PLIEGO DE PRESCRIPCIONES TÉCNICAS
MANTENIMIENTO DE LA SOLUCIÓN FORTINET PARA SEGURIDAD Y MOVILIDAD PARA EL AYUNTAMIENTO DE PAMPLONA (Exp.536)

El objeto de este Pliego es el establecimiento de las especificaciones técnicas con arreglo a las cuales ha de llevarse a cabo la contratación del mantenimiento de cortafuegos del Ayuntamiento de Pamplona.

1) DESCRIPCIÓN GENERAL DEL ALCANCE Y OBJETO DEL CONTRATO

El objeto del presente contrato es el mantenimiento de la solución de seguridad y movilidad basada en un ecosistema conformado por productos del fabricante Fortinet, y que es propiedad del Ayuntamiento de Pamplona.

El ecosistema consta de los siguientes elementos:

- Dos appliances Fortigate 601E con números de serie FG6H1ETB20902153 y FG6H1ETB20902418, dotados cada uno de las siguientes licencias:
  - Paquete UTM bundle Fortiguard con IPS, control de aplicaciones, antivirus, filtrado web, filtrado antispam.
  - 275 licencias de Fortitoken Mobile perpetuas (adquiridas antes de 2025).
- Una máquina virtual FortiAuthenticator, con número de serie FAC-VMTM26000856, dotada de las siguientes licencias:
  - 200 licencias de usuario, a las que se van a añadir próximamente 300 más que estarán activas al inicio del presente contrato.
  - 200 licencias de Fortitoken Mobile, a las que se van a añadir próximamente 200 más que estarán activas al inicio del presente contrato.
- Una solución FortiSASE, integrada con la infraestructura de seguridad corporativa, dotada de las siguientes licencias y componentes:
  - 50 licencias de usuario FortiSASE para acceso remoto seguro y acceso a aplicaciones corporativas mediante arquitectura SASE con número de serie FCTEMS8825015825
  - 2 licencias FC-10-F6H1E-662-02-12 (FortiGate-601E FortiSASE Secure Private Access Connector for SD-WAN), una por cada appliance FortiGate 601E, que proporcionan la conectividad segura entre la plataforma FortiSASE y la infraestructura de seguridad perimetral con números de serie FG6H1ETB20902153 y FG6H1ETB20902418.
  - Integración con la plataforma FortiAuthenticator para la autenticación centralizada de usuarios y la aplicación de mecanismos de autenticación multifactor (MFA) mediante FortiToken Mobile.

La solución FortiSASE se encuentra integrada con los dos equipos FortiGate 601E, que actúan como conectores de acceso privado a las aplicaciones y recursos corporativos, así como con la plataforma FortiAuthenticator para la validación de identidades y la gestión de la autenticación multifactor de los usuarios remotos.

Los dos appliances físicos Fortigate 601E, ubicados cada uno en uno de los dos CPDs municipales, están configurados en alta disponibilidad a través de VLANs propagadas por fibra óptica propia y con cuatro VDOMs definidos, de forma que en condiciones correctas de funcionamiento un VDOM reside en uno de los dos appliances, y los otros dos VDOMs en el otro, y en caso de fallo o caída de uno de los dos appliances, los cuatro VDOMs están activos en el appliance superviviente.

El alcance del presente contrato incluye:

- La renovación durante todo el periodo de vigencia del contrato del bundle UTM instalado, que expira el 31 de diciembre de 2026.
- El mantenimiento de los appliances físicos Fortigate y de la máquina virtual Fortiauthenticator durante todo el contrato, incluyendo reposición del material averiado y actualización de firmware para resolución de bugs o para acceso a nuevas funcionalidades o a mejoras en el funcionamiento que el fabricante publique.
- Cualquier acción necesaria para que las licencias, tanto las de usuario instaladas en la máquina virtual Fortiauthenticator, como las de Fortitoken Mobile instaladas tanto en los appliances Fortigate, como en la máquina virtual Fortiauthenticator, sigan en estado vigente y de buen funcionamiento y conserven (las que lo tienen) su carácter de licencias perpetuas.
- El mantenimiento de la solución FortiSASE durante todo el periodo de vigencia del contrato, incluyendo la renovación de las licencias Secure Private Access Connector, la renovación de las 50 licencias de usuario FortiSASE actualmente existentes y el suministro y mantenimiento durante el periodo de vigencia del contrato de otras 50 licencias de usuario FortiSASE adicionales (al inicio de la ejecución del contrato deberán encontrarse operativas un total de 100 licencias de usuario FortiSASE, resultantes de las 50 licencias existentes y de las 50 licencias adicionales incluidas en el alcance del presente contrato), así como también cualquier acción necesaria para que las licencias de usuario FortiSASE y las licencias Secure Private Access Connector permanezcan vigentes y operativas durante toda la duración del contrato, asegurando la continuidad del servicio y la correcta conectividad entre la plataforma FortiSASE y la infraestructura municipal. Dentro del alcance del contrato estará incluida también cualquier actuación necesaria para garantizar el correcto funcionamiento de la integración entre la plataforma FortiSASE, los appliances Fortigate 601E y la máquina virtual FortiAuthenticator.

