



PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA SOLUCIÓN DE RELAY Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL AYUNTAMIENTO DE PAMPLONA (Exp. 509)

El objeto de este Pliego es el establecimiento de las especificaciones técnicas con arreglo a las cuales ha de llevarse a cabo la contratación de una solución en la nube que realice las funciones de relay de correo electrónico y de protección del mismo para uso del Ayuntamiento de Pamplona (Expediente nº 509).

Con la mera presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

1. OBJETO DEL CONTRATO Y ALCANCE

El objeto del presente contrato es la prestación en formato nube de servicios de relay y de protección de correo electrónico para el Ayuntamiento de Pamplona.

Dado que a día de hoy el Ayuntamiento de Pamplona dispone de un appliance que proporciona estas funcionalidades on premise, el contrato incluye la migración de estos servicios a la nube. También a día de hoy, el Ayuntamiento dispone de servidor de correo electrónico propio en modalidad on premise. En caso de que el Ayuntamiento de Pamplona decidiera migrar el servicio de correo electrónico a formato nube durante el periodo de vigencia del contrato, el alcance del mismo incluirá también los cambios necesarios en el servicio para adaptarse a esta migración.

Dentro del alcance del contrato estarán incluidas las adquisiciones o pagos por uso de medios físicos, licencias, suscripciones, etc. necesarias para garantizar todas las funcionalidades deseadas, así como la resolución de cualquier incidencia que se presente para garantizar el correcto funcionamiento del servicio en todo momento. Los plazos de resolución de incidencias, así como las funcionalidades deseadas para el sistema se detallan más adelante dentro de este mismo pliego.

El alcance del contrato incluirá finalmente formación en la solución y apoyo experto a la explotación de la misma a fin de que los técnicos designados por el Ayuntamiento de Pamplona dispongan de la información y conocimientos necesarios tanto para su funcionamiento diario como para analizar información recogida por la solución y/o implantar cambios.

2. CONTEXTO

Actualmente el Ayuntamiento de Pamplona cuenta con una solución de relay de correo electrónico Cisco Ironport, redundada con dos appliances físicos ESA-C390-K9. Sobre esta plataforma se encuentra activo un Bundle ESA Inbound Essentials (Antispam, Antivirus, Outbreak Filters) para entre 1000 y 1999 usuarios. Esta solución de relay y protección actúa sobre correo enviado y recibido desde un servidor Microsoft Exchange 2016 propiedad del Ayuntamiento de Pamplona y ubicado on premise en CPDs municipales. Esta solución de relay y protección es la que deberá ser sustituida por la que es objeto de este contrato, y el adjudicatario deberá migrar los servicios desde esta solución a la contratada.



**ASOCIACIÓN NAVARRA DE
INFORMÁTICA MUNICIPAL, S.A.**

Avda. del Ejército, 2 – Planta 8 • 31002 PAMPLONA / IRUÑA • Tel. 948 420 800 • Fax: 948 420 808 • www.animsa.es





La gestión de presencia para correo electrónico se realiza a través de dominios y entradas DNS gestionados por técnicos designados por el Ayuntamiento de Pamplona. Actualmente, el correo entrante se dirige hacia infraestructura municipal, y el correo saliente se identifica con IPs públicas del Ayuntamiento de Pamplona. Se encuentran configurados registros SPF, DKIM y DMARC para identificar y firmar correo saliente y para poder evitar a futuro la suplantación del Ayuntamiento de Pamplona como remitente de correos. Dado que la resolución DNS está gestionada por técnicos designados por el Ayuntamiento, cualquier cambio en las entradas DNS existentes, así como nuevas entradas necesarias, deberá ser comunicado por el adjudicatario a estos técnicos con la suficiente antelación para coordinar los cambios con el resto de acciones necesarias para puesta en marcha, migración, modificación de servicios, y en general para cualquier necesidad que surja durante el periodo de duración de contrato para mantener los servicios y funcionalidades activos y en perfecto estado de funcionamiento.

3. CARACTERÍSTICAS GENERALES DE LA SOLUCIÓN

Ante el aumento continuo de ataques a los que se ven sometidas todas las organizaciones, es vital y por lo tanto requisito técnico mínimo que la solución adoptada tenga robustez y continuidad, eficacia contrastada en la defensa de ataques y proyección de futuro con previsión de actualización continua durante el periodo de vigencia del contrato para hacer frente a nuevos tipos de ataques.

