TeleMadrid

Telecomunicaciones y Seguridad Lógica

SERVICIO GESTIONADO DE MANTENIMIENTO, SOPORTE, OPERACIÓN Y ADMINISTRACIÓN

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Dirección de Ingeniería y Tecnología
Subdirección de Sistemas de Información

Febrero 2024

ÍNDICE

OBJETO

El objeto del presente Pliego es establecer las condiciones que han de regir la contratación del Servicio de Telecomunicaciones y Seguridad: Servicios Gestionado de Mantenimiento, Soporte, Operación y Administración, con el alcance que se detalla a continuación.

RTVM precisa contratar un Servicio de Telecomunicaciones y Seguridad que dé cobertura a los siguientes servicios:

- Telefonía Fija:
  Prestación de los servicios de telefonía fija incluyendo tráfico, accesos, suministro, mantenimiento y gestión de los elementos constituyentes de la red de telefonía fija de RTVM mediante el uso de voz sobre IP.

- Telefonía y Datos Móvil:
  Voz móvil, (2G/3G, 4G,5G), servicios de datos móvil (HSxPA/3G/4G), mensajería móvil.

- Servicio de Acceso a Internet y Conexiones WAN:
  Líneas de acceso a Internet, ampliación ancho banda, así como la monitorización, mantenimiento y gestión del mismo. Interconexión para la transmisión de datos entre las distintas sedes (Ayuntamiento de Madrid, Comunidad de Madrid, Asamblea de Madrid, Congreso, DGT, Moncloa).

- Mantenimiento LAN-WIFI:
  Mantenimiento de Infraestructura LAN entendiendo también los puntos WI-FI desplegados en la sede de RTVM.

- Seguridad Lógica:
  Oficina de Seguridad, SOC 24x7, Concienciación, Cumplimiento normativo. Medidas técnicas adicionales: Anti DDoS, XDR/EDR, Agentes de seguridad para móviles.

RTVM ha decidido estructurar el alcance de esta licitación en tres lotes, con objetos "naturalmente" diferentes, atendiendo a la evolución de la tecnología de los últimos años y al modelo actual de provisión de estos servicios:

LOTE-1: Servicios de Voz Fija y Voz y Datos Móviles.
LOTE-2: Servicios de Comunicaciones Internet, WAN, LAN.
LOTE-3: Servicios de Seguridad Lógica.

Se requiere, por tanto, la provisión, instalación, configuración, puesta en marcha, así como el mantenimiento de todos los elementos que constituyan estos servicios, garantizando su plena operatividad durante todo el periodo de vigencia del presente pliego, siendo requerimiento de esta licitación que todos los servicios sean gestionados plenamente por el adjudicatario.

Los licitadores deberán presentar una única oferta técnica para cada uno de los Lotes a los que concurran. En el caso de concurrir a los tres lotes, deben presentar una única propuesta económica por lote, si bien, de forma opcional, el licitador puede incluir además una propuesta económica global desglosando los importes de cada lote para ese supuesto.

Cualquier oferta que NO cumpla con alguno de los requerimientos solicitados por RTVM NO SERÁ analizada.

ALCANCE

LOTE 1: SERVICIOS DE VOZ FIJA Y VOZ Y DATOS MÓVILES

SERVICIOS DE VOZ FIJA

Prestación de los servicios de telefonía, sobre tecnología VoIP, incluyendo la infraestructura requerida para la provisión de los servicios, preferiblemente en la nube, incluyendo tráfico, accesos a redes públicas en IP, suministro, mantenimiento y gestión de los elementos constituyentes de la red de telefonía fija de RTVM, integración con los servicios de correo electrónico corporativo para comunicación de servicios de voz e integración de servicios convergentes F/M/TI y de colaboración.

SERVICIOS DE VOZ MÓVIL Y DATOS MÓVILES

Prestación de los servicios de voz móvil, (2G/3G/4G y 5G cuando exista disponibilidad), servicios de datos móvil (HSxPA/3G/4G tanto en terminales como equipamiento para laptop, PDA y tablets – 5G cuando exista disponibilidad), mensajería móvil, incluyendo tráfico, accesos, terminales, suministro, configuración y mantenimiento de los elementos constituyentes de la red de telefonía móvil de RTVM, entre los que se incluyen terminales móviles, smartphones, Tablets, PDAs, etc.

LOTE 2: SERVICIOS DE INTERNET, WAN, LAN

SERVICIOS DE INTERNET Y WAN

Prestación de los servicios:

- Interconexión para la transmisión de datos entre las distintas sedes de RTVM, redundantes, con capacidad de crecimiento y ampliación, incluyendo la provisión, instalación, configuración, mantenimiento y gestión del equipamiento necesario para la prestación del servicio.
- Conexión a Internet de RTVM, donde se requiere la integración del equipamiento necesario en la sede de RTVM, routers, líneas de datos, así como la monitorización, mantenimiento y gestión del mismo. Serán requerimientos obligatorios aquellos destinados de dotar de los mecanismos de seguridad necesarios, la disponibilidad de los mismos y la gestión de la calidad de los servicios publicados en internet.

SERVICIOS DE MANTENIMIENTO RED LAN-WIFI

Servicio gestionado y mantenimiento de la infraestructura de comunicaciones LAN y WIFI de RTVM, incluyendo los procesos de gestión de incidencias, gestión de peticiones, gestión de cambios, gestión de configuración, gestión de la monitorización, gestión de la capacidad en red, mantenimiento preventivo, soporte fabricante hardware y software.

SERVICIOS DE SEGURIDAD EN RED

El proveedor debe incluir servicios imprescindibles para garantizar en la red:

- AntiDDos.

- Correo Seguro, Guarda y Custodia de Correo, Antispam.
- Gestión de Ancho de Banda y Calidad de Servicio.
- IDS/IPS.
- Antivirus de Navegación.
- Filtrado URL.
- Firewall en Red.

Todos los servicios estarán alineados con las políticas de seguridad que desde RTVM se definan.

LOTE 3: SERVICIOS DE SEGURIDAD LÓGICA

MEDIDAS TÉCNICAS: LICENCIAS

- Licencias en 50 móviles (asignado a personal directivo y ciertos responsables de área) de un agente para la defensa contra las amenazas móviles.
- Licencias de agentes XDR/EDR: para los puestos de usuario, servidores y cortafuegos, que realicen funciones de monitorización, detección, bloqueo de amenazas y operen en diferentes capas del sistema.

CENTRO DE OPERACIONES DE SEGURIDAD - SOC

Tendrá por objeto la creación un Centro de Operaciones de Seguridad, SOC, que centralice las capacidades actuales y futuras en materia de ciberseguridad de RTVM. Para ello se suministrará e instalará un sistema de gestión de eventos e información de seguridad (SIEM –Security Information and Event Management), como herramienta principal de monitorización de la seguridad de las infraestructuras TIC, además de capacidades para la prevención y detección temprana de amenazas e incidentes, análisis de vulnerabilidades técnicas, y análisis y resolución de incidentes de seguridad, todo ello de forma centralizada y con procesos y procedimientos operativos de seguridad consistentes, que permitan reportes efectivos sobre el estado global de la seguridad y los riesgos TIC.

SERVICIO ESPECIALIZADO DE DISEÑO SEGURO - SDS

Como complemento al SOC se crea e implanta el Servicio Especializado en Diseño Seguro, SDS, que permitirá disponer de un soporte especializado para la definición y establecimiento de controles de seguridad, nativos y complementarios en las infraestructuras TIC, y la definición e implantación de nuevos procesos y procedimientos, integrados con los ya existentes de gestión TIC y de respuesta a incidentes de seguridad.

OFICINA TÉCNICA DE GOBIERNO Y DPD

Oficina Técnica de Gobierno (OTG) y DPD con el objetivo de mejorar la madurez de sus procesos relacionados con la Seguridad de la Información

Se ha identificado y valorado, como parte troncal del proyecto de Seguridad Gestionada, la necesidad de contar con servicios de alto valor relativos a la Gestión de Seguridad Lógica, más concretamente entendidos como propios de consultoría de cumplimiento normativo y seguridad: Oficina Técnica de Gobierno.

En este marco, y como parte del servicio de Oficina Técnica de Gobierno, se habrán de atender como mínimo las siguientes tareas:

- Revisión y mejora del marco normativo de seguridad.
- Revisión, mejora y gestión del plan de seguridad.
- Revisión y mejora de medidas organizativas. Apoyo a la implantación.
- Convergencia al ENS
- Cumplimiento de la normativa ISO 270001 en dos ámbitos:
  - Técnico en lo que se refiere a los sistemas.
  - Validación jurídica.
- Servicios de Delegado de Protección de Datos (DPO)
- Auditoría de seguridad Protección de Datos (bienal).
- Programas de concienciación.