  Las licencias suministradas y mantenidas deberán proporcionar, como mínimo, las funcionalidades actualmente desplegadas y operativas en el entorno del Ayuntamiento de Pamplona, no admitiéndose la sustitución por licencias o modalidades que impliquen pérdida de funcionalidades o degradación del servicio.
- Soporte experto para la explotación de todo el ecosistema con sus funcionalidades.
- Suministro de 200 licencias de usuario adicionales a instalarse en la máquina virtual Fortiauthenticator objeto de este contrato, y de 200 licencias Fortitoken Mobile adicionales a instalarse también en la máquina virtual Fortiauthenticator.

  Como resultado de las ampliaciones previstas y de los suministros incluidos en el presente contrato, la plataforma FortiAuthenticator deberá disponer durante la vigencia del mismo de un mínimo de 700 licencias de usuario y 600 licencias FortiToken Mobile.

2) PRESCRIPCIONES TÉCNICAS PARA LA PRESTACIÓN DEL SERVICIO DE MANTENIMIENTO DE SOLUCIÓN FORTINET PARA SEGURIDAD Y MOVILIDAD DEL AYUNTAMIENTO DE PAMPLONA

2.1) Descripción detallada de los servicios a prestar

Las actividades de mantenimiento a realizar durante el periodo de vigencia del contrato son las siguientes:

- Suministro de 200 licencias adicionales de usuario para Fortiauthenticator, 200 licencias de Fortitoken Mobile para Fortiauthenticator y 50 licencias adicionales de usuario FortiSASE.
- Reposición de material averiado. El adjudicatario deberá disponer de los medios propios o de los acuerdos necesarios con el fabricante que le permitan cumplir los plazos de resolución establecidos en el presente pliego, incluyendo la disponibilidad de equipamiento de sustitución temporal cuando resulte necesario.
- Resolución de averías, si es preciso incluyendo reposición de material averiado y/o desplazamiento de personal técnico a las instalaciones del Ayuntamiento de Pamplona.

- Mantenimiento de todas las licencias existentes y de nuevo suministro en vigencia, incluyendo tanto el bundle Fortiguard que incluye IPS, antivirus, filtrado web y anti-spam, como las 100 licencias de usuario FortiSASE (50 existentes y 50 nuevas) y las dos licencias FortiSASE Secure Private Access Connector asociadas a los appliances Fortigate 601E, las licencias de usuario instaladas en la máquina virtual Fortiauthenticator, como las licencias de Fortitoken Mobile instaladas en máquina virtual Fortiauthenticator y en appliances físicos Fortigate, prestando especial atención a que las instaladas en los appliances físicos Fortigate que tienen carácter de perpetuas mantengan dicho carácter durante y después del periodo de vigencia del contrato.
- Resolución de incidencias relacionadas con la integración entre FortiSASE, los appliances Fortigate 601E y la máquina virtual FortiAuthenticator, incluyendo aquellas derivadas de actualizaciones, cambios de versión, renovación de licencias o funcionamiento de los conectores Secure Private Access.
- Labores de mantenimiento preventivo, que pueden incluir, entre otras acciones, la monitorización y la realización de auditorías.
- Soporte experto a la explotación, incluyendo el asesoramiento y asistencia técnica durante implantación de nuevas funcionalidades bien de la propia red, bien soportadas a través de la red de comunicaciones.
- Gestión y seguimiento de incidencias ante el soporte oficial del fabricante Fortinet cuando resulte necesario para la resolución de averías, incidencias o problemas de funcionamiento de cualquiera de los componentes incluidos en el alcance del contrato.
- Entrega de documentación relacionada con las actuaciones realizadas dentro del marco del contrato.

