámbito de la seguridad.

En este contexto, el adjudicatario deberá crear un proceso de Gestión de la Seguridad específico para la Sociedad Estatal de Correos y Telégrafos, S.A, a través del cual se gestionen los procesos y responsabilidades de Seguridad que se le han transferido. Dicho proceso será liderado por el responsable de seguridad del servicio, que deberá compartir periódicamente un cuadro de mando con métricas e indicadores de seguridad integradas, así como realizar reuniones de seguimiento en las que se puedan tratar riesgos o aspectos críticos de seguridad de la información en la solución ofertada.

Adicionalmente, el proveedor deberá de disponer tanto de **personal experto como de herramientas específicas** para desarrollar de manera satisfactoria todos los procesos y funciones de Seguridad que le son transferidos.

La monitorización de la seguridad y la respuesta ante incidentes se deben considerar como un servicio 24x7.

2. REQUISITOS DE GESTIÓN DE LA SEGURIDAD POR PARTE DEL PROVEEDOR

La presente licitación, supone la delegación de ciertos procesos de la seguridad, que serán responsabilidad exclusiva del proveedor prestador del servicio.

En este sentido, la solución objeto del contrato, además de cumplir con los requisitos de seguridad trasladados por la Sociedad Estatal de Correos y Telégrafos, S.A y firmar el acuerdo de "Compromiso de aceptación de políticas de acceso y uso de infraestructuras de correos" (ver apartado 4.8), deberá asumir (tener implantados, y mantener), todos los controles y procesos que se identifican a continuación, con alcance de la prestación del servicio:

2.1 Controles de protección de las comunicaciones

El adjudicatario deberá implantar medidas de seguridad apropiadas, cifrando las comunicaciones a través de las cuales viaje información de Correos, especialmente cuando se manejan datos confidenciales o sujetos a alguna regulación. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.1)

2.2 Controles de Fortificación de sistemas

El adjudicatario deberá implantar medidas de fortificación sobre todos los elementos involucrados en la prestación del servicio bajo su responsabilidad y control, de acuerdo con las recomendaciones de los fabricantes, para lo que deberán existir

procedimientos específicos. La Subdirección de Ciberseguridad de Correos podrá solicitar los controles aplicados en cada ámbito y en cada dispositivo o software dedicado para el servicio, los procedimientos de fortificación. (ver apartado 4.3).

2.3 Proceso de gestión de identidades y control de acceso lógico

El adjudicatario deberá seguir unas directrices de gestión de identidades alineadas con las políticas de Correos, administrando y controlando, a través de las herramientas pertinentes, los accesos cuya gestión recaiga bajo su responsabilidad. **Cuando aplique, el proceso deberá estar integrado con el de Correos** (ver apartado 3.2).

2.4 Proceso de generación y explotación de eventos de seguridad

El adjudicatario deberá contar con un proceso formal de gestión de eventos que englobe la solución ofertada y que facilite la gestión de incidentes y la implantación de los requisitos de seguridad definidos en este ámbito dentro del proceso de seguridad en el ciclo de vida de las aplicaciones de Correos. Los eventos y alertas de seguridad generados deberán estar a disposición de Correos para su revisión en caso de ser requeridos (ver apartado 3.3).

2.5 Proceso de seguridad en el ciclo de vida de las aplicaciones

El adjudicatario deberá contar con un proceso propio para la construcción de SSII que incorpore la seguridad desde diseño, definiendo y aplicando requisitos de seguridad a las aplicaciones que se desarrollen. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.4).

2.6 Proceso de gestión y notificación de incidentes

El adjudicatario deberá contar con un proceso formal de gestión y notificación de incidentes de seguridad (diferenciando brechas RGPD) que le permita actuar siempre en tiempo y forma, de modo que se cumplan los requisitos legales y de disponibilidad definidos. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.5).

2.7 Proceso de contingencia y recuperación ante desastres

El adjudicatario deberá disponer de un plan de contingencia TI ante desastres que incluya las tareas y prioridades de recuperación de los activos impactados en el servicio. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.6).

2.8 Proceso de configuración segura del entorno tecnológico

El adjudicatario deberá manejar de manera automatizada la configuración de los recursos tecnológicos de su exclusiva responsabilidad, teniendo en cuenta las normativas de Seguridad y principios de Arquitectura de Correos. En particular, dentro del ámbito del cloud, deberá utilizar herramientas de control como CSPM (Cloud Security Posture Management) o CWPP (Cloud Workload Protection Platforms) de acuerdo al caso de uso específico y siguiendo los procesos de seguridad establecidos.

2.9 Proceso de gestión de vulnerabilidades y parcheado

El adjudicatario deberá contar con un proceso formal para gestionar, en la medida de lo posible de manera automatizada, la remediación de vulnerabilidades, aplicando controles para su detección automática y realizando pruebas antes de su instalación.

2.10 Proceso de Gestión de la Seguridad Global

Se trata del proceso que engloba todos los anteriores con alcance del servicio contratado.

Dicho proceso, deberá definir indicadores y métricas, que sean útiles de cara a comprobar la madurez de seguridad de la información, y elaborar un cuadro de mando visual, de cara a realizar un reporte periódico al equipo de Seguridad de la Información de Correos.

3 REQUISITOS DE SEGURIDAD PARA LA INTEGRACIÓN TÉCNICA DEL SERVICIO

3.1 Integración de 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.

3.2 Integración con el Sistema de Gestión de Identidades

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.

3.3 Generación, explotación y aportación de eventos de seguridad

A través del proceso de seguridad en el ciclo de vida de las aplicaciones, la Sociedad Estatal de Correos y Telégrafos, S.A, para cada desarrollo, podrá requerir la generación y explotación, como mínimo, de los siguientes eventos y alertas:

- Autenticación y accesos a la solución (acertados y fallidos).
- Cambios en las cuentas y grupos de usuarios y contraseñas (acertados y fallidos).
- Cambios accesos y modificaciones del sistema de log o auditoría (acertados y fallidos).
- Acciones realizadas con privilegios de administrador.
- Cambios en los privilegios asociados a cada rol.
- Registro de accesos a Información Personal (cumplimiento LOPD/RGPD).

La generación de los citados eventos y trazas de auditoría de la solución deberán permitir comprobar las siguientes políticas:

- Registro de accesos.
- Control de privilegios administrativos.
- Cumplimiento de la LOPD/RGPD.

Los eventos de auditoría generados deberán estar disponibles para la Sociedad Estatal de Correos y Telégrafos, S.A, en caso de que esta los solicite para su revisión o integración con su sistema de correlación de eventos (SIEM). En este sentido, el adjudicatario no deberá borrar los logs y trazas al menos durante un periodo de tiempo razonable.

3.4 Integración con el proceso de seguridad en el ciclo de vida de las aplicaciones

La Sociedad Estatal de Correos y Telégrafos, S.A dispone de un proceso que incluye la Seguridad en el Ciclo de Vida de los Sistemas de Información. Este proceso fija una serie de requisitos de seguridad detallados a cada nuevo sistema de Información y los grandes evolutivos, en función de los parámetros de Exposición del Sistema, Criticidad de la Información, Tipología de Usuarios y Normativa Legal Aplicable.

La adecuación a estos requisitos será revisada y acreditada, si procede, por el Área de Seguridad de la Información de la Sociedad Estatal de Correos y Telégrafos, S.A por lo que el adjudicatario se compromete a describir los controles de seguridad destinados a esta adecuación y a documentarlos en el documento denominado "Diseño de Seguridad" de la solución objeto del contrato.

En caso de que el Área de Seguridad de la Información no establezca este conjunto de requisitos, el adjudicatario deberá identificar en qué riesgos incurre la Sociedad Estatal de Correos y Telégrafos, S.A, qué medidas los mitigan y el plan de acción que tiene para mitigarlos. Para poder realizar este Análisis de Riesgos la Sociedad Estatal de Correos y Telégrafos, S.A facilitará el valor de la información gestionada en la solución.

3.5 Integración con el proceso gestión de 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.

Integración con el proceso de continuidad y recuperación ante desastres

Se establecerán procedimientos para integrar los servicios objeto del pliego con el Plan de Recuperación ante Desastres de Correos, de acuerdo con los escenarios de contingencia como a las condiciones de Tiempo de Recuperación Objetivo (RTO) y de Punto de Recuperación Objetivo (RPO) definidos por la Sociedad Estatal de Correos y Telégrafos, S.A. El adjudicatario deberá consensuar previamente la tipología de pruebas a realizar y el calendario de realización de las mismas

Se considerará un valor añadido que el adjudicatario del servicio disponga de la certificación ISO/IEC 22301 o equivalente.

4 OTROS REQUERIMIENTOS DE SEGURIDAD

4.1 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.

4.2 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.

4.3 Auditabilidad

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

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

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

4.4 Niveles de servicio

Todas las categorías de servicios descritas en el "Objetivo del contrato" de este acuerdo dispondrán de monitorización que permita un seguimiento en tiempo real del grado de cumplimiento de los niveles de servicio.

Por otra parte, se proporcionará a Correos informes mensuales que indicarán el rendimiento de los niveles de servicio. Este informe se pondrá a disposición de Correos siempre que sea requerido.

4.5 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.

4.6 Ubicación de los datos

Se tiene que explicar en un apartado específico en qué país van a residir los datos. En caso de que el servicio 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 contratado tendrán que cumplir con la nueva normativa Europea de protección de datos (GDPR).

4.7 Compromiso de aceptación de políticas de acceso y uso de infraestructuras de correos

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

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

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

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

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

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

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

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

Anexo XIX.- Requisitos de Arquitectura y Explotación que deben cumplir las nuevas soluciones tecnológicas. El incumplimiento de estos requisitos tendrá carácter excluyente y supondrá la no admisión de la oferta.

- Acuerdos de Nivel de Servicio (ANS) de disponibilidad proporcionado por el fabricante del producto propuesto. La herramienta garantizará ANS de disponibilidad de sus entornos de producción de, al menos, el 99.8%

- Garantía de calidad del fabricante de cara a las actualizaciones de versión de la herramienta ITSM: Se requiere que el fabricante de la herramienta ITSM ofertada proporcione una garantía de calidad integral para las actualizaciones de versión del software. Esto implica que las actualizaciones de versión deben ser sometidas a rigurosas pruebas de calidad internas por parte del fabricante antes de su lanzamiento al mercado. Estas pruebas deben incluir pruebas de funcionalidad, rendimiento, seguridad y compatibilidad con otros sistemas y aplicaciones. Las pruebas de tipo UATs específicas de proyecto serán garantizadas por parte del integrador, antes de su lanzamiento en entorno productivo.

- Automatización y simplificación de procesos de TI: Debe facilitar la automatización de los procesos de gestión de servicios de TI, como la gestión de incidentes, cambios y solicitudes, para mejorar la eficiencia operativa y reducir los tiempos de respuesta.

- Fomento del trabajo colaborativo: Debe proporcionar herramientas que permitan a los equipos de soporte y operaciones de TI colaborar de forma efectiva, compartiendo información y resolviendo problemas de manera conjunta.

- Comunicación continua con los usuarios: Debe permitir una comunicación fluida con los usuarios durante todo el ciclo de vida de los servicios de TI, desde la solicitud hasta la resolución, a través de diferentes canales, incluyendo correo electrónico, chat y el portal de autoservicio.

- Integración de plataformas de TI: Debe posibilitar la integración con distintas herramientas del grupo correos haciendo uso de estándares de mercado.

- Seguridad y confidencialidad de la información: Debe permitir la creación de perfiles de usuario y roles con niveles de acceso específicos para garantizar que la información de diferentes departamentos o áreas de la empresa esté adecuadamente protegida y segmentada. Además, debe ofrecer roles globales que den acceso completo a la información cuando sea necesario.

- Actualizaciones periódicas y mantenimiento transparente: El sistema debe contar con actualizaciones periódicas, transparentes y sin afectar a las personalizaciones y configuraciones existentes.

- Generación de alertas y notificaciones: Debe generar alertas y notificaciones ante eventos críticos, como la ocurrencia de un incidente importante o la necesidad de realizar un cambio urgente, para facilitar la toma de decisiones proactivas.

- Movilidad y acceso remoto: Debe facilitar el acceso a los servicios desde cualquier lugar y en cualquier momento, permitiendo a los empleados gestionar tareas de soporte y responder a incidencias desde dispositivos móviles.

- Reducción de tiempos de desarrollo y costos de mantenimiento: Debe acortar los tiempos de desarrollo para nuevas funcionalidades y reducir los costes asociados con el mantenimiento evolutivo y correctivo, optimizando el ciclo de vida de los servicios.

- Nivel de personalización: La herramienta debe ser capaz de soportar las personalizaciones ya implementadas, adaptándose a las necesidades y flujos específicos de la organización, asegurando que los procesos existentes sean completamente compatibles con las configuraciones y mejoras previas realizadas que se requieran mantener.

2.1.2. Requisitos Funcionales

La solución a implantar debe cubrir los siguientes requisitos funcionales:

- Manejo de todos los aspectos del ciclo de vida ITSM: La herramienta ofrecida será capaz de gestionar de manera integral todos los aspectos del ciclo de vida del Servicio de Gestión de Tecnologías de la Información (ITSM). Además de facilitar la gestión eficiente de incidencias, problemas, cambios, configuraciones, y activos de TI, la herramienta contemplará la gestión de los niveles de servicio. El licitador demostrará que el producto propuesto abarca todos los aspectos del ciclo de vida ITSM y proporcionará evidencia de su capacidad para gestionar eficazmente cada etapa del ciclo de vida del servicio.

- Procesos alineados con ITIL: La herramienta propuesta implementará procesos de gestión de servicios basados en las mejores prácticas establecidas por ITIL (Information Technology Infrastructure Library). Adoptará los procedimientos recomendados para la gestión eficiente de servicios de TI, asegurando así el cumplimiento y la certificación con los estándares internacionales reconocidos en la gestión de servicios de TI.

- Herramienta accesible, intuitiva y personalizable: La herramienta estará disponible en dispositivos móviles a través de una aplicación nativa y un portal web con diseño adaptativo. Su interfaz será intuitiva y amigable, permitiendo a los usuarios acceder a servicios digitales según su rol desde cualquier dispositivo. Permitirá configurar notificaciones para eventos como registro, resolución o aprobación de tickets, además de personalizar su apariencia con el logo corporativo. Siempre que las configuraciones del dispositivo lo permitan, se enviarán notificaciones push junto con las notificaciones por correo electrónico.

- Gestión de Incidencias: El sistema debe permitir el registro de incidentes a través de correo electrónico, portal web, chat, aplicación móvil y agente virtual y mostrar artículos de conocimiento relevantes durante su creación. Debe facilitar investigaciones y resoluciones mediante métricas contextuales y un espacio de trabajo configurable para gestionar incidentes, problemas y cambios. Además, los

agentes deben contar con una aplicación móvil nativa para la actualización de registros y trabajo sin conexión. Debe ofrecer vistas de dependencias para identificar servicios afectados, permitir la configuración de horarios de guardia y escalamientos, y proporcionar informes nativos para la monitorización del servicio. También debe incluir un espacio colaborativo para la gestión de incidentes críticos.

- Gestión de Comunicaciones de Incidentes: El sistema debe permitir la creación de planes de comunicación para incidentes, asignando responsabilidades de contacto y enviando notificaciones automáticas a los destinatarios correspondientes. También debe permitir que los usuarios de autoservicio se suscriban a estos planes. Además, debe integrar funciones de comunicación o servicios externos para enviar notificaciones por SMS, mensajes de voz, chat y configurar conferencias. Finalmente, debe ofrecer seguimiento del estado de las notificaciones enviadas a través de estos canales.

- Gestión de cambios: El sistema debe permitir la gestión avanzada del ciclo de vida de cambios, extendiendo los tipos tradicionales de ITIL y automatizando transiciones de estado. Debe evaluar automáticamente el impacto del cambio y activar dinámicamente políticas de aprobación, ya sean automáticas o manuales. Además, debe detectar conflictos, como períodos de restricción y asignaciones superpuestas, y representarlos visualmente. También debe contar con un asistente automatizado para programar cambios sin conflictos y ofrecer análisis de riesgos basados en datos e inteligencia artificial. Estas capacidades deberán alinearse con lo establecido en el apartado Anexo XX.- Cláusula sobre el uso de IA en contratos con Correos.

- Gestión de Solicitudes: El sistema debe registrar incidentes y solicitudes en tablas separadas y permitir a los administradores crear ítems de catálogo accesibles desde navegadores y aplicaciones móviles. Debe contar con flujos de trabajo gráficos para automatizar la gestión de solicitudes y permitir la asignación de tareas a múltiples grupos. Además, debe ofrecer vistas del catálogo de servicios según criterios como el departamento del usuario y proporcionar una aplicación móvil nativa para realizar solicitudes y obtener ayuda. También debe garantizar una experiencia unificada, permitiendo a los usuarios enviar solicitudes sin necesidad de conocer el departamento correcto, y ofrecer informes transversales desde la solicitud inicial hasta la resolución final.

- Gestión de Problemas: La herramienta agilizará la investigación de problemas a partir de una incidencia, heredando su información clave para facilitar su creación. Permitirá documentar el resumen de la investigación, incluyendo impacto, urgencia, prioridad, áreas afectadas, categorizaciones personalizables y detalles de la resolución aplicada. Además, contará con un espacio para registrar Errores Conocidos, Causa Raíz y Soluciones Temporales.

  Mediante inteligencia artificial, identificará incidencias recurrentes, clasificándolas por resolución y vinculándolas a un problema existente o creando uno nuevo. Su configuración será intuitiva, permitiendo definir criterios de agrupación como servicio, elementos impactados y descripción de las incidencias. Estas capacidades

deberán alinearse con lo establecido en el apartado Anexo XX.- Cláusula sobre el uso de IA en contratos con Correos.

- Informes y Dashboards de forma nativa: La herramienta proporcionará capacidades de generación de informes y paneles de control de forma nativa, sin necesidad de complementos o desarrollos adicionales. La herramienta debe incluir una variedad de informes predefinidos y personalizables que cubran diferentes resúmenes e informaciones obtenidos de los datos registrados, así como la capacidad de crear paneles de control intuitivos que permitan supervisar, medir (ANS de grupos de soporte), analizar el rendimiento y la salud de la gestión de tareas.

  Además, debe tener capacidades de analítica avanzada para poder analizar tendencias de una métrica en el tiempo definido.

  Igualmente debe permitir la capacidad de prever los valores de los KPIs para identificar si se alcanzará la meta en la fecha esperada, y permitir la creación de KPIs basados en cálculos de múltiples KPIs. Además, debe permitir a los usuarios realizar análisis estadísticos, mostrar diferentes cálculos, incluyendo cambios y porcentajes de cambio.

- Asistente Virtual: La herramienta contará con un asistente virtual o chatbot para facilitar la interacción del usuario con el sistema de gestión, simplificando procesos como el registro de tickets, seguimiento, actualización de información, reclamaciones y cancelaciones. El chatbot permitirá a los usuarios crear nuevos tickets, consultar el estado de los existentes, agregar detalles adicionales o archivos a un ticket, presentar reclamaciones, y gestionar cancelaciones de servicios o tickets. Además, resolverá dudas y consultas frecuentes, integrándose con la base de conocimiento de la empresa. Los usuarios podrán acceder a información sobre sus activos y elementos de configuración, mientras que los gestores tendrán acceso a información más detallada. El chatbot también medirá su rendimiento mediante encuestas de satisfacción y análisis para identificar áreas de mejora, además de permitir la solicitud de interacción con un agente en vivo cuando sea necesario.

  El asistente virtual y las capacidades de IA deberán apoyarse en modelos de lenguaje bajo control del proveedor o del órgano de contratación, garantizando en todo caso:

  - que los datos no se utilizan para el entrenamiento de modelos de terceros,
  - la información no se transfiere fuera de entornos controlados,
  - y se cumple con los requisitos de seguridad, privacidad y normativa aplicable (ENS, RGPD).

  Será requisito necesario la integración con la base de conocimientos y, además, la interacción con el agente virtual debe poder integrarse a través de MS Teams.

- La herramienta incluirá capacidades de IA predictiva: La herramienta debe permitir agrupar registros similares en clústeres para abordar incidencias de forma colectiva y detectar patrones, como la identificación de incidentes relacionados que puedan indicar un problema mayor. Además, debe categorizar y enrutar automáticamente los incidentes mediante una solución entrenada con registros históricos. La

herramienta debe incluir marcos para clasificar, agrupar y entrenar el sistema en la predicción y organización de datos. También debe ofrecer la capacidad de crear modelos predictivos únicos aplicables a procesos empresariales y proporcionar plantillas predefinidas para facilitar la implementación del aprendizaje automático. Además, debe contar con modelos de aprendizaje automático auto entrenados, así como la posibilidad de crear y afinar nuevos modelos, evaluarlos con conjuntos de datos familiares e integrarlos en los procesos de negocio. La herramienta debe permitir crear modelos predictivos duplicando y refinando modelos existentes, monitorear estos modelos a través de un panel de control, y realizar pruebas de diferentes versiones para evaluar su desempeño. Finalmente, debe facilitar la creación, evaluación, prueba e integración de modelos de manera sencilla y automatizada, permitiendo realizar pruebas individuales o por lotes y exportar los resultados.

- Base de datos de la gestión de la configuración (CMDB): Debe contar con una base de datos CMDB para almacenar representaciones lógicas de activos, servicios y sus relaciones, así como vistas de dependencias gráficas. Es crucial que integre datos de diversas fuentes, con capacidad de automatización para mantener la integridad de la CMDB y generar indicadores de salud, tanto predeterminados como personalizados. La gestión debe automatizar la validación de datos y establecer reglas de cumplimiento para evitar configuraciones erróneas. La interfaz debe ser moderna y fácil de usar, permitiendo la búsqueda rápida y la asignación de tareas. Finalmente, debe permitir pruebas rápidas para verificar la integridad de la CMDB tras actualizaciones o despliegues.

  Debe permitir el seguimiento independiente de activos y elementos de configuración (CIs) con sincronización automática cuando sea necesario.

  La herramienta tendrá la capacidad de establecer relaciones entre las clases de CI, incluyendo uno a uno, uno a muchos y muchos a muchos.

  La herramienta ofrecerá un modelo nativo de clases, atributos y relaciones entre clases que permita la clasificación de diversos tipos, como servidores, dispositivos de red, componentes de hardware, software, sistemas operativos, almacenamiento y recursos en la nube. Además, facilitará la personalización del modelo, permitiendo, por ejemplo, agregar nuevos atributos a las clases de activos existentes o crear nuevas clases y relaciones de manera sencilla.

  La herramienta contará con la capacidad de normalizar datos provenientes de diferentes fuentes, mediante la configuración de reglas que los ajusten a un formato estándar.

- Gestión de activos: La herramienta debe permitir la publicación de modelos de activos en un catálogo y agrupar hardware y software en un único modelo. La herramienta debe gestionar inventarios de artículos consumibles y no consumibles, y ofrecer opciones de consulta mediante códigos QR desde dispositivos móviles. También debe contar con aplicaciones móviles para que los agentes y usuarios vean y gestionen activos, reporten incidentes y escaneen activos en lotes. Además, debe facilitar la asignación de activos desde el almacén local y crear órdenes de

transferencia o compra si es necesario. Finalmente, debe ejecutar pruebas rápidas para asegurar la integridad de la gestión de activos tras actualizaciones y despliegues.

- Gestión del coste: La herramienta debe permitir el seguimiento de costes para elementos de configuración, contratos, tareas y mano de obra. Debe ser posible crear líneas de gasto y reglas de asignación de gastos. Además, debe permitir agregar los costes de los elementos de configuración y asignar el coste total a un servicio de negocio o aplicación utilizando rutas de relación.

- Gestión de Contratos: La nueva herramienta permitirá gestionar de manera eficiente los contratos existentes, facilitando la supervisión y la generación de informes detallados que respalden la toma de decisiones. Incluirá funcionalidades clave como la configuración de centros de coste, lo que permitirá asignar importes a unidades de negocio y subdividirlos si es necesario. Además, permitirá establecer relaciones jerárquicas entre centros de coste, facilitando la asignación y división de los costes según el consumo.

  La herramienta también ofrecerá métodos de asignación flexibles, como la distribución de costes mediante porcentajes definidos por el usuario. Permitirá configurar períodos de devolución de cargos, especificando el plazo en que los costes de activos deben ser devueltos a los centros de coste u organizaciones empresariales correspondientes. Finalmente, permitirá registrar las relaciones entre los CIs y sus contratos de mantenimiento, así como su vínculo con los grupos responsables de la resolución de incidencias.

