



TeleMadrid

Renovación Infraestructura
Cortafuegos de Nueva Generación
Servicios de Seguridad Perimetral

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Dirección de Ingeniería y Tecnología
Subdirección de Sistemas de Información

Noviembre 2017

ÍNDICE

1. INTRODUCCIÓN	3
2. CONTEXTO DE LA PROPUESTA	3
SITUACIÓN ACTUAL.....	3
SITUACIÓN OBJETIVO.....	6
3. DESCRIPCIÓN DEL SERVICIO	7
SERVICIOS PREVISTOS	7
SUMINISTRO NUEVO EQUIPAMIENTO	8
SERVICIO GESTIONADO: ADMINISTRACIÓN & EXPLOTACIÓN.....	14
Alcance Funcional.....	14
Alcance Tecnológico	17
Metodología	18
Organización del Servicio	19
PLAN DE IMPLANTACIÓN DEL SERVICIO.....	20
PLAN DE DEVOLUCIÓN DEL SERVICIO	21
GOBIERNO DEL SERVICIO Y REPORTING	21
RECURSOS Y PERFILES INVOLUCRADOS.....	23
4. MODELO DE FACTURACIÓN	25
5. NIVELES DE SERVICIO Y PENALIZACIONES	25
6. CONTENIDO DE LAS OFERTAS TÉCNICAS	30

1. INTRODUCCIÓN

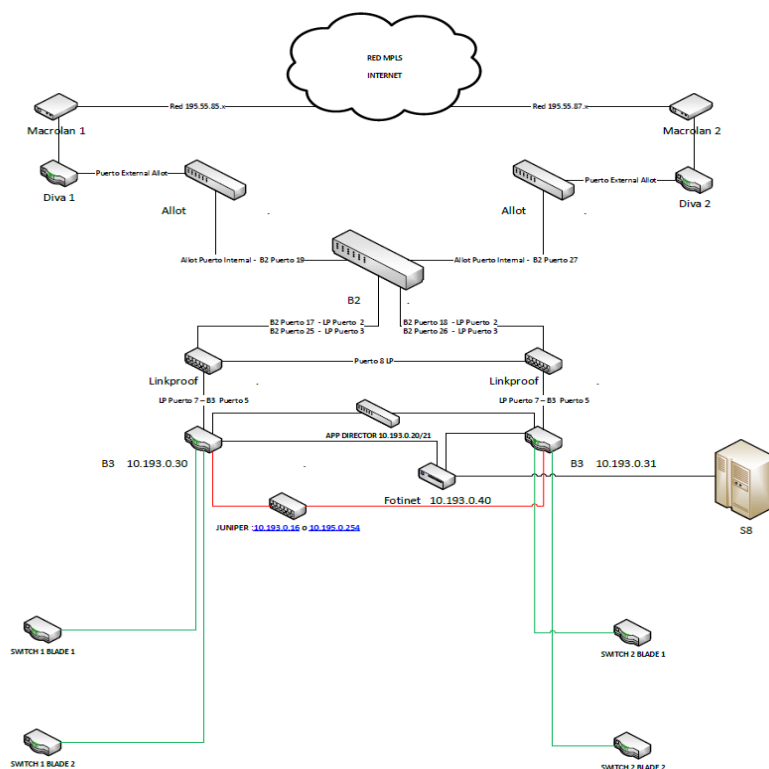
El objetivo de este documento es presentar el catálogo completo de premisas, condicionantes, requerimientos y especificaciones (funcionales, operativas, tecnológicas y de gestión) establecidos por RTVM, para la prestación de un servicio, orientado a la renovación de la infraestructura de FW-NGN de RTVM que incluye la adquisición, provisión, instalación, configuración, diseño de la solución dentro del ecosistema de infraestructura de Perimetral de la organización, así como el Servicio Gestionado de Soporte y Mantenimiento del Servicio de Seguridad Perimetral.

En la actualidad estas funcionalidades se encuentran cubiertas, si bien, por motivos estratégicos y obsolescencia tecnológica, se plantea el diseño de una nueva arquitectura, renovando, consolidando e incorporando nuevos servicios para el soporte de los procesos de Negocio de RTVM.

2. CONTEXTO DE LA PROPUESTA

SITUACIÓN ACTUAL

RTVM dispone de infraestructura de Seguridad Perimetral, esta infraestructura se encuentra estructurada para dar soporte a los servicios desde y hacia internet con la siguiente arquitectura:

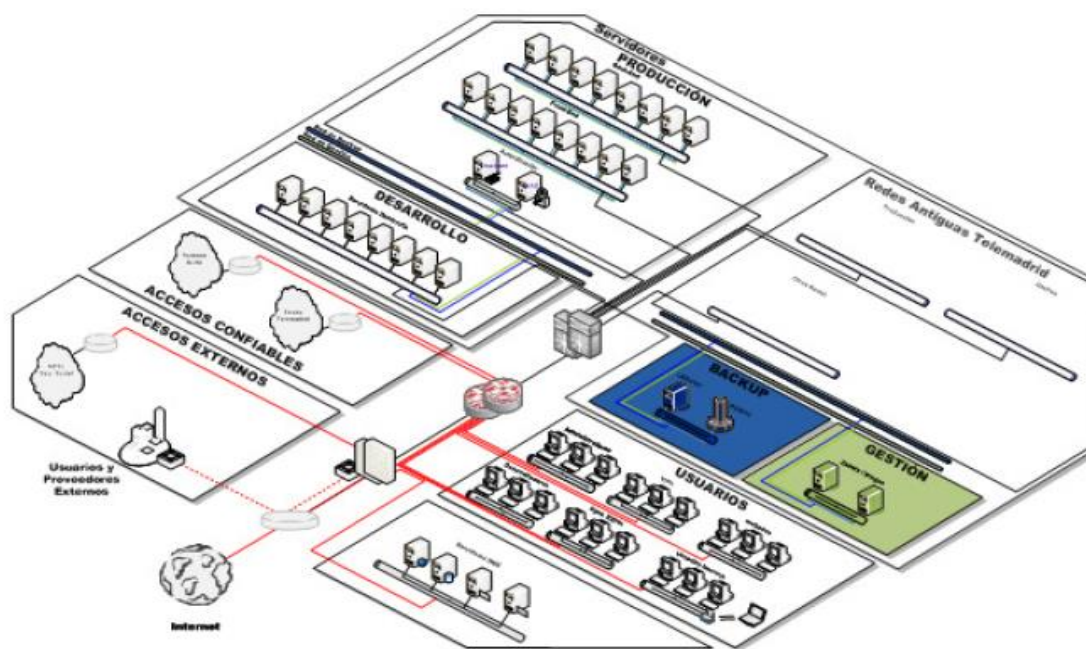


RTVM cuenta con un servicio de gestión de incidencias, peticiones, administración y gestión de cambio de la siguiente infraestructura:

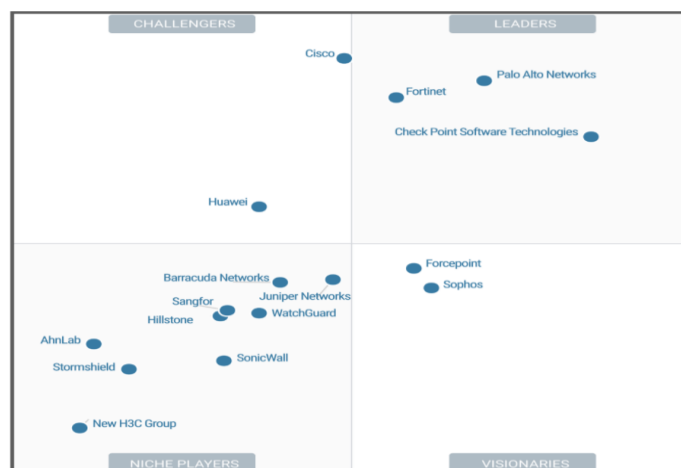
Fabricante	Producto	Sw/Hw	Cantidad
JUNIPER NETWORKS	JU SVC-SD-ISG1000-SMS	Hw	1
	JU SVC-COR-NSM-5	Hw	1
	JU NS-ISG-1000	Hw	1
	CL1 for LinkProof 200/ASI/8xFE/ 256MB RoHS, S/N 20706289	Hw	1
RADWARE	CL1 for LinkProof 200/ASI/8xFE/ 256MB RoHS, S/N 20706290	Hw	1
	CL3 for AppDirector1004/OSD1/2Gb/HDD/RoHS S/N 31902464	Hw	1
	CL3 for AppDirector4004/OSD1/2Gb/HDD/RoHS S/N 21902864	Hw	1
	FIREPASS SERVICE: STANDARD, (Level 1-3) -F5-FP-4110-RS	Hw	1
VPN-SSL FIREPASS	FIREPASS SERVICE: RMA HW REPLACEMENT (NEXT DAY) - F5	Hw	1
	SERVICE: LAPSED SERVICE FEE	Hw	1
BLUECOAT	RENEWAL SG810-10-PR	Hw	1
	RENEWAL SOFTWARE ONLY, 1 YR, SG810-10-PR	Sw	1
FORTINET	FG-310B	Hw	1
	FG-310B	Hw	1
DRAGON	DSIMBA7-SE	Sw	1
NAC	NAC-A-20 / NS-AB-50	Sw	2

RTVM, dispone de dos barreras de Firewall, una orientada a establecer las políticas de acceso y control en su perímetro de comunicaciones (ISG-1000 Juniper), la otra orientada al control de acceso de la Red corporativa, así como el enrutamiento entre VLAN'S.

RTVM, acometió una segmentación de su LAN que actualmente soportan los dos Firewall Fortinet G310, y cuya consolidación formará parte de este proceso, a alto nivel este es el diseño de la RED definido en la política de segmentación de RTVM:



Por este motivo, la infraestructura de nueva provisión debe ser FORTINET, el objetivo es consolidar las políticas de seguridad actuales y ampliar la aplicación de nuevas funcionalidades con el objetivo de cumplir con las expectativas de la organización. En este sentido FORTINET es líder en este tipo de tecnologías tal y como se recoge en los análisis realizados por GARTNER.



SITUACIÓN OBJETIVO

RTVM requiere la renovación de su infraestructura de su cluster de Firewall de Perímetro, así como de su cluster de Firewall NAC, con el objetivo de paliar obsolescencia tecnológica y consolidar infraestructura de servicio en una nueva arquitectura.

Se debe garantizar la disponibilidad y correcto funcionamiento de los sistemas del esquema anterior y detallados a continuación, estableciendo las acciones necesarias para la resolución de las incidencias presentadas en dicha infraestructura y aportando el nivel de servicio necesario para la administración y explotación de la misma.

Por tanto y con el objetivo descrito de nuevos equipos Firewall de nueva generación FORTINET 500E, como modelo anteriormente, RTVM requiere también el suministro, instalación y puesta en marcha de un cluster base de requerimientos mínimos, que garanticen el correcto funcionamiento del sistema con el siguiente alcance:

1. Diseño Arquitectura:

- Elaboración de una nueva arquitectura de comunicaciones de Seguridad Perimetral a partir de los elementos de LAN, WAN existentes.

2. Diseño Políticas:

- Definición y establecimiento de las políticas de seguridad, comunicaciones in/out, calidad de servicio, disponibilidad, antivirus, antimalware, e integración con el Directorio Corporativo.

3. Equipamiento Firewall:

- Provisión, instalación, configuración y soporte tecnológico de un cluster Next Generation Firewall que reemplace y consolide los equipos actuales JUNIPER ISG-1000 x 2 (obsolescencia tecnológica) y los Fortigate FG310 (2).

4. Reacondicionamiento Infraestructura:

- Integración infraestructura.
- Interconexión de componentes.
- Recableado.
- Identificación de cableado y saneamiento de los actuales.

5. Servicio de Soporte y Mantenimiento

- Administración y explotación de los sistemas que se describen en este apartado mediante la ejecución de las peticiones remitidas al servicio por RTVM.
- Soporte y mantenimiento de los sistemas que se indican objeto de renovación de acuerdos con fabricante, mediante la resolución de

incidencias y la gestión de solicitudes.

- Servicio de soporte incidencias 24x7x365.
- En el ámbito del servicio, el proveedor realizará un cambio de versión mayor para cada una de los sistemas incluidos en el alcance tecnológico donde se incluya la renovación con acuerdos de fabricante.
- El proveedor debe definir el coste/jornada para las tareas de análisis, definición y apoyo a integración de sistemas de seguridad – estas tareas no están incluidas dentro del alcance del servicio-.
- El proveedor debe realizar las correspondientes tareas de seguimiento y control del servicio, tareas de gestión, en definitiva, para garantizar los niveles de servicio comprometidos.
- Se requiere de un canal para la gestión de incidencias, peticiones y/o cambios que garantice la trazabilidad de las actividades realizadas mediante su correspondiente registro.

3. DESCRIPCIÓN DEL SERVICIO

RTVM se propone mantener el modelo, es decir, contar con un servicio único, cuyo objetivo principal sea gestionar y ejecutar los trabajos necesarios para asegurar el correcto funcionamiento y evolución de la infraestructura, procesos y sistemas considerados.

SERVICIOS PREVISTOS

Los servicios considerados son en términos generales:

- Diseño, implantación e integración de la nueva Arquitectura de Seguridad Perimetral.
- Suministro, instalación y puesta en producción del nuevo equipamiento de Seguridad Perimetral. (Retirada del equipamiento obsoleto)
- Diseño y aplicación de políticas de seguridad:
 - Integración Directorio Activo.
 - Antivirus.
 - Análisis de Tráfico.
 - QOS.
 - Antimalware,
 - SSL remoto.
 - Despliegue de los elementos de valor añadido de la solución con todas sus capacidades tal y como quedan descritos en los requerimientos técnicos.
- El soporte a usuarios de SSII y la resolución de incidencias, en horario 24x7x365.
- El soporte operativo necesario para la explotación y operación de los sistemas y tecnologías que lo soportan, en horario de 09:00h a 19:00h de lunes a viernes.
- El mantenimiento correctivo, preventivo y evolutivo de los sistemas y módulos. Acuerdos de tercer nivel con fabricante.

- Mantenimiento preventivo de la infraestructura objeto del servicio 24x7.
- Duración del contrato **3 años** que incluyen:
 - Garantía, mantenimiento hw/sw de nueva provisión.
 - Servicio gestionado de seguridad Perimetral.
 - Renovación hw/sw: AppDirector, NAC, Netsight.

Adicionalmente, el proveedor se compromete a facilitar los indicadores y configuraciones necesarias para integrar esos indicadores dentro de la plataforma de monitorización de RTVM.