El seguimiento y actualización del Plan de Seguridad, así como la implantación de las recomendaciones resultado de los análisis, dará como resultado la implantación de un modelo de gobierno de los servicios TI, que propicie un Sistema de Gestión Unificado de la Seguridad práctico, robusto y en continuo crecimiento. Se requiere de un servicio continuado de soporte en ésta y otras tareas de Gobierno, Riesgo y Cumplimiento, que velen por la mejora continua, atendiendo tanto aquellas medidas de carácter más técnico/tecnológico, acompañadas del soporte jurídico asociado a las mismas (según establece la **ISO 27001/02 y ENS**, para las medidas organizativas, técnicas y jurídicas dentro del enfoque de la seguridad de las TIC). Asimismo, el licitador debe contemplar los requisitos trasladables desde el Delegado de Protección de Datos (**DPD**) a incluir en la propuesta desde la exigencia y aplicabilidad del Reglamento General de Protección de Datos de la Unión Europea (**RGPD**), y las auditorías pertinentes -cada dos años-.

LOTE 1: SERVICIOS DE VOZ FIJA, MÓVIL Y DE DATOS MÓVILES

SERVICIOS DE VOZ FIJA.

Descripción del Servicio Actual

Actualmente RTVM cuenta con una centralita en la nube, Cisco HCS (Cisco Unified Communications Manager), es en una 'Solución de Telefonía IP completa', extremo a extremo, incluyendo los elementos de conmutación interna (Servidor de telefonía), extensiones IP (teléfonos), accesos a la red pública (accesos virtuales IP a través de la red NGN del proveedor actual) y servicios avanzados en red dentro del servicio IBERCOM IP.

Los accesos de voz a Red Pública, en el CDP de RTVM, se realizan en IP, mediante trunk SIP con la red del operador, concentrando mediante canales de voz en Red las comunicaciones de voz "off-net".

Se dispone de redundancia espacial, en dos CPDs diferentes del proveedor, incluyendo redundancia en los SBCs de la red, tanto para comunicaciones fijas, como para móviles.

El acceso a la Red NGN desde Pozuelo se realiza vía accesos Macrolan redundados, propiedad del proveedor actual.
Se dispone de 50 canales en la red para servicios fijo y 30 para móviles.

La infraestructura de accesos a red pública es:

- Accesos en IP: 50 canales de voz fija.

- Accesos en IP: 30 canales de voz móvil.
- DDIS: 859
- Extensiones: 500
- Líneas de enlace PaP:
  - Analógicos radiofónico ámbito nacional: 69
  - Líneas analógicas individuales (STB): 44

Adaptadores analógicos

Actualmente por necesidades del servicio, se dispone de adaptadores analógicos a digital, 4 dispositivos vg 310, para realizar el transporte de la señal a través de la red VoIP.

Será responsabilidad del adjudicatario su mantenimiento o reemplazo por equipos que cumplan con la misma funcionalidad, así como su instalación, configuración, puesta en marcha y soporte.

Descripción del Servicio de Voz:

Los servicios prestados actualmente son:

Tipología	Descripción	Unidades
Extensiones IP	Extensiones IP	574
Licencias	Essential HCS Foundation HCS Standard HCS	96 276 202
Canales NGN	AUIP Tráfico Móvil APV Tráfico Fijo	30 50

Tipología	Descripción	Unidades
Terminales	Terminal fijo de gama baja Terminal fijo de gama media Terminal fijo de gama alta	0 436 42
Auriculares	Auriculares gama baja	2
Expansores		2
Adaptadores analógicos 24P		4

Aparte de la infraestructura anteriormente indicada, el actual proveedor de servicio es responsable de la gestión y mantenimiento integral de la centralita de telefonía fija y de los buzones de voz, en régimen de 24x7.

SERVICIOS CONVERGENTES F/M/TI

En la actualidad RTVM dispone de una serie de servicios de valor añadido, en el entorno de las comunicaciones unificadas, para la totalidad de los usuarios, 450:

- Agenda Única: Permite disponer de una copia de los contactos personales de un usuario, tanto de la tarjeta SIM, la agenda del teléfono móvil o la agenda de Outlook.
- Mensajería: Servicio centralizado de mensajería SMS y MMS tanto para la voz fija como móvil.
- Buzón Único: Repositorio único para las comunicaciones de voz fija y móvil, integrado con el correo corporativo de RTVM. Permitiendo además la recepción de fax.

- Número único: Servicio que permite a RTVM disponer de un "número único", independientemente del terminal de voz que tenga el usuario (fijo, móvil y/o PC-Soft Phone).
- Herramientas colaborativas: IM, presencia (Fijo/Móvil y PC) y audio conferencia entre PCs.

Todos estos servicios se encuentran integrados con el directorio corporativo de RTVM.

Servicios requeridos Telefonía Fija

RTVM requiere una solución cloud de centralita profesional convergente fijo y móvil y de comunicaciones unificadas y colaborativas, con capacidad de disponer de un catálogo de puestos, de terminales y servicios de valor añadido, la solución debe apoyarse en infraestructura de partners líderes en tecnología, con capacidad de soportar los procesos de transformación digital de la organización.
La infraestructura que soporte el proceso debe estar alojada en dos centros totalmente diversificados del proveedor. En la sede de Telemadrid únicamente se instalarían terminales IP y conversores analógico-IP para la convivencia con el nuevo servicio de la infraestructura analógica actual, con el dimensionamiento en calidad y cantidad establecido por RTVM.

La solución debe reunir a alto nivel los servicios que posteriormente se desarrollarán:

- Centralita profesional en la nube: todas las funcionalidades específicas de una centralita para gestionar de forma eficiente las comunicaciones internas y externas de la empresa.

- Comunicaciones Unificadas seguras: servicio convergente fijo-móvil y servicios de colaboración integrados directamente en la solución.

- Movilidad de usuarios: funcionalidades y opciones específicas para empleados en movilidad, en tele-trabajo o en sedes remotas.
- Suite de aplicaciones de colaboración: chat, presencia, audio/videoconferencia, compartición de documentos, escritorio, aplicaciones, pizarra y anotaciones, entre otras, salas de reuniones virtuales: reuniones más eficientes para usuarios internos y/o invitados externos vía Navegador Web PC (WebRTC).

- Servicios SIP Trunk: es un servicio de telefonía punto a punto que se implementa sobre una conexión de datos IP y que es capaz de integrar cualquier centralita IP On-premise de RTVM.

- Fax virtual: servicio de recepción y envío de fax en formato correo electrónico.

- Grabación de llamadas: servicio de grabación de llamadas entrantes y salientes compatible con cualquier tipo de puesto.

- Operadora Automática: con funciones de Interactive Voice Response (IVR).

- Gestión de colas de llamadas (ACD): con diferentes opciones de encolado y Grupos de Salto de llamadas.

- Servicio de Call Center: con perfiles de Supervisor y Agentes para optimizar la atención y evaluar la eficiencia de los servicios de atención telefónica.

- Call Analytics: que permita recoge todos los registros de llamadas externas e internas.

La convergencia de la solución debe permitir ofrecer las mismas funcionalidades de voz en puestos fijos con terminales IP, o puestos de movilidad con terminales móviles y/o terminales móviles con aspecto de fijo y usuarios con las aplicaciones de colaboración.

Requerimientos:

- Servidor de Telefonía IP redundando (plataforma de telefonía IP con protocolo SIP).

- Los accesos deben ser de fibra dedicada para el cliente, no valiendo soluciones de medio compartido como FTTH o de bajas prestaciones como ADSL.
- Los equipos en domicilio de cliente deben ser en alquiler y gestionados por el operador.
- Los accesos pueden ser reutilizados para el servicio de red privada virtual y para el de Internet, pero los equipos deben ser diferentes para cada servicio.
- Debe ser una solución de Voz IP, no admitiendo la instalación de RDSI. El tráfico de voz debe ser transmitido a través de la red de datos corporativa con la adecuada calidad de servicio. No se admiten soluciones de voz sobre Internet.
- La lógica de la PBX (centralita) de RTVM debe estar virtualizada y redundada en la red del operador, no admitiéndose la instalación de equipamiento en las sedes de RTVM más allá de los terminales y conversores analógico-IP. No se admite la instalación en dependencias de RTVM del servidor de llamadas ni de pasarelas de medios.
- Sólo se valorarán aquellas soluciones orientadas a fabricantes de alta gama.
- Terminales IP. (diferentes gamas y funcionalidades).
- Todos los terminales deben incluir un switch Ethernet integrado de 1 GbE.
- Sistema de Gestión, Supervisión y Monitorización.
- Sistema de tarificación, que permita:
  - Monitorización llamadas entrantes/salientes.
  - De cualesquiera de los usuarios fijos, móvil, trunksip.
  - Gestión de call centers y grupos de salto.
  - Información: duración, coste, horario, origen, destino, etc.
  - Informes.
- Mantenimiento.
- Servicios de Operadora (Recepción)
- El proveedor debe ofrecer el servicio desde una red corporativa basada en una capa de acceso de nivel 2.
- Gestión del servicio, el proveedor facilitará herramientas que faciliten un cuadro de mando de infraestructuras para el control del negocio, con capacidades de supervisión de los elementos del servicio que integre los servicios y permita generación de informes personalizados.