- Gestión de Conocimiento: La herramienta permitirá a los usuarios gestores visualizar y controlar los artículos de la base de conocimiento mediante una consola, con filtros configurables para localizar rápidamente artículos. Contará con un potente motor de búsqueda que permitirá ordenar, recuperar y buscar contenido en varios formatos, así como dentro de registros y archivos adjuntos. Además, facilitará la identificación de información duplicada o redundante, alertando al usuario sobre artículos similares para decidir si crear uno nuevo o modificar el existente. La base de conocimientos ofrecerá artículos relevantes durante la creación de registros (Incidencias/Solicitudes) y pondrá a disposición de los usuarios finales artículos a través de canales de autoservicio. También se integrarán documentos y procedimientos existentes de Correos en la base de conocimiento de la herramienta.

- Gestión del portfolio digital: La herramienta debe contar con un espacio de trabajo unificado que permita a los responsables de las soluciones gestionar de manera integral sus servicios, aplicaciones y productos durante todo su ciclo de vida. Debe combinar la gestión de portafolios de servicios y aplicaciones, ofreciendo una vista combinada y coherente sobre la ideación, planificación, estado de construcción, rendimiento e información contextual.

- Gestión integral de iniciativas, proyectos, programas y carteras: alineada con el Modelo de Gestión de Iniciativas de Correos y adaptable a las distintas tipologías y equipos intervinientes, que permita la planificación y seguimiento de proyectos y programas estratégicos; la planificación económica integrada con Clarity y Geprex a

nivel micro y macro (imputación de costes internos, externos y de inversión, gestión de CAPEX y OPEX, control de desviaciones con alarmas e informes); la gestión de riesgos; la gestión de servicios de los equipos transversales; la gestión, priorización y cierre anual de carteras por Unidad de Negocio y de la Dirección de Tecnología, incluyendo presupuesto asignado, control de consumo e incurridos por hitos; la gestión de la capacidad a corto y medio plazo con escenarios de planificación y reordenación de prioridades; el seguimiento y control transversal de versiones y despliegues (mantenimientos periódicos, proyectos en paralelo y ventanas propias coordinadas); la gestión documental colaborativa; y la generación de informes y cuadros de mando sobre el estado de las iniciativas (recursos, plazos, costes y dependencias), hitos y ANS multi-propietario, desviaciones justificadas y aprobadas, y diferencias entre el tallaje inicial y el coste final.

- Traducción dinámica: La herramienta debe facilitar la traducción en tiempo real del contenido dentro de la plataforma, permitiendo que los usuarios y agentes se comuniquen en diferentes idiomas sin barreras lingüísticas. Con una integración con un sistema de traducción, se tendría traducción en tiempo real en el chat entre agentes y usuarios para que los agentes y solicitantes puedan interactuar en diferentes idiomas, y el sistema traduce automáticamente las conversaciones, asegurando una comunicación fluida. La herramienta debe facilitar conectores con los servicios de traducción de Google y Microsoft, o posibilitar la conexión con un traductor tercero.

- Gestión de citas: La herramienta debe proporcionar una aplicación para gestionar las citas para un servicio de soporte IT presencial o virtual. Los usuarios deben poder agendar citas para sí mismos o para otros, así como realizar el check-in en línea para el centro de servicio. La herramienta también debe permitir que los usuarios vean, se registren y obtengan detalles sobre las ubicaciones de la cola en sus dispositivos móviles, y se registren escaneando sus tarjetas para recibir un mensaje de confirmación sobre su posición en la cola. Además, los usuarios deben poder agregar sus citas a su calendario y los administradores deben poder configurar opciones de reserva basadas en el motivo del servicio.

- Gestión de encuestas: La herramienta debe incluir un diseñador de encuestas integrado que permita crear categorías y preguntas, configurar los detalles y publicar la encuesta a usuarios o grupos específicos. Debe ofrecer flexibilidad en el diseño de encuestas, como la posibilidad de crear preguntas condicionales que solo aparezcan cuando los usuarios respondan de cierta manera a otras preguntas. Además, debe permitir personalizar la apariencia de los cuestionarios y estar disponible a través de una aplicación móvil nativa.

- Gestión de proveedores: La herramienta debe ofrecer una experiencia de usuario intuitiva y visual para gestionar y monitorizar toda la información relacionada con el rendimiento de los proveedores en un solo lugar. Debe permitir configurar el peso, los modelos y las métricas para automatizar las puntuaciones de los proveedores, así como agregar y definir proveedores en los modelos de puntuación.

- Conectores: Se deben proporcionar conectores nativos preconfigurados compuestos de acciones preconfiguradas con las siguientes herramientas: Plivo, Slack, Cisco

Webex (Teams, Meetings), Microsoft Teams (Communications, Graph), Miro, Twilio, Microsoft Teams, Zoom, Workplace from Facebook, Google Chat, Google Hangouts, Ansible, Amazon (Connect, EC2, S3, etc.), Azure (Automation, DevOps *, etc.), Microsoft Azure (AD, Application Insights, etc.), Microsoft Dynamics, Microsoft 365, Crowdstrike, Docker, Kubernetes, Genesys, GitLab, Google Cloud, Jira, Okta, SAP (S4, Fieldglass …

- Gestión ágil: Se deben incluir capacidades para planificar, realizar seguimiento y gestionar el progreso de las tareas y sprints, asegurando la entrega continua de valor. Así, los equipos ágiles podrán colaborar, priorizar las tareas, gestionar el backlog de trabajo, hacer retroalimentaciones rápidas y ajustar las prioridades según los resultados obtenidos de cada iteración.

- Guiado de los procesos: Se debe proporcionar un guiado a los equipos a través de flujos de trabajo complejos, asegurando que los procesos empresariales se ejecuten de manera consistente y eficiente. Así, facilitan la toma de decisiones diseñando un conjunto de tareas a realizar garantizando el cumplimiento de las mejores prácticas y el seguimiento en tiempo real. Además, al ser personalizables, se adaptan a las necesidades específicas de cada organización, proporcionando una solución flexible y escalable para gestionar diversos procesos operativos.

- Integración DevOps: La herramienta debe permitir su integración con procesos y herramientas de DevOps para facilitar una gestión eficiente del ciclo de vida del desarrollo. Se integrará con herramientas de automatización DevOps, lo que permitirá definir flujos de trabajo, configuraciones y procesos mediante código, con el objetivo de agilizar la implementación y mejorar la colaboración entre los equipos de desarrollo y operaciones. Los conectores preconstruidos incluidos deberán ser con las siguientes herramientas: Azure Boards, GitHub, GitRally, Azure Repos, Bitbucket, Azure Pipelines, Jenkins, JFrog, Azure Artifacts, Argo CD y Veracode. Los conectores deberán ser preconfigurados, nativos de la plataforma y actualizados regularmente por el proveedor, sin necesidad de desarrollos personalizados.

- Otros módulos corporativos: La herramienta debe contar con otras aplicaciones y módulos en su portfolio de tal manera que Grupo Correos tenga disponibilidad para escalar en su uso más allá del área de TI, incluyendo la gestión de proyectos, riesgos, incidencias de seguridad, del ciclo de vida de empleados, CRM, sostenibilidad, agentes de campo, desarrollo de aplicaciones low-code, aplicaciones (APM), entre otras.

- Inteligencia Artificial Generativa: La solución deberá contar con un conjunto de casos de uso predefinidos de inteligencia artificial generativa nativa, aplicados a procesos de ITSM como gestión de incidencias, generación de resoluciones, generación de conversación para Agente Virtual, análisis de cambios, mantenimiento de CMDB, entre otros, de tal manera que Correos tenga disponibilidad para escalar en su uso en el futuro. Estas capacidades deberán alinearse con lo establecido en el apartado Anexo XX.- Cláusula sobre el uso de IA en contratos con Correos.

2.1.3. Requisitos de Licenciamiento

La solución propuesta debería cubrir mediante el licenciamiento ofertado las siguientes características demandadas por el grupo Correos:

- Usuarios solicitantes: **25.000 usuarios**

Son aquellos usuarios que requieren capacidades de acceso web y/o desde dispositivos móviles al portal de autoservicio de la solución, habilitados para apertura de peticiones, seguimiento de sus solicitudes, consulta de artículos de conocimiento, uso del asistente conversacional, etc.

- Usuarios técnicos y/o prestadores de servicios: **900 usuarios**

Referido a agentes y técnicos resolutores con capacidades para la gestión de los servicios prestados, incluyendo:

  - Atención de solicitudes realizadas por los usuarios solicitantes
  - Trabajo en las distintas actividades de cumplimiento de cada uno de los procesos (gestión de incidentes, gestión de peticiones, gestión de cambios, etc.)
  - Acceso a los diferentes módulos o aplicaciones propuestas: Gestión de Peticiones, Gestión de incidencias, Gestión de problemas, CMDB y Gestión de Activos, Gestión de Cambios, Gestión de Conocimiento, Gestión de Niveles de Servicio, Gestión de Contratos, etc.
  - Aprobación de solicitudes que requieren de revisión.
  - Colaboración con otros agentes
  - Reporting y monitoreo

- Usuarios visualizadores y aprobadores de flujos: **300 usuarios**

Relativo a usuarios que requieren aprobar peticiones de su ámbito o área, así como ver los diferentes registros solicitados.

- Entornos: se requiere de, al menos**, 3 instancias**.

  - Entorno de Desarrollo: para crear y probar nuevas funcionalidades, corregir errores y realizar cambios mediante iteraciones rápidas.
  - Entorno de Preproducción: para realizar pruebas de validación previas al lanzamiento, ejecutadas sobre funcionalidades completas, sin afectación a usuario final, y en un entorno estable y con los sistemas integrados.
  - Entorno de Producción: como entorno productivo para los usuarios finales.

2.2. Servicios de Implantación y Puesta en Marcha

Esta primera fase, cuya duración orientativa se propone en el entorno de los 12 meses, deberá ser la dedicada al proyecto de migración de la herramienta actual on-premise a la nueva herramienta en la nube. Esta etapa deberá asegurar la transferencia de todas las funcionalidades clave, la integración adecuada en el nuevo entorno y en la organización de Correos, así como una correcta puesta en producción de un producto viable y sin errores.

Ilustración 15. Fase 1 - Migración del sistema

No se espera del proveedor una migración "tal cual" de las configuraciones actuales. Por parte de Correos se contempla el presente expediente como un ejercicio de transformación y mejora de la herramienta actual.

Las configuraciones existentes, descritas en detalle en el apartado Anexo I.- Características técnicas específicas del contrato. del presente documento, deberán servir como referencia para, en el marco de las mejores prácticas de la nueva herramienta SaaS, mantener, mejorar e incrementar la funcionalidad que actualmente tiene Correos en el ámbito de sus procesos de negocio.

Correos tratará de adaptarse a los estándares de la nueva herramienta en el ámbito de cada uno de los procesos, siempre y cuando no exista pérdida de funcionalidad.

2.2.1. Alcance de actividades

En el contexto de la solución SaaS, el alcance mínimo de las actividades que el licitador deberá incluir en su propuesta de proyecto será:

- Configuración de entornos. Configuraciones base, tales como: configuración regional, idioma base (castellano), formatos de fecha, opciones de navegación, temas y esquemas de colores corporativos de Correos, sistema de notificación, políticas de seguridad, etc.

- Análisis, reingeniería e implantación de los procesos de gestión de incidencias, peticiones y cambios. Las configuraciones y desarrollos sobre la herramienta descritos en este documento se han venido realizando en los últimos años para dar cobertura a las necesidades y particularidades de los servicios prestados por Correos. Por tanto, se hace necesaria una tarea inicial de análisis de la situación actual, de forma que sobre el marco de la operativa de la nueva herramienta en el ámbito de estos procesos se asegure que Correos mantiene las funcionalidades requeridas.

- Las integraciones de la plataforma actual con sistemas terceros han de ser igualmente contempladas por el nuevo sistema en nube. El proveedor deberá analizar cada una de las integraciones listadas en el Anexo I.- Características técnicas específicas del

contrato., así como cualquier otra que sea identificada y comunicada por Correos en la fase inicial del diseño del proyecto, y proponer en cada caso el mecanismo de integración más adecuado de acuerdo con las capacidades de integración de la nueva plataforma.

Muchos de los sistemas a integrar son soluciones que actualmente residen en el CPD de Correos, por lo que el licitador deberá detallar el mecanismo de interconexión segura entre la solución ITSM en la nube y los sistemas en el CPD de Correos.

- Datos fundamentales de herramienta. En el contexto de la implementación de la nueva plataforma ITSM, será esencial que el proveedor configure adecuadamente los datos fundamentales que sustentarán los procesos y la operación del sistema. Esto incluye la definición y gestión de elementos clave como: las entidades organizacionales, tipos de empresas, localizaciones geográficas, estructuras jerárquicas de grupos y roles dentro de la organización. Estos datos deberán proporcionar la base para la correcta asignación de incidentes, solicitudes, y cambios, así como para la correcta visualización de informes y estadísticas.

- Gestión de usuarios. En el ámbito de la gestión de usuarios la plataforma deberá poder integrarse con el Gestor de Identidades corporativo de la organización, permitiendo una gestión centralizada y segura de los usuarios desde este sistema.

La integración debe garantizar una sincronización fluida entre el gestor de identidades y la plataforma, permitiendo la creación, modificación y desactivación de usuarios de forma automatizada y alineada con los procesos de control de acceso corporativo. Además, la solución debe cumplir con los requisitos de seguridad establecidos por la organización, asegurando que el acceso a la plataforma se realice de manera segura y eficiente, con un control adecuado de los permisos y roles asignados a cada usuario desde el Gestor de Identidades.

- En el ámbito de la autenticación, se deberá facilitar la autenticación de usuarios a través de la modalidad de Single Sign-On (SSO), asegurando que los empleados puedan acceder a la plataforma utilizando sus credenciales corporativas sin necesidad de recordar múltiples contraseñas. La herramienta delegará la autenticación de usuarios en el DA de Correos o en la solución de autenticación que Correos disponga en el momento del despliegue de la nueva plataforma.

- El portal de autoservicio es un canal imprescindible para los usuarios de Correos. El proveedor deberá realizar una configuración de portal que permita a los usuarios solicitantes interactuar con la solución de una forma fácil e intuitiva para acceder al catálogo de servicios, al área de reporte de incidencias, a la consulta del estado de sus solicitudes o a la base de datos de conocimiento. El portal de autoservicio se personalizará con la imagen de Correos y con una estructura adaptada a su organización y necesidades. Estará integrado con la solución de autenticación.

En la página principal del portal se presentará información relevante sobre el estado de incidencias, peticiones de servicio y aprobaciones del usuario, acceso a la apertura rápida de incidencias, acceso al catálogo de servicios, noticias relevantes de la

organización… así como a una función de búsqueda que permita al usuario acceder al conocimiento y a cualquier funcionalidad del portal.

- El catálogo de Servicios actual será trasladado a la nueva herramienta y estará accesible desde el portal de autoservicio. Se pretende que el licitador realice un análisis previo del conjunto de servicios actualmente publicados, con el objetivo de identificar el nivel de complejidad de las solicitudes actualmente configuradas, determinar la mejor vía para configurar dicho catálogo en la nueva herramienta y proponer a Correos, si así se estima conveniente una nueva estructura de catálogo. Se ha de perseguir el objetivo de disponer, por un lado, de un catálogo de servicios, intuitivo y orientado al usuario y, por otro, fácilmente mantenible en el futuro. Se mantendrán los permisos de acceso / visualización sobre los elementos del catálogo.

- Aunque Correos no dispone en la actualidad de un proceso de Gestión del Conocimiento, sí dispone de un conjunto de artículos de conocimiento que han de ser migrados a la nueva plataforma, juntamente con su visibilidad.

- El licitador deberá realizar un análisis del estado de la CMDB actual y realizar una propuesta de modelo de clases a usar en la herramienta en nube, utilizando al máximo el estándar de clases de CMDB de la nueva plataforma. En este análisis se determinará, a su vez, qué datos de la CMDB actual serán migrados a la solución en nube. El proyecto ha de contemplar las integraciones con los sistemas terceros que actualmente pueblan la CMDB, de forma que ésta se mantenga actualizada en todo momento. A su vez, el licitador debe proponer el modo más viable de integrar la actual solución de Discovery de Correos (BMC Discovery) con la nueva CMDB de la plataforma SaaS. Esta integración ha de ser incluida dentro del alcance.

- Para la gestión de activos y contratos, se hace necesaria una tarea inicial de análisis de la situación actual e implantación, de forma que sobre el marco de la operativa de la nueva herramienta se asegure que Correos mantiene las funcionalidades requeridas.

- El módulo de informes de la plataforma SaaS sustituirá a las actuales herramientas BMC Smart Reporting e INFOPoST. Dado el elevado número de informes configurados actualmente en una y otra herramienta, Correos determinará en su momento qué informes son prioritarios y tienen que estar incluidos en el go-live en nube. En la Fase 2 del presente contrato y, de acuerdo, al roadmap que Correos determine, se irán trasladando al sistema de reporting de la nube el resto de los informes.

- Los acuerdos de nivel de servicio activos en el momento de despliegue de la nueva solución han de ser configurados en la nueva herramienta. Se consideran fundamentales para la medición por parte de Correos del servicio prestado por sus proveedores.

- No se requiere la migración de tickets. Ambos sistemas convivirán durante un tiempo hasta que los tickets del antiguo sistema hayan sido cerrados. En el caso en que, por alguna circunstancia y transcurrido un periodo determinado acordado con Correos (por ejemplo, 1 mes) desde el go-live al nuevo sistema, existan aún tickets

en el sistema antiguo pendientes de cierre, se realizará un análisis de estos y se determinara la mejor forma de trasladar éstos al nuevo sistema.

2.2.2. Proyecto de migración

El licitador deberá presentar su plan propuesto para la migración, garantizando que sean cubiertos todos los aspectos fundamentales del proceso de migración a la nueva herramienta ITSM en la nube.

La propuesta de proyecto de migración deberá incluir, al menos, aspectos relativos a:

Alcance del proyecto y funcionalidades: Se deberá aportar una descripción del alcance de proyecto y funcionalidades, indicando la trazabilidad con el alcance propuesto para esta primera fase de implantación, así como aquellas funcionalidades o características propuestas para las siguientes fases.

Estrategia de implementación y migración: Se deberán definir las fases del proyecto con hitos clave y plazos.

- Esta planificación aportada deberá contemplar un enfoque flexible pero ajustado, con el fin de asegurar el éxito del proyecto en su totalidad.

- Se deberá garantizar que la solución implementada se alinee con los objetivos estratégicos y operativos de Correos, así como el cumplimiento de los requisitos reflejados en el presente pliego.

- Se deberán especificar los medios, herramientas, recursos humanos, así como las dependencias necesarias para la implementación y migración.

- Durante el periodo de ejecución de la migración el adjudicatario habrá de llevar a cabo las actividades de manera detallada y estructurada, garantizando una transición fluida y sin interrupciones en los servicios de Correos. Un aspecto fundamental será la minimización del impacto en las operaciones diarias, por lo que el licitador deberá especificar cómo se gestionarán las ventanas de migración, el soporte durante el proceso y cualquier otro aspecto relevante en este ámbito.

Metodología de gestión del proyecto:

- El licitador deberá proponer y describir la metodología de proyecto a emplear (ágil, tradicional o híbrida), junto con su justificación para la correcta migración a la nueva herramienta ITSM.

- Se deberá incluir detalle claro de las características de la metodología, así como de sus etapas, entradas, salidas y aspectos clave que garanticen la correcta adherencia a la misma.

- La propuesta metodológica deberá incluir, así mismo, un conjunto definido y claro de entregables a liberar a lo largo de la fase de migración, así como las herramientas y técnicas para la planificación, monitoreo y control de plazos, recursos y presupuesto.

- *Cumplimiento de estándares y metodología:*

  La empresa proveedora de servicios se compromete a llevar a cabo todas sus iniciativas en conformidad con las directrices establecidas por la Oficina de Proyectos TI de Correos. Esto implica adherirse a los estándares, procedimientos, directrices, prácticas recomendadas y requisitos de informes especificados por Correos para la ejecución de proyectos dentro del ámbito de la Dirección de Tecnología y Transformación Digital.

  La oficina de proyectos TI de Correos basa su funcionamiento en estándares reconocidos de gestión de proyectos, servicio y gobierno (PMBOK, marcos ágiles, ITIL , COBIT), y su funcionamiento está alineado y promueve los mismos.

  Así los entregables que la PMO solicita a las empresas proveedoras no difieren de los específicamente indicados en cada uno de estos estándares de trabajo, si bien la PO se reserva el derecho de solicitar la información que estime oportuna para satisfacer la demanda de sus peticionarios.

  Para clarificar, se muestra a continuación un ejemplo de algunos entregables que intervienen en la gestión de proyectos:

Entregable	Nomenclatura	Descripción
Correo Go-No Go	[AcrónimoProyecto] Descripción	Plantilla correo de Autorización o no de la Iniciativa.
Presentación de Kick-Off	AcrónimoProyecto_KO	Presentación del arranque del proyecto con las distintas partes involucradas.
Actas del proyecto	AcrProy_Fecha_COR/EXT_ACTA_Descripción	Acta de sesión donde se resume decisiones, acuerdos y próximos pasos discutidos.
Gestión de Riesgos	AcrónimoProyecto_GR	Identificación del riesgo, evaluación y categorización y respuesta al riesgo.
Listado de Requisitos	AcrónimoProyecto_LR	Detalle sobre la iniciativa, análisis de la necesidad y el tallaje.
Comité Operativo	AcrónimoProyecto_CO	Documento que recoge información sobre el estado, planificación, actividades y riesgos
Comité Ejecutivo	AcrónimoProyecto_CE	Documento que recoge información sobre el proyecto: Hitos, Riesgos y solicitud de cambios.
Análisis Funcional	AcrónimoProyecto_AF	Detalle sobre la toma de requisitos funcionales de negocio y técnicos.
Estimación OPSE (si aplica)	AcrónimoProyecto_EO	Plantilla a realizar por el proveedor para poder realizar la estimación en puntos función cuando aplique.
Diseño de seguridad	AcrónimoProyecto_DS	Documento elaborado por Seguridad que detalla el impacto del proyecto en los Dominios Funcionales.

Entregable	Nomenclatura	Descripción
Plan de proyecto	AcrónimoProyecto_PP	Documenta el modelo de gobierno y los procesos que se seguirán durante la ejecución del proyecto.
Diseño de Arquitectura	AcrónimoProyecto_DA	Documento donde se detalla la estructura del sistema, sus componentes e interacciones y los requisitos documentados.
Planificación del proyecto	AcrónimoProyecto_PL	Documento que contiene toda la información relevante a la calendarización del proyecto (inicio, fin, hitos...). Se extraerá mediante una captura de pantalla de ALBA.
Plan de pruebas	AcrónimoProyecto_PU	Documento que recoge información sobre el plan de pruebas: Entorno, pruebas, resultados, etc.
Trazabilidad de pruebas	AcrónimoProyecto_TP	Excel con detalle sobre las pruebas (PPI, PPC, AUT) y la visualización del estado de las mismas.
Manual de Explotación	AcrónimoProyecto_ME	Documento que recoge información técnica sobre el sistema a utilizar e información sobre los responsables involucrados.
Plan de Implantación	AcrónimoProyecto_PI	Plan detallado de cómo realizar la puesta en marcha de un proyecto, una vez realizado el desarrollo y se pasa a una situación de PaP.
Checklist de Despliegue	AcrónimoProyecto_CD	Documento que verifica que todas las tareas, aprobaciones y entregables necesarios para implementar un proyecto están completos.
Criterios para el traspaso a mantenimiento	AcrónimoProyecto_CM	Documento que detalla las condiciones que debe cumplir un proyecto para pasar a la fase de mantenimiento.
Cierre de Proyecto	AcrónimoProyecto_CP	Documento que incluye las lecciones aprendidas, entregables y traspaso de responsabilidades.

  Adicionalmente, la PMO podrá solicitar informes y documentación de apoyo a los comités establecidos en la Dirección de Tecnología y transformación cuyo objetivo y periodicidad se indican a continuación:

La empresa proveedora de servicios reconoce que cualquier desviación o propuesta de cambio respecto a los estándares y metodologías establecidos requerirá una 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.