Las condiciones técnicas ofertadas para estas tareas deberán ser presentadas bajo la forma de un Procedimiento de Actuación. Este Procedimiento deberá incluir toda la información necesaria para el acceso a los servicios contratados, la descripción de los medios materiales y humanos que empleará el adjudicatario para prestar dichos servicios, los plazos que deberá cumplir el adjudicatario, y la documentación a entregarse.

El Ayuntamiento de Pamplona accederá a los servicios de asistencia técnica y soporte 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 peticiones de mantenimiento y soporte experto contempladas en el contrato. Si es posible, se resolverán a través de este punto único de contacto aquellas solicitudes o incidencias de escasa complejidad, si bien se aceptarán y valorarán otras opciones o variantes que permitan un tratamiento más ágil, competente y eficiente de las incidencias y peticiones comunicadas.

El licitador deberá detallar en su Procedimiento de Actuación cuál será el tratamiento que seguirá cada incidencia o solicitud comunicada, detallando los medios que se involucrarán, y los tiempos a los que se comprometa para su resolución o respuesta.

Si el licitador lo estima conveniente para una mejor prestación del servicio, podrá proponer la sustitución de cualquier elemento hardware o software del ecosistema por otro del mismo tipo (es decir, no se puede proponer la sustitución de la máquina virtual Fortiauthenticator por un appliance físico, o la sustitución de una licencia perpetua por una temporal), de características iguales o superiores, y siempre incluido en el precio del contrato. Esta sustitución no deberá en ningún caso suponer ninguna pérdida de funcionalidad del sistema, así como de características y/o periodo de vigencia de las licencias que forman parte del mismo.

2.2) Acceso remoto a la infraestructura del Ayuntamiento de Pamplona y monitorización

El Ayuntamiento de Pamplona proveerá al adjudicatario de un método de acceso remoto a la red de comunicaciones, a través del cual personal del adjudicatario podrá acceder al ecosistema Fortinet para realizar tareas de monitorización y mantenimiento preventivo y correctivo. Con este acceso, se pretende facilitar al adjudicatario la prestación de los servicios, así como un tratamiento más ágil de las incidencias y de las solicitudes de información, apoyo y soporte. Cualquier otro método de acceso del que desee disponer el adjudicatario correrá a su cuenta, tanto en su establecimiento como en su mantenimiento, debiendo además ser previamente aprobado por el Ayuntamiento de Pamplona.

El adjudicatario deberá establecer un sistema automático de monitorización que registre las incidencias y comportamientos anormales del ecosistema Fortinet, e informe tanto a los técnicos de ANIMSA como a los técnicos del propio adjudicatario

de cualquier comportamiento que pueda constituir una incidencia. Se valorará el grado en que la monitorización permita detectar comportamientos anómalos susceptibles de producir caídas en el servicio, y que el licitador se comprometa a tratar alarmas producidas por este sistema de monitorización, como si se tratara de peticiones de mantenimiento realizadas por el personal del Ayuntamiento de Pamplona. Es decir, preferentemente, el adjudicatario se comprometerá a actuar al recibir alarmas de monitorización, sin necesidad de esperar comunicación por parte del Ayuntamiento de Pamplona.

Como mínimo, la monitorización deberá contemplar el estado de los appliances FortiGate, la correcta sincronización de la alta disponibilidad, el estado de los VDOMs, la utilización de recursos críticos, el estado de las VPNs y túneles de comunicación, la operatividad de FortiAuthenticator, el estado de integración con FortiSASE, la vigencia de certificados y la proximidad de vencimiento de licencias y suscripciones.