Con esta intención, el licitador deberá hacer una propuesta de VoIP para un total de 829 puestos de trabajo aproximadamente con los siguientes requerimientos:

- Numeración pública/privada:

Numeración Publica Privada	Nº propuesto
28100 ----- 28899	799
9200 ----- 9229	30
Total	829

- Números con tarificación especial "902": 8 líneas.
- Distribución de líneas en función de su naturaleza:

Líneas fijas	Nº propuesto
Líneas analógicas	96
Líneas digitales	32
Líneas estándar	829
Total	957

El licitador debe considerar en su propuesta una previsión de incremento del 15%, durante la vida del contrato, de cada uno de los tipos identificados, sin coste adicional para RTVM.

El licitador propondrá un diseño completo de la red de Telefonía IP que permita garantizar la calidad y disponibilidad de los servicios de valor añadido actualmente disponibles descritos en este pliego, así como los servicios de comunicaciones unificadas y a nivel de arquitectura se debe contemplar, al menos, por los siguientes componentes:

- Servidor de Telefonía IP redundando.
- Gateways o adaptadores para terminales analógicos (líneas para faxes y módems).
- Sistema de Gestión, Supervisión y Monitorización.

El diseño de la arquitectura deberá considerar todos los equipos, componentes y materiales necesarios para que el servicio se preste en alta disponibilidad.

El licitador detallará los protocolos de señalización disponibles en la solución ofertada, teniendo en cuenta que ésta deberá ser compatible con las infraestructuras de otros fabricantes.

La infraestructura de Telefonía IP deberá poder integrarse con cualquier operador de telefonía fija o móvil, así como soportar la integración de dispositivos de diferentes fabricantes. Entre otros, deberá soportarse al menos el protocolo SIP.

El licitador deberá garantizar la compatibilidad e interoperabilidad entre todos los elementos ofrecidos, así como la interoperabilidad con sistemas PABX convencionales y con las troncales y canales E1 que el RTVM pueda requerir.

La infraestructura de Telefonía IP propuesta por los licitadores deberá basarse en los siguientes principios:

- Flexibilidad: Las infraestructuras propuestas deberán permitir la posibilidad de incluir, bien por hardware o por software, nuevas tecnologías y servicios de cara a futuros cambios en las necesidades de los distintos grupos de usuarios.
- Capacidad de procesamiento: La solución ofertada deberá contar con procesadores de última generación, con posibilidad de incorporar mejoras hardware para aquellas aplicaciones que requieran un alto rendimiento, permitiendo mantener un nivel adecuado de procesamiento, aunque se incluyan más servicios en el futuro.
- Redundancia del Gestor de llamadas con funcionalidad total para no tener un único punto de fallo y asegurar la escalabilidad.
- Capacidad de enrutamiento alternativo de llamadas salientes en el caso de que el enlace principal falle o esté saturado.
- Definición de códigos de autorización para acceder a determinadas funcionalidades.

- Bloqueo de grupos y/o facilidades específicas tales como acceso a números internacionales, cierto número de cifras, etc.
- Realización de copias de seguridad y su restauración.
- Protección de acceso a la plataforma de gestión mediante clave y posibilidad de forzar el cambio de la misma periódicamente.

Funcionalidades del Servicio de Voz:

Como funcionalidades básicas de voz se entenderán al menos los siguientes:

- Llamada.
- Captura de llamada.
- Retrollamada.
- Desvío de llamadas, indicándose los posibles tipos (incondicional, si ocupado, si ausente, desvío a buzón de voz, desvío a otro número o grupo, etc.)
- Transferencia de llamadas, indicándose los posibles tipos (directa, con consulta, si no responde, identificación de número redirigido, etc.)
- Conferencia a tres, indicándose la posibilidad de que sea iniciada por un usuario o preestablecida de antemano.
- Llamada en Espera: funciones avanzadas.
- Ocultación de Llamada.
- Devolución de Llamada.
- Remarcado de llamada.
- Restricción de Llamadas salientes.
- Directorio corporativo.
- Agenda Corporativa.
- Grupo de Salto.
- Función No molestar.
- Gestión selectiva de llamadas.
- Identificación de usuarios. En los terminales telefónicos aparecerán los datos públicos de los usuarios, en ningún caso aparecerán datos privados.
- Como funcionalidades avanzadas de voz se entenderán al menos los siguientes:
  - Jefe/Asistente.
  - Discriminación en llamadas.
  - Manos libres. Al menos los terminales de gama alta.
  - No molestar.
  - Como funcionalidades

Accesos a Redes Públicas:

Se proporcionarán todos los accesos necesarios a redes públicas, siendo preferibles la conectividad basada en IP, compatible con la plataforma de voz IP objeto de este concurso, que se justifiquen por obtener así, una mayor disponibilidad y eficiencia o porque permitan la conexión a servicios en red del operador licitante. Los licitadores deberán justificar el dimensionamiento extra necesarios en los parámetros de la RPV de datos del apartado anterior.

Terminales IP:

Se requiere nuevo equipamiento de dispositivos IP para la totalidad de los dispositivos actuales con los siguientes requerimientos:

- Los terminales de TODAS las gamas deben disponer de conexión Gigabit Ethernet.

- Terminales IP gama alta, destinados a los usuarios clasificados como altos cargos. Estos terminales incluirán como mínimo los siguientes requisitos:
- Display alfanumérico de alta resolución con soporte XML capaz de presentar extensión y nombre y apellidos simultáneamente.
- Teclas de función programables.
- Memorización de números.
- Funcionalidad de manos libres.
- Soporte para varias líneas de voz.
- Puerto para conectar, al menos, un PC.
- Posibilidad de conexión de auriculares.
- Acceso a todas las funcionalidades básicas y avanzadas de la centralita IP a instalar.

RTVM ha previsto:

- Terminales IP gama media (Cisco IP Phone 8851, o similar), 500 terminales. Estos terminales incluirán como mínimo los siguientes requisitos:
  - Display alfanumérico capaz de presentar extensión y nombre y apellidos simultáneamente.
  - Teclas de función programables.
  - Memorización de números.
  - Soporte para dos líneas de voz.
  - Puerto para conectar, al menos, un PC.
  - Posibilidad de conexión de auriculares.
  - Acceso a todas las funcionalidades básicas y avanzadas de la centralita IP a instalar.

- Terminales IP gama alta (Cisco IP Phone 8865 o similar), el proveedor provisionará al menos 40 terminales de estas características.
- Terminales IP gama operadora, (Cisco Ip Phone 8851 + Expansión o similar) 2 terminales, destinados a los usuarios operadores. Estos terminales incluirán como mínimo los siguientes requisitos:
  - Display alfanumérico con soporte XML capaz de presentar extensión y nombre y apellidos simultáneamente.
  - Teclas de función programables.
  - Memorización de números.
  - Funcionalidad de manos libres.
  - Diadema con auricular/micrófono.
  - Múltiples líneas de voz y módulo de expansión con teclas adicionales.
  - Gestión de múltiples colas de llamada.
  - Acceso a todas las funcionalidades básicas y avanzadas de la centralita IP a instalar.

Servicios de Comunicaciones Unificadas

Como servicios de Comunicaciones Unificadas Integradas se entienden los siguientes, como mínimo, y otros que se describen detalladamente en este pliego, RTVM dispone actualmente de servicio CiscoJabber, como referencia:

- Buzón Único de Voz
- Extensión única.
- Voz, video y presencia.
- Historial de llamadas.

- Gestión de contactos, calendario y búsquedas.
- Compartición de pantalla, aplicación, pizarra, etc (en modo llamada).
- Integración con Servicios tipo teams en servicios de llamadas.
- Provisión de auriculares y micrófonos con cable para 150 usuarios.

Servicios Especiales

RTVM necesita, debido a las características especiales del negocio, de la disposición del prestador de los servicios para atender las necesidades "urgentes "que puedan surgir para cubrir eventos especiales como retransmisiones en directo, elecciones, eventos deportivos, con la necesidad de disponer de ellos en los siguientes periodos de tiempo después de su solicitud:

- Líneas FTTH, STB, 48-72 horas en días hábiles.
- Líneas internacionales (FTTH, STB FIBRA y/o cualesquiera de modo de conexión que el proveedor internacional disponga) 15 días hábiles.

El adjudicatario deberá proveer un servicio de atención específico para la tramitación de las solicitudes y seguimiento de las mismas.

Plan de Numeración

Se garantizará la conservación de la numeración requerida, llevándose a cabo, sin coste adicional y a cargo del adjudicatario, la adecuada portabilidad numérica, en caso necesario.