Para poder valorar estos aspectos, las ofertas presentadas deberán indicar para las soluciones ofertadas los siguientes aspectos:

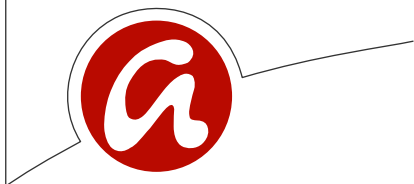
- Diseño general de la arquitectura de la solución en la nube, indicando mecanismos de redundancia o alta disponibilidad.
- Valoración de la solución de acuerdo a informes independientes de los 3 últimos años (tales como Gartner, Forrester-Wave o similares) en los que se analice tanto la calidad técnica de la solución como la posibilidad de implantarla eficazmente y/o estrategia de la misma.
- Certificación u homologación de la solución por parte del Centro Criptológico Nacional, o como mínimo algún tipo de aval de la seguridad de la solución por parte del CCN tal como una guía de utilización segura CCN-STIC de la solución propuesta.

Si bien se requieren ciertos mínimos (debe existir valoración de la solución por parte de informes independientes y algún tipo de reconocimiento de su validez por parte del CCN), se podrán también asignar puntos de valoración en base al grado de fiabilidad y eficacia reconocidos que la documentación aportada avale.

4. FUNCIONALIDADES DE LA SOLUCIÓN

La solución deberá prestarse en modo servicio en la nube y aplicará a todo el correo entrante y saliente del Ayuntamiento de Pamplona. Para ello, los técnicos designados por el Ayuntamiento de Pamplona modificarán las entradas DNS necesarias para encaminar el correo entrante hacia la infraestructura en la que se prestará el servicio, y dirigirán hacia ella el correo saliente. Las entradas DNS necesarias serán comunicadas a estos técnicos por el adjudicatario, responsabilizándose éste de la bondad de esa información.

Se detallan a continuación las diferentes funcionalidades concretas que deberán tener las soluciones ofertadas, indicando los aspectos sujetos a valoración.



4.1. Autenticación y verificación de correo entrante y saliente

Cada vez más proveedores de correo electrónico exigen una autenticación del correo recibido, mediante mecanismos como SPF, DKIM o DMARC. Se implantarán como mínimo estos 3 mecanismos tanto en entrada como en salida, es decir, se verificará la autenticidad del correo entrante y sus remitentes en base a estos tres mecanismos, y se aplicarán al correo saliente. Para esto último, el adjudicatario deberá indicar a los técnicos designados por el Ayuntamiento las entradas DNS que éstos deban configurar, responsabilizándose el adjudicatario de la bondad de la información suministrada a tal efecto. Bajo petición municipal, se podrán establecer excepciones a la aplicación de estos mecanismos de verificación en el correo entrante o saliente.

Se podrán valorar otros mecanismos de autenticación y verificación de correo entrante y saliente, así como las diferentes medidas que se puedan tomar con respecto al correo entrante en función del resultado de la aplicación de todos los mecanismos presentes en la solución ofertada para este fin. Entre otros aspectos, se podrán valorar todos los mecanismos que aporte la solución a fin de evitar suplantación de identidades, tanto en correo entrante como saliente.

4.2. Protección ante spam y phishing genéricos en correo entrante

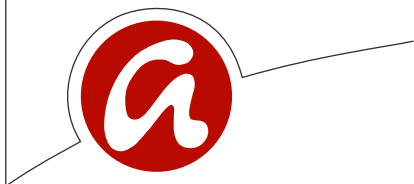
La solución deberá contar con protección ante envíos genéricos de spam y phishing en el correo entrante. Para ello, deberá contar con listas blancas y/o negras automáticamente actualizadas de remitentes conocidos de spam y phishing, o medios equivalentes o superiores para reconocer este tipo de correos recibidos. Se podrán parametrizar las acciones a tomar sobre el correo entrante así identificado como no deseado, tales como eliminación, puesta en cuarentena, marcado, etc., así como configurar excepciones a las listas blancas y/o negras para excluir y/o permitir remitentes particulares.

Se podrán valorar otros mecanismos presentes en la solución para proteger el correo entrante ante este tipo de envíos genéricos no deseados.