El Ayuntamiento de Pamplona pondrá a disposición del adjudicatario una cuenta de correo en los servidores corporativos del Ayuntamiento de Pamplona, de forma que procesos automáticos de monitorización puedan informar mediante correo electrónico de averías o incidencias, tanto a técnicos del adjudicatario, como a los técnicos de ANIMSA responsables del servicio, a fin de minimizar el tiempo entre una incidencia, y su detección por el personal que vaya a tratarla. Cualquier otro método de información al adjudicatario por parte de los procesos automáticos de monitorización correrá a cargo de éste, tanto en su establecimiento como en su mantenimiento, debiendo además ser previamente aprobado por el Ayuntamiento de Pamplona.

2.3) Clasificación de incidencias y solicitudes y plazos de respuesta y resolución

Se definen en cuanto a su tipo tres clases de servicio que el adjudicatario deberá realizar en el marco del contrato:

- Incidencias: reporte de todo funcionamiento anómalo o inadecuado del ecosistema en su conjunto, de cualquiera de sus elementos componentes, o de cualquiera de las funcionalidades que provee.
- Solicitud de asistencia técnica: petición de asesoramiento para la realización de cualquier tarea que, sin constituir parte de la resolución de una incidencia, implique un grado de dificultad o de conocimiento que hagan que no sea abordable directamente por personal de ANIMSA, bien por falta de medios o por falta de formación. Una solicitud de asistencia puede precisar para su resolución tanto de suministro de información, como de actuaciones por parte del adjudicatario (por ejemplo, cambios en las configuraciones de los equipos para integración de alguna funcionalidad nueva). No podrá conllevar sin embargo el suministro de ningún equipamiento o licencia nuevos.
- Solicitud de soporte experto: petición de información sobre cualquier tema relacionado con el funcionamiento del ecosistema o sus funcionalidades, que sea desconocida por parte del personal de ANIMSA. La resolución de una solicitud de soporte experto será siempre la transmisión de información al personal de ANIMSA por parte del adjudicatario (por ejemplo, envío de “white papers” acerca de configuraciones específicas del equipamiento o de las funcionalidades licenciadas).

A su vez, las incidencias se pueden clasificar respecto a su criticidad, teniendo en cuenta que el ecosistema es un elemento esencial, ya que sin él no es posible la comunicación entre la red del Ayuntamiento y el exterior.

- Incidencias de criticidad máxima: Aquellas que supongan una paralización total o parcial del servicio por caída o funcionamiento anómalo del ecosistema, especialmente si se ven afectados ambos appliances Fortigate o la máquina virtual Fortiauthenticator.
- Incidencias de criticidad alta: Aquellas que afecten a la redundancia del sistema pero no resulten en pérdida de servicio (por ejemplo caída de uno de los dos appliance Fortigate 601E), o resulten en pérdida de alguno de las funcionalidades esenciales (por ejemplo, fallos en la autenticación de usuarios remotos).
- Incidencias de criticidad media: Aquellas que no produzcan caída ni del servicio ni de ninguno de los elementos componentes del ecosistema, pero resulten en funcionalidades reducidas o prestaciones insuficientes (por ejemplo, ausencia de la funcionalidad de gestión de ancho de banda, lentitud general en la navegación atribuible al cortafuegos o similares)

Para una incidencia o una solicitud de asistencia técnica, se definen:

- Plazo de respuesta: el tiempo transcurrido desde la comunicación al adjudicatario de la incidencia o solicitud (bien por medios del Ayuntamiento de Pamplona o del adjudicatario, incluidos los sistemas automáticos de monitorización) hasta que un técnico especialista asignado por el adjudicatario se pone en contacto con personal técnico de ANIMSA conocedor de la incidencia o solicitud.
- Plazo de resolución para una incidencia: el tiempo transcurrido desde la comunicación al adjudicatario de la incidencia (bien por medios del Ayuntamiento de Pamplona o del adjudicatario, incluidos los sistemas automáticos de monitorización) hasta que el ecosistema y todas sus funcionalidades vuelven a comportarse de forma adecuada.
- Plazo de resolución para una solicitud de asistencia: el tiempo transcurrido desde la comunicación al adjudicatario de la solicitud de asistencia, hasta que ésta haya sido atendida, y aprobadas las actuaciones realizadas y/o los entregables correspondientes.
- Plazo de resolución para una solicitud de soporte experto: el tiempo transcurrido desde la comunicación al adjudicatario de la solicitud de soporte experto, hasta que la información pertinente y suficiente ha sido entregada a los técnicos de ANIMSA.