El licitador deberá describir las características, limitaciones y virtudes de la solución planteada de cara mejorar el Plan Privado de Numeración de forma que éste permita una mejor integración de todas las comunicaciones, tanto fijas como móviles. Siguiendo la línea integradora de todo el pliego, los requerimientos del nuevo PPN son los establecidos en este pliego.
Deberá plantearse lo anterior en un único apartado y de forma global para todas las extensiones del RTVM, sean éstas fijas o móviles, valorándose la flexibilidad del PPN, su sencillez y la migración del actual PPN al nuevo.

Las llamadas que se realicen mediante la marcación de 9 cifras a teléfonos móviles corporativos se deberán encaminar y facturar de la misma forma que las llamadas a móviles corporativos realizadas mediante la marcación reducida.

El adjudicatario deberá pertenecer a la entidad de referencia de portabilidad y garantizará que la numeración propuesta para este servicio será portable a la finalización del presente contrato.

Volumetrías

A continuación, a modo ilustrativo, se detalla la volumetría del número de llamadas y duración en segundos de 6 meses de servicio (junio-octubre 2023):

Tipología de Llamadas	Suma de LLAMADAS	Suma de SEGUNDOS
Llamadas a móviles	545	89776
Llamadas a Numeraciones 800/900	279	82443
Llamadas a Numeraciones 901	16	1912
Llamadas a Numeraciones 902	16	6157
Llamadas a Sº de Información y Emergencia	55	14112

Llamadas Internacionales	169	55937
Llamadas Interprovinciales	2102	451031
Llamadas Metropolitanas	18077	2748269
Llamadas Provinciales	18	1229
Servicios de información telefónica y tarificación adicional	2	630
Total	**21.358**	**3.453.688**

En cuanto al tráfico de red inteligente (prefijos 90X) cursado durante el mismo período, se detalla a continuación:

Tipología de Llamadas	Suma de LLAMADAS	Suma de SEGUNDOS
Fijo - Fijo Nacional	11	905
Fijo - Locución	2	23
Móvil - Fijo Nacional	64	1207
Móvil - Locución	2	57
Total	**21.358**	**3.453.688**

Los servicios de telefonía a ofertar serán:

- Tráfico metropolitano
- Tráfico provincial
- Tráfico interprovincial
- Tráfico internacional según destinos
- Tráfico a móvil
- Servicios de inteligencia de red
- Llamadas en grupo cerrado de usuarios
- Otras llamadas

Modelo de Facturación:

El proveedor presentará dos modelos de facturación y RTVM seleccionará anualmente la opción que le resulta favorable.

Opción A:
Coste por línea en base a tarifa plana de tráfico nacional, VPN y móvil, resto de tráfico facturable por minuto.
Tarifa plana por línea con un máximo de gasto mensual para tráfico nacional, interno y móvil.
Facturación por minutos al resto de tráfico (internacional/especiales).

Opción B:
Volumen de tráfico real consumido/mes o año por destino (nacional/VPN, móvil, internacional, servicios u otros).
Opción de tarifa por volumen de tráfico:
El adjudicatario deberá asumir dentro del contrato todos los servicios contratados actualmente sobre las líneas objeto del contrato (servicios contestador, desvíos de llamadas, llamada en espera, etc.), y deberá hacer las gestiones necesarias para dar de baja dichos servicios en el operador que actualmente los ofrece, todo ello sin modificaciones en los servicios ni costes añadidos, valorándose mejoras en estos servicios en lo que pueda tener que ver con los servicios de Comunicaciones Unificadas también objeto del concurso.

Fax Virtual

Se requiere de un servicio de Fax virtual, que permita a un usuario de un puesto, enviar un fax, a cualquier destino externo o interno, mediante el envío de un correo electrónico, y recibir un fax, desde cualquier origen externo o interno, en el correo electrónico del propio usuario.
La plataforma, debe permitir a los usuarios administradores:

- Crear nuevos usuarios con perfil de Autorizado
- Administrar usuarios existentes con perfil de Autorizado
- Modificar la contraseña de un usuario con perfil Autorizado
- Acceso a la lista de números de teléfono activos asociados a los puestos Fax2Mail
- Asociar números de teléfono a usuarios Autorizados para gestión de faxes
- Administrar todos los faxes
- Gestión de su propio perfil
- Gestionar todos los faxes de los números asociado a su perfil
- Estadísticas del servicio de fax
- Gestión de su propio perfil

- Número de fax disponibles para: 915123700 al 915123814 actualmente estos números son de disponibilidad para RTVM, a través de una línea RDSI ISPBX.

Integración TrunkSip

RTVM dispone de un sistema de telefonía de emisiones con multiconferencia, para la explotación de las comunicaciones desde sus controles de estudios con el exterior, esto mejora la operativa, aumenta la flexibilidad y reduce la complejidad, el sistema está integrado con la Centralita bajo protocolo SIP anteriormente descrita, por lo tanto, se requiere la integración del equipamiento con la nueva solución que aporte el proveedor.

Los modelos de dispositivo de referencia con los que está integrado el trunksip actualmente son: AEQ Systel IP-12 y Yeastar P560, por lo tanto, cualquier solución de servicios de voz debe ser compatible con este dispositivo, será responsabilidad del adjudicatario realizar las configuraciones adecuadas bajo los requerimientos del dispositivo para asegurar el servicio, así como disponer del número de DDI suficientes para la integración.

Plataforma Colaborativa

Para desarrollar las capacidades de trabajo colaborativo, RTVM dispone de una solución colaborativa desarrollada en la plataforma Cisco – Webex.

RTVM cuenta con 13 licencias de usuario de la plataforma, un dispositivo roomkit de videoconferencia CISCO serie Webex Room (Modelo:CS KITPLUS K 9 Room Kit Plus w/ CodecPlus, Quad Camera and Touch 10, con micrófono y altavoz como opción).

El proveedor deberá facilitar una solución de colaboración durante toda la vigencia del servicio que al menos disponga de las capacidades actuales.

El dispositivo roomkit que se despliegue deberá tener la capacidad de conectarse a sesiones de colaboración, no solo de la solución propuesta (ej. Webex), sino que también debe tener la capacidad de acceder a plataformas de colaboración de terceros como: Hangouts, GoogleMeet, Ms Teams.

Gestión e Informes:

El adjudicatario pondrá a disposición de RTVM información suficiente para el conocimiento del estado de la red, fundamentalmente informes periódicos de uso de servicios:

- Niveles de Servicio.
- Incidencias.
- Cambios.
- Rendimiento (calidad, disponibilidad, tráfico, etc…).
- Facturación y consumo.
- Plan de mejoras.

Estos datos se entregarán con periodicidad mensual en el formato electrónico que se acuerde con RTVM antes del 5º día de cada mes.

Mantenimiento, disponibilidad y QOS:

El mantenimiento de las centralitas o equipamiento necesario englobados dentro de esta plataforma de telefonía IP (VoIP) para proporcionar los servicios de voz fija serán responsabilidad del adjudicatario del concurso independientemente de la solución y arquitecturas propuestas. Deberá detallarse el servicio específicamente en el Plan de Operación, Gestión y Mantenimiento y, a este respecto, éste incluirá:

- Supervisión permanente de los equipos
- Desplazamientos
- Mano de Obra
- Materiales y componentes requeridos para arreglar las averías

El horario de atención de reclamaciones será de 24 horas x 365 días.

El adjudicatario deberá disponer de un stock de terminales adecuado para garantizar la sustitución de los mismos en caso necesario.

Sobre los acuerdos de servicio el licitador indicará, al menos, los siguientes parámetros y sus valores máximos:

- Tiempo de respuesta: tiempo transcurrido entre la llamada denunciando la avería y la comunicación por parte del técnico que tenga asignada la incidencia. El tiempo de respuesta nunca superará 30 minutos.
- Tiempo de resolución de incidencias: habrá un escalado en función de la criticidad de la avería, teniendo en cuenta que se espera un tiempo de reparación máximo en casos de incomunicación total. El tiempo de resolución de incidencias, en averías graves, nunca superará las 2 horas.
- Disponibilidad del servicio para caídas totales, no inferior al 99,2% mensual ni al 99,8% anual. Estos valores servirán para el cálculo del tiempo máximo de indisponibilidad.
- Disponibilidad del servicio para caídas parciales, en las que funcione el servicio, pero de manera degradada (no entren llamadas de móviles, haya problemas de saturación anormales, etc.). Para este caso, la disponibilidad será no inferior al 98,4% mensual ni al 99,6% anual.

Porcentaje máximo de llamadas fallidas:

- Nacionales, no debe ser superior al 1%.
- Internacionales, no debe ser superior al 2,5%.
- A móviles, no debe ser superior al 2%.
- Tiempo de establecimiento de llamada, cuyo valor medio no debe ser superior a 3 segundos.

Estos valores mínimos pueden ser mejorados en la oferta.

La valoración de la disponibilidad mensual se tendrá en cuenta desde el día 1 natural de cada mes hasta el último día de ese mes.