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, incluida la terminación del contrato y la exigencia de compensación por cualquier daño o pérdida resultante.

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

Equipo de proyecto: Se deberá detallar la organización y los perfiles del equipo humano encargado de realizar el proyecto de implantación y el del servicio de Evolución, innovación y mantenimiento. Además, se incluirán los conocimientos y la experiencia de cada uno de los recursos atendiendo a los requerimientos descritos en el apartado 2.6.
Estructura de la propuesta
La propuesta presentada por el licitador para dar cobertura a los requerimientos recogidos en el presente Pliego ha de seguir la siguiente estructura:

N.º	Sección de la oferta técnica	Contenido obligatorio	Criterio(s)
1	**Resumen ejecutivo de la solución**	Visión general de la solución propuesta, alcance y enfoque (máx. 2 páginas).	N/A
3	**Adecuación funcional estándar y madurez ITSM**	Documento estructurado en los 4 subcriterios S1 (ver detalle abajo).	S1 (12 pts)
3.1	Matriz de cumplimiento de requisitos	Matriz conforme al modelo del pliego, con grado de cobertura y evidencia verificable.	S1.1
3.2	Estrategia de configuración vs desarrollo	Descripción clara de parametrización y desarrollos específicos, impacto en upgrades.	S1.2

3.3	Madurez funcional ITSM / ITIL v4	Prácticas ITIL cubiertas de forma nativa e integración entre procesos.	S1.3
3.4	Mantenibilidad y evolución	Modelo de releases, upgrades y evolución funcional.	S1.4
4	**Arquitectura enterprise, CMDB y gobierno del dato**	Documento estructurado en los 3 subcriterios S2 (ver detalle abajo).	S2 (9 pts)
4.1	Arquitectura de la plataforma	Modelo SaaS, multitenancy, segregación de entornos, upgrades, dependencia del integrador.	S2.1
4.2	CMDB y modelo de datos	Modelo CMDB, tipos de CI, relaciones, impacto y uso transversal en ITSM.	S2.2
4.3	Gobierno del dato y cumplimiento	Trazabilidad, auditoría, control de cambios, ENS / ISO.	S2.3
5	**Implantación, metodología y gobierno del proyecto**	Plan de proyecto integrado (ver detalle abajo).	S3 (8 pts)
5.1	Planificación y cronograma	Fases, hitos, entregables y dependencias.	S3.1
5.2	Metodología y control de calidad	Metodología, QA, pruebas, validación y aceptación.	S3.2
5.3	Gobierno y gestión de riesgos	Comités, reporting, gestión de riesgos y escalados.	S3.3
6	**Equipo de trabajo y experiencia acreditada**	Descripción del equipo propuesto (ver detalle abajo).	S4 (8 pts)
6.1	Experiencia en proyectos comparables	Referencias reales (sector, tamaño, alcance).	S4.1
6.2	Perfiles clave y certificaciones	Roles, experiencias y certificaciones relevantes.	S4.2
6.3	Estabilidad y dedicación del equipo	Asignación real y continuidad del equipo.	S4.3
7	**Mejoras comparables y maduras**	Propuesta de mejoras cerradas y verificables.	S5 (4 pts)
7.1	Automatizaciones adicionales nativas	Capacidades adicionales ya existentes (no roadmap).	S5.1
7.2	Capacidades avanzadas de autoservicio / IA	Funcionalidades operativas y maduras.	S5.2
8	**Anexos técnicos**	Evidencias, manuales, fichas técnicas, referencias cruzadas.	N/A

EQUIPO DE TRABAJO.

Gestión de la calidad y planes de pruebas: Se deberá detallar el plan de pruebas a seguir, incluyendo las distintas tipologías de pruebas que apliquen (pruebas unitarias, de integración, de aceptación del usuario, de rendimiento…), los criterios de éxito, mecanismos de control, así como los procedimientos para la corrección de incidencias detectadas.

Gestión de riesgos y planes de mitigación: Se deberán identificar los principales riesgos técnicos, operacionales y organizativos, junto con las estrategias de mitigación para cada uno.

Plan de despliegue y transición:

- Estrategia para el despliegue de la solución, incluyendo la planificación del lanzamiento y los mecanismos de control durante el proceso.

- Incluyendo asimismo detalles sobre la transición a la siguiente etapa del proyecto, con énfasis en la gestión de la continuidad y reducción de riesgos.

Plan de formación y capacitación:

- Se deberá aportar el programa de formación en castellano para los usuarios y el personal técnico, incluyendo los contenidos, cronograma y modalidad de entrega (presencial, virtual, materiales didácticos, …). Este material se preparará para que esté disponible antes del paso a producción. La formación a formadores deberá estar disponible también.

- Se realizarán vídeos y píldoras informativas que permitirán centrarse en una funcionalidad concreta, sin coste adicional para Correos. El licitador indicará el número de vídeos y píldoras formativas que desarrollará.

- De igual forma, será necesario indicar las estrategias para garantizar una transición efectiva y asegurar que los usuarios puedan utilizar la nueva herramienta sin inconvenientes.

Gestión del cambio:

- Se deberá definir la estrategia de gestión del cambio en Correos, enfocada en asegurar la aceptación del nuevo sistema por parte de los usuarios y minimizar la resistencia.

- Esto incluirá un plan de comunicación interna, involucrando a las partes interesadas clave y proporcionando recursos de apoyo durante la transición.

Informes de seguimiento y entregables del proyecto:

- Será necesario definir los informes a entregar durante el proyecto, con una descripción de estos (por ejemplo, indicadores de avance, plazos y responsables)

Go-Live y soporte post-implementación:

- Se deberá indicar un plan de soporte y mantenimiento post-implementación orientado a la estabilización. Se deberán detallar los procedimientos y herramientas para la gestión de incidencias en este período.

- La salida a producción (Go-Live) será determinada por la consecución de los objetivos de migración propuestos y acordados previamente con Correos, y será llevada a cabo tras la aprobación emitida por parte de Correos.

- Durante esta etapa, será prioritario garantizar el correcto funcionamiento de la herramienta, la adopción por parte de los usuarios, así como la resolución de cualquier incidencia que pudiera afectar al nuevo entorno.

La finalización del proyecto de migración a la nube tendrá lugar mediante la transición a la etapa de mantenimiento y evolución.

2.3. Evolución, innovación y mantenimiento.

Una segunda fase de duración de 24 meses se centrará en la evolución e innovación de la plataforma, así como en el soporte y mantenimiento correctivo necesario para garantizar su óptimo funcionamiento y adaptación a los cambios tecnológicos y operativos.

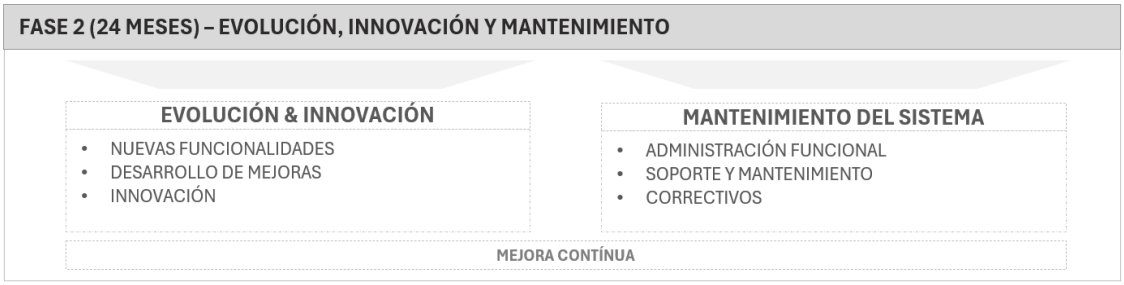


Ilustración 16. Fase 2 - Evolución, Innovación y Mantenimiento

Se requiere que en la Fase 2, en el ámbito de los proyectos de evolución e innovación, el licitador presente un roadmap de transformación, con un plan de despliegue de las nuevas capacidades incluidas en la solución en nube solicitada.

Esta etapa no debe ser contemplada únicamente como un mantenimiento de la nueva solución implantada en la nube, sino que se deberá diseñar como periodo de mejora y evolución progresiva, innovación y adopción de nuevas funcionalidades y características, escalando el valor aporta la nueva herramienta SaaS a Correos.

2.3.1. Líneas de servicio

Para estructurar esta nueva etapa, se contempla un modelo de servicio integral constituido por dos líneas de servicio diferenciadas:

1. Un Servicio de: "Mantenimiento integral de la solución"
2. Un Servicio de: "Evolución e Innovación de la solución"

El licitador deberá definir claramente en su propuesta las características ofertadas para estos servicios, incluyendo, al menos:

- **Servicio de "Mantenimiento integral de la solución".**

Se contempla como un servicio, el cual incluye todas aquellas actividades destinadas a mantener plenamente operativos los sistemas migrados mediante la corrección de cualquier disfunción e ineficiencia que se ponga de manifiesto durante el periodo. Esto incluirá, como mínimo:

- Mantenimiento correctivo: optimizaciones motivadas generalmente por la degradación en el funcionamiento de alguna parte de los sistemas. La resolución de incidencias queda incluida dentro de las tareas de mantenimiento. En caso de incidencias críticas, este servicio estará disponible 24x7x365.

- Mantenimiento adaptativo: labores adaptativas motivadas por la evolución del entorno tecnológico del sistema

- Mantenimiento preventivo: aquellos trabajos encaminados a cambiar el software para hacerlo más fácil de mantener, o detectar y corregir problemas no identificados aún por los usuarios.

- Pequeño evolutivo: aquellos evolutivos que no superen las 24 horas de esfuerzo.

- Atención a Usuarios: contemplando los siguientes servicios.

    - Centro de Atención al Usuario (CAU) de segundo nivel.
    - Soporte al CAU de primer nivel como grupo de apoyo de este.
    - Solución de las incidencias asignadas por el CAU de primer nivel al grupo. Cuando ésta no sea posible, se escalará la misma al grupo de apoyo que corresponda.
    - Atención y aclaración sobre funcionalidades de aplicaciones y aspectos básicos de los sistemas objeto del contrato.
    - Atención de consultas y resolución de los problemas que surjan durante el funcionamiento de los sistemas objeto del contrato que se encuentran en producción.
    - Documentación de las incidencias y su resolución

- Administración funcional del nuevo sistema, entendida como la realización de taras que no requieran desarrollo como son:

    - Gestión de grupos, usuarios y permisos
    - Configuración de nuevos servicios en el Portal de Autoservicio.
    - Creación de flujos de gestión de peticiones y automatización de tareas
    - Configuración de Acuerdos de Nivel de Servicio.
    - Configuración de la CMDB.
    - Configuración Gestión Conocimiento
    - Identificar componentes funcionales críticos del sistema para su monitorización y definición de procedimientos de escalado.
    - Implementación de tareas programadas y procesos batch de mantenimiento de la herramienta.
    - Colaboración y soporte funcional a los diferentes equipos de Correos.
    - Definición, configuración y soporte a usuarios de creación de informes impulsando la creación de estándares.

- Creación de Cuadros de Mando diferenciados por roles.
- Cualquier otra funcionalidad que se pueda configurar desde el módulo de Administración de la solución.

- Análisis de Impacto y documentación de estos

  - Toma de requisitos: identificación y recopilación de las necesidades trasladadas, obteniendo los requisitos necesarios para realizar el Análisis de impacto.
  - Definir el impacto funcional de una solicitud de cambio. Para ello, se realizará una identificación y análisis preliminar de la funcionalidad involucrada, que incluirá un estudio de las adaptaciones necesarias sobre la solución estándar de forma que estas sean mínimas. Esta identificación y análisis preliminar serán completados y detallados, en su momento, en el Análisis funcional.
  - Valorar el esfuerzo de los trabajos a realizar a lo largo de todo el ciclo de vida de la implantación de los cambios.
  - Planificación y fecha objetivo-estimada para la implantación.
  - Así, los Análisis de impacto deberán especificar, al menos, el coste, esfuerzo y fecha objetivo para la implantación de los cambios solicitados.

- **Servicio de "Evolución e Innovación de la solución"**

Se contempla como un servicio diferenciado del mantenimiento, e incluye todas aquellas actividades destinadas a mejoras y ampliaciones de funcionalidad del nuevo PoST en SaaS.

En este servicio, Correos podrá solicitar la realización de estudios de consultoría, peticiones de construcción de prototipos o de implementación de entornos definitivos que puedan incluir elementos que no formen parte de los servicios recogidos en este expediente, es decir, que impliquen nuevas tecnologías y/o proyectos de complejidad especial, siempre dentro del ámbito de este pliego. Previsiblemente serán proyectos de rápida ejecución y que requerirán perfiles profesionales específicos.

Cada una de las funcionalidades a implantar, se gestionará como un proyecto llave en mano independiente, para lo que el adjudicatario realizará un análisis de impacto previo que incluirá, al menos, una descripción de los requisitos a alto nivel, una planificación detallada, la definición de un equipo de trabajo y su dedicación, además del coste del evolutivo, que deberán ser aprobados por Correos.

Este coste constituirá el importe por el que se facture a su finalización el evolutivo, reducido en su caso por las posibles correcciones a la facturación derivadas del Acuerdo de Nivel de Servicio que se describe en el presente pliego.

Para esta parte del servicio, se requerirá un perfil de consultor ITIL que, atendiendo a los mínimos exigidos en el apartado "Equipo de Trabajo", deberá acreditar los conocimientos y la experiencia necesaria para la ejecución del evolutivo. Dicha acreditación podrá ser solicitada por Correos, previo al Análisis de Impacto, si así lo considera.

El consultor designado por el adjudicatario será, a partir de este momento, el único interlocutor con Correos en lo relativo al evolutivo y responsable último del mismo, a lo largo de las distintas fases de su ciclo de vida y comprendiendo al menos las siguientes tareas:

- Toma de requisitos y documentación de estos: identificación y recopilación detallada de las necesidades, obteniendo en cada momento los requisitos necesarios para las fases de análisis, diseño y construcción.
- Análisis funcional, construcción y parametrización de la funcionalidad solicitada, incluyendo las pruebas de todo tipo que sean precisas.
- Migración de datos, en caso de que el evolutivo desarrollado lo requiera.
- Generación de toda la documentación nueva que requiera y/o actualización de la documentación existente que esté afectada por el evolutivo, como manuales de usuario, manuales de explotación, etc.
- Desarrollo de un plan de formación y comunicación, que incluya el material de autoaprendizaje necesario para la formación continua de los usuarios del sistema.

La realización de los Análisis de Impacto se llevará a cabo en los plazos fijados en los Acuerdos de Nivel de Servicio, independientemente de si la demanda finalmente es aprobada para su desarrollo y puesta en producción. Asimismo, su ejecución estará sujeta a un ANS de desviación de consecución de hitos, fijados en base a la planificación detallada en el correspondiente Análisis de Impacto.

Para este servicio de "Evolución e Innovación de la solución", en la oferta se incluirán un mínimo de 2000 horas por año, siendo facturable solamente la parte que se consuma. Estas horas serán ofertadas en los perfiles indicados anteriormente. El coste en horas que requiera cada desarrollo a realizar deberá ser aprobado por Correos.

En la presente propuesta se deberá aportar un roadmap para esta fase, incluyendo una estrategia de adopción de nuevas funcionalidades y mejoras sobre la solución SaaS implantada, que contribuya al cumplimiento de los objetivos estratégicos de Correos a largo plazo, y permita aprovechar al máximo el potencial que la solución SaaS pueda ofrecer.

2.3.2. Modelo de gobierno

Aunque el Grupo Correos ya dispone de un modelo de gobierno de trabajo vigente, se requiere que los licitantes propongan en las ofertas sus propios modelos de gobierno, así como la metodología de trabajo.

Los licitantes deberán incluir una propuesta detallada de cómo será el plan de comunicación tanto interna como con los responsables del servicio en Correos:

- El principal objetivo del modelo de gobierno del proyecto será la función de control y coordinación, de manera que se garantice la máxima calidad en todos los servicios objeto del expediente. En concreto, asegurará que se cubren los siguientes aspectos:
    - Controlar la calidad del servicio y garantizar la mejora continua e innovación.

  - Garantizar que se cubren las necesidades de Correos en cualquier etapa del proyecto.
  - Involucrar a las figuras adecuadas tanto de Correos como del adjudicatario.

- Se implantará un modelo de gobierno colaborativo, de manera que la responsabilidad operativa sobre los servicios y recursos objeto del expediente estarán a cargo del adjudicatario, mientras que las tareas de control, de aprobación y de establecimiento de las directrices estratégicas se mantendrán en Correos.

- El adjudicatario deberá tener carácter proactivo en la propuesta de soluciones que aporten mejoras en el servicio y una reducción de costes a Correos:

  - Deberá realizar propuestas técnicas de valor añadido en sus ofertas (proyectos adicionales, iniciativas de innovación, etc.)
  - A lo largo del contrato, y con carácter periódico, el adjudicatario formulará a Correos propuestas de innovación que mejorarán el servicio.

- Correos mantendrá en todo momento la capacidad de aprobar o rechazar cualquier medida relacionada con los servicios objeto del contrato.

- Las relaciones con el resto de las direcciones y filiales de Correos continuarán siendo responsabilidad de la Dirección de Tecnología y Transformación Digital del Grupo Correos.

- Es necesario señalar que la prestación del servicio será en un entorno multi proveedor, en el que deberá tenerse en cuenta la necesidad de interacción con los proveedores del resto de expedientes de Correos. En este entorno, Correos tiene como objetivo la recepción de servicios con una calidad integral, en la que los proveedores no se limitarán al cumplimiento estricto de sus ANS, sino que proporcionarán garantías para el cumplimiento de la calidad esperada en los servicios.

- El marco de trabajo establecido deberá permitir al grupo Correos el cumplimiento de los requisitos legales ante auditores, reguladores, clientes y otras partes interesadas.

- El marco de trabajo deberá ser lo más flexible y ágil posible además de sencillo, no sólo en cuanto al número de personas involucradas en el gobierno, sino también en cuanto a procesos, distribución de responsabilidades, toma de decisiones, comités establecidos, etc. Sin embargo, dicho objetivo no debe afectar a la eficiencia y eficacia en las funciones de control y coordinación del gobierno del proyecto.

- Por último, el modelo de gobierno deberá responder a sus objetivos durante todas las fases del proyecto. En este sentido, podrá ser necesario establecer roles y funciones adicionales en el modelo de gobierno durante la fase de transición. De la misma manera, el modelo de gobierno deberá ser flexible ante cambios de cualquier tipo durante la ejecución del expediente.

Los licitadores deberán incluir en sus ofertas sus propuestas de Modelo de Gobierno y Operativo.

Los Modelos de Gobierno y Operativo deberán ser definidos en oferta y durante los primeros 15 días de la fase de prestación del servicio se terminarán de definir con el equipo del Grupo Correos. Ambos modelos serán abiertos y podrán ser modificados durante la duración del contrato para incluir y/o modificar tareas adicionales no contempladas que se requieran para el correcto funcionamiento de las prestaciones especificadas en el pliego de condiciones técnicas.

2.3.3. Metodología y documentación mínima

Las tareas objeto del presente contrato deberán realizarse en el marco de la metodología de Correos. El adjudicatario deberá entregar toda aquella documentación técnica y de gestión del proyecto contemplada en la citada metodología, la cual está basada en estándares de mercado, así como cualquier documentación adicional que, a juicio del adjudicatario, sea necesaria para alcanzar los objetivos del proyecto en cada momento.

Con carácter general, la documentación mínima a entregar incluirá los siguientes aspectos:

- Documentación de Gestión:
    - Plan de servicio: documento que debe recoger aspectos fundamentales de la organización y gestión del servicio, entre los que deben incluirse: la descripción del servicio (objetivos, enfoque, alcance, duración, etc.), la organización, estructura de este y su planificación y la relación de entregables si fueran necesarios.
    - Plan de gobierno transitorio y definitivo: documentación actualizada sobre los procesos de gobierno implantados.
    - Modelo de relación.
    - Informes de estado del servicio incluyendo los principales indicadores que sean requeridos por los responsables de Correos y con diferentes niveles (operativo, táctico y estratégico) con la periodicidad que se fije por Correos al inicio del proyecto.
    - Cuadro de mando: para el seguimiento mensual de los KPI's del servicio.
    - Informes sobre el cumplimiento de los ANS con la periodicidad que se fije por Correos al inicio del proyecto.
    - Plan de gestión de riesgos del proyecto
    - Informe de cierre: balance final del proyecto con la situación al cierre, resultados obtenidos, experiencias aprendidas y propuestas de nuevas iniciativas.
    - Actas de reunión que recogerán los temas tratados, así como los acuerdos o conclusiones a las que se han llegado, en las reuniones celebradas en el marco del proyecto.

- Documentación Técnica:
    - Catálogo de Requisitos Técnicos: requisitos técnicos del sistema y requisitos técnicos estándares de Correos.

- Análisis funcional: requisitos funcionales y descripción de modelos del sistema.
- Entorno tecnológico: requisitos técnicos, descripción de la arquitectura lógica y física, descripción de la seguridad y descripción de los requerimientos de capacidad de los distintos componentes y entornos del sistema.
- Diseño técnico: diseño de las diferentes capas y componentes del sistema a construir, y de los aspectos de seguridad de estos.
- Diseño de Seguridad: diseño de los requisitos técnicos de Seguridad estándares de Correos.
- Pruebas: estrategia, planificación, especificación e informes de las pruebas realizadas que cubran las pruebas unitarias, de integración, rendimiento, seguridad, funcionales, usabilidad y de aceptación.
- Plan de Contingencia: procedimiento detallado de recuperación del servicio sobre instalaciones e infraestructuras TI alternativas.
- Implantación: acciones, operaciones y procedimientos necesarios para implantar la aplicación en el entorno de producción. Incluirá el manual de implantación y los planes de comunicación, formación e implantación.
- Explotación: acciones, operaciones y procedimientos necesarios para el pleno funcionamiento de la aplicación en cualquier tipo de circunstancias, incluyendo condiciones extraordinarias.
- Usuario: presentación y descripción de las funcionalidades nuevas del sistema para su uso y administración.
- Manual del CAU: presentación del sistema y descripción de los procedimientos de actuación ante incidencias.

- Código fuente del software desarrollado: Se deberá entregar el código fuente de todo el software desarrollado, así como los ficheros necesarios para poder generar el fichero desplegable en su caso (EAR en caso de desarrollos java).

- Pruebas funcionales: El software debe haber superado las pruebas unitarias, de integración, funcionales, de usabilidad, seguridad y de aceptación que permitan asegurar que el sistema funciona correctamente, debiendo cumplir así mismo con las normativas de Usabilidad y Seguridad vigentes en Correos.

- Componentes Reutilizables: En Correos hay una política establecida para los componentes reutilizables. Cuando se detecta que una funcionalidad que se está desarrollando para un proyecto concreto puede ser útil para futuros desarrollos, se pide a dicho proyecto que implemente dicha funcionalidad de forma que pueda ser reutilizada en el futuro.

2.3.4. Sub-fases de la prestación del servicio

Las tareas relativas a las "*Evolución, innovación y mantenimiento*", se dividen en las siguientes sub-fases.

Cambio a modelo de servicio

El proyecto de migración a la nube de la herramienta ITSM debe incorporar en su definición una propuesta de transición desde proyecto un modelo de servicio que corresponderá con esta sub-fase.

En caso de que se produjera algún cambio en el equipo de proyecto en este cambio a servicio, será necesario contemplar un periodo de solapamiento de, al menos 15 días naturales previo a la entrada en esta *Evolución, innovación y mantenimiento*. En este periodo los técnicos integrantes del nuevo equipo de trabajo deben adquirir los conocimientos particulares de las prestaciones a realizar, junto con las peculiaridades y características de las aplicaciones, herramientas a utilizar, metodología de trabajo, es decir adquirir todos los conocimientos necesarios para poder prestar el servicio de forma independiente y adecuada a las necesidades de Correos.

Durante este periodo de tiempo el equipo de trabajo debe ser mixto, formado por integrantes del equipo técnico de proyecto y del entrante a servicio de mantenimiento y evolución.

Las empresas licitantes deberán presentar en su oferta, con carácter obligatorio, la organización de tareas, equipo, actividades, entregables, etc. para la asimilación del servicio en un detallado Plan de Transición, organizándose en fases solapadas en el tiempo y estableciéndose los correspondientes mecanismos de control y seguimiento: reuniones específicas, documentación e informes.