4.3. Protección ante ficheros y enlaces adjuntos en correo entrante

La inclusión de ficheros o enlaces infectados o maliciosos en correo electrónico es un vector de ataque cada vez más presente. La solución deberá proteger el correo municipal frente a este tipo de amenazas, incluyendo análisis tanto basados en firmas o hash como mediante sandboxing de los ficheros adjuntos o enlaces incluidos en correo electrónico entrante. Se describirán en la solución los mecanismos presentes en la solución a tal efecto, distinguiendo los basados en firmas o hashes (que deberán estar continuamente actualizados para reconocer ataques existentes) y los que usen técnicas de sandboxing o similares. La propuesta deberá detallar frecuencia de actualización de listas de firmas y hashes, así como entornos de sandboxing utilizados. Deberá asimismo describir las diferentes acciones que se puedan realizar (eliminación de fichero, puesta en cuarentena, reenvío condicional o con marcado, ...) y las opciones de parametrización de estas acciones según el resultado del análisis, así como la posibilidad si existe de configurar excepciones tanto positivas como negativas (por ejemplo, eliminar todo fichero adjunto de tipo .exe, o reenviar los ficheros de tipo .pdf que vengan de una lista de remitentes conocidos).

Se valorarán tanto los mecanismos presentes para protección ante ficheros y enlaces infectados o maliciosos como la capacidad de parametrizar dichos mecanismos.



4.4. Protección ante otras amenazas avanzadas

Utilizando el correo electrónico como vector de entrada existen en la actualidad múltiples ataques que sin duda aumentarán con el tiempo. Al efecto de proteger el correo corporativo de estas amenazas, se podrán valorar otras protecciones ante amenazas tales como robo o exfiltración de datos sensibles y/o credenciales, ataques dirigidos persistentes que utilicen el correo electrónico como uno de sus componentes, etc. Las ofertas deberán detallar las protecciones frente a este tipo de amenazas, mecanismos involucrados y parametrización disponible de los mismos.

4.5. Información y visibilidad

Toda la actividad de la solución deberá quedar registrada de forma que pueda ser consultada o analizada por los técnicos designados por el Ayuntamiento. Esto incluirá al menos log de cada correo entrante o saliente indicando sus parámetros principales (remitente, destinatario, asunto, fecha y hora de envío o recepción, presencia de adjuntos,...), análisis realizado y resultado del mismo (por ejemplo presencia de archivo inocuo o de enlace a web atacante, verificación o no del correo a través de SPF, DKIM o DMARC, etc.), acción tomada sobre el correo (rechazo, eliminación, cuarentena, reenvío,...) y regla o reglas que se han aplicado para decidir la acción a ejecutarse.

Estos registros de actividad deberán ser visibles para los técnicos municipales a través de herramientas de gestión descritas más adelante, debiendo también ser exportables en formatos estándar hacia herramientas de tipo syslog o SIEM para su tratamiento y/o correlación con otras fuentes de información municipales. La propuesta debe incluir esta posibilidad de exportación de información detallando la manera de hacerlo y formatos disponibles, aunque no necesariamente realizar la correlación de información con otras fuentes.

Uno de los propósitos del registro de actividad es ofrecer al Ayuntamiento una visibilidad lo más completa posible de la actividad, amenazas, riesgos y ataques sufridos con el correo electrónico como vector en entrada. Para ello, se valorará el que la solución proporcione información (posiblemente tratada dentro de la propia solución) que ayude a tener esta visibilidad, indicando datos tales como tipos de ataques más frecuentes, cuentas de correo más atacadas, ataques sufridos por usuarios concretos (por ejemplo miembros del Pleno de la Corporación municipal o personas con cargos y/o funciones específicos dentro del Ayuntamiento) y otros datos similares, así como cualquier otra información bruta o tratada que pueda ser de interés para el Ayuntamiento de Pamplona de cara a conocer, prevenir o protegerse más eficientemente de los ataques más susceptibles de sufrirse.