La valoración de la disponibilidad anual se tendrá en cuenta desde el día 1 de enero de cada año hasta el último día de ese año.

No se tendrán en cuenta a efectos del cómputo de tiempo aquellas averías que no sean responsabilidad del operador. Tampoco las indisponibilidades que sean fruto de pruebas o paradas técnicas, siempre y cuando hayan sido advertidas con la suficiente antelación, y autorizadas por RTVM.

Migración:

Los licitadores deberán incluir un plan de migración de servicios.

En cuanto al impacto en los actuales servicios, y cuando exista cambio de operador, los licitadores deberán especificar en sus propuestas el procedimiento de portabilidad numérica, que tendrá que coincidir con el cambio de red al objeto de minimizar el tiempo de indisponibilidad.

El calendario del plan de migración tendrá que incluir la ejecución de las actividades necesarias fuera del horario de actividad habitual de cada sede.

En cuanto al cambio de infraestructura, se procederá de la misma forma, minimizando siempre el tiempo de indisponibilidad y fuera del horario de actividad del edificio.

El plan de migración incluirá como mínimo:

- un procedimiento con el detalle de las actividades a realizar,
- los requerimientos estimados por parte del responsable del edificio correspondiente,

- el equipo de trabajo que intervendrá,
- el tiempo previsto para la finalización de los trabajos y
- el tiempo previsto de indisponibilidad.

En caso de alta de nuevas líneas por la red, el operador adjudicatario puede asumir como mejora facilitar y asumir el coste de la publicación de los nuevos números de teléfono en todos aquellos medios de fácil acceso para los usuarios.

En cuanto a las líneas existentes, la numeración actual deberá conservarse, de tal modo que los licitadores deberán proporcionar la facilidad de portabilidad numérica en caso de cambio de operador.

Apoyo y Atención al Cliente:

Se requiere una propuesta concreta respecto a la disponibilidad de, como mínimo, un responsable comercial de la cuenta de RTVM, un ingeniero responsable de los nuevos proyectos, y un responsable del seguimiento y la evolución de los servicios contratados.

Asimismo, se describirán todos los sistemas y mecanismos (centros de atención, personal a su disposición, metodología, etc.) a disposición de RTVM. Entre estos sistemas, es necesario disponer de un sistema de atención telefónica personalizada (“ventanilla única”)

y un sistema de gestión accesible remotamente. Este sistema de atención al usuario tendrá que ser totalmente flexible para adaptarse a las necesidades de RTVM y deberá funcionar con un horario 24x7.

El adjudicatario deberá mantener reuniones mensuales con los responsables de RTVM para tratar los asuntos de este contrato. La periodicidad de dichas reuniones será definida por RTVM y será mayor durante la implantación del proyecto.

SERVICIOS DE VOZ Y DATOS MÓVILES.

Comprende los servicios de voz y de datos en movilidad. Dicho servicio deberá disponer de las máximas prestaciones permitidas por la tecnología actual.

Actualmente, RTVM dispone de 283 líneas repartidas de esta manera:

- 215 líneas activas voz/datos con unos 210 terminales.
- 68 líneas activas datos, de las cuales:
  - 27 se utilizan en USB
  - 27 en equipos de retransmisiones de Radio y TV
  - 14 en Tablet/IPad
- Terminales de alta gama (directores u otras necesidades) 23.
- Adicionalmente se dispone de, al menos, 2 terminales de gama alta para urgencias de cambios de directores y al menos 10 terminales de gama media/baja para cambios urgentes por rotura/pérdida, etc.

Se describen a continuación los servicios de que dispone actualmente RTVM. Los licitadores deberán garantizar la continuidad de estos servicios, además de los servicios requeridos en este pliego.

Volumetría correspondiente a los últimos 6 meses:

La volumetría del número de llamadas y duración en segundos de 6 meses (junio-octubre 2023), se detalla, a modo ilustrativo, a continuación:

Tipo de Llamada	Suma LLAMADAS/sesiones	Suma Segundos/Megas
A.CONTENIDOS PREMIUM PROMOCIONADOS	1	
ACCESOS A CONTENIDOS	9	
DATOS EN ROAMING	372	37.473
DATOS INTERNET	22.358	3.826.954
DATOS INTERNET EN UE	121	49.487
EN ROAMING	70	14.588
INTERNACIONAL	55	11.241
INTERNO BUZON	397	26.017
INTERNO CORPORATIVO	34.590	9.216.029
INTERNO CORPORATIVO EN UE	14	1.567
INTERNO MOVILES	40.584	17.758.003
INTERNO MOVILES EN UE	84	12.158
LLAMADAS A 800/900	254	67.491
LLAMADAS A 800/900 EN UE	2	253
LLAMADAS A 901	4	131

LLAMADAS A 902	29	6.948

Tipo de Llamada	Suma LLAMADAS/sesiones	Suma Segundos/Megas
LLAMADAS A INFORMACIÓN Y EMERGENCIAS	34	9.005
LLAMADAS ILIMITADAS	63	12.318
MENSAJES A INFORMACIÓN Y EMERGENCIAS	45	
MENSAJES DICTADOS	71	
MENSAJES ESPECIALES	29	
MENSAJES INTERNACIONALES	3	
MENSAJES MOVISTAR	370	
MENSAJES MOVISTAR ROAMING	5	
MENSAJES MULTIMEDIA	11	1
MENSAJES OPERADORES NACIONALES	205	
RECIBIDAS EN ROAMING	31	4.755
RESTO DE TRAFICO NACIONAL	31	11.046
SMS	13	
TRAF NACIONAL OTROS OPER. MOVILES EN UE	79	10.932
TRAFICO NAC.OTROS OPER.MOVILES	35.996	23.138.938
TRAFICO NACIONAL A FIJOS	6.048	1.115.067
TRAFICO NACIONAL A FIJOS EN UE	15	2.169
Total	**141.993**	**55.332.572**

Servicios Básicos de Voz:

Todas las líneas que actualmente tiene RTVM disponen de:

- Ocultación de Identidad
- Identificación de número
- Desvío de llamadas
- Buzón de Voz
- Facilidad de transferencia y multiconferencia
- Llamada en espera
- Retención de Llamada
- Servicio de varias SIM con el mismo número.
- Herramienta MDM para el control de todas las líneas móviles con enrolado automático de dispositivos.

Servicios Convergentes Fijo & Móvil & TI:

En la actualidad RTVM dispone de una serie de servicios de valor añadido, en el entorno de las comunicaciones unificadas, para la totalidad de los usuarios (600):

- **Agenda Única:** Permite disponer de una copia de los contactos personales de un usuario, tanto de la tarjeta SIM, la agenda del teléfono móvil ó la agenda de Outlook.
- **Mensajería:** Servicio centralizado de mensajería SMS y MMS tanto para la voz fija como móvil.
- **Buzón Único:** Repositorio único para las comunicaciones de voz fija y móvil, integrado con el correo corporativo de RTVM. Permitiendo además la recepción de fax.

- **Número único**: Servicio que permite a RTVM disponer de un "número único", independientemente del terminal de voz que tenga el usuario (fijo, móvil y/o PC-Soft Phone).
- **Herramientas colaborativas:** IM, presencia (Fijo/Móvil y PC) y audio conferencia entre PCs.

Todos estos servicios se encuentran integrados con el directorio corporativo de RTVM.

Integración con Servicios de Voz Fija:

En la actualidad RTVM dispone de un servicio de integración de la Red Privada Virtual de voz móvil con la red de telefonía fija, a través de la interconexión de ambas en IP mediante una Red de nueva generación, incluyendo su integración en un mismo Plan Privado de Numeración, el proveedor debe incluir la migración de los números en uso actualmente por RTVM dentro de su infraestructura.

Datos Móviles:

RTVM dispone de dispositivos de datos 3G/4G/5G que permiten el acceso desde PC a la red de área local LAN del RTVM. El sistema asigna direccionamiento IP privado y conecta directamente los equipos en movilidad con la LAN del RTVM a través de un circuito que la conecta con la red IP móvil. El servicio permite, además, la creación de diferentes pooles de IP para diferentes servicios, existiendo una red de equipos remotos conectados a través de un pool específico con la LAN de RTVM.

Estos dispositivos pueden ser equipos USB que permitan acceso a la red de datos móviles, así como equipos autónomos que dispongan de las capacidades necesarias para el acceso a la red móvil y convertirse en hotspot WIFI para dar servicio a los equipos corporativos.