Asimismo, el licitante detallará en la oferta, unos hitos temporales, indicando durante cada una de las 2 semanas de solapamiento, la parte de conocimiento ya adquirido. Si finalizado el solapamiento, el nuevo equipo no ha asumido todo el conocimiento, se considerará únicamente facturable el coste del porcentaje del servicio efectivo.

Los Modelos de Gobierno y Operativo deberán ser definidos en oferta e implantarse durante los primeros 15 días de la fase de transición. Ambos modelos serán abiertos y podrán ser modificados durante la duración del contrato para incluir y/o modificar tareas adicionales no contempladas que se requieran para el correcto funcionamiento de las prestaciones especificadas en el pliego de condiciones técnicas.

Fase de prestación y mejora continua del servicio

Esta es la fase principal y se inicia inmediatamente después de la finalización de la transición del proyecto de migración.

Durante esta fase el adjudicatario prestará todos los servicios requeridos en este pliego, de acuerdo con lo solicitado por Correos y a lo detallado en la oferta del adjudicatario. En caso de que Correos estime la necesidad de iniciar alguna prestación identificada con posterioridad a la redacción del presente documento, toda la información necesaria será suministrada antes del comienzo de la fase de asimilación.

En esta fase será imprescindible la "Gestión del Servicio" cuyo objetivo, entre otros, es la creación de un sistema de control y seguimiento del trabajo que permita a Correos evaluar la calidad y adecuación de los servicios prestados. El adjudicatario deberá implantar dicho sistema de control inmediatamente desde la fecha de comienzo de la fase de prestación, de acuerdo con el mecanismo presentado en la oferta.

Fase de traspaso o recuperación del servicio

A la finalización del contrato, y en previsión de que pueda producirse un cambio de adjudicatario es necesario contemplar un período de solapamiento de una mensualidad, en el que los técnicos integrantes del nuevo equipo de trabajo adquirirán los conocimientos particulares asociados a los procedimientos, arquitecturas, implantaciones e instalaciones en Correos, junto con las peculiaridades y características de los servicios, las aplicaciones, productos, herramientas y metodología de trabajo, incluyendo todos los desarrollos realizados para Correos.

Durante este periodo de tiempo el equipo de trabajo debe ser mixto, formado por integrantes del equipo técnico del adjudicatario saliente (como mínimo el 60% del equipo habitual y compuesto como mínimo por un integrante habitual seleccionado por Correos para cada uno de los servicios) y del entrante.

Esta fase coincidirá con la última mensualidad del plazo de ejecución del adjudicatario saliente.

Este traspaso se realizará conforme al Plan de Finalización o Reversión del servicio presentado en su oferta y cuyos requisitos mínimos serán los siguientes:

- Facilitar toda la documentación completa y totalmente actualizada relacionada con los servicios (documentos soluciones, evolutivos, documentos de valoraciones de productos, estándares, normativas, inventarios, documentos de seguimientos, documentos de estudios y pruebas de conceptos, etc.)

- La documentación se entregará en formato electrónico y con referencia a repositorios de documentación e irá acompañada de una relación de esta por servicio.

- Diseñar y planificar las actividades necesarias para el traspaso de todos los servicios contemplados en el pliego al nuevo proveedor.

- El adjudicatario facilitará al nuevo adjudicatario, o a quien Correos designe, acceso previo a los servicios de Correos, siempre que el nuevo adjudicatario se comprometa a cumplir los requisitos de seguridad y confidencialidad razonables exigidos por el adjudicatario.

- Acceso a consulta, después de la finalización del contrato, a las personas responsables de los equipos del nuevo proveedor que dan servicio a Correos.

- Asignar el esfuerzo necesario de los recursos clave para conseguir una transición de salida exitosa.

- Poner a disposición del Grupo Correos un equipo de personas clave para garantizar el traspaso de conocimiento al nuevo proveedor.

- Notificar a Correos de los riesgos potenciales.

- Establecer y mantener una relación de trabajo efectiva con la organización receptora del servicio, tanto sea la del Grupo Correos como la de un Tercero designado por Correos.

- Cualquier otra actividad razonablemente requerida por Correos para el soporte en la ejecución del plan de finalización.

A la finalización de esta fase, todos los servicios deberán ser asumidos por el siguiente adjudicatario.

Durante este periodo se continuarán registrando solicitudes y midiendo plenamente los ANS al adjudicatario del presente pliego y, en su caso, se efectuarán las correcciones a la facturación previstas al 100%.

A lo largo de esta fase, el proveedor saliente deberá actualizar y hacer entrega a Correos de toda la documentación. Hasta que esta entrega no se haya realizado y aprobado por Correos no se considerará finalizado el servicio y, por tanto, no se podrá facturar el último mes de coste fijo ni cualquier otro trabajo que estuviera pendiente de facturarse.

2.4. Mejoras de valor añadido

Se invita a los licitadores a complementar su propuesta con iniciativas de valor añadido que aporten innovación y mejora continua a lo largo del ciclo de vida del proyecto.

En particular, se valorarán positivamente aquellas propuestas que incorporen capacidades avanzadas de automatización de procesos, herramientas de desarrollo low-code que faciliten la agilidad en la evolución de la solución, funcionalidades basadas en inteligencia artificial, así como mejoras en la calidad, proactividad o eficiencia del servicio de soporte y mantenimiento. Estas capacidades deberán alinearse con lo establecido en el apartado Anexo XX.- Cláusula sobre el uso de IA en contratos con Correos.

Estas aportaciones deberán presentarse de forma clara y justificada, destacando su aplicabilidad práctica y el valor que aportan a la organización.

2.5. Otros requerimientos

Requerimiento de facturación en euros de todos los servicios: Todos los servicios deberán ser facturados en euros. El licitador deberá detallar, en fase de oferta, su metodología de cambio de moneda en caso de ser necesaria conversión.

Requerimientos de idioma y localización de ejecución del contrato: Todos los documentos del expediente deberán ser redactados y firmados por las partes en castellano al igual que las ofertas y posibles aclaraciones de los licitadores.

Tanto la interlocución y relación entre los profesionales de Correos y el adjudicatario como la documentación generada durante el expediente (especificaciones técnicas, operaciones y procesos de gestión, informes, etc.) deberá ser en castellano.

Plan de formación: Será necesario por parte del licitador que en las ofertas se incluyan cursos de formación para toda la organización.

La empresa adjudicataria contactará con el Área de Formación de Correos, a fin de coordinar, desde el inicio del proyecto, la preparación, diseño, calendario, metodología

y contenidos de la formación a impartir, para garantizar su planificación y prever y subsanar las posibles dificultades o necesidades que se deriven del proyecto.

Al tratarse de aplicaciones corporativas, el proveedor adjudicatario tendrá en cuenta los requerimientos técnicos de los PC's de las aulas de formación o de los puestos de trabajo en los que se van a realizar los cursos, tanto a nivel hardware, como software, así como la compatibilidad (o incompatibilidad) con otras aplicaciones ya instaladas en dichos PC's.

Se deberá aportar, al menos:

- Presentación del curso (objetivos, contenidos, metodología, ayudas)
- Guía didáctica del curso
- Material Pedagógico de Monitores y Alumnos: Presentaciones, Manuales o guías específicos de formación (independientes de los de la aplicación), que deberán entregarse a Formación con, al menos, quince días hábiles de anticipación para su diseño pedagógico, reproducción y envío a aulas.

2.6. Estructura de la propuesta

La propuesta presentada por el licitador para dar cobertura a los requerimientos recogidos en el presente Pliego ha de seguir la siguiente estructura:

N.º	Sección de la oferta técnica	Contenido obligatorio	Criterio(s)
1	**Resumen ejecutivo de la solución**	Visión general de la solución propuesta, alcance y enfoque (máx. 2 páginas).	N/A
3	**Adecuación funcional estándar y madurez ITSM**	Documento estructurado en los 4 subcriterios S1 (ver detalle abajo).	S1 (12 pts)
3.1	Matriz de cumplimiento de requisitos	Matriz conforme al modelo del pliego, con grado de cobertura y evidencia verificable.	S1.1
3.2	Estrategia de configuración vs desarrollo	Descripción clara de parametrización y desarrollos específicos, impacto en upgrades.	S1.2
3.3	Madurez funcional ITSM / ITIL v4	Prácticas ITIL cubiertas de forma nativa e integración entre procesos.	S1.3
3.4	Mantenibilidad y evolución	Modelo de releases, upgrades y evolución funcional.	S1.4
4	**Arquitectura enterprise, CMDB y gobierno del dato**	Documento estructurado en los 3 subcriterios S2 (ver detalle abajo).	S2 (9 pts)
4.1	Arquitectura de la plataforma	Modelo SaaS, multitenancy, segregación de entornos, upgrades, dependencia del integrador.	S2.1
4.2	CMDB y modelo de datos	Modelo CMDB, tipos de CI, relaciones, impacto y uso transversal en ITSM.	S2.2

4.3	Gobierno del dato y cumplimiento	Trazabilidad, auditoría, control de cambios, ENS / ISO.	S2.3
5	**Implantación, metodología y gobierno del proyecto**	Plan de proyecto integrado (ver detalle abajo).	S3 (8 pts)
5.1	Planificación y cronograma	Fases, hitos, entregables y dependencias.	S3.1
5.2	Metodología y control de calidad	Metodología, QA, pruebas, validación y aceptación.	S3.2
5.3	Gobierno y gestión de riesgos	Comités, reporting, gestión de riesgos y escalados.	S3.3
6	**Equipo de trabajo y experiencia acreditada**	Descripción del equipo propuesto (ver detalle abajo).	S4 (8 pts)
6.1	Experiencia en proyectos comparables	Referencias reales (sector, tamaño, alcance).	S4.1
6.2	Perfiles clave y certificaciones	Roles, experiencias y certificaciones relevantes.	S4.2
6.3	Estabilidad y dedicación del equipo	Asignación real y continuidad del equipo.	S4.3
7	**Mejoras comparables y maduras**	Propuesta de mejoras cerradas y verificables.	S5 (4 pts)
7.1	Automatizaciones adicionales nativas	Capacidades adicionales ya existentes (no roadmap).	S5.1
7.2	Capacidades avanzadas de autoservicio / IA	Funcionalidades operativas y maduras.	S5.2
8	**Anexos técnicos**	Evidencias, manuales, fichas técnicas, referencias cruzadas.	N/A

3. EQUIPO DE TRABAJO

El licitador en su propuesta incluirá un apartado llamado "Equipo de trabajo" donde detallará la organización y los perfiles del equipo humano encargado de realizar el proyecto de implantación y el del servicio de Evolución, innovación y mantenimiento. Además, se incluirán los conocimientos y la experiencia de cada uno de los recursos con las que planea ejecutarlo.

3.1. Equipo base de Trabajo

El equipo propuesto estará debidamente dimensionado para realizar las tareas de implantación del proyecto y con el conocimiento y la experiencia requeridos en despliegues de soluciones de ITSM y servicios de soporte y evolución similares. A continuación, se presenta el equipo mínimo estimado para llevar a cabo el proyecto que debe tener una dedicación completa (100%) durante las fases de implantación (1 jefe de proyecto, 2 consultores sénior y 2 técnicos especialistas, el resto de los perfiles propuestos por el licitador podrán tener una dedicación variable):

1 Jefe de Proyecto

- 10 años de experiencia demostrable realizando las funciones solicitadas en el presente Pliego.
- 10 años de experiencia en la implantación de soluciones de ITSM

- Posee, al menos, una de las certificaciones siguientes en la herramienta ITSM propuesta:
  - Certificación profesional en Gestión de Servicios TI.
  - Certificación profesional en Gestión de la Configuración.
  - Certificación profesional en Gestión de portal de servicios.
  - Certificación profesional en el core de la herramienta.
- Titulación: licenciado, ingeniero superior o técnico en cualquiera de las áreas de ingeniería, informática o ciencias, o su titulación equivalente después de Bolonia
- Al menos, certificación ITIL Foundation.

2 Consultores sénior

- 8 años de experiencia demostrable realizando las funciones solicitadas en el presente Pliego.
- 5 años de experiencia en la implantación de soluciones de ITSM.
- Posee, al menos, una de las certificaciones siguientes en la herramienta ITSM propuesta:
  - Certificación profesional en Gestión de Servicios TI.
  - Certificación profesional en Gestión de la Configuración.
  - Certificación profesional en Gestión de portal de servicios.
  - Certificación profesional en el core de la herramienta.
  - Certificación Informes y Dashboard en la herramienta.

  Se valorará positivamente disponer de 2 o más certificaciones oficiales del fabricante.

- Titulación: licenciado, ingeniero superior o técnico en cualquiera de las áreas de ingeniería, informática o ciencias, o su titulación equivalente después de Bolonia.
- Al menos, certificación ITIL Foundation.

2 Técnicos especialistas

- 3 años de experiencia demostrable realizando las funciones solicitadas en el presente Pliego.
- 2 años de experiencia en la implantación de soluciones de ITSM.
- Posee, al menos, una de las certificaciones siguientes en la herramienta ITSM propuesta:
  - Certificación profesional en Gestión de Servicios TI.
  - Certificación profesional en Gestión de la Configuración.
  - Certificación profesional en Gestión de portal de servicios.
  - Certificación profesional en el core de la herramienta.

  Se valorará positivamente disponer de 2 o más certificaciones oficiales del fabricante.

- Titulación: diplomado o ingeniero técnico en cualquiera de las áreas de ingeniería, informática o ciencias, o su titulación equivalente después de Bolonia. Alternativamente se admitirá una titulación de FP Ciclo Formativo de Grado

Superior en las áreas anteriormente descritas cuando se acrediten 12 meses adicionales de experiencia como técnico especialista.
- Al menos, certificación ITIL Foundation.

En ausencia de certificaciones de los perfiles se podrá acreditar formación oficial de la herramienta ITSM propuesta en alguno de los componentes de la herramienta que apliquen al objeto de la licitación y ejecución de los proyectos.

Para las tareas relacionadas con la Gestión del Cambio, se estima al menos un perfil como el descrito a continuación, que participará en el proyecto en las etapas propuestas por el licitador:

Consultor sénior de Gestión del Cambio

- Perfil con más de 5 años de experiencia en proyectos de Gestión del Cambio y acompañamiento al usuario.
- Certificado en metodologías de Gestión del Cambio, tales como HCMBOK y/o PROSCI.
- Titulación: diplomado o ingeniero técnico en cualquiera de las áreas de ingeniería, informática, ciencias o ADE, o su titulación equivalente después de Bolonia.

Para las tareas relacionadas con el servicio de Evolución, innovación y mantenimiento, se estima el equipo mínimo que debe estar compuesto por al menos tres personas, siendo valorable incorporar más miembros al equipo, tal y como se establece en los criterios de valoración:

1 Jefe de Proyecto

- 5 años de experiencia demostrable realizando funciones de soporte y mantenimiento en el ámbito de las prestaciones requeridas en el presente Pliego.
- 3 años de experiencia en la implantación de soluciones de ITSM
- Titulación: licenciado, ingeniero superior o técnico en cualquiera de las áreas de ingeniería, informática o ciencias, o su titulación equivalente después de Bolonia.
- Al menos, certificación ITIL Foundation.

2 Técnicos especialistas

- 3 años de experiencia demostrable realizando funciones de soporte y mantenimiento en el ámbito de las prestaciones requeridas en el presente Pliego.
- 2 años de experiencia en la implantación de soluciones de ITSM
- Titulación: diplomado o ingeniero técnico en cualquiera de las áreas de ingeniería, informática o ciencias, o su titulación equivalente después de Bolonia. Alternativamente se admitirá una titulación de FP Ciclo Formativo de Grado Superior en las áreas anteriormente descritas cuando se acrediten 12 meses adicionales de experiencia como técnico especialista.

Para la prestación de los servicios objeto del presente Pliego, las empresas licitantes deberán ofrecer un servicio integral, que permita disponer de los recursos técnicos

necesarios en cada momento para poder dar respuesta con los niveles de calidad requeridos y dentro de los plazos exigidos en el correspondiente acuerdo de nivel de servicio.

Si bien los licitadores deberán concretar en sus respectivas ofertas el equipo técnico ofrecido que, ajustándose a lo solicitado en el Pliego, se considere idóneo para atender las necesidades en éste especificadas, no es objetivo de este el contratar un equipo de personas sino el disponer de un servicio integral ligado a un acuerdo de nivel de servicio previamente establecido al inicio del contrato (ver apartado correspondiente).

De este modo, los licitadores deberán dirigir sus proposiciones técnicas hacia un enfoque orientado al servicio y no a los recursos, debiendo concretar en sus respectivas ofertas el nivel de flexibilidad ofrecido en cuanto a composición del equipo de trabajo, ubicación de este (que podrá ser tanto en las oficinas de Correos como en las del licitante, incluyendo soluciones mixtas), disponibilidad de equipos expertos para absorber trabajos específicos y/o puntas de trabajo, etc.

El personal que por su cuenta aporte o utilice la empresa adjudicataria para la prestación del servicio objeto de este Pliego, no tendrá vinculación alguna con CORREOS, por lo que no tendrá derecho alguno respecto a ésta, toda vez que depende única y exclusivamente del contratista, el cual asume todos los derechos y deberes respecto de dicho personal, con arreglo a la legislación vigente y a la que en lo sucesivo se promulgue, siendo responsable, por tanto, de cuantas obligaciones hubiere contraído respecto de sus trabajadores, sean o no consecuencia directa o indirecta del desarrollo del Proyecto.

Todo aquel personal de la empresa que desarrolle su actividad en las dependencias de Correos deberá portar una acreditación identificativa de las empresas a que pertenecen y se les facilitará un puesto que Correos señalizará debidamente como “asignado a personal externo”.

El equipo de personas que, tras la formalización del presente contrato, se encargue de llevar a cabo la prestación del servicio objeto de este, deberá estar formado por los perfiles relacionados en la oferta y consecuentemente valorados.

El equipo de técnicos ofrecido deberá cubrir conjuntamente todo el entorno tecnológico de los sistemas, debiendo reunir la suficiente experiencia y conocimientos en el mismo como para trabajar de forma autónoma, sin requerir el apoyo de técnicos de Correos más allá del tratamiento de las interfaces con otros sistemas.

Correos se reserva el derecho de solicitar la sustitución de técnicos del equipo de trabajo que desempeñen funciones críticas para el servicio y cuyos resultados, de manera reiterada (en al menos 3 ocasiones, comunicadas por escrito por Correos), incumplan las directrices, niveles de calidad y/o los plazos requeridos.

El adjudicatario se compromete a reponer adecuadamente los técnicos rechazados en un plazo máximo de 15 días naturales desde la comunicación por escrito de Correos. Si el cambio en el equipo de trabajo es solicitado por el adjudicatario, y con el fin de conseguir una adecuada transmisión de conocimientos, el adjudicatario deberá incorporar el reemplazo adecuado (es decir, con perfil y experiencia similares) al menos quince días naturales antes del cambio.

Este período de solape no supondrá coste adicional para Correos. En cualquier caso, para cada nueva incorporación al equipo de trabajo, el adjudicatario deberá informar por escrito al menos con cinco días naturales de antelación a Correos, informando y acreditando la formación, conocimientos, certificaciones y experiencia de las nuevas personas que se incorporan.

3.2. Requerimientos de colaboración del fabricante

Con el objetivo de asegurar el éxito en la implantación de la solución, será imprescindible contar con la colaboración directa de servicios profesionales del fabricante de la herramienta.

Con carácter obligatorio se establece una colaboración mínima de 250 horas del fabricante a lo largo de los 3 años de contrato.

El licitador deberá garantizar la participación del fabricante durante las fases clave del proyecto, incluyendo el diseño de la solución, la definición de buenas prácticas, la validación técnica de la arquitectura, el acompañamiento en la configuración inicial y el soporte experto durante la puesta en producción.

Esta colaboración deberá reflejarse explícitamente en la propuesta, identificando los perfiles involucrados, su experiencia y el grado de compromiso previsto por parte del fabricante.

3.3. Consideraciones adicionales sobre el equipo de trabajo

A continuación, se exponen una serie de puntos que aplican a todo el equipo de trabajo.

Perfiles mínimos: Los requisitos de los perfiles aquí expuestos se consideran requisitos mínimos que se exigirán en las ofertas. Se entiende que el adjudicatario proveerá de los perfiles requeridos o superiores, nunca con nivel inferior a lo especificado.

Ubicación de los técnicos: El equipo de trabajo realizará sus tareas de forma habitual en las dependencias del adjudicatario. Éste está obligado a disponer de la infraestructura técnica (Comunicaciones, Software y Hardware) adecuada para poder desarrollar los trabajos de forma remota. Dicha infraestructura deberá seguir los estándares que Correos fije al respecto, cumpliendo las políticas y normas de seguridad y arquitectura establecidas.

Por cada técnico que esté trabajando en remoto se dispondrá de un número de teléfono fijo o móvil con conexión directa (sin necesidad de pasar por una centralita o por otras personas para establecer la comunicación) en el que se podrá contactar con el técnico durante el horario de trabajo.

El adjudicatario también se compromete a proporcionar los medios necesarios para poder establecer reuniones virtuales con varios participantes simultáneos

Dado que en esta contratación el servicio de mantenimiento y soporte de los sistemas se prestará bajo la modalidad de 24X7 con carácter permanente, el adjudicatario garantizará que las incidencias tipificadas como críticas (ver cláusula de ANS) serán atendidas de forma inmediata a la comunicación por Correos por equipos remotos.

Una vez comunicada la incidencia, y en caso de ser necesario a juicio de Correos o del adjudicatario, los responsables de la resolución de la incidencia deberán desplazarse de forma inmediata a las instalaciones de Correos en un plazo máximo de una hora. El tiempo máximo de resolución será el especificado en la cláusula de ANS.

El proveedor se compromete a facilitar con plena operatividad un procedimiento de comunicación de estas incidencias, que deberá tener la misma operatividad del propio servicio, es decir 24x7.

El incumplimiento de cualquiera de los parámetros que configuran el anterior servicio será considerado como incumplimiento global de la prestación del servicio.

Estas condiciones serán las que se tengan en cuenta en el seguimiento del ANS.

Trabajo en coordinación con otros grupos de Correos.

Es posible que en determinados proyectos estratégicos para Correos se requiera la participación continuada de otros departamentos del Grupo Correos para darles soporte y guiarles desde el inicio.

Por ello es posible que se requiera en determinados momentos que ciertos técnicos se tengan que "integrar" con dedicación parcial en proyectos estratégicos del Grupo Correos.

Así que también se requerirá en determinados proyectos la participación de los técnicos (se escogerá en cada caso según la tecnología necesaria) en determinados puntos de los proyectos (reuniones diarias, Kanban, etc).

Compromiso de Flexibilidad.

Los perfiles demandados en el punto anterior son los que Correos considera necesarios para llevar a cabo las tareas necesarias dentro de los servicios especificados en el pliego de condiciones técnicas y con la duración prevista del contrato.

El adjudicatario deberá proporcionar un equipo flexible de trabajo que permita aumentar/disminuir el número de personas del servicio de una tecnología concreta en función de la carga de trabajo.

Las ofertas deberán recoger específicamente y en un párrafo separado el compromiso de flexibilidad, de forma que, en función de las necesidades tecnológicas del momento, puedan existir cambios de unos perfiles por otros en función de las necesidades tecnológicas en cada momento

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 según se indica en el artículo 52.3 b) Real Decreto-Ley 3/2020: *"El hecho de que, la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara la correcta ejecución del mismo desde el punto de vista técnico; o bien que el riesgo para la correcta ejecución del contrato proceda de la naturaleza del objeto del mismo, al implicar la necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada por su división en lotes y ejecución por una pluralidad de contratistas diferentes."*

En este caso, se cumple la justificación del citado supuesto, en la medida en que la realización independiente de las diversas prestaciones comprendidas en el contrato, todas ellas interrelacionadas, dificultaría la correcta ejecución de éste desde el punto de vista técnico. Se solicita un trabajo íntegro, que contempla el mantenimiento y soporte de las suscripciones Primeur Data One, de tal modo que se permita disponer de los recursos necesarios en cada momento para poder dar respuesta, con los niveles de calidad requeridos, a las necesidades de gestión de las áreas usuarias. Adicionalmente, en caso de que hubiera varias empresas adjudicatarias, la realización independiente de las diversas prestaciones comprendidas dentro del ámbito del contrato por parte de cada adjudicatario, podría ocasionar incidentes y problemas, lo que no es asumible. Por lo tanto, la naturaleza del servicio imposibilita su división en partes y, en consecuencia, su división en lotes.