Se establecen los siguientes plazos máximos de respuesta y de resolución:

Tipo	Criticidad	Plazo de respuesta	Plazo de resolución
Incidencia	Máxima	1 hora	12 horas
	Alta	2 horas	24 horas
	Media	4 horas	7 días
Solicitud de asistencia	-	7 días	Variable
Solicitud de soporte	-	4 días	1 semana

En el caso de solicitudes de asistencia, el plazo de resolución se acordará entre ANIMSA y adjudicatario, quedando reflejado en un plan de acción consensuado que detallará las tareas, plazos y responsables para llevarlo a cabo.

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 sustitución de material averiado, que siempre deberá realizarse dentro de los plazos establecidos.

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:

Tipo	Criticidad	Leve	Grave	Muy grave
Incidencia	Máxima	>plazo máximo <2 x plazo máximo	>2 x plazo máximo <3 x plazo máximo	>3 x plazo máximo
	Alta	>plazo máximo <2 x plazo máximo	>2 x plazo máximo <4 x plazo máximo	>4 x plazo máximo
	Media	>plazo máximo <2 x plazo máximo	>2 x plazo máximo <4 x plazo máximo	>4 x plazo máximo

Solicitud de asistencia	-	>plazo máximo <2 x plazo máximo	>2 x plazo máximo <4 x plazo máximo	>4 x plazo máximo
Solicitud de soporte	-	>plazo máximo <2 x plazo máximo	>2 x plazo máximo <4 x plazo máximo	>4 x plazo máximo

Plazos de resolución reales que resultan en infracciones, para diferentes severidades de infracción, expresados en múltiplos del correspondiente plazo máximo de resolución contratado

2.4) Mantenimiento correctivo

El mantenimiento correctivo incluirá toda actuación necesaria para garantizar el adecuado comportamiento del cortafuegos y todas las funcionalidades licenciadas, incluso reposición de equipamiento averiado, así como resolución de bugs de software o firmware necesario para su correcto funcionamiento, aplicándose para ello los criterios y plazos recogidos en el apartado anterior.

2.5) Mantenimiento preventivo

El mantenimiento preventivo deberá incluir la monitorización del ecosistema Fortinet objeto de este contrato, en los términos que cada licitador detallará en su oferta y que podrán ser objeto de valoración. Fruto de los datos obtenidos de esta monitorización, así como de otros datos sobre el funcionamiento del cortafuegos (incidencias, comportamientos anómalos, etc.), el adjudicatario incluirá en la documentación entregada periódicamente como parte del seguimiento del contrato, sugerencias para optimizar el funcionamiento del mismo y/o de sus funcionalidades licenciadas. Se valorará el que con periodicidad anual a partir de que la solución esté en funcionamiento, el adjudicatario realice una auditoría cuyos entregables incluyan aviso de posibles problemas futuros, así como sugerencia de actuaciones tanto para evitar estos problemas como para optimizar el funcionamiento general del cortafuegos.

2.6) Soporte experto para la explotación del cortafuegos, necesidades previsibles durante el periodo de vigencia del contrato y evolución tecnológica

Los appliances Fortigate 601E tienen a día de hoy configurados 4 VDOMs para diferentes funciones:

- Uno es la segunda barrera de protección en el tráfico Norte-Sur de entrada y salida de la red corporativa del Ayuntamiento de Pamplona.
- Uno controla todos los accesos remotos seguros, incluyendo VPNs site-to-site, fundamentalmente entre Ayuntamiento y empresas proveedoras de servicios.
- Uno controla el tráfico entre Ayuntamiento de Pamplona y ANIMSA.
- Uno tiene doble función, conectando por una parte el Ayuntamiento de Pamplona a entidades y organismos considerados “confiables” (Gobierno de Navarra y empresas asociadas, red SARA, …), y controlando por otra parte el tráfico Este-Oeste dentro de la red corporativa y gestionando accesos controlados a elementos críticos ubicados dentro de la red corporativa.