4.6. Herramientas de gestión de la solución

El adjudicatario deberá poner a disposición de los técnicos que el Ayuntamiento designe herramientas de gestión de la solución. A través de estas herramientas, los técnicos podrán realizar acciones rutinarias de revisión de configuración y reglas de la solución, modificación de las mismas (configuración de excepciones y/o acciones a alguno de los mecanismos de protección presentes), acceso a la información recabada por la solución para su análisis, búsquedas de correo entrante y saliente gestionado por la solución en base a diferentes parámetros (tales como remitente, destinatario, asunto, presencia o no de adjuntos, etc.). Los resultados de las búsquedas deberán ser exportables en formatos tratables electrónicamente (por ejemplo ficheros de tipo .csv).

Se valorará tanto la ergonomía en el uso como el grado de autonomía en la gestión y la visibilidad proporcionadas por la herramientas de gestión, para lo que cada oferta deberá incluir descripción de las mismas incluyendo capturas de pantalla para las diferentes acciones y configuraciones que se puedan realizar incluyendo parametrización de protecciones y establecimiento de excepciones, ejemplos de búsquedas y listado de parámetros en base a los que se puedan filtrar éstas, y ejemplos y/o capturas de pantalla de cualquier información bruta o tratada que la solución pueda proveer.



5. TAREAS ENCOMENDADAS AL ADJUDICATARIO

Para la correcta ejecución del contrato, el adjudicatario deberá realizar las tareas que se desarrollan más adelante. En su oferta, cada licitador deberá detallar los medios materiales y humanos adscritos al cumplimiento de cada parte del contrato, así como los mecanismos y procedimientos implantados para la correcta ejecución de cada parte del objeto y alcance del mismo.

Para la comunicación de incidencias y/o para cualquier intercambio de información necesaria para el cumplimiento de objeto y alcance del contrato, el Ayuntamiento de Pamplona accederá a los servicios prestados por el adjudicatario a través de un punto único de contacto, pudiendo utilizarse para ello un mínimo de dos canales, siendo uno de ellos un número de teléfono, y al menos uno electrónico (correo electrónico o formulario web). A través de este punto único de contacto, se encaminarán todas las incidencias y peticiones de ejecución de tareas incluidas en el contrato.

5.1. Migración de los servicios

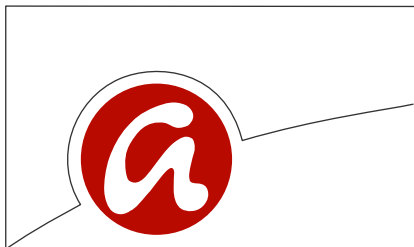
Como se detalla en el apartado de contexto, el Ayuntamiento de Pamplona dispone de solución de relay y protección de correo electrónico Cisco Ironport on premise, conformada por dos appliances físicos ESA-C390-K9 sobre los que está activo un paquete de protecciones Bundle ESA Inbound Essentials. Como parte del contrato, el adjudicatario deberá realizar la migración de los servicios de relay y protección de correo electrónico desde esta solución on premise a la solución en la nube contratada.

La migración de los servicios debe incluir en un primer momento la configuración de la solución ofertada manteniendo al menos las funcionalidades actualmente implantadas en la solución on premise en uso a día de hoy, y posteriormente el traslado de los servicios de modalidad on premise a modalidad nube. Otras funcionalidades incluidas en la oferta que no se hallen activas en la solución actual podrán ponerse en marcha tanto antes como después del traslado de los servicios a la nube, siempre en un plazo prudencial tras el inicio del contrato.

A fin de garantizar el éxito de la migración con el menor tiempo posible de caída de los servicios y con la máxima seguridad, el licitador deberá indicar en su oferta un procedimiento de migración donde detallará los medios y mecanismos empleados en la preparación y traslado de los servicios, describiendo fases, tareas, responsables de las mismas, y medios humanos y materiales empleados. Se deberá indicar explícitamente los puntos del proceso de migración en los que será necesaria la participación directa de los técnicos municipales y en qué acciones concretas deberían realizar, así como los momentos en los que pueda haber corte o riesgo de corte en los servicios y de las acciones tomadas para minimizar su duración e impacto. Se valorará la adecuación de mecanismos y medios propuestos en este plan de migración, así como la confianza que se derive del mismo en cuanto al éxito del proceso con afección mínima a los servicios de correo electrónico y protección del mismo.

