

MEMORIA JUSTIFICATIVA

Se emite la presente memoria en cumplimiento de lo dispuesto en los artículos 28, 63 y 116.4 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, así como en el artículo 73 del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado mediante Real Decreto 1098/2001, de 12 de octubre.

I. SITUACIÓN ACTUAL Y NECESIDADES A SATISFACER

a) Situación actual

RTVM, desde 2010, dispone de una red multiservicio que permite transportar de forma segura, diferentes tipos de tráfico, según la prioridad, en función del tipo de aplicación (datos, voz, internet, videoconferencia, etc.), atendiendo a las necesidades de la compañía y con una capacidad de crecimiento de los servicios de datos corporativos, así como el establecimiento de nuevos servicios.

Para el soporte de comunicaciones y seguridad de los servicios corporativos cuya presencia y/o servicio son imprescindibles en "internet", RTVM, dispone de líneas de comunicaciones a internet redundantes.

La infraestructura de Seguridad Perimetral, consiste en una serie de sistemas integrados para la protección de perímetros "lógicos". Sobre esta infraestructura pivota el acceso a Internet de diferentes servicios corporativos que son necesarios para los procesos de soporte al Negocio - navegación, transferencia de ficheros, correo electrónico, etc. - y para los procesos de Negocio como la ingesta/contribución de contenidos a través de mochilas 4G que intervienen en la producción de programas (directos/grabados) y/o los diferentes canales multimedia que están bajo el ámbito de responsabilidad de la Dirección Digital - telemadrid.es, redes sociales, etc.-.

Para posicionar nuestra organización en un nivel de seguridad "razonable" se debe garantizar la integridad, la confidencialidad y la disponibilidad, con lo que se hace necesario mitigar los riesgos conocidos en los siguientes términos:

- Monitorización tráfico y visibilidad uso Internet.
- Políticas basadas en aplicaciones/usuarios.
- Filtrado de URLs.
- Antivirus/Antimalware.

La infraestructura de Seguridad Perimetral permite desempeñar las siguientes funciones:

- Identificar accesos externos no controlados y alertar de ellos.
- Contener accesos externos no controlados
- Aislar y segmentar los distintos servicios y sistemas en función de su grado de exposición a ataques.
- Filtrar y bloquear el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

Desde 2010, RTVM cuenta con un servicio externo para gestionar los procesos asociados, básicamente:

- Gestión de incidencias,
- Gestión de cambios y peticiones
- Soporte a la operación y explotación
- Help-Desk de segundo nivel – Acceso tercer nivel (fabricante)
- Mantenimiento Correctivo
- Mantenimiento Preventivo

En este tiempo, en el marco del servicio:

- Se han revisado y mejorado las políticas de seguridad.
- Se ha renovado la infraestructura por razones de obsolescencia tecnológica y se ha optimizado la arquitectura de red, eliminando equipos y puntos de fallo (balanceadores de línea) y consolidando la infraestructura.
- Se ha securizado la infraestructura para dar cobertura a producciones que se realizan en exteriores mejorando las comunicaciones entre la localización Exterior y la Sede Principal, adquiriéndose dos cortafuegos móviles, uno principal y otro de backup, del mismo fabricante que el resto del equipamiento implantado en RTVM para securizar el perímetro, Fortinet, con el objetivo de garantizar la compatibilidad, facilitar la gestión y no aumentar la complejidad operativa.
- Se ha mejorado la operativa, se han revisado y mejorado los procesos.

El servicio actual finaliza el 14 de enero de 2024, sin posibilidad de prórroga.

b) Necesidades a satisfacer

El contrato de servicio que cubre actualmente el soporte y mantenimiento de la infraestructura de Seguridad Perimetral finaliza el 14 de enero de 2024, considerando que los servicios que se soportan son críticos y han de tener asegurada su disponibilidad y buen funcionamiento, se propone, la renovación del equipamiento que ha quedado obsoleto tecnológicamente, la renovación de licencias y el servicio de soporte de fabricantes y el servicio gestionado de mantenimiento de acuerdo al esquema de servicio actualmente contratado.

II. JUSTIFICACIÓN E IDONEIDAD DEL OBJETO Y CONTENIDO

La Seguridad Perimetral es el proceso mediante el cual se asegura el perímetro de la organización a través de la implementación de una combinación de software, dispositivos y técnicas. La estrategia en RTVM incluye, para reforzar la seguridad, la vigilancia, la detección de amenazas y el análisis de patrones, en definitiva, recursos encargados de realizar la exploración constante y la evaluación del perímetro.

Es importante entender que la seguridad perimetral es un proceso en constante evolución, aparecen nuevas amenazas, vulnerabilidades que levantan riesgos que están en conflicto con las estrategias de ciberseguridad.