El presupuesto base de licitación se fija en (incluido IVA o cualquier otro impuesto indirecto equivalente) la cantidad de **2.721.774,00 € (DOS MILLONES SETECIENTOS VEINTIUN MIL SETECIENTOS SETENTA Y CUATRO EUROS)**, de acuerdo con la siguiente distribución:

- **Base Imponible del Presupuesto base de Licitación** (excluido IVA o cualquier otro impuesto indirecto equivalente): de **2.249.400,00 € (DOS MILLONES DOSCIENTOS CUARENTA Y NUEVE MIL CUATROCIENTOS EUROS).**

- **Importe del IVA** o cualquier otro impuesto indirecto equivalente: **472.374,00 € (CUATROCIENTOS SETENTA Y DOS MIL TRESCIENTOS SETENTA Y CUATRO EUROS).**

El 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	Costes Directos (84%)	Costes Indirectos (10%)	Beneficio Industrial (6%)	IVA o Impuesto Indirecto equivalente 21%	Presupuesto base de licitación (IVA o cualquier otro impuesto indirecto equivalente incluido)
2026	851.000,00 €	714.840,00 €	85.100,00 €	51.060,00 €	178.710,00 €	1.029.710,00 €
2027	699.200,00 €	587.328,00 €	69.920,00 €	41.952,00 €	146.832,00 €	846.032,00 €
2028	699.200,00 €	587.328,00 €	69.920,00 €	41.952,00 €	146.832,00 €	846.032,00 €
TOTAL	**2.249.400,00 €**	**1.889.496,00 €**	**224.940,00 €**	**134.964,00 €**	**472.374,00 €**	**2.721.774,00 €**

Para calcular el importe, se han considerado los siguientes conceptos, y su distribución anual:

Año	Concepto	Importe (IVA no incluido)	Observaciones
2026	Proyecto (CAPEX)	460.000,00 €	Proyecto de migración (Fase I)
	Proserv (OPEX)	46.000,00 €	Servicios profesionales fabricante
	Licencias ITSM (CAPEX)	345.000,00 €	Suscripción anual 2026-2027
	TOTAL 2026	**851.000,00 €**	
2027	Mantenimiento (OPEX)	220.800,00 €	Manto. Posterior a GoLive
	Evolución (CAPEX)	70.150,00 €	Evol. Posterior a GoLive
	Proyecto (CAPEX)	57.500,00 €	Proyecto de migración (Fase II)
	Proserv (OPEX)	5.750,00 €	Servicios profesionales fabricante
	Licencias ITSM (CAPEX)	345.000,00 €	Suscripción anual 2027-2028
	TOTAL 2027	**699.200,00 €**	
2028	Mantenimiento (OPEX)	220.800,00 €	Manto. Posterior a GoLive
	Evolución (CAPEX)	70.150,00 €	Evol. Posterior a GoLive
	Proyecto (CAPEX)	57.500,00 €	Proyecto de migración (Fase II)
	Proserv (OPEX)	5.750,00 €	Servicios profesionales fabricante
	Licencias ITSM (CAPEX)	345.000,00 €	Suscripción anual 2028-2029
	TOTAL 2028	**699.200,00 €**	

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

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

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

Costes salariales (20%)	Costes servicios (80%)
377.899,20 €	1.511.596,80

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

Se establece como **Valor Estimado** de la contratación, la cantidad de **3.186.650,00 € (TRES MILLONES CIENTO OCHENTA Y SEIS MIL SEISCIENTOS CINCUENTA EUROS)**, excluido IVA o impuesto indirecto equivalente.

El valor estimado del contrato se ha evaluado de la siguiente forma:

	Cantidades en euros IVA no incluido
Presupuesto de ejecución	2.249.400,00 €
Importe de prórrogas previstas (15 meses)	937.250,00 €
Otros	- €
Valor estimado del contrato	3.186.650,00 €

El contrato podrá ser prorrogado por dos prórrogas, una de 12 meses y otra de tres meses de duración, en las mismas condiciones técnicas y económicas y restantes previsiones contractuales, con la salvedad de que **no habrá que prorrogar el proyecto de migración ni la partida de servicios profesionales ya que esto se realizará una única vez al comienzo del contrato.** 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 ejecución.

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

- Forma de acreditación de la solvencia económica y financiera:

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

Cuando se admita como forma de acreditar la solvencia, la suscripción de un seguro de responsabilidad civil se acreditará mediante la presentación de a) copia de la póliza o certificado de compañía aseguradora o el mediador de conformidad de la cobertura suscrita con el objeto de la licitación, b) copia del último recibo de pago de la póliza y c) declaración responsable sobre su vigencia, y compromiso de renovación, donde deberán recogerse las siguientes condiciones:

- La cobertura temporal de la póliza deberá comprender, como mínimo, el período de duración inicial del contrato, y contemplarse expresamente la posibilidad de prórroga de dicha póliza en caso de acordarse la prórroga del contrato.
- La cobertura económica deberá ser equivalente a la
  - ☐ Anualidad media del contrato, o al presupuesto de licitación, en caso de contratos con una duración inferior a un año.
  - ☐ (Otra cantidad…….), atendiendo al riesgo estimable presente en el contrato

- Forma de acreditación de la solvencia técnica y profesional:

☒	Certificado de correcta ejecución de los servicios o trabajos realizados, expedidos o visados por la entidad para la que hayan sido realizados
☒	Relación y perfil o *Curriculum Vitae* del personal, integradas o no en la empresa, que participará en el contrato. Se aportará el CV ciego del personal o equipo humano (es decir, sin referencia a datos de carácter personal) disponible para el cumplimiento 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.
☐	Descripción de las medidas que se emplearán para garantizar la calidad. Se admitirán como justificativas del cumplimiento de los requisitos exigidos los siguientes certificados emitidos por instituciones o servicios oficiales: …
☐	Indicación de las medidas de gestión medioambiental que el empresario aplicará al ejecutar el contrato.
☐	Documentación acreditativa de la maquinaria, material y equipo técnico del que se dispondrá para la ejecución de los trabajos.
☒	Otros. • Cumplimiento del ENS en categoría ALTA

	• Certificados ISO en vigor (aportando copia de este):
	  o Certificación ISO 9001. Sistema de Gestión de la Calidad
	  o Certificación ISO 27001. Sistema de Gestión de Seguridad de la Información
	  o Certificación ISO 20000-1. Sistema de Gestión de Servicio de Tecnologías de la Información
	• Declaración responsable del proveedor/fabricante que los servidores que presten los servicios en modo SaaS de la herramienta se encuentren alojados en la UE.

Anexo V.- Modelo de aval.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Toda proposición que, por cualquier causa, no sea presentada por medios telemáticos a través del portal será automáticamente inadmitida en el procedimiento de licitación.
En el caso de que cualquiera de los documentos de una proposición no pueda visualizarse correctamente, se permitirá que, en un plazo de 24 horas desde la notificación de la incidencia, el licitador presente nuevamente dicho documento en formato digital. El documento presentado posteriormente no podrá sufrir modificación respecto al original incluido en la proposición. Si la entidad contratante comprueba que el documento ha sido alterado, la proposición del licitador no será tenida en cuenta.

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

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

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

Anexo VII.- Instrucciones para cumplimentar el DEUC.

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

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

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

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

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

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

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

☒ PARTE I: INFORMACIÓN SOBRE EL PROCEDIMIENTO DE CONTRATACIÓN Y EL PODER ADJUDICADOR (Identificación del contrato y la entidad contratante; estos datos deben ser facilitados o puestos por el poder adjudicador)

☒ PARTE II: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

☒ Sección A: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

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

☒ Sección B: INFORMACIÓN SOBRE LOS REPRESENTANTES DEL OPERADOR ECONÓMICO

- Representación, en su caso (datos del representante)

☒ Sección C: INFORMACIÓN SOBRE EL RECURSO A LA CAPACIDAD DE OTRAS ENTIDADES

- Recurso (Sí o No)

☒ Sección D: INFORMACIÓN RELATIVA A LOS SUBCONTRATISTAS

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

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

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

☒ Sección B: MOTIVOS REFERIDOS AL PAGO DE IMPUESTOS O DE COTIZACIONES A LA SEG. SOCIAL. Pago de impuestos o de cotizaciones a la Seguridad Social (declara cumplimiento de obligaciones)

☒ Sección C: MOTIVOS REFERIDOS A LA INSOLVENCIA, LOS CONFLICTOS DE INTERESES O LA FALTA PROFESIONAL. Información relativa a toda posible insolvencia, conflicto de intereses o falta profesional

☒ Sección D: OTROS MOTIVOS DE EXCLUSIÓN QUE ESTÉN PREVISTOS EN LA LEGISLACIÓN NACIONAL. Motivos de exclusión puramente nacionales (si los hay, declaración al respecto)

PARTE IV: CRITERIOS DE SELECCIÓN

☒ OPCIÓN 1: INDICACIÓN GLOBAL DE CUMPLIMIENTO DE TODOS LOS CRITERIOS DE SELECCIÓN

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

- Sección A: IDONEIDAD: (información referida a la inscripción en el Registro Mercantil u oficial o disponibilidad de autorizaciones habilitantes).
- Sección B: SOLVENCIA ECONÓMICA Y FINANCIERA (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección C: CAPACIDAD TÉCNICA Y PROFESIONAL (datos a facilitar según las indicaciones del pliego, anuncio o invitación).
- Sección D: SISTEMAS DE ASEGURAMIENTO DE LA CALIDAD Y NORMAS DE GESTIÓN MEDIOAMBIENTAL.

☐ PARTE V: REDUCCIÓN DEL NÚMERO DE CANDIDATOS CUALIFICADOS.

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

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

Se otorgará hasta la máxima puntuación en cada criterio a la oferta que ofrezca las mejores propuestas y aporte el mayor valor para la prestación del servicio, de manera concisa y ordenada, sobre los aspectos relacionados con:

1. Adecuación funcional estándar y madurez de la plataforma ITSM.			
Descripción	Se evaluará cómo la solución propuesta cubre los requisitos funcionales y técnicos detallados en los pliegos, valorando su grado de cumplimiento, cobertura nativa, personalización y escalabilidad.	Ponderación	9 puntos
Forma de valoración	La puntuación se asignará en función del nivel de detalle en la exposición de los siguientes aspectos: • Matriz de cumplimiento de requisitos, indicando el grado de cobertura (out-of-the-box, configurable o requiere desarrollo) específico de cada uno y evidencia verificable: hasta 4 puntos • Descripción de la estrategia de configuración y parametrización, identificando los desarrollos específicos necesarios, en su caso: hasta 2 puntos. • Relación de prácticas ITIL v4 cubiertas de forma nativa y su grado de integración en los procesos ITSM: hasta 1 puntos. • Impacto de la solución en el mantenimiento y evolución futura (upgrades, impacto de configuraciones/desarrollos en futuras versiones, coste evolución): hasta 2 puntos.		

2. Arquitectura enterprise, CMDB y gobierno del dato.			
Descripción	Se valorará la madurez de la plataforma desde el punto de vista arquitectónico, la robustez de su CMDB como eje de gobierno del servicio y las capacidades de control, trazabilidad y calidad del dato.	Ponderación	7 puntos
Forma de valoración	La puntuación se asignará en función del nivel de detalle en la exposición de los siguientes aspectos: • Arquitectura SaaS enterprise real (multitenant, upgrades automáticos, independencia del integrador): hasta 3 puntos. • CMDB avanzada (modelo de datos, relaciones, impacto, uso real en procesos ITSM): hasta 2 puntos.		

	• Gobierno del dato: trazabilidad, auditoria, calidad, cumplimiento ENS / ISO: hasta 2 puntos.

3. Implantación, metodología y gobierno del proyecto.			
Descripción	Se evaluará la metodología y modelo de gobierno propuesto, así como la planificación para la implantación, considerando la secuencia de actividades, duración estimada, cronograma, dependencias, entregables y definición de hitos clave.	Ponderación	6 puntos
Forma de valoración	Se puntuará en función del realismo, coherencia y solidez del plan propuesto, así como la claridad de los hitos, entregables por fase, y capacidad de adaptación ante imprevistos: • Cronograma general con hitos, fases, actividades y duración estimada. Descripción de dependencias entre actividades y entregables asociados a cada fase: hasta 3 puntos. • Metodología y control de calidad (QA, pruebas, aceptación): hasta 2 puntos. • Modelo de gobierno, reporting y gestión de riesgos: Hasta 1 punto.		

4. Plan de formación y gestión del cambio.			
Descripción	Se valorará la estrategia de formación propuesta para los distintos perfiles de usuario, así como las acciones previstas para la gestión del cambio organizacional.	Ponderación	3 puntos
Forma de valoración	La valoración se basará en la adecuación de los contenidos, formatos, número de sesiones, materiales entregables, así como en la capacidad del plan de acompañar eficazmente a los usuarios durante la transición. • Estrategia de formación diferenciada por perfiles (usuarios finales, administradores, soporte). Tipología de formación: presencial, online, autoformación, manuales, tutoriales. Nº de sesiones, duración, materiales y certificaciones (si aplica): hasta 1 punto. • Plan de gestión del cambio organizacional: comunicación, soporte al usuario, campañas de adopción: hasta 1 punto. • Acompañamiento post-implantación: hasta 1 punto.		

5. Propuesta de mejora.			
Descripción	Se valorarán las propuestas adicionales no exigidas en los pliegos que supongan un valor añadido para el proyecto o los servicios a prestar: mejoras en automatización, IA o autoservicio.	Ponderación	3 puntos
Forma de valoración	La puntuación se determinará por la relevancia, innovación, madurez y viabilidad de las mejoras propuestas, así como por su impacto positivo en la eficiencia, sostenibilidad o calidad del servicio. • Automatizaciones adicionales nativas (sin desarrollo): hasta 1,5 puntos. • Capacidades adicionales de autoservicio / IA ya disponibles: hasta 1,5 puntos.		

6. Equipo de trabajo.			
Descripción	Se valorará la composición, experiencia y competencias adicionales del equipo propuesto en base a los requerimientos especificados en el presente pliego.	Ponderación	2 puntos
Forma de valoración	La puntuación se determinará en base a la experiencia global del equipo en proyectos similares, competencias técnicas o certificaciones relevantes de cada miembro, la claridad en la definición de roles y responsabilidades, así como la aportación de perfiles adicionales, que puedan ofrecer especialización, innovación o mejoras en la ejecución del proyecto: • Organigrama del equipo propuesto, y roles y responsabilidades de cada miembro: hasta 0,5 puntos. • Experiencia profesional en proyectos similares (ITSM, sector público, gran empresa): hasta 0,5 punto. • Rol clave cubiertos por perfiles senior y certificaciones relevantes (ITIL, PMP, Scrum, ISO, ENS): hasta 0,5 punto. • Estabilidad y dedicación real del equipo. Perfiles complementarios para innovación o soporte especializado: hasta 0,5 punto.		

Para continuar en la fase de valoración de ofertas será necesario que, en los criterios sujetos a un juicio de valor, los licitadores alcancen el siguiente umbral mínimo de puntuación:

☒ 15 puntos en la valoración global del conjunto de los criterios de adjudicación
☒ 6 puntos en la valoración del criterio de adjudicación 1 (Adecuación funcional

estándar y madurez de la plataforma ITSM)
☒ 4 puntos en la valoración del criterio de adjudicación 2 (Arquitectura enterprise, CMDB y gobierno del dato)

La valoración de los criterios sujetos a un juicio de valor de una oferta estará constituida por la suma de las puntuaciones parciales asignadas a cada uno de los criterios y subcriterios técnicos definidos en el Pliego, con un máximo de 30 puntos.

Dicha valoración se realizará atendiendo al grado de cumplimiento objetivo de los subcriterios definidos, a la madurez de la solución propuesta y a su sostenibilidad técnica y operativa, evitando valoraciones basadas exclusivamente en descripciones comerciales o compromisos futuros.

La matriz de cumplimiento de requisitos y las declaraciones realizadas en el marco del criterio **1. Adecuación funcional estándar y madurez de la plataforma ITSM.** tendrán carácter vinculante durante la ejecución del contrato.

Anexo IX.- Criterios de adjudicación de evaluación automática

Con el fin de valorar a todos los licitantes que concurran a esta contratación de manera equitativa, Correos requiere la siguiente documentación:

- Proposición económica siguiendo el modelo que se incluye como Anexo X.- Modelo de proposición económica. para valorar el criterio de adjudicación 1 de evaluación automática.
- Documento con la información necesaria para valorar los criterios de adjudicación 2 a 6 de evaluación automática. Este documento debe recoger la siguiente información:

Criterio de adjudicación 1 evaluación automática			
Descripción	Oferta económica	Ponderación	49 puntos
Formula de valoración	$PE = PEm * \left(0{,}60 * \frac{Lmin}{Li} + 0{,}40 * \frac{Smin}{Si}\right)$ Donde: PE = Puntuación oferta "n" PEm = Ponderación asignada al criterio económica Lmin = Presupuesto ofertado en licencias más económico Li = Presupuesto ofertado en licencias "n" Smin = Presupuesto ofertado en servicios más económico Si = Presupuesto ofertado en servicios "n"		

El licitador que presente la mejor oferta obtendrá la máxima puntuación económica posible para cada licitación específica. Al resto de los licitadores se les otorgará una puntuación proporcional o lineal.

La ponderación del criterio económico se distribuye asignando un 60% a la partida de licencias y un 40% a la partida de servicios (resto del presupuesto), atendiendo a la estructura económica del contrato y al peso relativo que cada componente representa en el presupuesto base de licitación.

Asimismo, se establecen importes máximos por partida, cuyo incumplimiento determinará la exclusión de la oferta:

	Presupuesto
Licencias máx	1.035.000 €
Servicios máx	1.214.400 €

El incumplimiento de cualquiera de estos límites supondrá la exclusión de la oferta.

Criterio de adjudicación 2 evaluación automática			
Descripción	Modelo de Licenciamiento	Ponderación	5 puntos
Formula de valoración	Se valorará el modelo de licenciamiento de la solución propuesta, atendiendo a su carácter SaaS enterprise, multitenant, la escalabilidad funcional y técnica, la previsibilidad de costes y la ausencia de costes ocultos de infraestructura o base de datos. La puntuación arriba indicada se desglosa de la siguiente forma: • Licencia nominal SaaS enterprise con escalabilidad y costos previsibles: 5 puntos • Licencia concurrente/híbrida con limitaciones de escalabilidad o que requiera componentes adicionales: 2 puntos • Nominal rígido local sin escalabilidad / con costos ocultos: 0,25 puntos.		
Evidencia obligatoria	Modelo de licenciamiento oficial del fabricante.		

Criterio de adjudicación 3 evaluación automática			
Descripción	Eficiencia en consumo de recursos	Ponderación	3 puntos
Formula de valoración	Se valorará la eficiencia en el uso de recursos y el grado de gestión asumido por el fabricante frente al cliente, en función del modelo de despliegue de la solución (SaaS, híbrido, on-premise). La puntuación arriba indicada se desglosa de la siguiente forma: • SaaS con hosting incluido, totalmente gestionado por el fabricante, sin necesidad de infraestructura adicional por parte del cliente: 3 puntos • SaaS, pero requiere infraestructura adicional (IaaS, base de datos u otros componentes críticos) gestionada por el cliente: 1 punto. • On-premise: 0 puntos.		
Evidencia obligatoria	Arquitectura técnica y responsabilidades del servicio.		

Criterio de adjudicación 4 evaluación automática			
Descripción	Cobertura funcional ITIL/ITSM	Ponderación	3 puntos
Formula de valoración	Se valorará la cobertura funcional nativa ofrecida por la herramienta respecto a prácticas ITIL v4 y procesos ITSM, acreditada mediante certificaciones o documentación oficial. La puntuación arriba indicada se desglosa en función de la siguiente cobertura nativa ofrecida por la herramienta: • ≥ 10 prácticas ITIL v4 certificados: 3 puntos • 6-9 prácticas ITIL v4 certificados: 1 puntos • 3-5 prácticas ITIL v4 certificados: 0,25 puntos.		

	• Menos de 1 proceso: 0 puntos.
Evidencia obligatoria	Certificación / Documentación oficial.

Criterio de adjudicación 5 evaluación automática			
Descripción	Integraciones estándar	Ponderación	2 puntos
Formula de valoración	La puntuación arriba indicada se desglosa en función de la disponibilidad de los siguientes conectores de manera estándar certificados por el fabricante: Microsoft 365 / Azure / AWS / GCP, herramientas DevOps (Jira, GitHub), ERP (SAP, Oracle), herramientas de monitorización (Dynatrace, Splunk, etc.): • ≥ 7 integraciones estándar certificadas por fabricante: 2 puntos. • 3-6 integraciones estándar certificadas (…): 1 punto. • Menos 3 integraciones estándar certificadas (…): 0,25 puntos. • Ninguna: 0 puntos.		
Evidencia obligatoria	Catálogo oficial de integraciones.		

Criterio de adjudicación 6 evaluación automática			
Descripción	Configuración vs personalización	Ponderación	2 puntos
Formula de valoración	La puntuación arriba indicada se desglosa en función del porcentaje de funcionalidades configurables sin desarrollo específico ni código, incluyendo uso de motores de workflow y capacidades low-code/no-code, frente a la necesidad de personalizaciones o desarrollos a medida.: • ≥ 80% configurable sin desarrollo específico ni código: 2 puntos. • 60-79% configurable (…): 1 punto. • 40-59% configurable (…): 0,5 puntos. • Menos del 40% configurable (…): 0 puntos.		
Evidencia obligatoria	Manual técnico / Arquitectura.		

Criterio de adjudicación 7 evaluación automática			
Descripción	Capacitación y transferencia	Ponderación	2 puntos
Formula de valoración	La puntuación arriba indicada se desglosa en función de la intensidad del plan de formación y transferencia de conocimiento, medido en horas de formación estructurada y calidad de los materiales y recursos ofrecidos.: • ≥ 40 horas: 2 puntos. • 20-39 horas: 1 puntos. • 10-19 horas: 0,5 puntos. • Menos de 10 horas: 0 puntos.		

Evidencia obligatoria	Plan de formación.

Criterio de adjudicación 8 evaluación automática			
Descripción	Automatización y Autoservicio	Ponderación	2 puntos
Formula de valoración	La puntuación arriba indicada se desglosa en función de las capacidades nativas de automatización, autoservicio e inteligencia artificial aplicadas a la gestión de servicios TI, así como el número y madurez de los workflows preconfigurados disponibles.: • Inteligencia Artificial + chatbot + catálogo dinámico con workflows preconfigurados: 2 puntos. • Sólo workflows básicos: 0,5 puntos. • Sin automatización nativa: 0 puntos.		
Evidencia obligatoria	Documentación funcional / Roadmap		

Criterio de adjudicación 9 evaluación automática			
Descripción	Escalabilidad y elasticidad	Ponderación	2 puntos
Formula de valoración	La puntuación arriba indicada se desglosa en función de la capacidad de la plataforma para escalar en número de usuarios, volúmenes de datos y módulos funcionales, así como el grado de automatización de dicha escalabilidad.: • Escalabilidad automática sin intervención (incremento transparente de capacidad bajo modelo SaaS enterprise multitenant): 2 puntos. • Escalabilidad con intervención (acciones manuales de ampliación de infraestructura/licencias): 0,5 puntos. • Escalabilidad limitada: 0 puntos.		
Evidencia obligatoria	Arquitectura SaaS / técnica.		

La valoración de los criterios técnicos anteriores se realizará de forma automática en función de la opción seleccionada por el licitador y de la evidencia documental aportada, no procediendo valoración interpretativa adicional.

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: (los importes y porcentajes, vendrán expresados con un máximo de 2 decimales).

DESGLOSE ECONÓMICO DE OFERTA

Los importes deben reflejarse con dos decimales y sin incluir ningún impuesto. Se considerarán incluidos todos los gastos en los que necesite incurrir el adjudicatario para la ejecución mediante medios propios de los trabajos objeto del contrato, a modo de ejemplo: personal (incluidos potenciales desplazamientos y dietas), hardware, software, consumo de material de oficina, entre otros.

