

SOPORTE SOLUCIÓN SEGURIDAD PERIMETRAL PRODUCCIÓN RNE

PLIEGO DE CONDICIONES TÉCNICAS

El objeto del presente expediente es la renovación de los servicios de soporte y mantenimiento del sistema de seguridad perimetral de RNE, garantizando el correcto funcionamiento de los equipos (firewall) a lo largo del periodo de mantenimiento solicitado, minimizando la duración de las intervenciones. De esta manera es indispensable que el adjudicatario provea un servicio que se corresponda con los niveles de calidad y premura que se detallan más adelante en este pliego.

Para llevar a cabo estas tareas, es necesario contar con personal cualificado y que tengan los conocimientos específicos del hardware y software que conforman la plataforma. Es **imprescindible** que el adjudicatario tenga la **certificación de ForcePoint “Gold Certified Partner”**. En la oferta técnica se deberá indicar fecha de entrada en vigencia del certificado.

El equipamiento sobre el que se prestará el servicio es un **Clúster de dos nodos del Fabricante ForcePoint, modelo NGFW N3405-AC**.

Las funciones que se demandan y que más adelante se detallarán son las siguientes:

- Resolución de incidencias con soluciones eficientes, rápidas y de calidad técnica.
- Hacer seguimiento y proporcionar información del estado de la solución (Firewall).
- Elaborar informes personalizados entregados semestralmente.
- Garantizar el cumplimiento de tiempos de atención, resolución y reposición de piezas.
- Conformar un histórico de problemas conocidos que permita identificar problemas aplicando las mismas soluciones de forma rápida y eficaz.

1. Comunicación de incidencias

La comunicación de incidencias del soporte reactivo será a través de un único punto de contacto, pudiendo ser comunicación a través de un **portal de reporte de incidencias, por vía telefónica o por correo electrónico**.

Esta atención de primer nivel deberá ser realizada por profesionales expertos, con un conocimiento demostrado de la instalación a mantener.

Este servicio especializado debe atender la siguiente lista de demanda:

- Mantenimiento correctivo de segundo nivel
- Alerta temprana de incidencias o bugs
- Gestión de problemas técnicos
- Asesoramiento técnico
- Trabajos programados tales como corrección de bugs o actualizaciones
- Mantenimiento preventivo de la infraestructura
- Mantenimiento evolutivo de la infraestructura
- Escalado al fabricante de casos que requieran intervención por su parte
- Gestión de eventos
- Gestión de capacidad y rendimiento del equipamiento.

El objetivo de este grupo de servicios es el de actuar en todo tipo de incidencias y restaurar la operatividad normal del servicio definido por los tiempos de respuesta fijados a la mayor brevedad,

minimizando el impacto negativo en el servicio y asegurando los mejores niveles de disponibilidad y seguridad, así como la calidad del mismo.

El soporte se propone para los **dos** equipos de seguridad perimetral de ForcePoint que trabajan en clúster. Ambos son el modelo NGFW 3405-0-C1 con los números de serie:

- **1fe3658d1e-08367c320d**
- **012839c27e-b66413e612**

Se administran desde una consola Security Management Center en la versión 6.10.16 [11201]

Se contemplan los siguientes tiempos de resolución, según la incidencia

Nivel de Incidencia	Tiempos de resolución
Crítica	4 horas
Alta	24 horas
Media	NBD
Baja	Lo antes posible

Tabla 1

En cada nivel de incidencia, la reposición de piezas, si fuese necesario, queda incluido dentro del tiempo de resolución.

La prestación del servicio se realizará en remoto para incidencias de nivel bajo y medio y de manera presencial por parte de un técnico para la resolución de incidencias de nivel alto o crítico. En el caso de que las incidencias de nivel bajo o medio no puedan solucionarse en remoto se requerirá la presencia de un técnico si no puede ser resuelta en remoto.

CRÍTICA	Impacto severo. El sistema ha caído o no funciona. Interrupción de la producción, No se encuentra solución temporal.
Importancia ALTA	Alto impacto. La operación se ve afectada, pero se mantiene el nivel de producción suficiente, con recursos adicionales, durante el tiempo de resolución del problema.
Importancia MEDIA	Impacto medio. Fallo parcial, no crítico. Pérdida de algunas funcionalidades. La producción se mantiene operativa.
Importancia BAJA	Impacto bajo. Pérdida de funcionalidad limitada. No se precisa acción inmediata.

