



**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LOS SERVICIOS DE
SEGURIDAD AVANZADA Y SOPORTE TÉCNICO PARA LA GESTIÓN,
MONITOREO Y PROTECCIÓN DE LOS FIREWALLS DE LA FUNDACIÓN DE LA
ENERGÍA DE LA COMUNIDAD DE MADRID**

ENTIDAD CONTRATANTE	FUNDACIÓN DE LA ENERGÍA DE LA COMUNIDAD DE MADRID
Nº EXPEDIENTE:	F-LIC-2025-02
ÓRGANO DE CONTRATACIÓN:	Director Gerente de la Fundación de la Energía

OBJETO DEL CONTRATO:	CONTRATACIÓN DE SERVICIOS DE SEGURIDAD AVANZADA Y SOPORTE TÉCNICO PARA LA GESTIÓN, MONITOREO Y PROTECCIÓN DE LOS FIREWALLS DE LA FUNDACIÓN DE LA ENERGÍA DE LA COMUNIDAD DE MADRID
-----------------------------	--

Fecha:	06/02/2025	Doc.:	PLIEGO DE PRESCRIPCIONES TÉCNICAS
---------------	-------------------	--------------	--

1. Introducción y justificación.

La Fundación de la Energía de la Comunidad de Madrid (en adelante, la Fundación) es una fundación del sector público, que tiene entre sus fines el fomento, impulso y realización de iniciativas y programas de actuación para la investigación, el estudio y apoyo de las actuaciones de conocimiento, desarrollo y aplicación de las tecnologías energéticas, incluidas las renovables, la mejora del ahorro y la eficiencia energética, el fomento del uso racional de la energía, integrando la protección del medio ambiente y, en general, la óptima gestión de los recursos energéticos en los distintos sectores económicos de la Comunidad de Madrid, sirviendo así de soporte para el impulso y la ejecución de la política energética del Gobierno Regional. Desde su constitución, en 2006, ha gestionado los planes Renove y otros planes de impulso y promoción. Actualmente también gestiona las convocatorias de subvenciones con Fondos Europeos “Next Generation”, tanto en relación con los denominados “Planes Renove” sobre materias energéticas, como en relación con los fondos provenientes del Mecanismo de Recuperación y Resiliencia.

La Fundación ostenta la condición de poder adjudicador no administración pública a tenor de lo establecido en la Ley 9/2017, de 8 de noviembre, por la que se aprueba la ley de Contratos del Sector Público (en adelante, LCSP).

La Fundación requiere una serie de servicios de ciberseguridad que no puede proporcionar internamente, lo que hace necesaria la contratación de los servicios que se detallan en el presente pliego.

Los firewalls y productos de Fortinet han estado integrados en la infraestructura de seguridad de la Fundación desde 2020. Estos dispositivos conllevan estándares robustos para la

optimización del procesamiento, la inspección y el análisis del contenido del tráfico de red. Esta solución permite, por tanto, una gestión eficiente del tráfico sin comprometer el rendimiento de las comunicaciones, siendo una experiencia de usuario fluida y confiable, al tiempo que ofrece una protección integral frente a un amplio espectro de amenazas.

El mantenimiento de la infraestructura existente es crítico, ya que la migración a un nuevo programa de seguridad en el mercado conllevaría un esfuerzo inmenso, tanto en términos económicos como técnicos. La implementación de una nueva solución requeriría una revisión exhaustiva de la arquitectura de red actual y la reconstrucción de todas las interfaces de programación de aplicaciones que han sido desarrolladas y optimizadas para integrarse con el ecosistema de Fortinet. Este proceso no solo implicaría un tiempo de inactividad considerable durante la transición que la Fundación no puede permitirse actualmente dado el elevado volumen de expedientes de subvenciones que está gestionando y que ha de resolver dentro de los plazos estipulados, sino que también podría resultar en un aumento significativo en los costos operativos debido a la necesidad de formación del personal y la adaptación de los sistemas.