SUMINISTRO NUEVO EQUIPAMIENTO

RTVM requiere un nuevo sistema de protección Firewall de Nueva Generación FORTINET 500E o superior, con capacidad de configuración activo/pasivo o activo/activo con las siguientes capacidades:

- El cortafuegos debe tener las certificaciones de Internet Computer Security Association (ICSA): Cortafuegos, IPSec, IPS, Antivirus, SSL VPN; NSS Labs y Common Criteria.
- El cortafuegos dispondrá de hasta 36/36/32 Gbps de rendimiento de firewall con la unidad base, para el tipo de tamaño de paquete (1518/512/64 bytes, UDP).
- Debe ser capaz de manejar 8 Millones de sesiones concurrentes (TCP).
- El cortafuegos debe ser capaz de manejar hasta 300.000 nuevas sesiones por segundo (TCP).
- El cortafuegos debe tener una latencia de 2 μ s (para paquetes 64 byte UDP).
- El cortafuegos dispondrá de hasta 5.2 Gbps de rendimiento de IPS; y de 5 Gbps con IPS, control de aplicaciones y antivirus, los tres activados conjuntamente.
- Capacidad de web cache integrado en el mismo cortafuegos.
- Capacidad de configuración de proxy explícito por interfaz, con posibilidad de hacer caching en caso de ser necesario.
- Visualización de número de usos y cantidad de tráfico de cada regla. Así como de la última vez que se ha utilizado.
- Capacidad de realizar escaneo de vulnerabilidades de forma programada o expresa en ciertas redes.
- El sistema propuesto debe tener una funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante en la misma política de seguridad, incluyendo las siguientes características:
 - Capaz de establecer el ancho de banda garantizado dentro la política de cortafuegos.
 - Capaz de establecer el ancho de banda máximo asignado dentro la política de cortafuegos.
 - Capaz de establecer el ancho de banda máximo asignado por IP.
 - Capaz de establecer mínimamente 3 niveles de priorización.
 - Capaz de marcar el tráfico con DSCP.
- Los equipos deben tener las funcionalidades integradas de IPS, antivirus (en dos modos flujo o proxy), Antispam y filtrado de contenidos o categorías web. No se

acepta ningún acuerdo OEM con terceros, es decir, todas estas funcionalidades tienen que ser del propio fabricante de seguridad.

- El licenciamiento de las funcionalidades ha de basarse por equipo, no por usuario.
- El sistema propuesto deberá permitir tener un apoyo mínimo de:
 - 8 interfaces GE RJ45.
 - 8 interfaces GE SFP slot.
 - 2 interfaces 10GE SFP+ slot.
 - 2 interfaces de gestión GE RJ45.
 - 1 puerto de consola.
 - 1 puerto USB.
- El equipamiento no debe superar 1RU y montaje en rack.
- Capacidad de conexión de modem 3G/4G en el puerto USB para conexión WAN ya sea principal o secundaria.
- Capacidades de virtualización: Los equipos deben disponer de al menos 10 dominios virtuales incluidos en los cortafuegos sin coste adicional. El sistema tiene que indicar el uso de CPU/Memoria por cada uno de los dominios virtuales.
- Controlador Wireless integrado con rendimiento de CAPWAP 18 Gbps (sin licencias).
- Máximo número de APs 512/256 (Total/Túnel).

Adicionalmente, la solución debe tener las siguientes características avanzadas:

CONTROL DE APLICACIONES

- Capacidad para identificar un mínimo de 2800 aplicaciones activas actuales (incluyendo aplicaciones Web 2.0)
- La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación)
- Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
- Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red.
- Deberá permitir la creación de firmas personalizadas de IPS y control de aplicaciones.
- Capacidad para identificar las aplicaciones bajo túneles HTTPS.

IDENTIFICACIÓN DE USUARIOS

- Identificar usuarios integrándose con Microsoft Active Directory y Novel eDirectory
- Control de usuarios Citrix.
- Control de usuarios de Microsoft Terminal Server.
- Soporte de mensajes Radius Accounting para Single Sign On.
- Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+.
- Poder generar usuarios de tipo invitado que caduquen al cabo de un tiempo configurable una vez se creen o bien cuando se inicien sesión. Además, el sistema tiene que permitir el acceso de usuarios invitados con una GUI sencilla y sin acceso a ningún otro parámetro de la gestión del firewall.

VISIBILIDAD

- Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites y aplicaciones cloud) para su visualización.
- Esta visualización tiene que ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.
- Se tiene que poder seleccionar un tiempo de logs de hasta 24 horas, así como de tráfico que se está procesando en el firewall y que todavía no ha generado evento de log (o "Now"), conocer a que política de seguridad está aplicando y poder cerrar una sesión desde la misma visualización.

FILTRADO DE CONTENIDOS

- Monitorizar y controlar la navegación web sin penalizar el tiempo de respuesta ni la satisfacción del usuario.
- Tomar decisiones en tiempo real como permitir / denegar una URL basándose en políticas y en una base de datos de URLs mundiales que permita establecer controles para un filtrado granular de las URLs.
- Capacidad de asegurar la navegación segura en el buscador GoogleSearch, así como la capacidad de cambiar imágenes de url no licitas por espacios en blanco.
- El filtraje URL debe tener la funcionalidad de aplicar cuotas de tiempo para aquellas categorías deseadas. También ha de permitir crear categorías personalizables como listas blancas/negras.
- Además, la plataforma tiene que tener la capacidad de hacer filtrado basado en las peticiones DNS y las categorías URL, así como poder hacer un sinkhole engañando así a la amenaza.

SEGURIDAD

- Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.
- Capacidad para definir múltiples reglas de seguridad en las interfaces origen / destino, incluyendo "fecha".
- Debe soportar varios modos de funcionamiento:
 - Modo transparente.
 - Modo routed y / o modo sniffer.
- Prevención de amenazas en tiempo real, detectando un amplio abanico de malware y exploits de vulnerabilidades (virus, spyware, gusanos, etc.) sin incurrir en latencia.
- Funcionamiento como IPS basado tanto en patrones como en "Rule based". Posibilidad de crear firmas de IPS customizadas.
- DLP: capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como a asociaciones concretas. Más funcionalidades:

- Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de archivo, diccionario, plantillas corporativas
- Detección e identificación de documentos mediante "Fingerprint"
- Posibilidad de añadir marcas de agua en los documentos de office.
- Descarga y aplicación automática de actualizaciones de las firmas antivirus, antispyware, base de datos de URL's, firmas IPS y de las nuevas aplicaciones identificadas.
- Funcionalidad integrada de doble factor de autenticación vía token hardware o software, así como por SMS, integrado en la misma plataforma de seguridad.
- Funcionalidad de reconocimiento del tipo de dispositivo del cliente (Iphone, Ipad, Android, etc...) y poder hacer políticas en función del tipo de dispositivo, sin la instalación de ningún agente en el dispositivo remoto.
- Soporte para tráfico VoIP: SIP/H.323 /SCCP NAT transversal, RTP
- Soporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Definición de objetos para aplicación en políticas de seguridad, de diferentes tipos: IP, Subnet, intervalo de IPs, Geografía y FQDN
- Detección y bloqueo de botnets en base a listas de reputación globales.
- Inspección de tráfico cifrado SSL mediante rotura de túnel SSL y mediante inspección de certificados.

VPN

- El dispositivo dispondrá de hasta 5 Gbps de rendimiento de VPN SSL y 20 Gbps de rendimiento IPsec (paquetes de 512 bytes).
- El dispositivo admite hasta un máximo de 500 usuarios simultáneos VPN SSL sin licencia alguna.
- El sistema propuesto deberá cumplir los estándares de la industria, sin el apoyo externo adicional de hardware o módulos:
 - IPSEC VPN
 - PPTP VPN
 - L2TP VPN
 - SSL VPN
- Poder crear arquitecturas de creación dinámica de VPN site-to-site mediante estándar ADVPN.
- El sistema propuesto deberá soportar 3 modos de funcionamiento SSL VPN:
 - Sin cliente - Acceso web: para clientes remotos que sólo necesitan un navegador y no requiere la instalación de ningún software, a fin de acceder vía web en: HTTP / HTTPS Proxy, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP. El acceso RDP tiene que ser vía HTML, no con tecnología Java.
 - Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor

ALTA DISPONIBILIDAD

- Failover Activo / Pasivo, Activo / Activo y clustering sin necesidad de licencia.