Tabla 2

Independientemente de los tiempos de respuesta fijados en la tabla 1, la comunicación debe contar con flexibilidad horaria para la comunicación de altas de incidencias (24x7)

La gestión de incidencias debe cumplir con las siguientes tareas:

- Recogida de las averías e incidencias vía telefónica y/o web
- Registro de las incidencias en una base de datos de incidencias específica para el soporte que se describe
- Clasificación de las incidencias:
 - Detallado del servicio del firewall afectado
 - Asociación del nivel de Servicio acordado (SLA)
 - Asignación del técnico especialista para comunicación más fluida

- Definición de la prioridad
- Comentarios / Información adicional
- Investigación y diagnóstico remoto de 1er nivel para incidencias rutinarias de fácil resolución
- Seguimiento del procedimiento de comunicación acordado. Para ello, es necesario que el adjudicatario suministre la siguiente información sobre el caso:
 - Número de incidencia
 - Fecha y hora de entrada
 - Descripción de la incidencia
 - Servicios afectados
 - Acciones tomadas por el soporte de primer nivel
 - Medidas adoptadas para la mitigación de la incidencia
 - Fecha y hora de la neutralización y recuperación del servicio
- Escalado a los grupos de 2º y/o 3er nivel. Necesario para incidencias de alta complejidad que serán elevadas al fabricante del equipamiento y coordinado a través del departamento de gestión de incidencias del adjudicatario.
- Resolución y cierre de incidencias. Es necesario la generación de un reporte con los detalles de la acción tomada para resolver el problema de manera concisa y entendible. Es necesario establecer conjuntamente un período de seguimiento y monitorización de la incidencia previo al cierre del caso y estadísticas de casos similares en la infraestructura.

2. Gestión de Repuestos

El adjudicatario será responsable del servicio de gestión de reemplazos y la coordinación de la entrega de los mismos, en el caso de que la resolución de la incidencia requiera de la sustitución total o parcial del equipo o pieza averiado.

Es responsabilidad del adjudicatario el alta del equipamiento indicado en la gestión de repuestos oficial del fabricante o garantía extendida, para cumplir con los tiempos de respuesta establecidos. Esto implica que el adjudicatario asumirá la coordinación del servicio técnico de RTVE y el fabricante del equipamiento para poder realizar el seguimiento de la intervención necesaria. Todo ello se llevará a cabo de tal manera que se pueda controlar el nivel de servicios prestado, y determinar, en caso de eventuales incumplimientos, la responsabilidad de cada una de las partes.

3. Mantenimiento Correctivo

El adjudicatario deberá proveer servicios de mantenimiento correctivo en tres niveles, cuyo objetivo será proporcionar soporte técnico y/o actuaciones remotas para atender averías o problemas en la infraestructura para restablecer su estado normal de funcionamiento:

- *Asistencia técnica de primer nivel:*

Este mantenimiento se realizará directamente por el adjudicatario sobre el equipo afectado, actuando de manera inmediata tras la detección de cualquier anomalía en su funcionamiento. La intervención se limitará a la sustitución o reconfiguración de las piezas o servicios que hayan originado el problema, sin implicar modificaciones en la arquitectura de la solución.

- *Asistencia de segundo nivel:*

Si tras la primera actuación y verificación no se resolviese o ante problemas que no se consideran cotidianos ni de fácil resolución, esta atención será prestada por técnicos cualificados con el respaldo del fabricante

- *Asistencia técnica de tercer nivel:*

En aquellas incidencias de carácter especial, cuya resolución definitiva requiera el desarrollo de parches de software o hardware, el adjudicatario se pondrá en contacto con el servicio de soporte del fabricante para gestionar de forma ágil y eficaz la reparación correspondiente. El responsable asignado para la prestación del servicio, mantendrá una comunicación continua, informando en todo momento sobre las acciones realizadas, los pasos planificados y las posibles soluciones alternativas para restablecer el servicio.