La oferta deberá incluir el siguiente desglose económico:

SERVICIO/PARTIDA	2025	2026	2027	2028	TOTAL (IVA no incluido)
Subscripción licencias SaaS					
Mantenimiento integral					
Evolución e Innovación					
Implantación y puesta en marcha					
Serv. Profesionales Fabricante					
IMPORTE TOTAL OFERTADO					

* Todos los precios e importes deben reflejarse con dos decimales y sin incluir ningún impuesto. El importe total ofertado y su desglose de importes deberá cuadrar al segundo decimal sin mediar redondeo. En caso de reflejar cualquier importe con más de dos decimales, o de que el desglose de importes no cuadre al segundo decimal al realizar las multiplicaciones y sumas, supondrá la exclusión de la oferta.

El importe total ofertado se corresponderá con la suma de los importes de los 5 servicios desglosados, tanto en los importes por año de contrato, como en el importe total. Asimismo, se establecen importes máximos por partida, cuyo incumplimiento determinará la exclusión de la oferta:

	Presupuesto
Licencias máx (Subscripción licencias SaaS)	1.035.000 €
Servicios máx (Mantenimiento integral + Evolución e Innovación + Implantación y puesta en marcha + Serv. Profesionales Fabricante)	1.214.400 €

DESGLOSE DE SERVICIOS / PARTIDAS

En el caso de los siguientes servicios / partidas, se deberán detallar los precios unitarios mismos de acuerdo con:

Licencias. Adquisición, Suscripción y Mantenimiento

Si la solución ofertada incluye el uso de herramientas de terceros o soluciones de mercado, se debe detallar lo siguiente:

- En caso de que la oferta incluya la adquisición de licencias, se debe detallar el número de unidades (licencias) ofertadas totales, y el precio unitario de adquisición.
    - Si se incluyen diferentes tipos de licencias (sea porque la oferta incluye el uso de diferentes herramientas, o porque incluye diferentes tipos de licenciamiento por servicios de una herramienta concreta), se debe indicar una línea de concepto diferente para cada una de ellas.
    - El importe total de cada tipo de licencia se corresponderá con el producto del número total de unidades ofertadas y el precio unitario de adquisición de estas.
    - La suma de los importes totales de todos los tipos de licencia / conceptos se corresponderá con el Importe Total indicado en la tabla de Desglose Económico para el Servicio / Partida "Adquisición de licencias".
- En caso de que la oferta incluya el uso de licencias mediante pago por suscripción, se debe detallar el número de unidades (licencias) ofertadas totales, el tipo de periodo o frecuencia de pago de la suscripción (por ejemplo, mensual o anual), el número de periodos de suscripción a esas licencias contemplado en la oferta y el precio unitario de suscripción para cada licencia y periodo.
    - Si se incluyen diferentes tipos de suscripciones (sea porque la oferta incluye el uso de diferentes herramientas, o porque incluye diferentes tipos de

licenciamiento por servicios de una herramienta concreta), se debe indicar una línea de concepto diferente para cada una de ellas.
    - Para cada tipo de suscripción, se debe indicar el mes de inicio y mes de fin del intervalo temporal de pago de suscripción de dichas licencias, de acuerdo con el plan de ejecución de proyecto y el momento en el que sea necesaria la activación de sus suscripciones. Los meses de inicio y fin se deben expresar en relación con el inicio de la fase de prestación real de servicio, y el mes de fin no podrá ser mayor al último mes de dicha fase.
    - En caso de que, para un mismo tipo de suscripción, se contemple de acorde al plan de proyecto que la totalidad de suscripciones ofertadas no se activen en el mismo momento, sino que se haga en puntos diferentes, se deberá incluir una línea de intervalo diferente para cada momento de activación.
    - El importe total de cada tipo de suscripción / concepto en cada intervalo, se corresponderá con el producto del número total de unidades ofertadas, el número de periodos incluido en el intervalo y el precio unitario de pago por suscripción de estas.
    - La suma de los importes totales de todos los tipos de suscripción / conceptos e intervalos se corresponderá con el Importe Total indicado en la tabla de Desglose Económico para el Servicio / Partida "Suscripciones de licencias".
    - Si se indica más de un intervalo para el mismo tipo de suscripción, el importe unitario del último intervalo no podrá ser más del 10% superior al importe unitario del primero.
- En caso de que la oferta incluya la adquisición o uso de licencias por suscripción, que requieran de un pago de mantenimiento y soporte asociado a las mismas, se debe detallar el número de unidades (licencias) ofertadas totales, el tipo de periodo o frecuencia de pago del mantenimiento (por ejemplo, mensual o anual), el número de periodos de mantenimiento asociados a esas licencias contemplado en la oferta y el precio unitario de mantenimiento para cada licencia y periodo.
    - Si se incluyen diferentes tipos de licencias (sea porque la oferta incluye el uso de diferentes herramientas, o porque incluye diferentes tipos de licenciamiento por servicios de una herramienta concreta), se debe indicar una línea de concepto diferente para cada una de ellas.
    - Para cada tipo de licencia, se debe indicar el mes de inicio y mes de fin del intervalo temporal de pago de mantenimiento de dichas licencias, de acuerdo con el plan de ejecución de proyecto y el momento en el que sea necesario empezar a utilizar esas licencias. Los meses de inicio y fin se deben expresar en relación con el inicio de la fase de prestación real de servicio, y el mes de fin no podrá ser mayor al último mes de dicha fase.
    - En caso de que, para un mismo tipo de licencia, se contemple de acorde al plan de proyecto que la totalidad de licencias ofertadas no se adquieran o activen en el mismo momento, sino que se haga en puntos diferentes, se deberá incluir una línea de intervalo diferente para cada momento de adquisición o activación.
    - El importe total de cada tipo de licencia / concepto en cada intervalo, se corresponderá con el producto del número total de unidades ofertadas, el número de periodos incluido en el intervalo y el precio unitario de mantenimiento de estas.

- La suma de los importes totales de todos los tipos de suscripción / conceptos e intervalos se corresponderá con el Importe Total indicado en la tabla de Desglose Económico para el Servicio / Partida "Mantenimiento y soporte de licencias".
- Si se indica más de un intervalo para el mismo tipo de licencia, el importe unitario del último intervalo no podrá ser más del 10% superior al importe unitario del primero.

Adquisición de licencias			**Unidades ofertadas**	**Precio unitario adquisición**	**Importe total por concepto**	
Tipo de licencia / concepto 1			x.xxx	xx.xxx,xx €	xx.xxx,xx €	
…			x.xxx	xx.xxx,xx €	xx.xxx,xx €	
Tipo de licencia / concepto n			x.xxx	xx.xxx,xx €	xx.xxx,xx €	
Suscripciones de licencias	**Tipo de periodo / frecuencia**		**Número de periodos por concepto e intervalo**	**Unidades ofertadas por concepto e intervalo**	**Precio por unidad y periodo**	**Importe total por concepto e intervalo**
Tipo de suscripción / concepto 1	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto 1	…			XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto 1	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
…				XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto n	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto n	…			XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto n	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
Mantenimiento y soporte de licencias	**Tipo de periodo / frecuencia**		**Número de periodos por concepto e intervalo**	**Unidades ofertadas por concepto e intervalo**	**Precio por unidad y periodo**	**Importe total por concepto e intervalo**
Tipo de suscripción / concepto 1	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto 1	…			XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto 1	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
…				XX	xx.xxx,xx €	xx.xxx,xx €

Tipo de suscripción / concepto n	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto n	…			XX	xx.xxx,xx €	xx.xxx,xx €
Tipo de suscripción / concepto n	Inicio Intervalo 1 (Concepto 1)	Fin Intervalo 1 (Concepto 1)	Mensual / Anual / …	XX	xx.xxx,xx €	xx.xxx,xx €

Servicios de Puesta en marcha, mantenimiento y evolución:

Con relación a los servicios ofertados, se debe detallar lo siguiente:

- El importe total ofertado de cada servicio se corresponderá con el producto del número de horas ofertadas y el precio medio/hora ofertada para dicho servicio. A su vez corresponderá con lo indicado para dicho servicio en la tabla de Desglose Económico.
- Las horas ofertadas totales no podrán ser inferiores a las horas mínimas totales cuando así se definan. En caso de serlo supondrá la exclusión de la oferta.
- Los precios unitarios ofertados para cada perfil profesional y tipo de servicio tendrán carácter fijo y vinculante durante toda la vigencia del contrato, constituyendo la base económica de referencia para la ejecución de los servicios incluidos en el mismo.
- Dichos precios unitarios serán de aplicación, asimismo, a cualesquiera servicios adicionales, evolutivos o de refuerzo que, estando dentro del alcance funcional del contrato, puedan ser requeridos durante su ejecución, sin que pueda aplicarse incremento alguno distinto de los expresamente previstos en el pliego.
- Los precios unitarios ofertados para los servicios deberán ser coherentes con los perfiles profesionales propuestos, el número de horas ofertadas y el alcance del contrato. Cuando del análisis del desglose económico se desprenda que los precios unitarios o el esfuerzo estimado resultan manifiestamente insuficientes para garantizar la correcta ejecución del contrato, el órgano de contratación podrá requerir las aclaraciones oportunas conforme a lo previsto en la normativa de contratación pública vigente.

SERVICIO	TIPO DE PERFIL	HORAS OFERTADAS	PRECIO MEDIO /HORA	IMPORTE TOTAL OFERTADO
Servicio de mantenimiento y soporte	XXX	HH	XX,XX €	XX,XX €
Servicio de evolución e innovación	XXX	HH	XX,XX €	XX,XX €
Serv. Implantación y Puesta en Marcha	XXX	HH	XX,XX €	XX,XX €
Serv. Profesionales Fabricante	XXX	HH	XX,XX €	XX,XX €

Los precios unitarios ofertados para cada perfil profesional y tipo de servicio tendrán carácter fijo y vinculante durante toda la vigencia del contrato, constituyendo la base económica de referencia para la ejecución de los servicios incluidos en el mismo.

Dichos precios unitarios serán de aplicación, asimismo, a cualesquiera servicios

adicionales, evolutivos o de refuerzo que, estando dentro del alcance funcional del contrato, puedan ser requeridos durante su ejecución, sin que pueda aplicarse incremento alguno distinto de los expresamente previstos en el pliego.

En el supuesto de finalización del contrato, los precios unitarios ofertados serán igualmente de aplicación a los servicios necesarios para la correcta transferencia del servicio, conocimiento y documentación al órgano de contratación o al nuevo adjudicatario, conforme a lo previsto en el plan de reversión.

Lugar, fecha, sello del licitador y firma autorizada.

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

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

número de trabajadores	*categoría*	*tipo de contrato*	*vencimiento del contrato*	*jornada*	*fecha de antigüedad*	*salario bruto anual*	*Otras condiciones*

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

Anexo XII.- Modificaciones previstas del contrato.

CIRCUNSTANCIAS (supuesto de hecho objetivo que debe de darse para que se produzca la modificación): Implementar necesidades operativas tales como: - Ajustes técnicos imprescindibles para garantizar la continuidad operativa del sistema debido a cambios en la infraestructura tecnológica de Correos o en los servicios asociados. - Ampliación de suscripciones, capacidad del sistema o ajustes en las interfaces debido a un incremento en la demanda de servicios. - Inclusión de mejoras o adaptaciones funcionales necesarias para atender las demandas operativas. - Así como poder contemplar los requerimientos relativos a la evolución de la solución y todas las demás necesidades relacionadas con el objeto del contrato, en las mismas condiciones técnicas, económicas y restantes previsiones contractuales.
ALCANCE (elementos del contrato a los que podrá afectar): - Estas modificaciones podrán afectar a los servicios detallados en el Anexo I. Características Técnicas Especificas del Contrato.
PORCENTAJE DEL PRECIO DE ADJUDICACIÓN DEL CONTRATO AL QUE COMO MÁXIMO PUEDAN AFECTAR: ☐ Límite general (hasta un veinte por ciento del precio inicial, al alza o a la baja, para el conjunto de las modificaciones) ☐ Límite específico para esta causa de modificación del …… por ciento del precio inicial En cualquier caso, esta modificación no supondrá el establecimiento de nuevos precios unitarios no previstos en el contrato.
CONDICIONES DE LA MODIFICACIÓN La modificación del contrato será acordada por el órgano de contratación, de oficio o a instancia del contratista. La propuesta de modificación será informada por el responsable del contrato. Una vez acordada, la modificación será objeto de publicidad en el perfil de contratante de la entidad contratante, acompañada de los informes que, en su caso, se hubieran recabado con carácter previo a su aprobación, incluidos aquellos aportados por el adjudicatario o los emitidos por la propia entidad contratante.

Anexo XIII.- Régimen de penalidades.

A continuación, se indica el régimen de penalidades para cada uno de los indicadores recogidos en el Anexo XIV – Evaluación de Proveedores., según la gravedad de su incumplimiento.

A. ANS correspondientes a la solución ITSM:

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en la plena disponibilidad de la plataforma ITSM y el tratamiento de incidencias
Grave	Penalidad de hasta un 10% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en la plena disponibilidad de la plataforma ITSM y el tratamiento de incidencias
Muy Grave	Penalidad de hasta un 15% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en la plena disponibilidad de la plataforma ITSM y el tratamiento de incidencias

B. ANS correspondientes a la Implantación y Puesta en Marcha:

INCUMPLIMIENTO	PENALIZACIÓN
Leve	La penalización se aplicará con un 3% sobre el importe de facturación del bloque de tareas al que pertenece la tarea/hito con retraso, IVA excluido
Grave	La penalización se aplicará con un 5% sobre el importe de facturación del bloque de tareas al que pertenece la tarea/hito con retraso, IVA excluido
Muy Grave	La penalización se aplicará con un 10% sobre el importe de facturación del bloque de tareas al que pertenece la tarea/hito con retraso, IVA excluido

C. ANS para servicios de mantenimiento y evolución:

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 5% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en el seguimiento de prestación de servicios que aseguren la plena disponibilidad de la plataforma, la calidad de software y el tratamiento de incidencias
Grave	Penalidad de hasta un 10% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en el seguimiento de prestación de servicios que aseguren

	la plena disponibilidad de la plataforma, la calidad de software y el tratamiento de incidencias
Muy Grave	Penalidad de hasta un 15% sobre el importe de la facturación mensual € IVA excluido por el incumplimiento en el seguimiento de prestación de servicios que aseguren la plena disponibilidad de la plataforma, la calidad de software y el tratamiento de incidencias

D. Otros ANS asociados al servicio:

INCUMPLIMIENTO	PENALIZACIÓN
Leve	Penalidad de hasta un 3% sobre el importe de la facturación mensual € IVA excluido en el mes donde se produce el incumplimiento.
Grave	Penalidad de hasta un 5% sobre el importe de la facturación mensual € IVA excluido en el mes donde se produce el incumplimiento.
Muy Grave	Penalidad de hasta un 10% sobre el importe de la facturación mensual € IVA excluido en el mes donde se produce el incumplimiento.

Otras penalizaciones:

INCUMPLIMIENTO	DESCRIPCION	PENALIZACIÓN
Obligaciones generales	Incumplimiento de las obligaciones establecidas en este pliego y que no hayan sido tipificados como incumplimientos graves o muy graves	Hasta 1.000 euros
adscripción de medios	Por el incumplimiento de los compromisos de adscripción de medios	Penalidad de hasta el 2 por ciento del precio del contrato, IVA excluido.
información sobre subrogación de trabajadores	Por incumplimiento de la obligación de proporcionar la información relativa a las condiciones de subrogación de contratos de trabajo	Penalidad de hasta un 6 por 100 del precio del contrato, IVA excluido.
subcontratación	Incumplimiento de las condiciones de subcontratación	Penalidad de hasta un 50 por 100 del importe del subcontrato.
Reincidencia	La comisión de una tercera infracción de carácter leve en el plazo de un año	Penalidad de hasta el 2 por ciento del precio del contrato, IVA excluido.

Reincidencia:

INCUMPLIMIENTO	PENALIZACIÓN
Leve	La comisión de tres infracciones de carácter leve para cada uno de los ANS establecidos en un periodo de seis (6) meses implica una penalidad de hasta 6.000,00 € IVA excluido.
Grave	La comisión de una tercera infracción de carácter grave en el plazo de un año implica una penalidad de hasta 12.000,00 € IVA excluido
Muy Grave	La comisión de una tercera infracción de carácter muy grave en el plazo de un año implica una penalidad de hasta 18.000,00 € IVA excluido

Anexo XIV – Evaluación de Proveedores.

El adjudicatario, dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los valores objetivos 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. 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. Puesto que las condiciones de este nuevo indicador se negociarán con el adjudicatario, en caso de no haber acuerdo, el adjudicatario se compromete expresamente a aceptar los indicadores que Correos establezca en las condiciones que sean necesarias para evitar que el servicio se mantenga deteriorado.

Así mismo, el adjudicatario se compromete a realizar una revisión del ANS con una periodicidad no superior a seis meses, pudiendo acordarse entre Correos y el adjudicatario nuevas condiciones en el ANS (p.e. nuevos valores objetivo y/o porcentajes de cumplimiento, nuevos indicadores de servicio, etc.) 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 prestación real de cada servicio. El ANS se considera como una herramienta clave de medición de la calidad del servicio prestado por lo que es preciso que se definan algunos elementos clave que son objeto de evaluación.

A. Incidencias

Las incidencias se clasifican por prioridades conforme a las siguientes indicaciones:

- Incidencias de prioridad crítica o alta:
    - Toda aquella disfunción que deja una o varias aplicaciones o servicios en estado no operativo, total o parcialmente.
    - Disfunciones que dejan una o varias aplicaciones o servicios en estado de degradación en más de un 30%. El término "degradación" de una aplicación o de un servicio se define como el aumento en los tiempos de respuesta de dicha aplicación en más de un 30% frente a los valores de referencia medidos en la fase de transición.

- Incidencias de prioridad media:
  - Bajadas en el rendimiento de la aplicación o servicio dentro de límites tolerables, hasta un 30% de aumento de los tiempos de respuesta frente a los valores de referencia medidos en la fase de transición.
  - Errores en la monitorización y operaciones de administración que no provoquen incidencias de categorización superior.
  - En general, toda aquella disfunción que no suponga una interrupción de alguna de las aplicaciones o servicios en su globalidad.
- Incidencias de prioridad baja:
  - Incidencias en entornos no productivos.

De acuerdo con estos criterios de criticidad, las incidencias se registrarán en la herramienta de ticketing (PoST basada en Remedy o alternativa acordada) conforme a los procedimientos establecidos.

B. Solicitudes de Servicio (consultas y peticiones operativas).

Se trata de tiques registrados en la herramienta de ticketing como Tipo "Orden de Trabajo". Son cuestiones que realiza el usuario sobre operaciones básicas de administración y operación, que pueden llegar a impedir al usuario el uso de una aplicación o de una parte de ésta y que se resuelven normalmente sin realizar ninguna acción en el sistema, generalmente proporcionando información al usuario.

Las peticiones operativas incluidas son peticiones de diversa índole como, por ejemplo:

- ✓ Elaboración de informes
- ✓ Regularización de datos
- ✓ Modificación de configuraciones
- ✓ Extracción de información
- ✓ Etc.

Según la criticidad se distinguen:

- ✓ Solicitud de Servicio crítica: cuestiones sobre operaciones básicas de administración y operación, que impidan al usuario el uso del sistema o de una parte de este.
- ✓ Solicitud de Servicio no crítica: cuestiones que no impidan al usuario el uso del sistema.

De acuerdo con estos criterios de criticidad, las Solicitudes de Servicio se registrarán en PoST conforme a los procedimientos y valores que se establecerán al inicio del servicio y en sus posibles revisiones.

C. Tiempo de resolución de Incidencias y/o de Solicitudes de Servicio

El tiempo de resolución mide el tiempo máximo transcurrido desde el momento en que se registra en PosT el correspondiente tique, hasta que este se cierra.

No se considerará que estos tiques están cerrados hasta que no se haya conseguido la aceptación del usuario, entregado la correspondiente documentación, realizado las prestaciones complementarias que se definan en la oferta y aprobado por el Correos.

En cualquier caso, la clasificación de los diferentes tipos de solicitudes y la definición de la complejidad y/o criticidad de estas, se realizará al inicio del contrato.

D. Indicadores de Planificación

No se considerará que un hito está conseguido hasta que no se haya entregado la correspondiente documentación, realizado las prestaciones complementarias que se definan en la oferta y no se haya aprobado por parte de Correos.

Los tiempos de aprobación serán establecidos por Correos previa a la planificación de estos en función de la prioridad y el impacto en el servicio.

E. Niveles de aplicación de los indicadores

La medición de la calidad del servicio se realiza a diferentes niveles en función del objetivo perseguido.

En los apartados correspondientes a cada indicador se define el Valor de Cumplimiento y/o el Porcentaje de Cumplimiento con sus valores objetivos. 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, podrá acarrear la penalización definida en el apartado correspondiente.

El adjudicatario se compromete a realizar una revisión del ANS con una periodicidad **no superior a seis meses**, acordando con Correos nuevas definiciones, condiciones y mejoras de este en función de su evolución.

1. INDICADORES, OBJETIVOS Y NIVELES DE CUMPLIMIENTO

Se han definido una serie de Indicadores de Servicio, y para cada indicador los Valores Objetivo y Niveles de cumplimiento exigido, todo lo que en conjunto conforma el Acuerdo de Nivel de Servicio (ANS).

1.1. ANS correspondientes a la solución ITSM

Tipo	ID	Acción	Valor Objetivo %
Disponibilidad de la Plataforma	ANS-ITSM-01	Disponibilidad de la plataforma en su entorno productivo durante las 24 horas del día, todos los días del año (excluido ventanas informadas con antelación)	> = 99,8%
Tiempo de respuesta ante Incidencias Críticas	ANS-ISTM-02	Tiempo de respuesta aplicable a incidencias que afectan gravemente a la operativa del servicio	<30min

Resolución de Incidencias Críticas	ANS-ITSM-03	Tiempo de resolución desde la apertura del incidente hasta su resolución o estabilización temporal	<4horas
Gestión de Cambios Estándar	ANS-ITSM-04	Implementación de cambios clasificados como estándar (bajo riesgo e impacto) como configuraciones, ajustes menores o automatizaciones)	<5días
Cambios Urgentes o de Emergencia	ANS-ITSM-05	Evaluación y ejecución de cambios críticos que corrigen errores graves, fallos de seguridad o requerimientos regulatorios urgentes.	<8 horas
Notificación de mantenimientos programados	ANS-ITSM-06	Notificación de actualizaciones del core de la solución, módulos o integraciones que puedan afectar al servicio	<5días
Notificación proactiva de Incidencias Críticas	ANS-ITSM-07	Notificación de incidencias detectadas en la infraestructura, seguridad o disponibilidad que puedan afectar a cliente	<15 minutos

1.2. ANS correspondientes a la Implantación y Puesta en Marcha

Elemento	ID	Acción	Valor Objetivo %
Plan de implantación	ANS-MIG-01	Establecimiento antes de la aceptación del suministro de la nueva infraestructura	95%
Ventana de mantenimiento y tiempo de inactividad	ANS-MIG-02	Establecimiento y cumplimiento de tiempos máximos para cada migración	95%
Notificación de incidencias y retrasos	ANS-MIG-03	Tiempo de notificación de incidencias <1 hora y <1 día para desviaciones del cronograma establecido	95%
Integridad de los datos	ANS-MIG-04	Atención, restauración y restauración en <1 hora desde la detección del fallo	100%
Funcionalidad del sistema	ANS-MIG-05	Asegurar la operatividad y funcionalidad del sistema en el plazo aceptado	100%
Rendimiento	ANS-MIG-06	Asegurar un rendimiento igual o superior respecto al entorno de partida	100%
Soporte para pruebas	ANS-MIG-07	Prestación de soporte durante las pruebas de usuario para aceptación de la migración con un tiempo de	95%

		respuesta inferior a las 2 horas desde la solicitud	
Resolución de defectos	ANS-MIG-08	Tiempo de resolución < 2 días	90%
Entrega de documentación	ANS-MIG-09	Hasta dos semanas desde la finalización de la migración	95%
Calidad de la documentación	ANS-MIG-10	Exactitud de la documentación	95%

1.3. ANS para servicios de mantenimiento y evolución

Tipo	ID	Acción	Valor Objetivo %
INCIDENCIAS	ANS-MTO-01	Tiemp. Resp. Crítica o Alta < 10 min	90%
INCIDENCIAS	ANS-MTO-02	Tiemp. Resp. Media/Baja < 20 min	90%
INCIDENCIAS	ANS-MTO-03	Tiemp. Resol. Crítica o Alta < 5 horas	90%
INCIDENCIAS	ANS-MTO-04	Tiemp. Resol. Media/Baja < 3 días	90%
SOLICITUDES DE SERVICIO	ANS-MTO-05	Tiemp. Resol. Crítica o Alta < 2 días	90%
SOLICITUDES DE SERVICIO	ANS-MTO-06	Tiemp. Resol. Media/Baja < 4 días	90%
EVOLUTIVO	ANS-MTO-07	Desviación en consecución del hito de Evolutivo (2-20%)	90%
EVOLUTIVO	ANS-MTO-08	Análisis de impacto de un cambio crítico < 3 días	90%
EVOLUTIVO	ANS-MTO-09	Análisis de impacto de un cambio no crítico < 5 días	90%

1.4. Otros ANS asociados al servicio

Tipo	ID	Acción	Valor Objetivo %
GENERACIÓN Y REVISIÓN DE DOCUMENTOS	ANS.COM-01	Protocolos de Administración	95%
REAPERTURA DE TIQUES	ANS.COM-02	Reapertura de peticiones	<10
INCIDENCIAS PROVOCADAS POR ERRORES TÉCNICOS	ANS.COM-03	Número de Incidencias	<2
ENTREGA DE INFORMES DE SEGUIMIENTO DEL SERVICIO	ANS.COM-04	Desvíos de Plazos	<20%

CUMPLIMIENTO DE PLAZOS Y CONDICIONES EN CAMBIOS EN EL EQUIPO DE TRABAJO	ANS-COM-05	Desvío de plazos o incumplimiento de los tiempos de solape y resto de condiciones	<25%
IMPLANTACIÓN DE PROPUESTAS DE MEJORA	ANS-COM-06	Implantación anual de propuestas de mejora reflejadas en oferta a partir de la puesta en producción de la herramienta.	>3

2. SEGUIMIENTO DEL SERVICIO

Salvo alternativa acordada, los ANS se medirán según los tiques creados en la herramienta de Correos (POST). En el caso de este servicio, si el adjudicatario decidiese prestar el servicio con "n" grupos de soporte en POST, las mediciones se contabilizarán desde la asignación del tique a cualquier grupo de soporte asociado al servicio de infraestructuras hasta que el ticket sea satisfecho, es decir, los requerimientos de Correos consideran los plazos / porcentajes / cantidades independientemente de cuántos grupos de soporte hayan tratado el tique.