- Capacidad de virtual clustering con los dominios virtuales. Esta capacidad tiene que permitir configurar poder tener el nodo master de diferentes dominios virtuales de forma cruzada dentro del mismo cluster.
- Sincronización de configuración y sesiones.
- Interfaces reservados para gestión.
- Posibilidad de configurar interfaces HeartBeat redundantes.
- Reposición automática del Servicio:
 - Monitorización de interfaces (locales y remotos).
 - Sin pérdida de sesiones.
 - Conmutación en menos de 1 segundo.
- Diferentes opciones de arquitectura:
 - HA con agregación de enlaces.
 - Full mesh HA.
 - Soporte de clúster geográfico (equipos en distinta ubicación física).

NETWORKING

- Soporte de protocolos soportar RIP v1 y v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6.
- Routing basado en política.
- Soporte Dual Stack IPv4 e IPv6 simultáneamente.
- Network address translation NAT IPv4, NAT64 y NAT66.
- DHCP server / DHCP Relay
- DNS Server y DNS Proxy
- NTP Server
- 802.1Q VLANs
- Routing basado en contenidos: ICAP y WCCP
- Point-to-Point Protocol over Ethernet (PPPoE).
- 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.
- Capacidad de balanceo de servidores, con posibilidad de hacer SSL off-loading para el tráfico HTTPS.
- Capacidad de funcionalidad de VXLAN sobre túneles IPSec.
- Servicio de DDNS integrado en el equipo para más de una interface.

GESTIÓN Y ADMINISTRACIÓN

- Soporte de SNMP.
- Exportación de logs vía FTP, SCP y TFTP.
- Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente en máquina externa al firewall para su administración y / o cualquier otra función del firewall.
- Creación de diferentes cuentas de administración con diferentes niveles de acceso.
- Aplicación de cambios de forma inmediata, sin ninguna espera en su aplicación.
- Compatibilidad de sFlow y Netflow.

BALANCEO ACCESO INTERNET

- El sistema debe ser capaz de realizar un balanceo de carga de los enlaces de Internet de forma dinámica con métodos opcionales de:
 - Por volumen.
 - Por sesiones.
 - Por IP de origen.
 - Por IP de origen + IP destino.
 - Spill-over (también llamada basada en el uso).
 - Según la calidad de la línea de internet, utilizando la latencia y jitter (de forma dinámica).
- El sistema debe ser capaz de proporcionar redundancia de enlaces WAN monitorizando el estado de las líneas.
- También se debe poder balancear el tráfico de salida en función del servicio utilizado en internet. Para ello el equipo deberá contener una base de datos predefinida con las aplicaciones de internet identificadas por sus IP públicas, Protocolos y puertos.

SANDBOXING

- Se requiere que los equipos dispongan de un sistema de Sandboxing para detección de amenazas avanzadas mediante un equipamiento adicional físico o virtual (este equipamiento adicional no es objeto de la presente licitación) así como posibilidad de integración con un sistema de sandboxing en la nube mediante licencias adicionales (estas licencias no son objeto de la presente licitación).

SISTEMA DE REPORTING E INFORMES

La nueva plataforma de seguridad Firewall debe incluir un sistema de reporting centralizado que, mediante informes fácilmente personalizables, permita a los usuarios filtrar y revisar las grabaciones, analizar y visualizar rápidamente las amenazas de red, ineficiencias y su uso. Debe tratarse de una plataforma gráfica que entre otras características disponga de:

- Gráficos predefinidos y personalizables.
- Identificación de patrones de ataque y cumplimiento de políticas.
- Funciones de gestión de seguridad avanzadas:
 - Archivado de ficheros en cuarentena.
 - Correlación de eventos.
 - Evaluaciones de vulnerabilidad.
 - Análisis de tráfico.
 - Archivado de email, acceso web, mensajería instantánea y transferencia de archivos de contenido.

SERVICIO GESTIONADO: ADMINISTRACIÓN & EXPLOTACIÓN

ALCANCE FUNCIONAL

GESTIÓN DE INCIDENCIAS Y PETICIONES

La infraestructura que se soporta dentro del servicio es de uso exclusivo de RTVM.

RTVM plantea trabajar de acuerdo al siguiente esquema:

SOPORTE A LA OPERACIÓN & EXPLOTACIÓN

Se considerará en el ámbito del servicio las demandas procedentes del Grupo de Operaciones y Explotación. Son solicitudes que realizarán usuarios de Sistemas de Información de acuerdo al protocolo que se establezca.

Las acciones asociadas son:

- Soporte y apoyo a la explotación y administración de los diferentes entornos.
- Resolución de consultas técnicas.
- Soporte a incidencias.

Principales Actividades:

- Soporte al equipo funcional de RTVM:
 - Copia de seguridad de las configuraciones de los equipos objeto del servicio.
 - Incidencias hardware.
 - Recuperación datos.
 - Soporte a procesos de puesta en producción que pudieran verse afectados.

HELP DESK DE SEGUNDO NIVEL-ACCESO TERCER NIVEL (FABRICANTE)

El Help Desk de segundo nivel será cubierto íntegramente por el servicio, y:

- Recibirá las incidencias y peticiones del equipo de soporte de RTVM.
- A partir de ello, desarrollará cuantas acciones de tipificación, registro, solución o paliación, etc., resulten necesarias.
- Mantendrá disponible la información general sobre la incidencia o petición, para su consulta por RTVM.
- Una vez resuelta la incidencia o petición, informará al servicio de Soporte de primer nivel con un extracto de la solución.

El Help Desk de segundo nivel se ocupará típicamente de las incidencias y peticiones de tipo técnico, si fuera necesario acceder al soporte del fabricante (tercer nivel), será también responsabilidad de éste equipo gestionar la correspondiente solicitud y realizar las gestiones oportunas.

El Help Desk de segundo nivel estará disponible:

- En régimen remoto (sólo presencial en escenarios especiales).
- En régimen de guardia localizada, tal cual se consensue.

Deberá existir un tiempo acordado de respuesta, y otro de solución, para cada tipo concreto de incidencia y un mecanismo que permita asegurar la trazabilidad permanente.

MANTENIMIENTO CORRECTIVO

Se cubrirá en el ámbito del servicio el mantenimiento en operatividad de los sistemas en cuanto a su parametrización, solucionándose cualquier mal funcionamiento existente debido a errores en la parametrización, desarrollo o ejecución; contribuyendo al análisis y solución de problemas de acceso o rendimiento; y ejecutando maniobras sobre la información cuando ello sea necesario y esté autorizado por RTVM.

Estarán incluidas las actuaciones necesarias para resolver problemas incluso si fueron causados por malas operativas de los usuarios de RTVM, si bien, en este caso, se podrán proponer acciones de formación que contribuyan a elevar el grado de conocimiento de los usuarios y/o la implantación de medidas técnicas u organizativas para minimizar este tipo de escenarios.

En general el funcionamiento incorrecto del sistema podrá deberse a distintas causas:

- Problemas de firmware.
- Problemas de configuración o software.
- Problemas causados por una operación errónea de los usuarios.

Se considerará también incluida la revisión de parches de cualquier tipo. La instalación de los mismos está incluida en el alcance del servicio así como la correspondiente revisión, sobre los distintos entornos de cada sistema, que certifique si la aplicación del parche ha sido correcta, para evitar que se produzcan errores fortuitos y se asegure que están adecuadamente probados en los entornos previos.