El cambio a una nueva herramienta podría comprometer las políticas de seguridad establecidas y la efectividad de la protección ante amenazas, lo que podría dejar a la Fundación vulnerable durante el período de transición. Por estas razones, mantener la infraestructura de Fortinet no solo es una cuestión de eficiencia, sino también una decisión estratégica para garantizar la continuidad y seguridad de las operaciones de la Fundación cumpliendo con las obligaciones que en materia de protección de datos y de seguridad tiene la Fundación.

2. Objeto.

El objeto de la contratación es la adquisición de servicios de Seguridad Avanzada y de Soporte Técnico destinados a fortalecer la infraestructura de red y los dispositivos de seguridad de la Fundación.

La contratación incluye los siguientes componentes:

- **Servicios FortiCare y FortiGuard IPS:**
 - FortiCare: Contratación de soporte técnico 24x7 para los dispositivos FortiWiFi-60E y FortiGate-60F que la Fundación posee en su sede. Este servicio asegura asistencia continua en la gestión de incidencias, actualizaciones de firmware y parches de seguridad, así como asesoramiento técnico especializado para la resolución de problemas complejos.
 - FortiGuard IPS: consiste en la implementación de un servicio de prevención de intrusiones que incluye actualizaciones automáticas de firmas de amenazas, análisis de tráfico en tiempo real y defensa contra ataques de red. Este servicio proporciona un escudo proactivo que identifica y neutraliza amenazas antes de que puedan afectar la infraestructura. El servicio operará 24x7, asegurando protección constante frente a riesgos de seguridad.
- **Servicio de Seguridad Avanzada con SLA 8x5:**
 - Monitoreo Continuo: Este servicio incluye la supervisión constante de la red y los sistemas de seguridad para detectar actividades sospechosas y responder a incidentes en tiempo real. La vigilancia proactiva es crucial para identificar y mitigar amenazas antes de que puedan causar daños significativos.

- **Prevención de Amenazas:** Implementación de medidas de seguridad avanzadas, como análisis de comportamiento, filtrado de contenido y control de acceso, para prevenir accesos no autorizados y proteger la confidencialidad, integridad y disponibilidad de la información.
- **Gestión de Incidentes:** Provisión de un servicio de respuesta a incidentes que incluya la identificación, contención, erradicación y recuperación de cualquier brecha de seguridad. Esto garantizará que la Fundación pueda manejar eficazmente cualquier amenaza emergente y minimizar su impacto.
- **Soporte Técnico Avanzado en Horario Laboral:** El servicio contará con soporte técnico especializado disponible durante las horas laborales (SLA 8x5), garantizando asistencia rápida y eficiente para resolver problemas relacionados con la seguridad y el rendimiento de la red. El horario del soporte será de 08:00 a 16:00 horas de lunes a viernes.

Estos servicios son esenciales para mantener la seguridad integral de la red corporativa, optimizando la protección contra amenazas cibernéticas, intrusiones y ataques, así como asegurando el buen funcionamiento y la resiliencia de la infraestructura de red. La implementación de estos servicios permitirá a la Fundación adaptarse a un entorno de amenazas en constante evolución y cumplir con los estándares de seguridad y normativas vigentes en el sector.

3. Situación actual.

En la actualidad, la Fundación ya cuenta con licencias y servicios contratados que se extenderán hasta el 31 de marzo de 2025. Estos servicios han demostrado ser fundamentales para garantizar la protección contra ciberamenazas, asegurar la continuidad operativa y mantener el rendimiento óptimo de los sistemas de seguridad.