Servicios obligatorios y requeridos:

Los licitadores ofrecerán, al menos, los siguientes servicios:

- Tráfico telefónico móvil-fijo y móvil-móvil de todo tipo, tanto entre líneas corporativas como externas. En el caso de llamadas entre líneas corporativas, bien fijas o bien móviles, la llamada se podrá realizar mediante la marcación de un número abreviado, de acuerdo con el plan de numeración que especifica este pliego.
- Tráfico de datos en movilidad mediante tecnología GPRS, UMTS, HSPA, 3G, 4G, 5G o la tecnología que se considere más adecuada en cada momento. Deberá existir, sin coste adicional, una conexión directa entre la red del adjudicatario y la red corporativa de RTVM que permita el acceso a la red corporativa en movilidad de los usuarios autorizados de acuerdo, como mínimo, a las características actuales.
- Servicio de mensajería entre terminales móviles
- Servicio de buzón de voz con posibilidad de acceso a los buzones de voz desde las extensiones móviles y fijas, y aviso de la existencia de mensajes en el buzón mediante envío de mensajes
- Los sistemas permitirán la integración de los contratos individuales que los usuarios tengan para uso personal, de forma que las llamadas generadas puedan cargarse a cualquiera de las dos líneas de forma fácil y cómoda.
- Los sistemas permitirán la existencia de varias tarjetas SIM con la misma numeración que puedan operar de forma simultánea.
- Capacidad de establecer tarifas planas en función de los perfiles de usuarios.

Funcionalidades:

El Servicio de Telefonía Móvil Corporativa deberá ofrecer una serie de facilidades adicionales que se presentan a continuación.

Marcación y presentación de número

La marcación a números externos a la red corporativa se realizará tal y como se hace desde cualquier línea fija o móvil no integrada en la red. Las extensiones fijas o móviles internas podrán ser marcadas usando el número asignado en la red pública o mediante marcación abreviada. En ambos casos, a efectos de tarificación la llamada se considerará de la misma forma.
La presentación del número llamante será diferente en función del origen y destino de la llamada. Si el llamante es una extensión fija o móvil y el destino también es una extensión fija o móvil, se presentará a éste último el número abreviado. La llamada a éste número debe permitir el establecimiento de comunicación entre ambos. Si el llamante es una extensión fija o móvil y el destino es una línea externa, se presentará a éste último el número asignado en la red pública. La llamada a éste número debe permitir el establecimiento de comunicación entre ambos.

Restricciones por línea

El Servicio de Telefonía Móvil deberá ofrecer la posibilidad de restricción en cada una de las líneas en función de diferentes facilidades:

- Destino de llamado. Al menos debe proporcionar niveles de restricción entre llamadas corporativas, nacionales o internacionales.
- Roaming. Se debe ofrecer la capacidad de activación o desactivación del servicio de telefonía móvil fuera del territorio nacional.
- Listas Negras. Se debe ofrecer la capacidad de restricción de llamadas en exclusiva a una lista de números prefijados o agrupación de números en función de su numeración.
- Listas Blancas. Se debe ofrecer la capacidad de permiso de llamadas en exclusiva a una lista de números prefijados o agrupación de números en función de su numeración.
- Restricción de ser llamado en el extranjero sólo por los miembros de un grupo
- Horario. Se debe posibilitar la activación o restricción del servicio en función de un horario determinado.
- Consumo. Se debe permitir el establecimiento de límites de consumo por línea o grupo de líneas Se considera necesario que estas restricciones puedan ser gestionadas directamente por RTVM a través de una aplicación web y un Servicio de Atención Telefónica dedicado.

Facilidades asociadas a extensiones

El servicio de Telefonía Móvil Corporativa debe incluir facilidades asociadas a las extensiones móviles entre las que se valorarán las siguientes:

- Transferencia de llamadas activas entre líneas móviles corporativas.
- Aviso de disponibilidad cuando una línea móvil corporativa deja de estar ocupado.
- Grupo de salto entre líneas móviles corporativas. Esta facilidad deberá poder gestionarse en línea por RTVM.

Facilidades asociadas a tarjetas SIM

Se considera necesario el mantenimiento de los servicios asociados a tarjetas SIM especiales Entre estas facilidades adicionales se encuentran:

- Tarjetas con capacidad de incluir un número personal además del número asignado por RTVM al usuario afectado.
- Tarjetas con capacidad de compartir una misma línea móvil, con la posibilidad de aviso de llamada entrante simultánea a las diferentes tarjetas SIM.

Facilidades asociadas a buzón de voz

Se considera necesario que todas las líneas móviles corporativas tengan la posibilidad de usar un servicio de Buzón de Voz asociado. Se valorará la inclusión de, al menos, las siguientes facilidades:

- Notificación mediante SMS de la existencia de un nuevo mensaje indicando el número origen del mismo
- Configuración en línea de las características del buzón de voz
- Facilidades adicionales

El licitador debe poner al servicio de RTVM todas las facilidades adicionales que vaya incorporando a su catálogo de servicios sin coste adicional.

Servicio MdM – Gestión de Activos

Se considera necesario el disponer de una herramienta MdM, que permita al adjudicatario y proveedor del servicio, gestionar el parque móvil actual y futuro, de manera que soporte, como mínimo, los siguientes procesos de forma remota y centralizada:

- Gestión remota de los dispositivos móviles (teléfonos y tablets).
- Control de inventario tanto hardware como software.
- Actuaciones de seguridad: Bloquear, resetear, etc...
- Provisión, gestión y configuración de dispositivos bajo el Model BYOD.

El servicio debe concebirse como totalmente gestionado, desde la provisión del dispositivo y el alta en la plataforma, así como la aplicación de las políticas, despliegue de aplicaciones o cualesquiera de las acciones que fueran necesarias.

RTVM debe disponer de acceso a la plataforma de gestión para actuaciones en caso de emergencia y disponer de conocimiento para bloquear o borrar un dispositivo por sustracción o pérdida.

Comunicaciones Unificadas

Dado que el objeto del Pliego incluye servicios de datos y voz fija y móvil, así como el periodo de prestación del servicio, en el que cobra especialmente las garantías de evolución y nuevos servicios a implementar sobre la red de RTVM, se considera importante la posibilidad de ofrecer servicios y funcionalidades convergentes que permitan explotar al máximo la funcionalidad de los distintos servicios ofertados, dado que RTVM ya dispone de ellos.

De acuerdo con esto, se valorará favorablemente la capacidad de los licitadores para ofertar funcionalidades convergentes. Los licitadores deberán indicar el detalle de dichas funcionalidades, su roadmap de comercialización y la posibilidad de implantarlas sobre la red ofertada.

Cobertura

Las propuestas de los licitadores deberán cumplir los siguientes requerimientos en lo relativo a la cobertura:

- Cobertura nacional e internacional, suministrando los indicadores de cobertura y de servicio disponibles.
- Cobertura en los edificios del RTVM. El nivel de señal deberá ser suficiente para mantener una conversación en todos los puntos de dichos edificios al inicio del contrato. Se implantarán, sin coste adicional, soluciones para que la cobertura alcance la totalidad del interior de los edificios, especialmente salas técnicas, mediante repetidores, antenas, etc. previa conformidad de RTVM. El licitador deberá comprometerse a cubrir con tecnología UMTS/HSDPA/HSUPA, 4G, 5G, en un plazo menor de 6 meses, aquellos edificios de RTVM que se soliciten.
- El licitador se comprometerá a facilitar a RTVM los mapas de cobertura 2G, 2,5G, 3G, 3,5G, 4G, 5G, que éste le solicite durante la vigencia del contrato. Las zonas de cobertura de telefonía móvil deberán ser entregadas en formato digital.
- El licitador deberá detallar los acuerdos de roaming establecidos con otros operadores en el ámbito internacional.

Plan de Numeración

Tal como se ha indicado en el Plan de Numeración de la telefonía fija, se garantizará la conservación de la numeración pública actualmente asignada, llevándose a cabo, sin coste adicional y a cargo del adjudicatario, la adecuada portabilidad numérica, en caso necesario.

En cuanto al Plan Privado de Numeración, el licitador deberá describir las características, limitaciones y virtudes de la solución planteada de cara mejorar el Plan Privado de Numeración de forma que éste permita una mejor integración de todas las comunicaciones, tanto fijas como móviles, siguiendo la línea integradora de todo el pliego. Deberá plantearse de forma global para todas las extensiones del RTVM, sean éstas fijas o móviles, valorándose la flexibilidad del PPN, su sencillez y la migración del actual PPN al nuevo.

En todo caso, la numeración asignada a cada una de las extensiones deberá ser accesible directamente desde el exterior del RTVM, mediante la marcación del número completo.

Las llamadas que se realicen mediante la marcación de 9 cifras a teléfonos móviles corporativos se deberán encaminar y facturar de la misma forma que las llamadas a móviles corporativos realizadas mediante la marcación reducida.

El adjudicatario deberá pertenecer a la entidad de referencia de portabilidad y garantizará que la numeración propuesta para este servicio será portable a la finalización del presente contrato.

Integración con telefonía fija

Tanto líneas móviles como extensiones fijas están integradas dentro de un mismo plan de numeración y permiten, por tanto, el establecimiento de comunicaciones mediante marcación abreviada. Se requiere, además, la integración de la Red Privada de Telefonía fija y la Red Privada Virtual de telefonía móvil de forma que, desde el punto de vista del usuario, exista una única red de voz, accesible desde el móvil o desde el fijo (o desde un softphones), que contemple el Plan Privado de Numeración planteado en la solución de Comunicaciones Unificadas.