Las acciones asociadas son:

- Análisis y resolución de las consultas e incidencias.
- Realización de los cambios oportunos para corregir el funcionamiento incorrecto del sistema sin alterar las especificaciones funcionales/técnicas de la plataforma actual de RTVM.
- Gestión del proceso de mejora continua que permita la mejora de las aplicaciones actuales y la reducción progresiva de incidencias. (Mantenimiento Perfectivo)
- Gestión de la política de autorizaciones y actualización de parches de forma coordinada con el servicio de explotación de RTVM.

Principales Actividades:

- Soporte al responsable asignado por RTVM y a los usuarios claves.
- Análisis-diagnóstico de errores y sus causas.
- Instalación de soluciones eventuales.

- Realización de correcciones.
- Pruebas de las modificaciones.
- Implantación de los módulos corregidos.
- Análisis de incidencias recurrentes, propuesta de soluciones e implantación de las mismas.
- Seguimiento e información del avance de las alertas y/o incidentes.
- Actualización de la documentación.

MANTENIMIENTO PREVENTIVO

RTVM requiere una serie de procesos de carácter preventivo adicionales a los que ya dispone en la actualidad, basados en la monitorización continua, con objeto de garantizar el estado operativo de la plataforma y la disponibilidad de los servicios que proveen.

Las acciones asociadas son:

- Chequeo y seguimiento de la infraestructura.
- Chequeo y seguimiento de los procesos, servicios, aplicaciones, tareas, jobs, etc que se soportan en cada momento.

Principales Actividades:

- Revisión periódica, diaria y/o semanal, según se consensue por sistema/entorno:
 - Revisión del estado del sistema.
 - Monitorización de Log.
 - Revisión dumps y errores.
 - Monitorización de tiempos de respuesta.
 - Revisión de las copias de seguridad.
 - Plan de recuperación de entornos:
 - Firewall DMZ.
 - Balanceadores Línea.
 - Balanceadores Aplicaciones.
 - Firewall Internos.

Consideración.-

RTVM, cuenta con una plataforma de monitorización, basada en Zabbix, que debe considerarse como plataforma de soporte a este proceso. Actualmente ya soporta parte de los procesos de chequeo que se solicitan y que forman parte del ámbito servicio.

REGISTRO Y ESCALADO

La empresa adjudicataria deberá ofrecer a RTVM el servicio necesario con un único punto de entrada para registrar las diferentes peticiones de los usuarios.

Principales Actividades:

- Recibir y registrar las peticiones mediante herramientas propias.
- Documentar el estado de las peticiones e incidencias.
- Escalado de acuerdo al circuito consensuado.
- Acceso WEB, correo y teléfono para RTVM para el seguimiento de las peticiones.

ALCANCE TECNOLÓGICO

El siguiente cuadro detalla la infraestructura objeto de los servicios de administración, operación y explotación:

FABRICANTE	PRODUCTO	SW/HW	CANTIDAD
RADWARE	CL3 APPDIRECTOR 4004	HW	2
EXTREME NETWORKS	NAC-A-20 NS-AB-50	SW	2
FORTINET	FG310B	HW	2
JUNIPER NETWORKS	JU SVC-SD-ISG1000-SMS	HW	1

Adicionalmente a este equipamiento, el licitador deberá mantener la nueva plataforma de seguridad firewall propuesta, así como las herramientas de sandboxing y reporting exigidas.

A continuación, a título informativo, se exponen algunos aspectos de la infraestructura tecnológica asociada con las aplicaciones objeto del servicio que se solicita.

Toda la infraestructura objeto del servicio se encuentra redundada:

FIREWALL - NGN

El Nuevo equipamiento Firewall requerido dispondrá de las siguientes funcionalidades:

- Next Generation Firewall
- Antivirus
- Antispam
- IDS

- IPS
- Acceso Remoto SSL
- Balanceadores de Líneas
- Caché de Navegación
- Sandboxing
- Herramienta de Generación de Informes y Almacenamiento de Logs.

BALANCEADORES DE LÍNEA

RTVM dispone de dos líneas de internet con direccionamiento ip diferenciado, dispone de dos balanceadores de línea Linkproof 200, estos dispositivos posibilitan disponer de alta disponibilidad desde y hacia internet además de dotar a RTVM de HA y balanceo de carga. Uno de los objetivos del servicio es desacoplarlos de la arquitectura objetivo.

BALANCEADORES DE APLICACIÓN

RTVM dispone de dos balanceadores en HA de Nivel 7, Radware AppDirector, donde están configurados sus portales Web y servicios extranet.

ACCESO REMOTO SSL

El FW NG de nueva adquisición, debe proveer de esta funcionalidad.

FIREWALL

RTVM dispone de dos parejas de firewall:

- Juniper ISG1000: Control de perímetro.
- Fortinet: FG 310-B, servicios de routing y segmentación de VLAN'S.

Forman parte como objetivo de proyecto su sustitución por la nueva infraestructura NGN Fw.

NAC

RTVM dispone de NAC, con las siguientes características: NAC-A-20 / NS-AB-50, actualmente la red de RTVM está segmentada con protocolo 802.1x, e integrada con el NAC de Xtreme (Enterasys) y Directorio Activo.

METODOLOGÍA

Desde el punto de vista de enfoque metodológico los licitadores deberán:

- Aplicar una metodología basada en ITIL (Information Technology Infrastructure Library) en la solución propuesta.
- Especificar claramente la metodología propuesta para la prestación del servicio, incluyendo todas aquellas certificaciones que avalen el seguimiento y utilización de ésta.
- Presentar un modelo orientado hacia la gestión de servicios mediante la definición de ANS/SLA (Acuerdo de Nivel de Servicio) y OLA (Niveles de Servicio Objetivo)
- Presentar una propuesta normalizada de procesos y procedimientos de gestión.
- Presentar una propuesta normalizada de procesos y procedimientos operativos.

ORGANIZACIÓN DEL SERVICIO

El servicio requerido por RTVM deberá estructurarse sobre las siguientes hipótesis de partida:

- Servicio remoto con posibilidad de presencia local.
- Servicio técnico, funcional y de desarrollo de segundo y tercer nivel en español.
- Herramienta propia de gestión del servicio.
- Horarios de servicio: 24x7x365.

Consideración.-

RTVM considerará falta grave la no disponibilidad del servicio eventualmente en las franjas horarias previstas si previamente no se le ha notificado y se han presentado alternativas, siendo esto causa suficiente para proceder a la rescisión del contrato.