La existencia y división de funciones entre estos VDOMS ha venido dada por la evolución en la red corporativa del Ayuntamiento de Pamplona y por la secuencia de inclusión de conexiones de la misma con el exterior. No obstante, se ve en la actualidad como un inconveniente el que el cuarto VDOM descrito tenga funciones distintas, así como que la conexión entre el Ayuntamiento de Pamplona y ANIMSA no esté incluida en el grupo de conexiones con organismos considerados como confiables. Por ello, durante el periodo de vigencia del contrato y más específicamente en su inicio, se pretende reorganizar los dos últimos VDOMs descritos, de forma que pasen a estar organizados de la siguiente forma:

- Un VDOM que controle el tráfico entre Ayuntamiento de Pamplona y entidades consideradas como confiables, incluyéndose entre ellas también a ANIMSA.
- Un VDOM que controle el tráfico Este-Oeste dentro de la red corporativa y gestione accesos controlados a elementos críticos ubicados dentro de la red corporativa.

El adjudicatario deberá proporcionar soporte experto y participación activa en el diseño, validación, implantación y pruebas de los cambios necesarios, valorándose el alcance de este soporte, para lo que el licitador deberá describir en su propuesta los medios que adscribirá a la prestación del mismo, así como descripción de un plan propuesto para estos cambios.

En la actualidad se están modificando también los accesos remotos seguros con el Ayuntamiento de Pamplona, específicamente los basados en VPN client-to-site, de forma que en lugar de ser de tipo SSL-VPN sean de tipo IP-SEC. Se valorará el que el licitador incluya en su oferta medios para facilitar esta tarea a ANIMSA.

2.7) Coordinación con ANIMSA o con otras contratas municipales de cara a la prestación de los servicios contratados

El ecosistema Fortinet propiedad del Ayuntamiento de Pamplona, a través de los VDOMs que tiene configurados, provee de múltiples funcionalidades de seguridad y segmentación, algunas de ellas dentro de la propia red municipal, y otras más orientadas a conexiones con el exterior. Dada la complejidad y extensión de toda la red municipal, existen varias VLANs propagadas a diferentes equipos físicos que componen la infraestructura de red municipal, y que están gestionadas a través del ecosistema Fortinet. Así las cosas, no es extraño que para realizar diferentes labores de mantenimiento correctivo o de soporte experto, sea necesaria una colaboración estrecha entre el adjudicatario de este contrato y los prestadores de servicios análogos sobre la infraestructura de red del Ayuntamiento de Pamplona. Es además muy conveniente que el personal prestador de estos servicios de mantenimiento y soporte tenga también conocimientos y experiencia en redes similares a las del Ayuntamiento de Pamplona.

Por todo lo anterior, el adjudicatario deberá coordinarse siempre que sea necesario con el adjudicatario del contrato de mantenimiento de la red corporativa del Ayuntamiento de Pamplona, y se valorarán los conocimientos y experiencia aportados por personal adscrito a la ejecución del contrato en redes similares a la del Ayuntamiento de Pamplona. Como referencia para este último punto, reseñar que el grueso de la red del Ayuntamiento está constituida principalmente por switches Aruba 8325 y Aruba JL719C 8360 en el Core de Red y switches HPE 5130, Aruba 6000, Aruba 6100 en la parte de acceso de usuarios.

NIF: A31152150

Documento bajo custodia en Sede Electrónica

ASOCIACIÓN NAVARRA DE INFORMÁTICA MUNICIPAL (ANIMSA)

Pliego Prescripciones Técnicas (536) - SEFYCU 410136

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 AAQZ 2JT7 ZYQ4 CYEA

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
	JEFATURA JURIDICO Y CONTRATACIONES MARÍA LUCÍA SORBET BARRICARTE	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 12:04 MARIA LUCIA SORBET BARRICARTE
	Presidente de la mesa de contratación PATXI IRAIZOZ AGUERRI	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 12:34 JOSE FRANCISCO IRAIZOZ AGUERRI
	Vocal FERNANDO RUBIO BERASTEGUI	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 12:44 FERNANDO RUBIO BERASTEGUI
	DIR.ECON-FIN. MYRIAN LIZARBE CHOCARRO	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 12:45 MIRIAM LIZARBE CHOCARRO
	JEF.CC1 DANIEL LASAOSA MEDARDE	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 13:54 DANIEL LASAOSA MEDARDE
	Gerente JOSE MARIA AGUINAGA PEREZ	Firma electrónica avanzada - FNMT-RCM - 13/11/2026 19:21 JOSE MARIA AGUINAGA PEREZ