Mensajería

Se requiere, al menos, mantener el servicio de mensajería corporativa que actualmente se está prestando a RTVM, de manera que las líneas móviles dispongan de capacidad de envío de mensajes de texto SMS y envío de mensajes multimedia MMS, junto a la posibilidad de

envío y gestión del servicio de mensajería desde aplicaciones accesibles desde la red de comunicaciones de RTVM.

El operador adjudicatario de este servicio debe proporcionar los mecanismos adecuados para las funciones que se describen a continuación. En todos los casos, el operador debe permitir los mecanismos apropiados para que RTVM establezca las políticas de control adecuadas para cada función.

- Múltiples destinatarios. Se debe permitir el envío de mensajes cuyo destino sea una lista de números, tanto pertenecientes a la red pública como a la numeración privada.
- Envío mediante correo electrónico. El operador deberá proveer los mecanismos necesarios para permitir el envío de mensajes desde una cuenta de correo electrónico de RTVM y usando como destino direcciones de correo asociadas a estas líneas. Se permitirá la posibilidad de incluir múltiples destinatarios en un mismo mensaje. En la oferta se deberá indicar el dimensionamiento de este servicio, indicando el número máximo de mensajes por minuto, y los mecanismos para garantizar la recepción de dichos mensajes.
- Sistema de envío masivo de mensajes cortos. RTVM dispone actualmente de un número corto para comunicarse con los ciudadanos a través de mensajes a teléfonos móviles. El operador deberá proporcionar la conexión de RTVM a una plataforma de envío masivo de mensajes cortos, describiendo los conectores y protocolos disponibles, así como su capacidad y funcionalidades. RTVM podrá exigir el mantenimiento del número corto que dispone en la actualidad para la recepción de mensajes.

Datos móviles

Acceso a Internet en movilidad mediante equipos de datos USB con conexión 3G/4G/5G para PC o mediante teléfonos móviles, o cualquier otro dispositivo que requiera conexión a internet.

Perfiles. Volumetría. Facturación

RTVM dispone en la actualidad de un parque de terminales móviles que incluye teléfonos, módems USB, terminales smartphones, Tablets, etc. Que RTVM pondrá a disposición del adjudicatario al inicio del servicio.

El adjudicatario deberá precisar cuándo se iniciará el plan de renovación de cada uno de los terminales y ofrecerá por tanto un precio para una línea no renovada de acuerdo al tipo y modelo de tráfico y otro para una línea renovada.

En caso de ser necesaria una adaptación o programación de los terminales existentes para su operación en la red del adjudicatario, será el adjudicatario el encargado de realizar las gestiones para la adaptación de los terminales a la nueva red, evitando en lo posible las molestias a los usuarios de los terminales.

El adjudicatario deberá proporcionar los terminales adecuados para la prestación de todos los servicios. Se considera terminal a cualquier elemento de comunicación que pueda portar una tarjeta SIM.

RTVM ha establecido 4 tipos de perfiles de dispositivos para los que el adjudicatario debe establecer satisfacer el tipo de dispositivo.

El adjudicatario se responsabilizará de la gestión del cambio de los mismos, con la supervisión de RTVM y el usuario final. Partiendo de la renovación inicial, el proveedor atenderá a la renovación del dispositivo en base a una bolsa de reposición orientada a

satisfacer nuevas provisiones y/o renovaciones a lo largo de la vida del contrato que alcance al menos al 60% de la flota.

La gestión del cambio debe comprender el alta en el servicio gestionado de MDM, la migración de datos del dispositivo móvil.

Flota de dispositivos RTVM.

PERFIL	Cantidad	Modelo	Datos
Perfil 1	**27**	Iphone&Samsung última	80 GB
Perfil 2	**113**	Iphone&Samsung penúltima generación	40 GB
Perfil 3	**90**	Samsung&Huawei&Apple&LG	20 GB
Perfil 4	**40**	Samsung&Huawei&Apple&LG	2 GB
	270		

Todos los perfiles descritos han de disponer de funcionalidades comunes en cuanto a la facturación de servicios de voz, datos y uso de mensajería.

La bolsa de datos asociada al consumo de los dispositivos de RTVM puede ser gestionada de forma común a nivel nacional y UE, de tal forma que en caso de que haya usuarios que NO dispongan de datos y por sus características lo requieran para el desempeño de sus funciones, pueda balancearse de forma dinámica por parte del proveedor, sin coste en el caso de existir saldo positivo de datos.

RTVM se reservará la capacidad de decidir si alguno de los dispositivos debe disponer de consumos de datos restringido, por lo que será el proveedor quien se encargará de la gestión de la calidad de servicio de forma dinámica.

En todos los casos, el operador deberá ofrecer un catálogo de terminales actualizado periódicamente. En el catálogo debe describirse las características de cada modelo y el precio del mismo. Se considera deseable el establecimiento de un tipo de descuento fijo sobre la oferta del operador vigente en cada momento para la adquisición de terminales.

Los servicios de roaming de voz y datos, como el volumen de tráfico internacional y servicios serán facturados en base a una bolsa de minutos anual.

El licitador deberá especificar en su oferta las características mínimas de los terminales de gama baja, media y alta, en calidad y cantidad suficiente como para cumplir con la matriz anterior sobre la base de los requerimientos de RTVM, así como una previsión de incremento del 15% de los indicados en la tabla.

Servicios de Asistencia Técnica

El operador debe ofrecer un servicio de garantía y mantenimiento de terminales durante la vigencia del contrato. El servicio debe permitir que todos los usuarios de RTVM cuenten con terminales plenamente operativos, actualizados y capaces de soportar los servicios del operador en todo momento.

Con el objeto de ofrecer una respuesta eficaz ante los posibles daños o deterioro de terminales, se considera necesaria la existencia de un número de terminales almacenados en las dependencias de RTVM. El número de terminales (“botiquín”) debe ser del 3% del número total de líneas con servicio.

Estadísticas uso del servicio (Tarificación)

Se almacenarán todos los datos de las llamadas, tanto entrantes como salientes, de todas las extensiones. El propósito de estos datos será poder extraer cualquier tipo de estadística a posteriori que permita la optimización de los recursos.

Estos datos se entregarán periódicamente (periodicidad mensual) en formato electrónico, y estarán desglosados por unidades orgánicas según lo indicado por los responsables de RTVM.

El formato de detalle en el que se almacenarán deberá contener al menos la siguiente información:

- Fecha de llamada
- Hora de llamada
- Duración de la llamada (en segundos)
- Número de destino
- Número de origen

Este formato será parametrizable por extensión. Además, el adjudicatario pondrá a disposición de RTVM información suficiente para el conocimiento del estado de la red.
Fundamentalmente:

- Mecanismos de seguimiento online, vía web, y en tiempo real que permitan el seguimiento del estado de los servicios.
- Mecanismos de consulta online, vía web, que permitan el seguimiento de las llamadas realizadas por línea en cualquier momento.
- Instrumentos de detección de incidencias de funcionamiento y activación de su resolución. Estos mecanismos facilitarán el seguimiento en línea del estado de las incidencias.
- Realización de resúmenes estadísticos en línea, numéricos y gráficos con periodicidad diaria, mensual y anual del funcionamiento de los servicios, indicando tanto los volúmenes de tráfico como la calidad del funcionamiento.

Se proporcionará un sistema de gestión centralizado, vía web preferiblemente y con posibilidad de descarga de ficheros, para manejar los siguientes aspectos del servicio:

- Inventario de líneas existentes.
- Gestión de RPV.
- Gestión de averías.
- Reemplazo por rotura.
- Cobertura por robo.
- Detalle de facturación

Todos los informes se enviarán a RTVM antes del 5º día de cada mes.

Facturación Detallada

Se emitirán facturas mensualmente a los Responsables de Facturación que se darán a conocer al adjudicatario.

El formato podrá ser modificado por el RTVM previa consulta con el adjudicatario.
Las facturas deberán emitirse en formato electrónico y deberán poder estar accesibles en papel.

El formato electrónico deberá contener el detalle de cada uno de los conceptos facturados.

Las reclamaciones por discrepancia con alguno de los conceptos facturados se resolverán en el plazo máximo de un mes, no interrumpiéndose mientras tanto los pagos de facturación. En cualquier caso, se realizará el abono o cargo correspondiente en la factura siguiente (o en la siguiente a ésta, si ya se hubiese emitido).

El adjudicatario mantendrá un servicio accesible desde Internet para el acceso a datos de tarificación correspondiente al período de facturación en curso, en el que se podrán visualizar los datos de cada una de las líneas del RTVM. De esta forma, los usuarios de telefonía móvil del RTVM podrán consultar, en cualquier momento, el consumo y el gasto de su línea de telefonía móvil.

RTVM podrá definir números para los cuales no exista detalle ni resumen de facturación por motivos de seguridad u otros.