La situación actual de la Fundación presenta los siguientes aspectos:

1. **Infraestructura de Seguridad:** La infraestructura de seguridad de la Fundación se basa en dos dispositivos, un **FortiWiFi-60E** y un **FortiGate-60F**. Hasta la fecha, la gestión de actualizaciones y el mantenimiento preventivo de estos dispositivos han sido cubiertos por contratos anteriores que están próximos a vencer el **31 de marzo de 2025**. Esta protección ha demostrado ser robusta y ha permitido una defensa efectiva contra diversas ciberamenazas.
2. **Necesidad de Complementar la Solución:** A pesar de contar con una infraestructura sólida, se ha identificado la necesidad de implementar una solución de **Seguridad Avanzada** que complemente las funciones de los dispositivos mencionados. Esta solución es fundamental para reforzar la detección y prevención de amenazas en tiempo real, así como para responder de manera ágil a incidentes que puedan comprometer la seguridad de la red.
3. **Políticas de Seguridad Actuales:** En la actualidad, la Fundación cuenta con políticas de seguridad robustas, establecidas para proteger la infraestructura de red y los datos sensibles. Los dispositivos **FortiWiFi-60E** y **FortiGate-60F** están configurados con políticas de seguridad avanzadas que han demostrado ser efectivas en la mitigación de riesgos y en la defensa contra diversas ciberamenazas.

Sin embargo, dado el continuo crecimiento y evolución de las amenazas cibernéticas, es fundamental no solo mantener este alto nivel de protección, sino también adaptarlo a las nuevas realidades del entorno digital. Aunque las políticas de seguridad implementadas actualmente

son sólidas, la complejidad de las amenazas emergentes exige la incorporación de servicios adicionales que refuercen y complementen las capacidades existentes.

Por lo tanto, es imperativo contratar servicios que faciliten la mejora continua de las políticas de seguridad, asegurando su alineación con las mejores prácticas del sector y la implementación de tecnologías avanzadas de detección y prevención de amenazas. Esto garantizará que la Fundación no solo mantenga su posición actual de seguridad, sino que también esté preparada para enfrentar cualquier desafío futuro en el ámbito de la ciberseguridad.

4. **Reforzar la Protección:** La Fundación debe mantener, como mínimo, el nivel de protección robusta que ha tenido hasta ahora. Esto implica no solo contar con contratos de soporte técnico y actualización, sino también la incorporación de herramientas y servicios que optimicen la seguridad, como servicios de monitorización continua, respuesta a incidentes y análisis de tráfico en tiempo real.

En conclusión, la continuidad de los servicios de seguridad es crucial para asegurar la integridad, confidencialidad y disponibilidad de la información de la Fundación. Por lo tanto, es esencial que la contratación de los servicios se realice para evitar brechas en la protección y asegurar que la Fundación siga estando bien resguardada frente a las amenazas actuales y futuras.

5. Requisitos técnicos

Los servicios a contratar deberán cumplir con los siguientes requisitos:

1. **Soporte FortiCare y FortiGuard:**
 - **FortiWiFi-60E:**
 - Contrato de **FortiCare 24x7** durante 2 años, que incluya cobertura de asistencia técnica, actualización de software y reparación de hardware.
 - Servicio de **FortiGuard IPS** por 2 años, que incluya detección y prevención de intrusiones, con actualizaciones automáticas de amenazas.
 - **FortiGate-60F:**
 - Contrato de **FortiCare Premium Support**, que incluya soporte avanzado con tiempos de respuesta priorizados para garantizar la disponibilidad y rendimiento.
 - Servicio **FortiGuard IPS** durante 2 años, que brinde protección continua contra ataques y amenazas de red.
2. **Servicio de Seguridad Avanzada con SLA 8x5:**
 - Provisión de un servicio de seguridad avanzada con un SLA (Service Level Agreement) mínimo de **8 horas diarias, 5 días a la semana (8x5)**.
 - El servicio debe incluir monitoreo proactivo de la red, gestión de incidentes de seguridad, mitigación de vulnerabilidades, actualización de firmas y auditoría periódica del estado de seguridad.
 - Informes semanales que incluyan métricas de rendimiento y seguridad.
 - Soporte técnico especializado en horario laboral (lunes a viernes) con tiempos de respuesta acordes al SLA establecido en horario de 8:00 a 16:00h.
3. **Soporte y Gestión de VPN mediante FortiClient:**

La Fundación utiliza **FortiClient** para establecer conexiones seguras a su red corporativa. Aunque el software es de uso gratuito, su implementación y gestión requieren atención técnica especializada para garantizar un acceso seguro y fiable.