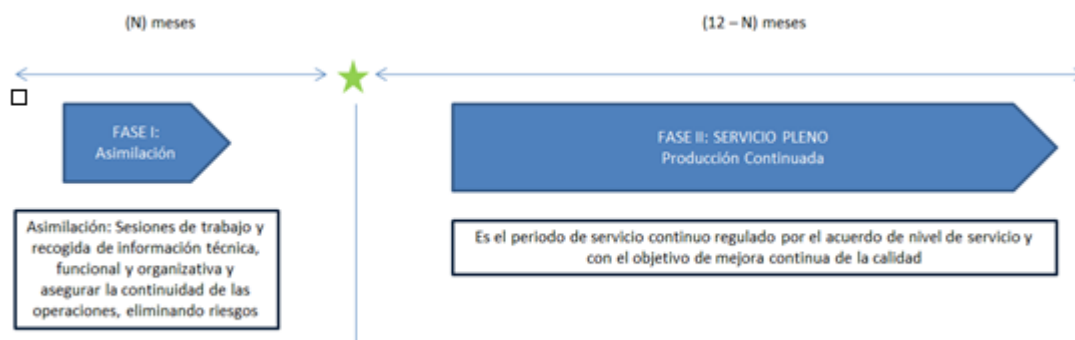
Infraestructura requerida para la prestación del servicio:

- El Centro de Soporte al Usuario se encontrará en las instalaciones del proveedor del servicio.
- El proveedor de servicio pondrá a disposición de RTVM al menos un número de teléfono para las llamadas que realicen los usuarios del servicio al centro de soporte.
- El proveedor de servicio dimensionará y establecerá una línea de conexión de datos con RTVM que garantice la seguridad, la capacidad y la disponibilidad. Toda la infraestructura necesaria, tanto hardware como software o de comunicaciones, correrá a cargo del adjudicatario, que deberá implementar las medidas de seguridad oportunas para garantizar la confidencialidad, integridad y disponibilidad de la información.
- El servicio deberá dimensionarse de forma no exclusiva para RTVM. El ofertante deberá presentar su hipótesis de dimensionamiento y los criterios a aplicar para cumplir con los requisitos de RTVM.

Dentro de la prestación del servicio, se podrán incluir nuevas tareas cuya necesidad se detecte durante la ejecución del contrato. Los ofertantes deben incluir en su propuesta aquellas actividades adicionales que deben asumir desde su centro de atención remota que no se hayan incluido anteriormente.

PLAN DE IMPLANTACIÓN DEL SERVICIO

Los ofertantes deberán presentar un plan de transferencia y transformación del servicio requerido, conteniendo al menos:



- Propuesta de **Plan de Asimilación** del servicio incluyendo (al menos):
 - Alcance y objetivos de la fase.
 - Cronograma detallado de la fase.
 - Hitos responsabilidad del ofertante.
 - Hitos responsabilidad de RTVM.
 - Niveles de servicio objetivo de esa fase y penalizaciones asumibles.
 - Quick Wins objetivo.
 - Documentación generada.
- Propuesta de **Plan para el Servicio Pleno** incluyendo (al menos):
 - Alcance y objetivos de la fase.
 - Cronograma detallado de la fase.
 - Hitos responsabilidad del ofertante.
 - Hitos responsabilidad de RTVM.
 - Niveles de servicio objetivo de esa fase y penalizaciones asumibles
 - Quick Wins objetivo.
 - Documentación generada.

RTVM garantiza una semana de asimilación del servicio desde la adjudicación con disponibilidad y presencia del proveedor saliente. Si el adjudicatario, proveedor entrante, considera oportuno un periodo de solapamiento más largo, será responsabilidad de éste, realizar las gestiones oportunas sin generar ningún impacto en el servicio.

PLAN DE DEVOLUCIÓN DEL SERVICIO

Los ofertantes deberán presentar un plan de devolución del servicio (independientemente de la causa), conteniendo al menos:

- Inventario.
- Base de datos de conocimiento.
- Incidencias generadas y análisis de tendencias.
- Planes para el cierre de acciones en curso (considerando garantías).
- Formación al nuevo equipo responsable de la prestación.
- Cronograma detallado de la fase.
- Hitos responsabilidad del ofertante.
- Hitos responsabilidad de RTVM.
- Documentación generada.
- Otros aspectos considerados por el ofertante.

GOBIERNO DEL SERVICIO Y REPORTING

El ofertante deberá realizar una propuesta de estructura de Gobierno del servicio, comprendiendo en ella niveles operativos, de gestión del servicio y de seguimiento del contrato.

De la misma forma, el ofertante deberá identificar un Responsable de Servicio como interlocutor con el Responsable del Servicio identificado en RTVM.

En línea con lo mencionado anteriormente:

- Existirán reuniones de seguimiento de la actividad de forma semanal entre el Responsable de Servicio de la empresa adjudicataria y el Responsable del Servicio de RTVM para el análisis de los indicadores diarios y semanales, identificación y seguimiento de planes de acción e identificación de problemas que requieran escalado a niveles superiores.
- Existirá un grupo de control del servicio por personal de RTVM y personal de la empresa adjudicataria para:
 - Supervisar el funcionamiento y evolución del servicio.
 - Analizar y aprobar las modificaciones del servicio, mejoras y su reestructuración para conseguir que el funcionamiento del servicio logre alcanzar los objetivos en un momento determinado.
 - Decidir la solución más adecuada en caso de conflicto o problemas de interpretación.
 - Movilizar los recursos que sean necesarios para responder a posibles situaciones críticas.
 - Revisión de objetivos a corto plazo.
 - Este grupo se reunirá de forma periódica al menos una al mes y extraordinariamente siempre que lo requiera alguno de sus miembros.
 - Otras acciones a proponer por el ofertante.
- Existirá un grupo de gobierno del contrato formado por personal de RTVM y personal de la empresa adjudicataria para:
 - Analizar los niveles de SLA y OLA.

- Revisar los cumplimientos de SLA y sus penalizaciones asociadas.
- Revisar el estado de los planes de acción en curso. Revisión de objetivos a medio y largo plazo.
- Tomar decisión en caso necesario para el desbloqueo o priorización de determinadas acciones.
- Otras acciones a proponer por el ofertante.

Además de la estructura de Gobierno del Servicio requerida anteriormente, RTVM desea recibir informes periódicos de actividad y de cumplimiento de los niveles de servicio para los distintos procesos objeto del contrato.

Los objetivos a cumplir con la generación de estos informes son los siguientes:

- Proporcionar información periódica de los niveles de servicio alcanzados en la prestación del servicio.
- Proporcionar una base documental para las reuniones de seguimiento del servicio.
- Obtener una visión clara de la situación del servicio y permitir actuar con eficacia en caso de cambios en el entorno o desviación de los resultados respecto de lo planificado.
- Identificar y destacar cualquier necesidad de cambio en el nivel de servicio estipulado.
- Identificar hechos relevantes y su impacto en el nivel de servicio.
- Proporcionar información periódica sobre los volúmenes reales de actividad de cada uno de los servicios.

La empresa adjudicataria habrá de realizar al menos los siguientes tipos de informes:

- **Informe operativo (semanal):** Este informe se centrará principalmente en la Gestión de Solicitudes e Incidencias, e incluirá al menos:
 - Hoja resumen con total de incidencias/peticiones.
 - Descripción detallada de las peticiones no resueltas de larga duración.
 - Distribución de peticiones e incidencias por servicio (causa raíz).
 - Estudio de SLA incumplidos si fuera el caso.
 - Resumen de Cambios, Problemas y las Incidencias asociadas a los mismos.
 - Otros a considerar por el ofertante o a incluir durante la vida del contrato.
- **Informe ejecutivo (mensual):** El propósito de este informe es proporcionar una visión general del servicio y contendrá al menos:
 - Indicadores claves del servicio (SLA y OLA): Medida de cada uno de los indicadores correspondientes a los diferentes procesos y representación gráfica en términos de cumplimiento actual y tendencia.
 - Aspectos relevantes acaecidos en el periodo en estudio.
 - Gráficos y resumen del estado general.
 - Tareas planificadas, resueltas y aún no resueltas.
 - Tareas planificadas pendientes de ejecución (tareas previstas para el siguiente periodo que permiten mejorar la calidad del servicio).
 - Información cuantitativa sobre el cumplimiento de los diferentes indicadores de gestión del servicio.
 - En caso de incumplimiento de los objetivos: justificación de los resultados, medidas correctoras que se piensan poner en funcionamiento para evitarlos en un futuro y valoración de los efectos e impactos derivados.
 - Mejora Continua (periodicidad al menos trimestral): plan con iniciativas

realistas, estrategia de implantación.