3. SISTEMA DE EVALUACIÓN

Se establecerá un sistema de evaluación continua y periódica (mensual) durante la ejecución del contrato.

Adicionalmente, el adjudicatario se compromete a adaptarse para poner en marcha los sistemas de seguimiento del ANS y de evaluación del servicio descritos en los apartados anteriores, desde el inicio del servicio. El adjudicatario se compromete también a aportar o desarrollar sistemas complementarios de gestión y seguimiento, si así lo requiere la obtención de los datos para el cálculo de los indicadores acordados inicialmente o de los resultantes de modificaciones posteriores. Los sistemas complementarios deberán ser validados y autorizados expresamente por Correos.

Respecto a la gobernanza del contrato, como norma general, se incluirá la participación en los Comités Operativos de periodicidad semanal o quincenal acordada con el Director de Proyecto y los equipos de Correos, y la participación en los Comités Tácticos mensuales/trimestrales acordados con la Direccion de Transformación Digital y Tecnología de Correos a la que deberán asistir los responsables del servicio del adjudicatario para hacer un seguimiento global de la ejecución del contrato o contratos en curso. Los detalles sobre la agenda, estructura de los Comités y de la documentación a aportar se concretará al inicio del servicio. Esta norma general podrá modificarse y adaptarse en base a la propuesta de modelo de gobierno ofertada por el adjudicatario.

4. GRAVEDAD DE LOS INCUMPLIMIENTOS DE ANS

De acuerdo con lo establecido en el Anexo XIII.- Régimen de penalidades., los incumplimientos serán calificados como leves, graves y muy graves en función del impacto en los sistemas y actividad de Correos.

Los casos serán acumulativos. Así, la acumulación de 3 incumplimientos leves equivaldrá a 1 incumplimiento grave y la acumulación de 3 graves supondrá 1 incumplimiento muy grave.

Para este contrato específico se establecen según cada actividad a desarrollar:

- Solución ITSM

Los desvíos en la disponibilidad de la plataforma por causas imputables al adjudicatario serán calificados como muy graves.

La desviación en la resolución de cambios/incidencias graves o urgentes serán calificados como graves, mientras que el resto de ANS de la presente categoría se considerarán leves.

- Implantación y puesta en marcha

Los incumplimientos de los acuerdos de nivel de servicio de esta categoría serán calificados como leves.

No obstante, podrán acumularse varios incumplimientos de cada elemento en caso de volver a requerirse la resolución transcurrido el plazo establecido a tal efecto.

- Mantenimiento y evolución

Según el tiempo límite establecido para la atención y resolución de cada caso, la acumulación de 2 incumplimientos de casos con criticidad calificada como baja o 1 incumplimiento de criticidad calificada como media será considerado como incumplimiento leve y aquéllos con un tiempo de acción considerado crítico, serán considerados como incumplimiento grave.

- Otros ANS asociados al servicio

Cada incumplimiento de este tipo será calificado como grave por considerarse como parte fundamental del servicio.

Anexo XV.- 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 A REALIZAR	□ Recogida □ Registro □ Estructuración □ Modificación

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

2. Obligaciones del adjudicatario

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

- Llevar a cabo del tratamiento de datos personales de conformidad con la normativa vigente en materia de protección de datos, y en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante,

RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

- Tratar los datos de acuerdo con las instrucciones de [_____] y no destinarlos para ninguna otra finalidad.
- Mantener actualizado un registro de todas las actividades de tratamiento efectuadas por cuenta de [_____], 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 [_____], 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 [_____].
- 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 [_____] toda la información necesaria para demostrar el cumplimiento de sus obligaciones, según el proceso establecido en el punto 5.
- Asistir a [_____] 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 [_____] 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 [_____] se obliga a realizarlo conforme las instrucciones de [_____], siguiendo la redacción y formato indicado y custodiando o dando traslado a [_____] (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 [_____] ; y
(ii) Lugar de prestación de servicios objeto de licitación.

4. Obligaciones de [_____]

Corresponden a [_____] 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 [_____] 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 [_____], 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.

A este respecto, se acompaña como Adenda al presente contrato el listado de medidas de seguridad que el adjudicatario debe observar según el análisis de riesgo efectuado a la fecha de firma del contrato. Este catálogo tiene la consideración de mínimo exigible y se establece sin perjuicio de posibles ulteriores modificaciones que se transmitirán al adjudicatario por los medios de comunicación establecidos.

6. Derecho de auditoría

[_____] , 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 [_____] .

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

[_____] , 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 [_____] 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 [_____] 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 [_____] 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 [_____] 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 [_____] 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 [_____]. 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

El adjudicatario no podrá subcontratar ninguna de las prestaciones que formen parte del objeto de este Contrato que comporten el tratamiento de datos personales, salvo previa autorización expresa y otorgada por escrito por parte de [_____], así como los servidores y servicios relacionados con los mismos comunicados a [_____] durante el procedimiento de licitación.

Si fuera necesario subcontratar algún tratamiento o existiese alguna novedad respecto a los servidores o los servicios relacionados con los mismos, este hecho se deberá comunicar previamente y por escrito a [_____], 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, [_____] tendrá un plazo de 30 días para oponerse.

Transcurrido el plazo de 30 días sin que [_____] 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, [_____] 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 [_____]. 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 [_____] 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 [_____] la documentación acreditativa de su vigencia.

11. Responsabilidad

El adjudicatario vendrá obligado a exonerar a [_____] 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 [_____].

12. Notificación de cambios

El adjudicatario comunicará a [_____] cualquier cambio que se produzca con respecto a los términos y condiciones en los que accederá y tratará los datos personales por cuenta de [_____], 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 [_____] 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 las siguientes direcciones

- 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 [-], según corresponda, o presentar una reclamación ante la Agencia Española de Protección de Datos u otra autoridad competente.

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

14. Actuación como subencargado

El contenido del presente contrato se aplicará, mutatis mutandis, en aquellos casos supuestos en los que [_____] 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 [_____]: 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 [_____] 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 [_____] acuerdan someterse de manera expresa a la normativa vigente en materia de protección de datos en España y, en particular, al RGPD y LOPDGDD.

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

MEDIDAS DE SEGURIDAD

I. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES

- Disponer de un organigrama de asignaciones en materia de seguridad de la información, incluyendo cargos y funciones atribuidas a cada puesto.
- Contar con un procedimiento de control de accesos que incluya, entre otros:
    - Gestión de altas/bajas en el registro de usuarios de repositorios de información asegurando que se asigna un identificador único a cada cuenta de usuario. Excepcionalmente, podrán permitirse identificadores de usuario (IDs) genéricos para ser utilizados por un individuo, en el caso de que las funciones accesibles o las acciones llevadas a cabo por ese identificador o necesiten ser detallada seguidas (por ejemplo, acceso de sólo lectura), o cuando están implantados otros controles (por ejemplo, si la contraseña para un ID genérico sólo se utiliza por una persona al mismo tiempo y se registra tal caso).
    - Gestión de derechos y credenciales de acceso asignados a los usuarios.
    - Gestión de privilegios especiales de acceso según el impacto que puede derivar de un uso inadecuado de los datos de carácter personal.
    - Gestión de información confidencial de autenticación de usuarios.
    - Política de retirada de cancelación de accesos y credenciales.
- Haber establecido un procedimiento de accesos a sistemas y aplicaciones que incluya:
    - La restricción de acceso a la información.
    - Procedimientos seguros de inicio de sesión en el que, como mínimo:
        - Se registre los intentos de entrada no satisfactorios.
        - Se limite el número máximo de intentos fallidos, de forma que La revisión de los privilegios de acceso de forma recurrente y

después de cualquier cambio, tal como promoción, degradación o terminación del empleo.
    - Procedimiento de uso de herramientas de administración de sistemas de información, tanto propias como externas.
- La revisión de los privilegios de acceso de forma recurrente y después de cualquier cambio, tal como promoción, degradación o terminación del empleo.

II. PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

- Contar con un procedimiento de gestión de contraseñas de usuario que incluya los siguientes aspectos:
    - Forzar el uso de los identificadores de usuario (IDs) individuales y de las contraseñas para mantener la responsabilidad.
    - Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación que tenga en cuenta los errores de entrada.
    - Forzar la elección de contraseñas de calidad.
        - Ser fáciles de recordar.
        - No se basen en algo que alguien más pueda fácilmente adivinar u obtener usando la información relativa a la persona, por ejemplo, nombres, números de teléfono, y fechas de nacimiento etc.
        - No sean vulnerables a ataques de diccionario (por ejemplo, que no consistan en palabras incluidas en diccionario).
        - No contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos
    - Forzar el cambio de contraseñas, por lo menos, cada 6 meses y siempre que existan indicios de que su confidencialidad ha podido verse comprometida.
    - Forzar a los usuarios el cambio de las contraseñas temporales después de la primera entrada.
    - Mantener un registro de las contraseñas de usuarios anteriores y prevenir su reutilización.
    - No mostrar las contraseñas en la pantalla cuando se están introduciendo.
    - No incluir contraseñas en ningún proceso de registro automático, por ejemplo, almacenamiento en una macro o en una función clave.
    - Almacenar los ficheros de contraseñas por separado de los datos de la aplicación del sistema.
    - Almacenar y transmitir las contraseñas de forma que se garantice su integridad y confidencialidad.
- Plantear el uso de contraseñas basadas sistemas de autenticación fuerte (p.ej. mediante el uso de tarjetas inteligentes combinado con una contraseña).

III. GESTIÓN DE SOPORTES

- Llevar a cabo un inventariado de soportes y gestión de activos, incluyendo:
    - Un registro de propiedad de los activos.
    - Una política interna de usos aceptables de los activos.
    - Una política de devolución/sustitución de activo.

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

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

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

IV. ACCESO FÍSICO AL LOCAL

- Contar con un procedimiento de control de entrada y "área segura" que incluya:
  - 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 media posible.
- MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales. El sistema de cortafuegos deberá ser actualizado de forma periódica.

- FUGA O SALIDA DE INFORMACIÓN: Introducir medidas técnicas en los sistemas de información que restrinjan la posibilidad que datos personales puedan ser exportados de forma no autorizada (p.ej. Restricción de las funcionalidades de descarga, impresión y almacenamiento de datos en los sistemas de información que procesan los datos personales) e implementar medidas técnicas que permitan detectar transmisiones no autorizadas de datos personales dentro de la organización y hacia fuera de la misma (p.ej. Sistemas de prevención de fugas de información, herramientas de monitorización de actividades de usuarios en los sistemas de información.

X. CIFRADO DE DATOS

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

XI. CONTROL DE CAMBIOS EN T.I

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

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

XII. CONTROL DE CAMBIOS EN APLICATIVOS

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

XIII. GESTIÓN DE INCIDENCIAS Y BRECHAS DE SEGURIDAD

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

XIV. VIDEOVIGILANCIA

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

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

Don/Doña _____

NIF _____

Con domicilio en _____

Calle/Plaza, nº _____

Telf. contacto nº _____

Correo electrónico _____

En caso de actuar en representación

Como apoderado de _____

CIF _____

Con domicilio en _____

Calle/Plaza, nº _____

Correo electrónico _____

DECLARA BAJO SU RESPONSABILIDAD:

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

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

☐ La empresa es de menos de 50 personas trabajadoras.

Lugar, fecha y firma del adjudicatario

Anexo XVII.- Declaración responsable en materia de protección de datos

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

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

*AVISO PARA PEQUEÑAS Y MEDIANAS EMPRESAS:

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

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

El enlace a esta herramienta es el siguiente:
https://www.servicios.agpd.es/AGPD/view/form/MDAwMDAwMDAwMDAwMDIwNTAwMDkxNTQ5NjEyMTMxMDMz?updated=true

Cuestionario para la Privacidad de Proveedores:

Marque y cumplimente lo que corresponda:

D. [ ] con NIF , actuando en
su propio nombre y derecho, como profesional autónomo,

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

DECLARA lo siguiente:

1. Cuestiones generales

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

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

0= no dispone del registro de actividades a pesar de ser obligatorio
5= dispone del registro de actividades actualizado y completado

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

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

0= no dispone de DPO siendo obligatorio.
3= no dispone de DPO siendo voluntario.
5= dispone de DPO siendo obligatorio. Identifíquelo: [ ]

2. Medidas de seguridad

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

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

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

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

A continuación, os facilitamos el enlace de la Guía de Análisis de Riesgos que facilita la AEPD:
https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

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

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

A continuación, os facilitamos el enlace de la Guía para la Gestión y Notificación de Brechas de Seguridad que facilita la AEPD:
https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

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

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

3. Confidencialidad

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

0= no
3= sí, disponen de código de conducta, o están sujetos a una obligación de naturaleza estatutaria.
5= sí, los empleados que van a realizar actividades en el marco del contrato a suscribir con [ ], han firmado un compromiso de confidencialidad.

4. Accountability y rendición de cuentas

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

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

0= no tiene implantados controles periódicos.
3=definidos no aplicados. Presentar planificación de aplicación con plazo determinado.
5= tiene definidos e implantados controles periódicos.

5. Subcontratación

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

0= se va a subcontratar el servicio contratado sin cumplir con las obligaciones de autorización previa.
5= se va a subcontratar el servicio y estará debidamente regulado.

6. Transferencias internacionales

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

0= se realiza Transferencias Internacionales de Datos a un país sin nivel adecuado de protección y sin ninguna garantía habilitante.
3= se realiza Transferencias Internacionales de Datos a un país con nivel adecuado de protección y utilizando alguna de las garantías habilitantes (cláusulas contractuales tipo, BCR´s, etc.). Indique cuál/cuáles: []
5= no se realiza Transferencias Internacionales de Datos.

7. Sanciones y procedimientos inspectores

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

1= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos idénticos a los prestados en este caso. Aportar documentación justificativa de haber corregido el motivo de la infracción.
3= ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años por tratamientos distintos a los prestados en este caso.
5= no ha sido sancionado por infracciones de la normativa de protección de datos en los 2 últimos años.

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

1= tiene abierto procedimiento sancionador por tratamientos idénticos a los prestados en este caso.
3= tiene abierto procedimiento sancionador por tratamientos distintos a los prestados en este caso.
5= no tiene abiertos procedimientos sancionadores por infracciones de la normativa de protección de datos.

Fdo.:

Anexo XVIII.- Requerimientos de Seguridad

1. ORGANIGRAMA Y ASIGNACIÓN DE FUNCIONES

Desde el punto de vista organizativo, el adjudicatario deberá asignar un responsable de seguridad para el servicio prestado a la Sociedad Estatal de Correos y Telégrafos, S.A, que será el interlocutor único en dicha materia con la Subdirección de Ciberseguridad de Correos. Este rol se encargará de revisar y auditar los procesos de seguridad delegados en él, así como de notificar cualquier incidente o aspecto relevante en el ámbito de la seguridad.

En este contexto, el adjudicatario deberá crear un proceso de Gestión de la Seguridad específico para la Sociedad Estatal de Correos y Telégrafos, S.A, a través del cual se gestionen los procesos y responsabilidades de Seguridad que se le han transferido. Dicho proceso será liderado por el responsable de seguridad del servicio, que deberá compartir periódicamente un cuadro de mando con métricas e indicadores de seguridad integradas, así como realizar reuniones de seguimiento en las que se puedan tratar riesgos o aspectos críticos de seguridad de la información en la solución ofertada.

Adicionalmente, el proveedor deberá de disponer tanto de **personal experto como de herramientas específicas** para desarrollar de manera satisfactoria todos los procesos y funciones de Seguridad que le son transferidos.

La monitorización de la seguridad y la respuesta ante incidentes se deben considerar como un servicio 24x7.

2. REQUISITOS DE GESTIÓN DE LA SEGURIDAD POR PARTE DEL PROVEEDOR

La presente licitación, supone la delegación de ciertos procesos de la seguridad, que serán responsabilidad exclusiva del proveedor prestador del servicio.

En este sentido, la solución objeto del contrato, además de cumplir con los requisitos de seguridad trasladados por la Sociedad Estatal de Correos y Telégrafos, S.A y firmar el acuerdo de "Compromiso de aceptación de políticas de acceso y uso de infraestructuras de correos" (ver apartado 4.8), deberá asumir (tener implantados, y mantener), todos los controles y procesos que se identifican a continuación, con alcance de la prestación del servicio:

2.3 Controles de protección de las comunicaciones

El adjudicatario deberá implantar medidas de seguridad apropiadas, cifrando las comunicaciones a través de las cuales viaje información de Correos, especialmente cuando se manejan datos confidenciales o sujetos a alguna regulación. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.1)

2.4 Controles de Fortificación de sistemas

El adjudicatario deberá implantar medidas de fortificación sobre todos los elementos involucrados en la prestación del servicio bajo su responsabilidad y control, de acuerdo con las recomendaciones de los fabricantes, para lo que deberán existir

procedimientos específicos. La Subdirección de Ciberseguridad de Correos podrá solicitar los controles aplicados en cada ámbito y en cada dispositivo o software dedicado para el servicio, los procedimientos de fortificación. (ver apartado 4.3).

2.3 Proceso de gestión de identidades y control de acceso lógico

El adjudicatario deberá seguir unas directrices de gestión de identidades alineadas con las políticas de Correos, administrando y controlando, a través de las herramientas pertinentes, los accesos cuya gestión recaiga bajo su responsabilidad. **Cuando aplique, el proceso deberá estar integrado con el de Correos** (ver apartado 3.2).

3.4 Proceso de generación y explotación de eventos de seguridad

El adjudicatario deberá contar con un proceso formal de gestión de eventos que englobe la solución ofertada y que facilite la gestión de incidentes y la implantación de los requisitos de seguridad definidos en este ámbito dentro del proceso de seguridad en el ciclo de vida de las aplicaciones de Correos. Los eventos y alertas de seguridad generados deberán estar a disposición de Correos para su revisión en caso de ser requeridos (ver apartado 3.3).

3.5 Proceso de seguridad en el ciclo de vida de las aplicaciones

El adjudicatario deberá contar con un proceso propio para la construcción de SSII que incorpore la seguridad desde diseño, definiendo y aplicando requisitos de seguridad a las aplicaciones que se desarrollen. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.4).

3.6 Proceso de gestión y notificación de incidentes

El adjudicatario deberá contar con un proceso formal de gestión y notificación de incidentes de seguridad (diferenciando brechas RGPD) que le permita actuar siempre en tiempo y forma, de modo que se cumplan los requisitos legales y de disponibilidad definidos. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.5).

3.7 Proceso de contingencia y recuperación ante desastres

El adjudicatario deberá disponer de un plan de contingencia TI ante desastres que incluya las tareas y prioridades de recuperación de los activos impactados en el servicio. **El proceso deberá estar integrado con el de Correos** (ver apartado 3.6).

3.8 Proceso de configuración segura del entorno tecnológico

El adjudicatario deberá manejar de manera automatizada la configuración de los recursos tecnológicos de su exclusiva responsabilidad, teniendo en cuenta las normativas de Seguridad y principios de Arquitectura de Correos. En particular, dentro del ámbito del cloud, deberá utilizar herramientas de control como CSPM (Cloud Security Posture Management) o CWPP (Cloud Workload Protection Platforms) de acuerdo al caso de uso específico y siguiendo los procesos de seguridad establecidos.

3.9 Proceso de gestión de vulnerabilidades y parcheado

El adjudicatario deberá contar con un proceso formal para gestionar, en la medida de lo posible de manera automatizada, la remediación de vulnerabilidades, aplicando controles para su detección automática y realizando pruebas antes de su instalación.

2.10 Proceso de Gestión de la Seguridad Global

Se trata del proceso que engloba todos los anteriores con alcance del servicio contratado.

Dicho proceso, deberá definir indicadores y métricas, que sean útiles de cara a comprobar la madurez de seguridad de la información, y elaborar un cuadro de mando visual, de cara a realizar un reporte periódico al equipo de Seguridad de la Información de Correos.

4 REQUISITOS DE SEGURIDAD PARA LA INTEGRACIÓN TÉCNICA DEL SERVICIO

3.1 Integración de 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.

3.2 Integración con el Sistema de Gestión de Identidades

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.

4.3 Generación, explotación y aportación de eventos de seguridad

A través del proceso de seguridad en el ciclo de vida de las aplicaciones, la Sociedad Estatal de Correos y Telégrafos, S.A, para cada desarrollo, podrá requerir la generación y explotación, como mínimo, de los siguientes eventos y alertas:

- Autenticación y accesos a la solución (acertados y fallidos).
- Cambios en las cuentas y grupos de usuarios y contraseñas (acertados y fallidos).
- Cambios accesos y modificaciones del sistema de log o auditoría (acertados y fallidos).
- Acciones realizadas con privilegios de administrador.
- Cambios en los privilegios asociados a cada rol.
- Registro de accesos a Información Personal (cumplimiento LOPD/RGPD).

La generación de los citados eventos y trazas de auditoría de la solución deberán permitir comprobar las siguientes políticas:

- Registro de accesos.
- Control de privilegios administrativos.
- Cumplimiento de la LOPD/RGPD.

Los eventos de auditoría generados deberán estar disponibles para la Sociedad Estatal de Correos y Telégrafos, S.A, en caso de que esta los solicite para su revisión o integración con su sistema de correlación de eventos (SIEM). En este sentido, el adjudicatario no deberá borrar los logs y trazas al menos durante un periodo de tiempo razonable.

4.4 Integración con el proceso de seguridad en el ciclo de vida de las aplicaciones

La Sociedad Estatal de Correos y Telégrafos, S.A dispone de un proceso que incluye la Seguridad en el Ciclo de Vida de los Sistemas de Información. Este proceso fija una serie de requisitos de seguridad detallados a cada nuevo sistema de Información y los grandes evolutivos, en función de los parámetros de Exposición del Sistema, Criticidad de la Información, Tipología de Usuarios y Normativa Legal Aplicable.

La adecuación a estos requisitos será revisada y acreditada, si procede, por el Área de Seguridad de la Información de la Sociedad Estatal de Correos y Telégrafos, S.A por lo que el adjudicatario se compromete a describir los controles de seguridad destinados a esta adecuación y a documentarlos en el documento denominado "Diseño de Seguridad" de la solución objeto del contrato.