El adjudicatario se compromete a realizar el traslado de los servicios a la nube en un plazo no superior a 15 días naturales tras la firma del contrato con las mismas funcionalidades que la solución on premise actual. El adjudicatario será responsable de todos los perjuicios ocasionados por un incorrecto traslado de estas funcionalidades. Asimismo, el adjudicatario se compromete a tener plenamente configurada la solución con todas las funcionalidades ofertadas en un plazo no superior a 1 mes natural tras el traslado de los servicios a la nube.

En este sentido, se definen las siguientes infracciones:



Infraacción	Leve	Grave	Muy grave
Retraso en el traslado de servicios	5 días	10 días	15 días
Retraso en la puesta en marcha de funcionalidades plenas	15 días	1 mes	2 meses

5.2. Mantenimiento de la vigencia y funcionamiento de la solución

El adjudicatario deberá velar en todo momento del contrato por la vigencia y funcionamiento de la solución completa. Esto incluye la garantía de aprovisionamiento de hardware y software en la nube para su correcto funcionamiento, así como la contratación y vigencia de cualquier licencia o suscripción necesarias.

El adjudicatario será responsable de todo perjuicio derivado del no cumplimiento de estos requisitos.

5.3. Mantenimiento correctivo de la solución

La solución debe estar activa y con plenas funcionalidades en todo momento. Para ello, la oferta deberá incluir los medios y mecanismos implantados para garantizar este punto, específicamente plan de continuidad del servicio y plan de recuperación ante desastres.

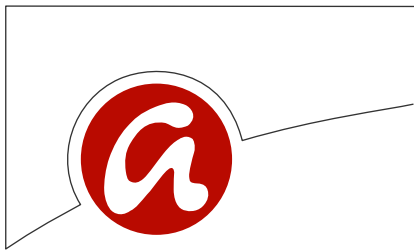
Cuando bien el adjudicatario a través de acciones de monitorización o mantenimiento preventivo, bien los técnicos municipales observen una deficiencia en el funcionamiento de la solución, el adjudicatario deberá resolverla cuanto antes a fin de garantizar la continuidad del servicio. Se define como incidencia a todo funcionamiento anómalo o inadecuado de la solución, o de cualquiera de sus funcionalidades. Las incidencias se pueden clasificar respecto a su criticidad:

- Incidencias de criticidad máxima: Aquellas que afecten al servicio de recepción y envío de correo electrónico en su totalidad.
- Incidencias de criticidad alta: Aquellas que afecten a servicios esenciales para la seguridad en el servicio de correo electrónico.
- Incidencias de criticidad media: Aquellas que afecten a usuarios concretos, o a funcionalidades de gestión, pero no de envío o recepción de correo, o de seguridad en el correo electrónico.

Para cada tipo de incidencia se establecen los siguientes plazos máximos de respuesta y de resolución:

Criticidad	Plazo de respuesta	Plazo de resolución
Máxima	1 hora	12 horas
Alta	2 horas	24 horas
Media	8 horas	5 días

En el supuesto de que la resolución de una incidencia, a pesar de dedicar el adjudicatario todos los esfuerzos y medios posibles, no sea viable en los plazos establecidos, se acordará entre adjudicatario y ANIMSA un plan de mínimos para resolver parcialmente y aminorar el efecto de la misma hasta su resolución, quedando constancia por escrito de dicho plan. La inviabilidad nunca podrá referirse a aprovisionamiento por parte del adjudicatario de hardware o software en la nube, ni a mantenimiento en vigencia de licencias o suscripciones necesarias.



El incumplimiento por parte del adjudicatario de los plazos de resolución contratados, salvo cuando causas fehacientes y ajenas al control del adjudicatario lo hagan materialmente imposible, constituye una infracción, cuya severidad depende tanto del tipo de actuación, de la criticidad caso de tratarse de una incidencia, y del tiempo transcurrido desde el plazo máximo de respuesta o de resolución, hasta que la respuesta o la resolución se produce. Se tipifican las siguientes infracciones en forma de retrasos en plazo de resolución para diferentes severidades de infracción (expresados en porcentaje del correspondiente plazo máximo de resolución contratado):

Criticidad	Leve	Grave	Muy grave
Máxima	<100%	>100% <200%	>200%
Alta	<100%	>100% <300%	>300%
Media	<100%	>100% <300%	>300%

Las anteriores infracciones suponen los plazos máximos para la prestación del servicio de mantenimiento correctivo contratado, y tienen el carácter de acuerdo de nivel de servicio.