- Gestión de peticiones e incidencias.
- Información sobre los procesos de gestión de incidencias y peticiones.
- Gráficos evolutivos del volumen de peticiones e incidencias.
- Información y gráficos de los diferentes servicios.

Consideración.-

El informe ejecutivo –mensual- debe contar con un apartado específico donde se señalice las penalizaciones, si procede, y se valore económicamente las mismas.

RECURSOS Y PERFILES INVOLUCRADOS

Todo el personal debe estar, al menos formado en metodología ITIL y globalmente el equipo debe estar certificado en todas las tecnologías implicadas. Se debe adjuntar las correspondientes acreditaciones.

Para garantizar el soporte de calidad en ITIL, la empresa poseerá al menos dos personas con titulación Service Manager en ITIL o equivalente que deben pertenecer a la empresa. Dentro de la documentación de la oferta, la empresa incluirá el curriculum y formación en ITIL de dichas personas así como las correspondientes certificaciones.

Además del personal necesario para la prestación del servicio, la empresa dispondrá la infraestructura organizativa, tanto material como personal, necesaria para la realización de las siguientes tareas:

- Coordinación con los técnicos responsables del Servicio de RTVM.
- Elaboración de los grupos de trabajo y control de ausencias. Coordinación de sus técnicos.
- Redacción y presentación de informes de seguimiento.
- Supervisión y control de las tareas de los técnicos y de los documentos e informes que presentan a usuarios claves.

Consideración.-

No se justificará en ningún caso que la documentación entregada no responda a versiones aceptables en forma y fondo. Los usuarios claves son además usuarios funcionales y la calidad de los contenidos debe ser la adecuada.

La empresa licitadora propondrá y especificará a RTVM el número y distribución horaria de los recursos destinados a la prestación del servicio del presente contrato, así como la estrategia propuesta para cubrir bajas eventuales en el personal del centro de soporte local.

La empresa adjudicataria se compromete a tener siempre disponible para el servicio un

número de personas suficiente para garantizar los SLAs exigidos, debiendo realizar la correspondiente sustitución del personal de baja o permiso por personal técnico de una titulación y experiencia similar a los técnicos titulares propuestos.

Cada ofertante deberá presentar una propuesta de perfiles para los técnicos y responsables de la prestación del servicio. RTVM requiere para cada uno de ellos la siguiente información:

- Gestor del Contrato (tiempo parcial):
 - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido. (RTVM requiere un ingeniero Técnico o Superior para la prestación de éste servicio o equivalente)
 - Currículum Vitae.
 - Perfil y certificaciones.
 - Experiencia demostrada de más 8 años.
- Responsable del Servicio (tiempo parcial):
 - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido. (RTVM requiere un ingeniero Técnico o Superior para la prestación de éste servicio o equivalente)
 - Currículum Vitae.
 - Perfil y certificaciones.
 - Experiencia demostrada de más 4 años.
- Técnico de Soporte:
 - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.
 - Dominio demostrable de las herramientas e infraestructuras para la prestación del servicio.
 - Currículum Vitae.
 - Perfil y certificaciones.
 - Experiencia demostrada de más 2 años.
- Consultor Especialista:
 - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.
 - Dominio demostrable de las herramientas e infraestructuras para la prestación del servicio.
 - Currículum Vitae.
 - Perfil y certificaciones.
 - Experiencia demostrada de más 3 años en la prestación de servicios similares.

Asimismo, la empresa entregará el currículum nominal de los consultores certificados en las diferentes plataformas objeto del servicio. Cualquier cambio en el equipo propuesto deberá ser validado previamente por RTVM y la empresa deberá justificar el porqué de dicho cambio. Sin detrimento de lo anteriormente expuesto, en caso de producirse algún cambio en el equipo titular propuesto, dicho cambio se podrá realizar únicamente por perfiles iguales o superiores a los ofertados.

4. MODELO DE FACTURACIÓN

El modelo de facturación responderá al siguiente esquema:

- Servicio mensual.
- Provisión de Infraestructura 30% (infra).
- Implantación y puesta en marcha nueva infraestructura 100% (infra).
- Renovación acuerdos fabricante un solo pago.
- Las tareas finalizadas y aceptadas por los correspondientes usuarios claves serán tareas facturables en base al cumplimiento de los SLAs que apliquen.
- No se aceptan servicios de gestión como conceptos variables de facturación.
- Las penalizaciones que procedan aplicarse se valorarán en el mes en curso, en la correspondiente sesión de seguimiento mensual y se harán efectivas en la facturación correspondiente al mes siguiente.

5. NIVELES DE SERVICIO Y PENALIZACIONES

Las empresas licitantes indicarán en sus ofertas los tiempos de actuación máximos a los que se compromete. A continuación se detallan los valores máximos para dichos compromisos, de tal forma que aquellas ofertas que los excedan serán desestimadas.

Es objeto del presente capítulo la definición detallada de los diferentes niveles y su alcance.

En todos los casos se entiende:

- Por tiempo de atención se entiende el tiempo transcurrido entre el momento en que el usuario comunica la incidencia (vía web, email, o telefónica) y el momento en el que la empresa adjudicataria acusa recibo de la misma.
- Por tiempo de resolución se entiende el tiempo transcurrido entre el momento en que el usuario comunica la solicitud o la incidencia y el momento de su resolución definitiva. En caso de que la resolución de la incidencia no sea posible en el tiempo máximo preestablecido, se tomará como tiempo de resolución el transcurrido entre el momento de comunicación de la incidencia y el momento en que el usuario disponga de una solución de contingencia válida que le permita continuar normalmente con su trabajo hasta que la incidencia pueda ser solucionada.

RTVM considera que los Acuerdos de Nivel de Servicio deben estar sometidos a revisiones periódicas como consecuencia de los planes de mejora continua implementados por el proveedor de servicio. En este sentido, los SLA mínimos propuestos por RTVM una vez finalizada la Fase de Transición de servicio son los siguientes:

Tipo de SLA	SLA	Valor	% Penalización
Accesibilidad al servicio	Disponibilidad de servicio (telefónico, mail, web)	➤ 99, 99%	2%
Gestión de Incidencias	Tiempo de atención ante incidencias (95% casos)	< 30 minutos	2%
	Tasa de reapertura de incidencias	< 3 %	2 %
	Tiempo de resolución de incidencias	➤ Críticas: 4 horas ➤ No críticas: 12 horas	2% 2%
Gestión de peticiones	Tiempo de resolución de peticiones de cambios (98% casos)	Sencillos < 48 horas Complejos < 7 días	2%
Documentación	Cumplimiento de procesos de inventario físico, lógico y de documentación. (Revisión Mensual)	➤ 98%	2%

Tipo de SLA	SLA	Valor	% Penalización
Reporting	Cumplimiento de tiempos comprometidos de entrega de informes (Antes del 5º día del mes)	➤ 99%	2%
Mantenimiento Preventivo	Cumplimiento de calendario de mantenimiento preventivo (semanal)	➤ 98%	2%
Configuración Actualizaciones Soft. Parches.	% Cumplimiento política actualización parches. (anual)	> 98 %	2%
Tiempo de Resolución Incidencias Software	Críticas	=< 4 horas	2%
	No Críticas	< 12 horas	2%

Indicadores de nivel de Servicio relativos a la provisión de infraestructura, diseño e implantación.