Este servicio será gestionado a través del adjudicatario y deberán estar coordinados por el responsable de mantenimiento, encargado de asignar un equipo técnico específico con el objetivo de asegurar un conocimiento profundo del entorno y así optimizar los tiempos y la eficacia en la resolución de incidencias. Este personal deberá contar con las certificaciones necesarias y una amplia experiencia en servicios similares para garantizar la calidad del soporte prestado.

- *Actuaciones “in Situ”*

Ante la imposibilidad de realizar los mantenimientos mencionados en remoto y cuando la resolución de la incidencia requiera de tareas que necesiten un conocimiento más profundo tanto del equipo en cuestión como de las distintas tecnologías involucradas, será necesario el desplazamiento de personal técnico in-situ por parte del adjudicatario. Este desplazamiento implicará una decisión conjunta entre los técnicos de RTVE y el personal que prestará el servicio, basándose en la complejidad del problema, su nivel de severidad, la influencia en el servicio o la disponibilidad de datos de análisis.

4. Mantenimiento Preventivo

Este servicio deberá tener un enfoque proactivo orientado a prevenir fallos potenciales en el firewall antes que lleguen a producirse para, no solo anticipar posibles incidencias o vulnerabilidades, sino disponer de una preventiva que mejora la eficiencia en la gestión de problemas, actuando sobre factores como el estado físico del equipamiento o la obsolescencia del software de los mismos.

Tendrá una periodicidad anual y será programado conjuntamente por el adjudicatario del pliego y los profesionales de RTVE responsables del equipamiento.

Tras cada intervención, se elaborará un informe detallado que recoge no solo los resultados obtenidos en las comprobaciones realizadas, sino también recomendaciones y acciones correctivas o de mejora basadas en la experiencia y el conocimiento técnico de los profesionales que prestan el servicio.

Este servicio no requerirá de técnicos in situ ni **deberá tener afección en el servicio**.

Las principales revisiones, comprobaciones y medidas que se llevarán a cabo durante el mantenimiento preventivo deberán ser las siguientes:

- Seguridad y filtrado de tráfico: Inspección profunda de paquetes, IPS, Prevención de evasiones avanzadas (AETs), control granular de aplicaciones y Filtrado Web y URL.
- Conectividad y rendimiento: VPNs, SD-WAN, Alta disponibilidad en el clúster, Inspección SSL/TLS.
- Gestión y visibilidad: Políticas definidas, Visibilidad del tráfico, usuarios y amenazas en tiempo real.
- Integración y defensa avanzada: Segmentación de red, Sandboxing para análisis de archivos sospechosos en entornos aislados y actualizaciones de inteligencia de amenazas en tiempo real desde Forcepoint Security Labs.
- Comprobación del estado del software de gestión para la detección de posibles fallos lógicos.

5. Actualizaciones de software e implementación de nuevas versiones

Este servicio indispensable consistirá en el suministro de la información y las actualizaciones de software y firmware, para la puesta a punto con las últimas mejoras que el fabricante saque a la luz.

Estas actuaciones se llevarán a cabo a partir de la necesidad de incluir alguna corrección que permita disponer de funcionalidades incluidas en la versión actual y que no estén funcionando correctamente. El adjudicatario será responsable de suministrar dichas actualizaciones con la documentación relativa a los mismos, caracterizando las mejoras que suponen estas nuevas versiones y los errores que corrigen con su implementación.

En coordinación con los profesionales de RTVE, será responsabilidad del proveedor de servicios la instalación y puesta en marcha de las versiones suministradas que además son recomendadas por el fabricante en materia de seguridad. En caso de ser necesario, se desplazará un técnico in-situ para completar estos trabajos en los equipos afectados. Este servicio será por petición previa, y en horario laboral (09h – 19h) o fuera de él para las intervenciones con impacto en el servicio.

6. Asesoramiento Técnico

Deberá estar incluido un asesoramiento técnico, compuesto de un servicio técnico avanzado para la resolución de consultas tecnológicas específicas sobre nuevas funcionalidades, configuraciones que se necesiten adoptar y mejoras, así como evoluciones del hardware y software de los productos.

Para poder prestar los mencionados servicios, es imprescindible que el adjudicatario tenga la certificación de ForcePoint “Gold Certified Partner”, y una experiencia mínima de dos años con este tipo de asesoramiento técnico.