Cada licitador deberá describir en su oferta los medios materiales y humanos adscritos, así como los mecanismos y procedimientos adoptados para garantizar el cumplimiento de estos acuerdos de nivel de servicio, valorándose su adecuación y la garantía de funcionamiento continuo de la solución que proporcionen.

5.4. Mantenimiento preventivo y proactivo de la solución

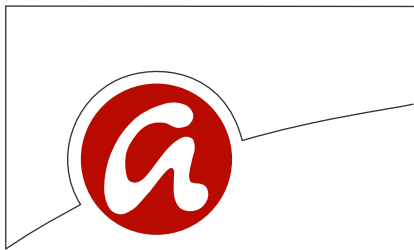
Cada licitador podrá proponer en su oferta diferentes acciones de mantenimiento preventivo y proactivo, destinadas a garantizar en la medida de lo posible que no se produzcan interrupciones en el servicio o incidencias en su funcionamiento. Se podrán valorar estas medidas en cuanto se considere que tienen un impacto real en la prevención de cortes e incidencias en el servicio. Las medidas podrán incluir monitorización de la solución y de su funcionamiento, incluyendo el hardware aprovisionado para ello, así como toma de datos o análisis de logs y/o forense para evaluar la eficacia de la parametrización de la solución a la hora de repeler ataques y amenazas.

Cuando fruto de acciones de mantenimiento preventivo y proactivo el adjudicatario descubra la necesidad de modificar el aprovisionamiento de medios en la nube para el cumplimiento del contrato, deberá realizarlo a su cargo. El adjudicatario será responsable de los perjuicios derivados de la no adopción de estas medidas.

Cuando fruto de acciones de mantenimiento preventivo o proactivo se descubra la necesidad o conveniencia de modificar la configuración y/o parametrización de la solución, se informará de este punto a los técnicos designados por el Ayuntamiento para la coordinación y adopción (posiblemente conjunta) de medidas remediadoras si procedieren.

5.5. Formación

El adjudicatario deberá formar a los técnicos designados por el Ayuntamiento de Pamplona en la gestión de la solución ofertada. La formación deberá ser suficiente para la realización de las tareas diarias de gestión de la solución, incluyendo la creación o modificación de reglas genéricas de funcionamiento, troubleshooting básico, análisis de la información recopilada por la solución, etc. A tal efecto, cada oferta deberá incluir un plan de formación para los técnicos, indicando objetivos, alcance, duración y metodología a emplearse. Se valorará el grado de confianza de que cuando termine la formación, los técnicos designados por el Ayuntamiento de Pamplona estén capacitados para la realización de estas tareas diarias de gestión de la solución.



A efectos de acuerdos de nivel de servicio, se entiende que la formación deberá darse en el mismo plazo previsto para la implantación de la funcionalidad plena de la solución ofertada. Se entenderá por lo tanto que se incumple el requisito de implantación plena de la solución si la formación no se ha prestado en el plazo establecido para ello, aplicándose las infracciones y sanciones previstas para ello en el apartado correspondiente de este Pliego.

5.6. Soporte experto

El adjudicatario deberá realizar tareas de soporte experto, realizando tareas de gestión complejas que requieran de conocimientos o experiencia que los técnicos designados por el Ayuntamiento no posean. Deberá asimismo prestar tareas de apoyo ante inclusión o variación de los servicios y funcionalidades actuales, debiendo estar incluidas en la oferta todas aquellas actuaciones que no impliquen la adquisición de nuevas licencias o suscripción a nuevos servicios. Este soporte experto podrá limitarse en algunos casos al envío de información (manuales de buenas prácticas o similares) y en otros requerirá de la actuación del adjudicatario. Si es necesario, el adjudicatario deberá poder acceder a los servicios de soporte del fabricante, punto que deberá justificarse mediante compromiso del fabricante de mantener y dar soporte a la tecnología componente de la solución durante el periodo de vigencia del contrato.