En caso de que el Área de Seguridad de la Información no establezca este conjunto de requisitos, el adjudicatario deberá identificar en qué riesgos incurre la Sociedad Estatal de Correos y Telégrafos, S.A, qué medidas los mitigan y el plan de acción que tiene para mitigarlos. Para poder realizar este Análisis de Riesgos la Sociedad Estatal de Correos y Telégrafos, S.A facilitará el valor de la información gestionada en la solución.

4.5 Integración con el proceso gestión de 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.

Integración con el proceso de continuidad y recuperación ante desastres

Se establecerán procedimientos para integrar los servicios objeto del pliego con el Plan de Recuperación ante Desastres de Correos, de acuerdo con los escenarios de contingencia como a las condiciones de Tiempo de Recuperación Objetivo (RTO) y de Punto de Recuperación Objetivo (RPO) definidos por la Sociedad Estatal de Correos y Telégrafos, S.A. El adjudicatario deberá consensuar previamente la tipología de pruebas a realizar y el calendario de realización de las mismas

Se considerará un valor añadido que el adjudicatario del servicio disponga de la certificación ISO/IEC 22301 o equivalente.

5 OTROS REQUERIMIENTOS DE SEGURIDAD

4.1 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.

4.8 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.

4.9 Auditabilidad

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

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

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

4.10 Niveles de servicio

Todas las categorías de servicios descritas en el "Objetivo del contrato" de este acuerdo dispondrán de monitorización que permita un seguimiento en tiempo real del grado de cumplimiento de los niveles de servicio.

Por otra parte, se proporcionará a Correos informes mensuales que indicarán el rendimiento de los niveles de servicio. Este informe se pondrá a disposición de Correos siempre que sea requerido.

4.11 Formación y concienciación

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

4.12 Ubicación de los datos

Se tiene que explicar en un apartado específico en qué país van a residir los datos. En caso de que el servicio 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 contratado tendrán que cumplir con la nueva normativa Europea de protección de datos (GDPR).

4.13 Compromiso de aceptación de políticas de acceso y uso de infraestructuras de correos

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

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

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

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

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

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

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

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

Anexo XIX.- Requisitos de Arquitectura y Explotación que deben cumplir las nuevas soluciones tecnológicas

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

- **Solución SaaS**

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

Requisitos de diseño

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

Requisitos de integración

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

Requisitos de mantenimiento, operación y monitorización de los sistemas

1. Los cambios en la configuración del servicio, los despliegues de las actualizaciones, los procesos de tunning interno, y resto de acciones de mejora continua del servicio, serán comunicados a Correos con una antelación de:
    a. 15 días, si el cambio no implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.
    b. 6 meses, si el cambio implica cambios en los desarrollos o trabajos que Correos realiza en la plataforma SaaS.
2. El adjudicatario debe responsabilizarse de la ejecución de implementaciones, configuraciones y acciones predictivas, que permitan la recuperación del servicio ante cualquier desastre. Correos exige que este tiempo de recuperación de los servicios sea de menos de 4 horas.
3. La solución debe dar servicio a Correos, sin perjuicio en el rendimiento o la disponibilidad del servicio, ante un incremento de hasta el 100% de la carga, y con un aviso previo de al menos 48 horas por parte de Correos.
4. El servicio debe ser convenientemente monitorizado por el prestatario del servicio, y esta monitorización ha de ser extremo a extremo, es decir, desde el nivel físico (hardware) hasta los procesos de negocio.
5. Al detectarse una incidencia en el servicio, el adjudicatario debe solucionarla y enviará un informe que incluya:
    a. La ventana temporal de afectación del servicio.

   b. Una explicación de las causas que han producido la incidencia
   c. Acciones puestas en marcha para solucionar la incidencia.
   d. Dentro de las 48 horas posteriores a la resolución de una incidencia, se enviará un análisis de la causa raíz (RCA), para eventos críticos.
6. Aquellos eventos que puedan afectar al servicio, incluyendo degradación de rendimiento, actualizaciones críticas o incidentes de seguridad, serán notificados de manera proactiva por parte del prestatario a Correos, indicando el impacto previsto y el plan de mejoras a implementar. El adjudicatario debe indicar el tiempo estimado de resolución de la incidencia.
7. La solución, o en su defecto el adjudicatario del servicio, deben proveer a Correos de información respecto a los parámetros del servicio prestado. Correos debe tener disponible tanto datos operativos como las métricas del servicio. Debe proveerse esta información a través de cuadros de mando, y esta información debe poder exportarse en algún formato estándar y consensuado con Correos, como XML, JSON o CSV.
8. En caso de que la solución tenga versiones del producto on premises y cloud, debe facilitar la migración de información entre las versiones del producto. El proceso de migración de datos, procesos y configuraciones específicas que ha implementado Correos en la plataforma, debe ser exportable en la plataforma origen, e importable en la plataforma destino, con algún mecanismo manual o automático que facilite esta migración.

Requisitos sobre acuerdos a nivel de servicio

1. La disponibilidad del servicio debe ser 99.9% o mayor. En esta métrica deben incluirse fines de semana sólo si Correos va a usar el servicio durante estos días.
2. Si el adjudicatario fuera capaz de mejorar los ANS exigidos por Correos, deberá presentar en su oferta dicha propuesta de nuevos ANS específicos para Correos, incluyendo indicadores y métricas del servicio. Una vez que Correos haya validado los indicadores propuestos por el adjudicatario y el cumplimiento de los mínimos requeridos, ambas partes suscribirán el correspondiente Acuerdo de Niveles de Servicio Definitivo, que será de aplicación durante todo el periodo de vigencia del contrato.
3. La solución (y el adjudicatario de esta) deben proponer un modelo de gobierno del servicio, que incluya un modelo de comunicación efectivo para Correos, y defina las funciones y responsabilidades de los distintos actores en el desarrollo del servicio.
4. 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.
5. 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.
6. Correos será el propietario de cuantos trabajos parciales o finales se deriven de esta colaboración, así como de todos los datos, y el adjudicatario se compromete a la devolución de estos, sin que el adjudicatario pueda conservarlos, ni obtener copia de estos o facilitarlos a terceros. El adjudicatario sólo podrá consultar o extraer estos datos con la autorización expresa de Correos.

7. En la oferta presentada por el adjudicatario, deben especificarse claramente las condiciones sobre las que se regirá la devolución de la información residente en la solución.

- **Solución PaaS**

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

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

Requisitos específicos de PaaS

1. La solución debe permitir la creación de nuevos tenant o mecanismos alternativos que permitan el crecimiento ordenado del servicio. El tiempo de respuesta y los recursos dedicados al servicio de Correos no se verá afectado por picos en los procesos que sean compartidos con otros clientes.
2. La solución debe incorporar políticas de respaldo de información, automatizadas, y el adjudicatario debe realizar pruebas de restauración, de forma periódica, con una retención de al menos 30 días.

- **Productos comerciales**

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

Requisitos de diseño

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

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

2. Los licitadores deberán describir la arquitectura propuesta de manera detallada indicando expresamente cualquier necesidad de servicio horizontal o hardware adicional para el funcionamiento de su solución. Entre los datos de la arquitectura, está la arquitectura del procesador, versionados de sistema operativo, middleware, bases de datos, y en general de todo el software de base y todo elemento que forme parte de la

infraestructura, bien sea de hardware o de software. Deberá facilitarse una propuesta de solución.

3. En la solución propuesta se admitirá el uso de componentes Hardware (Appliances) sólo en el caso de que no exista la posibilidad de realizarla con el hardware que aprovisiona Correos. Así mismo, todo Servidor que requiera un software base con tecnologías distintas al apartado de Entorno Tecnológico, excluyendo versiones, podría ser tratado también como appliance si el equipo de explotación no tuviera el conocimiento para su administración, teniendo que contemplar el licitante expresamente en la oferta como concepto de administración y mantenimiento por el conjunto de servidores y su software base, excluyendo el de producto o desarrollo que presta el servicio. Una vez adjudicado se evaluará la compatibilidad con las herramientas de monitorización, logs y de backup, junto los equipos de explotación de Correos.
4. El producto será escalable (horizontal y verticalmente), con la posibilidad de extender la plataforma a medida que se incorporan nuevos usuarios o cargas de trabajo, reduciendo el tiempo de provisión de equipamiento que soporte los nuevos servicios.

Entono tecnológico para el producto

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

1. Cloud

Elemento	Versiones
Sistemas Operativos	Red Hat Enterprise Linux 8 o superior (plataforma de 64 bits) Windows 2019 o superior (plataforma de 64 bits) Amazon Linux 2 o superior
Gestor de Base de Datos	Relacional: Amazon RDS (PostgreSQL 16.x) Amazon RDS (MySQL 8.0.39) Clave-valor: DynamoDB No relacional: Atlas MongoDB 8.x
Servidores de aplicaciones	NodeJS (lambda) 20 o superior
Runtimes e Interpretes	OpenJDK (caas)1.17 OpenJDK (lambda)1.17 OpenJDK (onPremise) - SpringBoot1.11 PHP (caas) 8.2 Python (lambda) 3.12 Javascript/Typescript para los frontales ReactJS
Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux. Nginx1.20
Orquestador Contendores	Openshift Container Platform 4.16 (Docker) para arquitecturas basadas en microservicios.

Imágenes de contenedores	Contenedores: Frontend: Nginx (1.22) / Apache (2.4.x) / Node.js (20 o superior) / Tom (9 o superior) Backend: Springboot con tomcat embebido (3.1.4)
Integración	API Gateway (CaaS): Mulesoft (4.3) ETL: Apache Nifi 1.23 y lambdas Intercambio de ficheros: Apache Nifi 1.23
Gestor de Contenidos	Adobe Experience Manager 6.5.20 o superior
Servicios nativos AWS	SQS, SNS, Eventbridge, Step Funtions, Lambda, Kinesis, Data firehose, Core, DMS, Glue, Sagemaker
Servicios nativos Azure	Webapp, API Management, OpenAI

2. On premises

Elemento	Versiones
Virtualizadores	IBM Power 8 VMware (versión 5.5 o superior).
Sistemas Operativos	Red Hat Enterprise Linux 8 o superior (plataforma de 64 bits) Windows 2019 R2 o superior (plataforma de 64 bits) IBM AIX 7.3 (plataforma IBM Power) Amazon Linux 2.0 o superior
Gestor de Base de Datos	Oracle 21C PostgreSQL 16 SQLServer 2019
Gestor Documental	Documentum 2023.4
Gestor de Contenidos	Adobe Experience Manager 6.5.0 o superior
Lenguajes de programación corporativos	OpenJDK 11 o superior para arquitectura basadas en Linux. Javascript/Typescript para la para los frontales en ReactJS. IBM SDK 7 o superior para arquitecturas basadas en AIX. .NET v4.8 para arquitectura basadas en Windows.
Servidores web	Apache 2.4 o superior para arquitecturas basadas en Linux. IBM HTTP Server 8.5.5 para arquitecturas basadas en AIX. IIS 10
Servidores de aplicaciones	JBossEAP 7.3 para arquitecturas basadas en Linux. WebSphere Application Server Network Deployment 8.5.5 p arquitecturas basadas en AIX. Internet Information Server 10 para arquitecturas basadas en Windo Tomcat 10 o superior para arquitecturas basadas en Linux.
Integración	Colas: IBM MQ 12 ETL: ACE112 Intercambio ficheros: Spazio 2.9

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

Requisitos de integración

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

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

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

Requisitos de mantenimiento, operación y monitorización de los sistemas

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

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

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

Requisitos sobre acuerdos a nivel de servicio

1. El producto debe estar soportada por el fabricante de esta. El adjudicatario deberá aportar certificación al respecto que lo acredite.
2. Roadmap de producto: el fabricante debe ofrecer un compromiso de evolución del producto que asegure la continuidad de este como mínimo durante un plazo de cinco años, o especificar en el caso de no cumplimiento.
3. Consolidación de producto: la fecha de lanzamiento de la primera versión del producto ofertado deberá ser como mínimo tres años anterior a la fecha de presentación de la oferta por parte del licitador o especificar en el caso de no cumplimiento.
4. Última versión liberada: la fecha de última versión/actualización del producto ofertado deberá ser como máximo seis meses anteriores a la fecha de presentación de la oferta por parte del licitador.
5. 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.

6. El adjudicatario debe informar a Correos en su oferta de los modos de licenciamiento y su coste asociado, así como aquellos aspectos que puedan ser determinantes en el coste del producto (por ejemplo, tramos de número de usuarios o el número de procesadores necesarios en el servicio a Correos). Deben también especificarse requerimientos de licenciamiento específicos en un Entorno Virtualizado La propuesta del adjudicatario debe estar desglosada por tipo de entorno (productivo o no productivo).
7. El adjudicatario debe proveer las licencias correspondientes para prestar de forma completa el servicio demandado por Correos. En su oferta debe proponer una solución que garantice la correcta custodia, uso y aprovechamiento de las licencias facilitadas. Una vez implantada la solución, Correos revisará estas condiciones para asegurar que se estén aprovechando correctamente las licencias ofertadas.
8. Correos podrá definir periodos de congelación de cambios y actualizaciones en el sistema, es decir, periodos en los que no debe alterarse la implementación ni la configuración del servicio por parte del fabricante o del adjudicatario, para minimizar posibles impactos en el negocio de Correos.

- **Desarrollo a medida**

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

Requisitos de arquitectura

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

Arquitectura de Referencia	Infraestructura	Pila tecnológica
Microservicios	cloud	Openshift CP SpringBoot Python ReactJs Mulesoft API Amazon Aurora PostgreSQL

B2B	cloud/on premises	IBM App Connect IBM Integration BUS Spazio Apache NIFI
Fast Data	cloud native	AWS Lambda AWS Kinesis AWS S3 AWS DynamoDB MongoDB
Sensorización	cloud native	AWS EMR AWS lambda AWS Kinesis AWS IoT
Experiencia Digital	on premises	Adobe EM ReactJS Storybook
Lake House	cloud native	AWS Glue AWS DMS AWS s3 SnowFlake
Arquitectura para IA	cloud	AWS Sagemaker AWS Bedrock Azure OpenAI Azure AI Services
Tradicional	cloud/on premises	Spring Jboss Websphere AS Oracle

2. La construcción del software debe ceñirse al ciclo de vida del software definido en Correos, cumpliendo con los procesos de ingeniería del software definidos por la metodología que Correos establezca durante las fases de análisis, diseño, implementación y pruebas, generando los entregables y documentación que se estipule necesaria.
3. La infraestructura de Correos se divide actualmente en tres entornos:
    a. Entorno de desarrollo Integrado: Utilizado para las pruebas de Aceptación de Usuario, validación de funcionalidad del código, y pruebas integradas con otras aplicaciones. También como entorno para acciones de formación. Por tanto, es importante recalcar que este entorno no está destinado a la construcción de software. El software debe ser construido en las instalaciones del cliente, y ser desplegado en Correos cuando sea el momento de validarlo e integrarlo.
    b. Entorno de preproducción: Utilizado para el análisis, verificación y validación del proceso de paso a producción.

c. Entorno de producción: Entorno productivo, de acceso por parte de los Usuarios de Correos para el desarrollo de su trabajo diario y por parte de empresas externas.

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

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

4. La construcción de software debe ser realizada utilizando los arquetipos de desarrollo que provee Correos, a través de las herramientas de integración continua. Estos arquetipos facilitan la construcción, implementando algunos aspectos comunes a las aplicaciones, y permitiendo la integración y despliegue continuo en las plataformas de Correos.
5. El adjudicatario de la solución debe responsabilizarse de realizar las tareas que le sean requeridas de cara a que su aplicación cumpla con los requerimientos de obsolescencia establecidos en Correos.
6. La aplicación construida debe albergar la posibilidad de integración con servicios y aplicaciones de Correos, mediante los mecanismos de integración estandarizados en Correos, descritos a continuación:
    a. API (REST y SOAP)
    b. Mensajería asíncrona mediante colas MQ
    c. Intercambio de ficheros con grandes volúmenes de datos (SFTP, FTPS).
7. Los desarrollos que se realicen no cumpliendo estos requisitos, con otras pilas tecnológicas o sin seguir las buenas prácticas de desarrollo en Correos, tendrán que ser adaptados por el adjudicatario y adecuados a la arquitectura de Correos, antes de ser desplegados en las plataformas corporativas.
8. Requisitos de ICDC. El proveedor debe utilizar el sistema de control de versiones basado en Git para la gestión del ciclo de vida del código fuente y los artefactos, garantizando:
    a. Repositorio Centralizado
        i. El código deberá alojarse en el repositorio Git corporativo designado por Correos.
    b. Estrategia de Branching
        i. Se deberá seguir una estrategia de ramas adecuada y alineada a la utilizada en Correos (GitFlow)

    Debe colaborar con los equipos internos de Correos para adaptar, en caso de existir, o crear, en caso de no existir, un circuito de integración y entrega continua (CI/CD) que sea compatible con la infraestructura y los procesos de Correos, asegurando:
9. Despliegues Automatizados
    a. Se deben definir pipelines para entornos de desarrollo, pruebas y producción con controles de calidad.

b. Los despliegues en producción deberán planificarse en el Comité de Implantaciones y aprobarse la fecha de implantación por parte de Correos.
c. Los despliegues se podrán hacer:
    i. sin interrupción.
    ii. gradualmente activando de manera controlada una funcionalidad para ciertos usuarios.
d. Se deberán establecer mecanismos de rollback automatizados para revertir cambios en caso de fallos de manera:
    i. Completa
    ii. O desactivando funciones problemáticas en producción sin necesidad de hacer un despliegue nuevo.

10. Gestión de Configuración y Secretos:
    a. La configuración debe manejarse a través de archivos versionados y parámetros de entorno.
    b. No se deben almacenar credenciales en el código fuente; se deberá usar el sistema de gestión de secretos que Correos determine.
    c. Se debe garantizar la trazabilidad de los cambios en la configuración.
11. Control de Calidad
    a. El código deberá pasar las reglas de certificación de código a través de la herramienta corporativa, Kiuwan.
12. Automatización de Builds y Tests:
    a. La compilación del código deberá ejecutarse automáticamente en cada commit a ramas principales o de integración.
    b. Se deberán ejecutar pruebas unitarias, de integración y funcionales como parte del pipeline.
    c. Se deberán hacer pruebas de performance y escalabilidad, con cargas variables.
13. Seguridad
    a. El código deberá pasar las reglas de seguridad estática (SAST) para detectar errores de seguridad y bloquear la promoción de código con vulnerabilidades críticas.
    b. En los casos que aplique, las aplicaciones deberán ser sometidas a pruebas de seguridad en entornos controlados antes de su despliegue en producción mediante el análisis dinámico de seguridad (DAST) para detectar vulnerabilidades en la aplicación y su configuración.
    c. Se deberán integrar herramientas de análisis de seguridad en el pipeline (SAST/DAST), asegurando la generación de informes con trazabilidad de vulnerabilidades y acciones correctivas.
    d. Se deberá validar configuraciones de seguridad en la nube a traves de CSPM (Cloud Security Posture Management)
    e. El proveedor será responsable de corregir cualquier vulnerabilidad detectada antes de la aprobación del despliegue en producción.
14. Monitorización y observabilidad
    a. Los pipelines deben incluir mecanismos de logging y monitorización de ejecución.

b. En caso de fallo, se deberá generar alertas en tiempo real y mantener un registro accesible con los eventos relevantes.
c. Se debe realizar, en la medida de lo posible, la integración con las herramientas de observabilidad de Correos que permitan detectar anomalías en la ejecución o rendimiento anómalo en la ejecución de las aplicaciones.
d. En caso de que la integración con las herramientas de observabilidad de Correos no sea posible, el proveedor deberá proporcionar e integrar alguna herramienta APM (Application Performance Monitoring) compatible que ofrezca visibilidad y seguimiento detallado del rendimiento de las aplicaciones y la infraestructura.

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

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

Condiciones en materia de inteligencia artificial

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

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

(i) Deberá informar a CORREOS de forma completa y previa acerca de cualesquiera decisiones automatizadas que, en su caso, se adopten mediante el uso de sistemas o modelos de inteligencia artificial en el marco de los servicios, cuando dichas decisiones afecten a interesados cuyos datos personales sean tratados, incluyendo una explicación suficiente de la lógica aplicada, el funcionamiento general del sistema y las consecuencias previstas, en los términos exigidos por la normativa de protección de datos y el RIA.

(ii) Deberá abstenerse de tratar, mediante sistemas o modelos de inteligencia artificial, la información confidencial de CORREOS —y en particular los datos personales— de forma incompatible con las finalidades expresamente autorizadas por CORREOS y comunicadas en el marco contractual o mediante instrucciones documentadas.

(iii) No podrá generar ni inferir nuevos datos personales relativos a las categorías de interesados cuyos datos sean tratados por cuenta de CORREOS, salvo instrucción expresa, previa y por escrito de CORREOS, y siempre que dicha generación resulte conforme con la normativa aplicable en materia de protección de datos.

(iv) Deberá colaborar activamente con CORREOS en el cumplimiento de cualesquiera obligaciones que resulten de aplicación en materia de inteligencia artificial, protección de datos y seguridad de la información, en la medida en que guarden relación con el uso de sistemas o modelos de inteligencia artificial y el tratamiento de información confidencial, incluyendo, en su caso, evaluaciones de riesgos, evaluaciones de impacto, medidas de mitigación y atención a derechos de los interesados.

(v) Deberá comunicar a CORREOS, con carácter previo a su despliegue o utilización, la intención de implementar cualesquiera sistemas o modelos de inteligencia artificial distintos de los expresamente autorizados, cuando dichos sistemas o modelos vayan

a tratar información confidencial de CORREOS o datos personales por su cuenta. Dicha comunicación deberá incluir, al menos:

- identificación del sistema o modelo de inteligencia artificial;
- identificación del proveedor o desarrollador del sistema o modelo;
- documentación técnica relevante;
- finalidad prevista del sistema o modelo;
- clasificación o nivel de riesgo del sistema o modelo conforme al RIA u otra normativa aplicable.

(vi) No podrá utilizar, ni permitir que terceros utilicen, la información confidencial de CORREOS —incluidos los datos personales tratados por su cuenta— con fines de entrenamiento, desarrollo, ajuste o mejora de modelos de inteligencia artificial de uso general o de sistemas de inteligencia artificial, ya sean propios o de terceros, salvo autorización previa, expresa y por escrito de CORREOS, y únicamente cuando dicho uso resulte estrictamente necesario para la correcta ejecución de las instrucciones de CORREOS.

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

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

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

Medidas de seguridad en el uso de Inteligencia Artificial

Cumplimiento Normativo y Estándares

El Adjudicatario/Proveedor garantiza el cumplimiento de la normativa aplicable, incluyendo (sin carácter limitativo) el Reglamento (UE) 2016/679 (RGPD), incluyendo el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018, de Protección de Datos

Personales y garantía de los derechos digitales (LOPDGDD), el Esquema Nacional de Seguridad (ENS), la normativa sectorial que resulte de aplicación y el Reglamento Europeo de Inteligencia Artificial (AI Act), en su versión vigente y aplicable al caso concreto.

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

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

Directrices generales de seguridad

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

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

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

CORREOS tendrá derecho a auditar, directamente o mediante un tercero independiente, los procesos y controles del Adjudicatario/Proveedor relacionados con el sistema de IA, incluyendo datos de entrenamiento, validación, seguridad y cumplimiento, con preaviso razonable y sin acceso a secretos industriales no estrictamente necesarios.

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

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

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

Otras consideraciones de seguridad:

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

Control de acceso, uso adecuado y limitaciones

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

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

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

Los siguientes usos para la IA se consideran prohibidos:

- Manipulación subliminal del comportamiento de una persona que tenga por objeto o efecto causar daños físicos o psicológicos a dicha persona o a terceros.
- Explotación de las vulnerabilidades de grupos sociales o personas en situación de especial vulnerabilidad, con el fin de manipular su comportamiento de manera que pueda causarles perjuicios a ellos mismos o a terceros.
- Evaluación, clasificación o puntuación de individuos o grupos (social scoring) basada en su comportamiento social o en características personales, ya sean conocidas, inferidas o predichas.
- Identificación biométrica remota en tiempo real en espacios de acceso público, salvo en los supuestos expresamente autorizados por una base jurídica previa.

- Predicción del riesgo de que una persona cometa un delito basado exclusiva o principalmente en el análisis de su perfil, características personales o patrones de comportamiento.
- Reconocimiento, inferencia o alteración de las emociones de personas en el ámbito laboral o en centros educativos, salvo cuando el uso del sistema esté debidamente justificado por razones médicas o de seguridad.