Tipo de SLA	SLA	Valor	% Penalización
Homologación	Homologación de arquitectura y diseño de comunicaciones.	< 14 días	2%
Integración	Cumplimiento de los requerimientos de Integración del proyecto.	> 7días Desde Plan de acción.	2%
	Cumplimiento calendario plan de acción	➤ 7 días	2%
	Incidencias con Impacto en servicio actual	➤ 1 incidencia	2%
	Reconfiguraciones emergencia	➤ 6 horas	2%

	Nº de cambios resueltos con reclamación posterior RTVM	< 3%	1 %
	Modificación de Servicios	➤ 1 día	2%
Implantación y Despliegue	Cumplimiento de procesos de inventario físico, lógico y de documentación	➤ 99%	2%
	Cumplimiento de tiempos comprometidos de entrega de informes	➤ 95%	2%
	Compromiso mínimo de despliegue: número mínimo de equipos a desplegar por mes	➤ 100	2%

Los trabajos asociados con el seguimiento y control, son imprescindibles para garantizar los niveles de servicio solicitados.

En la reunión de arranque del servicio deben consensuarse convenientemente con el objetivo de fijar de manera consensuada algunas métricas y los umbrales de tolerancia para algunos indicadores.

Se regirán de acuerdo al siguiente esquema:

Indicador de servicio	Valor objetivo	Porcentaje de Cumplimiento mínimo
Reunión de Seguimiento	<10º día del mes	100%
Entrega de Informes	<5º día del mes	100%
Porcentaje horas dedicadas a la gestión frente al global de horas consumidas	<10%	100%
Documentación: guías, procedimientos etc.	0	100%
Incidencias generadas por el servicio	0	100%
Reaperturas de solicitudes cerradas	0	100%
Encuesta trimestral de calidad	Mejora continua	100%

Observaciones:

- Los valores están expresados en períodos laborables.
- La periodicidad se considera mensual.
- Se entiende una gestión madura del servicio respecto al ratio:
Total labores de gestión vs. Resto de acciones.
- Cualquier entrega debe acompañarse del correspondiente documento escrito (control de calidad).
- Ninguna incidencia puede deberse a una mala gestión del servicio (puestas en producción con impacto, mala calidad del preventivo etc.)
- Las reaperturas de solicitudes atribuibles a una mala gestión (alcance, análisis, diseño, construcción, pruebas) no están permitidas.
- Encuesta trimestral de calidad del servicio a usuarios clave que permitan medir el porcentaje (%) de mejora continua respecto a la calidad del servicio y a la eficiencia del mismo. No sólo se ha de pulsar a los usuarios claves, hay que mejorar el grado de satisfacción trimestralmente.
- En la reunión de arranque del servicio, se consensuarán algunos aspectos cualitativos con el objetivo de cuantificar los SLAs de manera objetiva.

Los ofertantes deben incluir SLA adicionales u optimizar los SLA propuestos por RTVM.

Los SLA propuestos tendrán una vigencia no superior a 6 meses tras la finalización del plan de implementación. Con dicha periodicidad, dentro de los **planes de mejora continua** que debe proponer el ofertante, RTVM y el proveedor de servicio revisarán los umbrales de servicio comprometidos, estableciendo nuevos objetivos de mejora. De la misma forma, se podrán incluir o retirar SLA que no se consideren prioritarios para RTVM.

El nivel de servicio solicitado y propuesto comenzará como máximo treinta días después de la firma del contrato, ya que este periodo inicial se entiende como de puesta en marcha.

La empresa licitante deberá incluir en su oferta un plan de implantación del servicio asociado a un plan de penalizaciones en caso de incumplimiento. Estas penalizaciones se tendrán en cuenta a la hora del abono de las facturas presentadas por el servicio, y serán siempre justificadas mediante un informe técnico donde se detallen cada una de ellas. El cálculo de los indicadores y la aplicación de las penalizaciones se realizarán por cada mes natural que dure el contrato.

Para cada uno de los indicadores (de los propuestos en el pliego y de los que puedan surgir a lo largo del contrato), se establece una penalización del 2% del importe de la facturación mensual en caso de incumplimiento, con un tope del 20% de la facturación mensual total.

El incumplimiento prolongado durante más de 2 meses de dos o más niveles de servicio (SLA) será causa de rescisión del contrato.

6. CONTENIDO DE LAS OFERTAS TÉCNICAS

Con independencia de que el licitador pueda adjuntar a su oferta cuanta información complementaria considere de interés, la propuesta de colaboración no deberá extenderse a más de **80 páginas** y debe estar obligatoriamente estructurada de la forma que se indica.

La información adicional que se considere incluir, se presentará en documentos separados.

Cada ofertante deberá entregar una copia de las ofertas en formato electrónico de acuerdo a MS Office 2010/2013 o Acrobat, en un CD/Pendrive junto con sus respuestas.

Es muy importante que la propuesta de valor que se entregue como respuesta al sobre B, en cualquiera de los soportes solicitados, no contenga ninguna referencia económica, sería motivo de exclusión.

La propuesta de valor del ofertante debe incluir tras el índice una tabla resumen donde se marque los aspectos fundamentales que son de interés para RTVM. Es muy importante que sea el primer contenido de la oferta y la página correspondiente para facilitar la lectura y valoración durante el proceso de adjudicación.

	Cumplimiento SI/NO & Descripción corta (si aplica)	Referencia a la descripción detallada (página)
Propuesta de Servicio	Metodología de Gestión Servicio	
	Descripción del Servicio	
	Provisión de Infraestructura, instalación y puesta en marcha.	
	Gestión del Proyecto, Arquitectura del Sistema, Plan de Implantación.	
	Descripción del Servicio Gestionado: Incidencias, Peticiones, Cambios, Problemas.	

	Cumplimiento SI/NO & Descripción corta (si aplica)	Referencia a la descripción detallada (página)
Niveles de Servicio	Acuerdos de Nivel de servicio y Penalizaciones	
Valor añadido	Mejoras al alcance del servicio	
Ejecución	Fase de Asimilación. Fase de Ejecución. Fase de Devolución, Adecuación RTVM a las nuevas plataformas propuestas (sólo si aplica)	

A continuación se espera la propuesta de valor detallada y estructurada como sigue:

PROPUESTA DETALLADA

1. Índice

2. Tabla resumen en los términos indicados

3. Descripción del Servicio Propuesto

- Descripción de la metodología propuesta para la gestión del servicio
- Descripción del Servicio propuesto
 - Estructura del Centro de servicio: misión y funciones
 - Estructura de gobierno del servicio
 - Plazo de Ejecución
 - Planificación del proyecto conforme a la fase de implantación del servicio:
 - Plan de Asimilación,
 - Plan de Implantación,
 - Plan de Devolución del Servicio
 - Descripción de los trabajos a realizar
 - Descripción de los entregables
 - Descripción del Equipo de Trabajo

4. Prestaciones Superiores y Complementarias

- La referencia en costes que se exige, si el proveedor decide proveer alguna mejora al alcance del servicio de entre las consideradas como tales por RTVM, no debe incluirse en la propuesta que se entrega en el sobre B. esta información de carácter económico se debe entregar en el sobre C.

5. Acuerdos de Nivel de Servicio y Penalizaciones asociadas

6. Ejecución del Contrato:

- Se incluirá en este capítulo la descripción de las medidas dispuestas por el ofertante para asegurar la calidad de los trabajos: metodología, aseguramiento de calidad y seguridad, así como aquellas otras que se prevé aplicar para velar y garantizar el adecuado cumplimiento del contrato.
- Las propuestas de valor deben incluir los acuerdos de colaboración que los ofertantes tienen suscrito o suscribirían de ser adjudicatarios con los terceros implicados para garantizar los niveles de servicio comprometidos. Conviene considerar nuevamente que no se espera como en el sobre B ninguna referencia económica.

7. Otros datos de interés