4. **Respuesta a incidencias:** El soporte avanzado deberá cumplir los niveles de prioridad y tiempos mínimos establecidos para cada tipo de alerta:

- **Incidencias Críticas (Alta o Grave)**

En el caso de una caída del servicio, donde el producto se detiene o se encuentra a punto de dejar de funcionar, se considera una situación crítica. Este tipo de incidencia pone en peligro la operación completa y requiere una respuesta inmediata. El objetivo del equipo de soporte es intervenir y comenzar la resolución de la incidencia en un tiempo máximo de 1 hora desde la notificación.

- **Incidencias de Impacto Moderado (Media o Moderada)**

Las incidencias de servicio en riesgo se refieren a problemas que afectan de manera intermitente la operatividad del sistema o servicio. Aunque la funcionalidad no está completamente perdida, los problemas pueden impactar la eficiencia o causar inconvenientes para el usuario. Para estas situaciones, el tiempo máximo de respuesta es 4 horas, lo que garantiza una solución rápida y sin demoras.

- **Incidencias Menores (Baja o Leve)**

En situaciones donde se experimenta un bajo rendimiento o incidencias que no representan una amenaza directa a la operatividad, sino que causan una ligera disminución en el rendimiento, el tiempo de respuesta máximo establecido será de 8 horas. Aunque el impacto en el negocio es mínimo, el equipo de soporte se compromete a resolver el problema de manera eficiente dentro del plazo establecido.

- **Consultas Generales**

Las consultas que no están relacionadas con incidencias críticas, como asistencia general o consultas técnicas relacionadas con la configuración (por ejemplo, cómo realizar ajustes específicos o resolver dudas no urgentes), tienen un tiempo máximo de respuesta de 24 horas. Este tipo de consultas incluyen orientaciones sobre el uso del producto y aclaraciones generales.

El adjudicatario se encargará de la provisión de estos servicios. Dado el creciente panorama de amenazas cibernéticas y la evolución constante de los riesgos asociados, es crucial no solo mantener, sino también potenciar estas capacidades. Esto incluye asegurar la continuidad en el soporte técnico, así como la implementación de medidas de seguridad avanzadas que refuercen la defensa de la red corporativa.

4.- Plan de trabajo:

Los licitadores deberán presentar un **Plan de Trabajo** detallado que describa las tareas específicas que realizarán para cumplir con los objetivos del contrato, cumpliendo con los siguientes puntos clave:

1. **Descripción de Tareas:** Un desglose claro de todas las tareas a realizar, que abarque desde la implementación inicial de los servicios de **FortiCare** y **FortiGuard**, hasta la ejecución del servicio de **Seguridad Avanzada** con **SLA 8x5**. Cada tarea debe estar claramente definida y vinculada a los resultados esperados.
2. **Soporte y Gestión de VPN mediante FortiClient:** Deberán detallar cómo llevará a cabo la configuración, soporte técnico y gestión de la infraestructura de VPN que utiliza FortiClient. Esto incluye la capacitación del personal en su uso adecuado y la resolución de problemas relacionados con la conectividad VPN.
3. **Cronograma:** Un cronograma que indique las fechas de inicio y finalización de cada tarea, asegurando que todos los hitos se alineen con los plazos establecidos en el

contrato. Se espera que el cronograma contemple la implementación que comenzará el **10 de marzo de 2025**.

4. **Recursos Asignados:** Detallar los recursos humanos y técnicos que se destinarán a cada tarea, incluyendo la identificación de personal clave, sus competencias y funciones dentro del proyecto.
5. **Plan de Comunicación:** Un plan que describa cómo se comunicarán los avances del proyecto, la gestión de incidencias y la interacción con el personal de la Fundación. Se debe establecer la frecuencia de los informes de progreso y las reuniones de seguimiento.
6. **Evaluación y Ajustes:** Un enfoque sobre cómo se evaluarán los resultados de las tareas realizadas y cómo se realizarán los ajustes necesarios para garantizar el cumplimiento de los objetivos establecidos en el contrato.