5.7. Acciones en caso de migrarse el correo electrónico municipal a formato nube

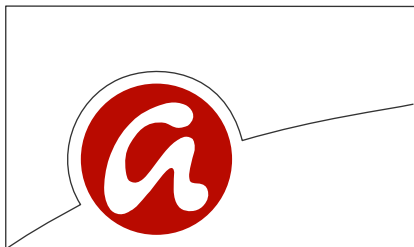
Es posible que, durante el periodo de vigencia del contrato, el Ayuntamiento de Pamplona decida migrar el servicio de correo electrónico de su formato actual on premise a formato en la nube. En caso de producirse este cambio, el adjudicatario deberá realizar todas las tareas oportunas para garantizar el servicio contratado durante y después de la migración, coordinándose cuando sea necesario con los técnicos designados por el Ayuntamiento y con el adjudicatario (si lo hubiere) de ejecutar un posible contrato de migración de servicios de correo a la nube. Estas acciones correrían a cargo del adjudicatario, entendiéndose que estarán incluidas en el precio ofertado por el adjudicatario.

6. FORMAS DE SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DE LAS CONDICIONES

El órgano de contratación debe designar a una persona que asuma el control y la coordinación de la ejecución contractual con la empresa contratista a fin de tratar directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego.

La empresa contratista debe designar a una persona responsable de la gestión de la ejecución del contrato, que deberá garantizar la calidad de la prestación objeto de este pliego, y tratar directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en el mismo pliego con la persona interlocutora designada por el órgano de contratación.

Dentro de las acciones de seguimiento y control del contrato, se incluirá una reunión de seguimiento con periodicidad al menos semestral, en la que adjudicatario aportará un informe resumiendo todas las actuaciones que hayan sucedido en el periodo que concluye, incluyendo finalización de actuaciones iniciadas en periodos anteriores, inicio de actuaciones todavía no concluidas, y actuaciones iniciadas y finalizadas desde la última reunión. El informe incluirá, cuando proceda, resultados de acciones preventivas o proactivas que hayan requerido o requieran de acciones remediadoras. Se consensuará el contenido de dicho informe y las actuaciones a realizarse en periodos sucesivos.



7. DOCUMENTACIÓN TÉCNICA QUE DEBEN APORTAR LAS EMPRESAS LICITADORAS

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si ésta se convierte en la adjudicataria.

Con el fin de acreditar el cumplimiento de cada especificación técnica exigida en este pliego, tal y como se prevé en la solvencia técnica (cláusula H del Pliego de Condiciones Particulares), la empresa que resulte adjudicataria deberá aportar certificado expedido por el fabricante de que el equipamiento hardware se encuentra bajo contrato de soporte, así como de que se encuentran contratadas las suscripciones y licencias necesarias durante el periodo de vigencia del contrato.

Pliego Prescripciones Técnicas Relay Pamplona (509) - SEFYCU 59180

Puede acceder a este documento en formato PDF - PAdES y comprobar su autenticidad en la Sede Electrónica usando el código CSV siguiente:



URL (dirección en Internet) de la Sede Electrónica: <https://sedeelectronica.animsa.es/>

Código Seguro de Verificación (CSV): FFCA AADW LUAM 4EZU H9L4

En dicha dirección puede obtener más información técnica sobre el proceso de firma, así como descargar las firmas y sellos en formato XAdES correspondientes.

Resumen de firmas y/o sellos electrónicos de este documento

Huella del documento para el firmante	Texto de la firma	Datos adicionales de la firma
	MARÍA LUCÍA SORBET BARRICARTE JEFATURA JURIDICO Y CONTRATACIONES	Firma electrónica avanzada - FNMT-RCM - 26/04/2024 10:40 MARIA LUCIA SORBET BARRICARTE
	DANIEL LASAOSA MEDARDE Jefatura Comunicaciones	Firma electrónica avanzada - FNMT-RCM - 26/04/2024 10:51 DANIEL LASAOSA MEDARDE
	JOSE MARIA AGUINAGA PEREZ Gerente	Firma electrónica avanzada - FNMT-RCM - 26/04/2024 12:22 JOSE MARIA AGUINAGA PEREZ
	ANA ISABEL BURGUI ALDUNATE DIRECCIÓN AREA DE INFRAESTRUCTURAS	Firma electrónica avanzada - FNMT-RCM - 02/05/2024 8:08 ANA ISABEL BURGUI ALDUNATE
	MYRIAN LIZARBE CHOCARRO Directora Economico-Financiera	Firma electrónica avanzada - FNMT-RCM - 02/05/2024 8:52 MIRIAM LIZARBE CHOCARRO