La infraestructura que soporta la Seguridad Perimetral actualmente desplegada en RTVM se compone de:

- Firewall CORPORATIVOS (FortiGate-Fortinet):
Routing, Cortafuegos y VPN – Access.
- FortiAnalyzer (Fortinet)
- Firewall para PRODUCCIONES de EXTERIORES (Fortinet).
- Balanceadores de nivel 7 de aplicaciones perimetrales (Alteon – Radware).
- Correlador de Eventos (LogICA).

Los fabricantes Fortinet y Radware finalizan, respectivamente, el soporte del equipo FortiAnalyzer y de los balanceadores Alteon, sin posibilidad de extenderlos, con lo que se ha abierto una ventana de oportunidad para renovarlos por otros soportados por el fabricante en los próximos 5 años, con la capacidad necesaria para soportar el volumen actual y el crecimiento a medio plazo, manteniéndose así la arquitectura, la operativa y en definitiva la estrategia de la Dirección de Tecnología.

FortiAnalyzer recopila, almacena y analiza automáticamente los historiales de todos los dispositivos de seguridad de Fortinet, incluidos los firewalls FortiGate, las VPN. El equipo actual está configurado, parametrizado y personalizado para RTVM.

Los balanceadores Alteon, son una solución de seguridad y entrega de aplicaciones que administra el tráfico de aplicaciones para optimizar la disponibilidad y el rendimiento. Integra servicios de protección de aplicaciones para brindar protección contra ciberamenazas. El servicio de análisis de Alteon brinda visibilidad detallada para que se pueda administrar los SLA de aplicaciones y de manera preventiva adelantarse a los ciberataques. Los equipos actuales, redundantes, están configurados, parametrizados, personalizados e integrados con las granjas de servidores de RTVM.

La renovación tecnológica es una solución que se lleva a cabo para garantizar una actualización constante y eficaz de los equipos.

El objeto del contrato en lo que respecta al equipamiento HW/SW es el de renovar, es decir reestablecer o reanudar los derechos de uso de unas licencias que se interrumpen porque el contrato actual llega a su fin y en tanto que el fabricante no permita la renovación de estos equipos deben ser sustituidos por los equivalentes. No es objeto del contrato adquirir nuevos equipos, se pretende mantener el nivel de seguridad de la Organización sobre la base de mantener la misma estrategia, es decir, mantener la misma arquitectura de seguridad, con el mismo equipamiento, en tanto esté soportado por el fabricante, si no, sustituirlos por otros que sí estén bajo soporte, explotarlo y administrarlo con los mismos procedimientos operativos, las mismas técnicas y métodos.

Adicionalmente, conviene señalar que:

1. RTVM ha hecho un esfuerzo a nivel de infraestructura, que suponen costes pendientes de amortizar y que permiten por tanto la evolución sobre la base de la estrategia actual alineada con estándares de calidad y buenas prácticas.
2. Se requiere que los equipos nuevos solicitados sean de los mismos fabricantes, ya que la infraestructura de seguridad perimetral de la organización está consolidada con los dispositivos de estos fabricantes, con

objeto de disponer de una infraestructura homogénea que facilite su gestión y administración. Si se mezclaran distintos fabricantes implicaría introducir más complejidad operativa, a la hora de desplegar medidas de seguridad, lo que pondría en riesgo el nivel de seguridad durante más tiempo, al ser más compleja esta operación.

3. Sin perjuicio de evaluar la posibilidad de desplegar una nueva infraestructura de Seguridad Perimetral, basado en otro tipo de tecnología, en el medio plazo, resulta crítico mantener operativo el sistema actual garantizando la disponibilidad de los procesos soportados y por tanto el nivel de Seguridad en el que está posicionada la Organización, en definitiva, manteniendo el grado de exposición de la misma.
4. Finalmente, se ha comprobado, con el objetivo de no limitar la concurrencia, que los fabricantes cuentan con diferentes partners, distribuidores y socios de integración con sede en España y en la Unión Europea pero también en otras localizaciones internacionales, que, a su vez, trabajan con otras empresas especializadas en la provisión de este tipo de soluciones para diferentes sectores.

La inclusión de marcas, fabricantes, modelos en el expediente técnico resulta necesaria a efectos de no afectar los sistemas que vienen funcionando, las integraciones con otros servicios y/o los procesos implementados. Así, de manera excepcional, se hace referencia a equipos concretos, por resultar indispensable para alcanzar los objetivos y habiéndose asegurado que no se afecta la libre concurrencia de proveedores bajo ninguna circunstancia.

III. OBJETO DEL CONTRATO

De acuerdo con todo lo expuesto, se hace imprescindible convocar una licitación pública para contratar el Servicio Gestionado de Mantenimiento y Soporte de la Seguridad Perimetral para garantizar el nivel de seguridad de la Organización en cuanto a la defensa del perímetro de red exterior se refiere:

- Por un lado, renovando el equipamiento obsoleto y asegurando el soporte de los fabricantes que son los que certifican que la funcionalidad que provee está actualizada,
- Por otro, renovando el servicio gestionado de mantenimiento y soporte a la operación y explotación.