El **Plan de Trabajo** presentado por los licitadores será fundamental para conocer su comprensión de los requisitos del contrato y su capacidad para cumplir con los mismos de manera efectiva.

Ha de ser un plan exhaustivo, profesional y adaptado a las necesidades específicas de la Fundación, garantizando así la continuidad y robustez de la infraestructura de seguridad. Se solicitará informe técnico sobre el plan de trabajo presentado en el que se determine su ajuste a lo requerido en este apartado.

En caso de no presentarse un plan de trabajo ajustado a lo previsto en este pliego se excluirá la oferta presentada.

5.- Dirección del servicio a prestar y seguimiento de los trabajos.

Los servicios se prestarán de forma remota para la **sede de la Fundación**. No obstante, cuando sea necesario, se requerirá soporte in situ para la resolución de problemas críticos que no puedan ser resueltos a distancia.

El seguimiento de los trabajos será responsabilidad del **Responsable del Departamento de Informática y Administración Digital**, quien estará encargado de supervisar la correcta implementación de los servicios contratados, garantizando el cumplimiento de los SLA y los objetivos de seguridad planteados.

Se deberá realizar un **informe mensual de estado** que incluirá:

- Incidentes atendidos y resueltos.
- Amenazas detectadas y mitigadas.
- Cumplimiento del SLA.
- Recomendaciones de mejora en seguridad.

6.- Confidencialidad de la información y protección de datos.

En materia de confidencialidad de la información y de protección de datos personales se estará a lo establecido en el Pliego de cláusulas administrativas particulares.

7.- Normativa a cumplir en la ejecución del contrato

El adjudicatario deberá cumplir con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y, en particular, en el apartado 2 de su artículo 16 en el que se establece que las organizaciones que presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

8.- Plazos de implementación y de ejecución.

El plazo de duración inicial del Contrato será de dos (2) años iniciándose su ejecución el día 10 de marzo de 2025 o al día siguiente de su firma, pudiendo prorrogarse una vez por un periodo de tres (3) años, previa valoración positiva del proveedor por el Responsable del contrato.

La implementación inicial de los servicios de **FortiCare** y **FortiGuard** se llevará a cabo a partir del **10 de marzo de 2025**. Esta fase incluirá la configuración, puesta en marcha y validación de las funcionalidades de ambos servicios, asegurando que estén alineados con las necesidades específicas de la Fundación. Se realizarán pruebas de funcionamiento para garantizar que todos los sistemas operen de manera efectiva y se ajusten a las políticas de seguridad previamente establecidas.

Además, el servicio de **Seguridad Avanzada** con **SLA 8x5** deberá estar completamente operativo a partir del **10 de marzo de 2025**. Esto implica que, desde ese día, la Fundación contará con un equipo de soporte técnico especializado disponible conforme a lo establecido en el apartado 5 de este PPT, listo para gestionar incidentes, realizar monitorización activa de la seguridad y ofrecer asistencia inmediata ante cualquier eventualidad que pueda surgir.

Es fundamental que todos los procesos de implementación y operación se lleven a cabo con la máxima eficiencia y en un marco de colaboración estrecha entre el adjudicatario y el personal de la Fundación, para asegurar que se mantenga la robustez de la protección existente y se potencie la seguridad de la infraestructura de red.

9.- Obligación de cumplir lo regulado por los artículos 201 y 202 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

A los efectos que procedan la empresa adjudicataria se obligará al cumplimiento de la normativa aplicable derivada de la relación contractual, respecto a las obligaciones sociales, medioambientales, laborales, y condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental o de otro orden que se establezcan en el Pliego de Cláusulas Administrativas Particulares.

CONFORME:

EL ADJUDICATARIO

FECHA Y FIRMA

**FUNDACION DE LA ENERGIA DE LA
COMUNIDAD DE MADRID**

FECHA Y FIRMA

TÉCNICO RESPONSABLE DEL CONTRATO

FECHA Y FIRMA