ORGANIZACIÓN DEL SERVICIO

HORARIO-UBICACIÓN

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 en español.
- Horarios de servicio:24x7x365 en dinámica ordinaria.
- El adjudicatario 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 adjudicatario pondrá a disposición del servicio un número de teléfono, una dirección de correo y/o el acceso remoto a través de navegador a una herramienta de gestión de peticiones, con el objetivo de resolver dudas y/o incidencias y/o peticiones de cambio / evolutivos, tanto técnicas como funcionales.

MODELO OPERATIVO

El modelo operativo relaciona todos los servicios que se prestan dentro de este lote, con las operaciones, procesos y procedimientos que las regulan, considerando las herramientas y tecnología que se requieren para su soporte. Es un modelo de Personas, Procesos y Tecnologías interrelacionadas, cuyo objetivo es prestar los servicios de forma eficaz y eficiente.
Todas estas operaciones deben de estar sujetas a la supervisión y control del Responsable del Servicio, responsable de las actividades de gobierno y estrategia de las personas, procesos y tecnologías empleadas, de las relaciones con otras unidades.
En lo que respecta al modelado de operaciones y tecnologías por cada servicio, el modelo operativo deber realiza las siguientes actividades para cada servicio:

- Descripción del servicio: detallando su objetivo, alcance y modelo de servicio.
- Definición de los procesos y procedimientos asociados: se deben documentar los procesos y procedimientos operativos, detallando los requisitos del proceso, responsables, actividades y resultados.

Esto incluye:
- Procedimientos de provisión.
- Procedimientos de operación: gestión de peticiones, consultas e incidencias.
- Procedimientos de soporte: gestión de cambios, gestión de la configuración, gestión de la capacidad, gestión de problemas, etc.
- Definición de los niveles de servicio: se deben especificar los diferentes indicadores de riesgo y de rendimiento asociados con cada uno de los servicios, que permita establecer niveles de acuerdo de servicio, ANS.

- Diseño de los interfaces, relaciones entre procesos, entradas salidas de información y flujos de información a integrar.
- Diseño de las herramientas y tecnologías que permitan prestar y gestionar los servicios de forma completa.

MODELO ORGANIZATIVO

El modelo organizativo recoge como deben organizarse los recursos para prestar los servicios de forma eficiente.

Bajo la dirección del Responsable del servicio de RTVM y su equipo, el adjudicatario deberá nombrar un Responsable único del servicio. Este responsable, organizará los recursos humanos en dos funciones que se corresponden con los servicios objeto de este lote.

Cada una de estas funciones contará con el equipo de trabajo y al frente de cada una de ellas el adjudicatario pondrá un responsable de función, con el objetivo de facilitar la comunicación con el equipo de RTVM.

Estas dos funciones son las siguientes:

- Gestión de voz fija y datos móviles
- Servicio gestionado de mantenimiento, soporte, operación y administración de la plataforma MdM.

Dentro de este modelo organizativo el adjudicatario deberá considerar los requisitos de equipo mínimo que se indican en el apartado **Equipo de trabajo,** y los horarios, ubicación del equipo, indicados en el apartado **Horario-Ubicación** para la prestación del servicio.

EQUIPO DE TRABAJO

La empresa licitadora propondrá 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.

Para garantizar el soporte de calidad en ITIL, el equipo de trabajo debe contar con, al menos, dos personas con titulación Service Manager en ITIL o equivalente que deben pertenecer a la empresa.

Cada licitador 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.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 10 años.
- Responsable del Servicio (tiempo parcial):
  - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 8 años.
- Técnicos de Soporte:
  - Descripción detallada de la misión y funciones a prestar dentro del servicio.
  - Dominio demostrable de las herramientas e infraestructuras para la prestación del servicio.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 4 años.
- Agente Personal:
  - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.

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 y garantizando impacto "cero" en los niveles de servicio.

TECNOLOGÍAS Y HERRAMIENTAS

Todos los servicios de este lote requieren de tecnología y herramientas para cumplir su cometido. Se distinguirán entre herramientas para prestar los servicios y herramientas de gestión y soporte a la operación.

El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para RTVM.

LOTE 2: SERVICIOS DE INTERNET, WAN, LAN

SERVICIOS DE INTERNET Y WAN.

La red de comunicaciones de RTVM se compone de los servicios MacroLAN y Data Internet.

- El primero es un servicio de red privada virtual que permite conectar las diferentes sedes de forma que todas se conecten como si de una sola red local se tratase, usando direccionamiento IP privado.

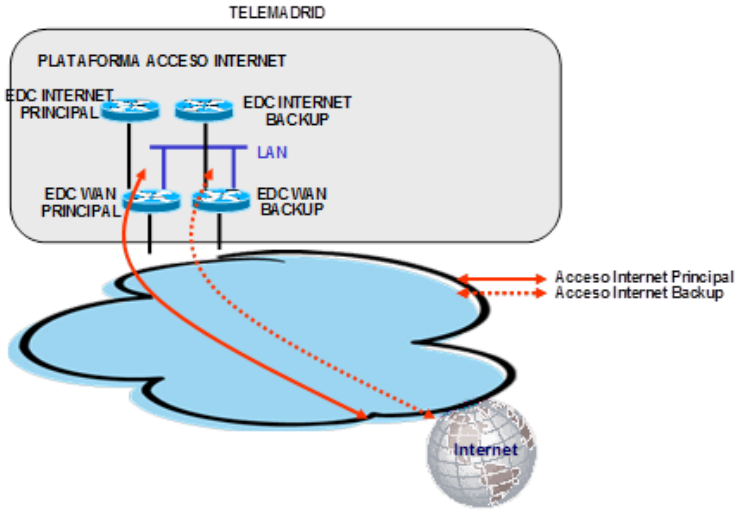
- El segundo es un servicio de acceso corporativo a Internet.

Las sedes que conforman la "Red Corporativa" de RTVM, se encuentran distribuidas en las siguientes ubicaciones y con los siguientes equipos que permiten su conectividad:
RTVM cuenta con las siguientes sedes:

SEDE	TIPO ACCESO	ACCESO	CAUDALES
Madrid / Pozuelo de Alarcón (Principal)	Acceso Principal	MLAN 10GB	2GB Plata, 100MB Multimedia
	Data Internet 2 nivel		
	Acceso Respaldo	MLAN 10GB	2GB Plata, 100MB Multimedia
	Data Internet 2 nivel		
SEDE	**TIPO ACCESO**	**ACCESO**	**CAUDALES**
Madrid / Congreso / San Jerónimo, sn	Acceso Principal	MLAN 100MB	100MB Plata
	Acceso Respaldo	VPN IP FTTO	100% Plata
Madrid / Asamblea de Madrid	Acceso Principal	MLAN 100MB	100MB Plata
	Acceso Respaldo	VPN IP FTTO	100% Plata
Madrid / Ayuntamiento de Madrid	Acceso Principal	MLAN 100MB	100MB Plata
	Acceso Respaldo	VPN IP FTTO	100% Plata
Madrid / Comunidad de Madrid	Acceso Principal	MLAN 100MB	100MB Plata
	Acceso Respaldo	VPN IP FTTO	100% Plata
Madrid / Palacio de la Moncloa	Acceso Principal	FTTH 600MB	
	Acceso Respaldo	FTTH 600MB	
Madrid / Dirección General de Tráfico	Acceso Principal	FTTH 600MB	
	Acceso Respaldo	FTTH 600MB	

Se requiere un **aumento de caudal a 1 Gbps** por línea en el acceso principal en Paseo del Príncipe, 3. El proveedor se encargará de provisionar la infraestructura necesaria para asegurar los caudales de las sedes interconectadas de la organización.

El servicio se encuentra diversificado en dos centrales diferentes con el objetivo de contar con HA en cuanto a la provisión de líneas, centrales y caminos desde y hacia RTVM:



RTVM dispone de un rango de direccionamiento IP público (160 IPs), el adjudicatario debe aumentar a 256 IPs públicas, para los servicios que la organización dispone en Internet, el adjudicatario debe asegurar su disponibilidad para que los servicios que disponen de direccionamiento IP público sigan operativos, en caso de NO poder adquirir el rango, se debe facilitar un nuevo rango de iguales características durante la vida del servicio y será responsabilidad del adjudicatario asegurar la disponibilidad del rango actual hasta la realización de la migración de los servicios actuales. Por motivos de seguridad, el rango ip se facilitará a todos aquellos que presenten propuesta para su valoración.

Todo el equipamiento correspondiente a la "Red Corporativa" es propiedad del prestatario del servicio, con gestión y mantenimiento de equipamiento en horario 24x7.

Ambos circuitos deben estar diversificados en dos centrales diferentes para garantizar la continuidad del servicio.

Se solicita el despliegue y mantenimiento de una "Red de Datos Corporativa" que establezca los medios de comunicación necesarios entre las sedes mencionadas en el apartado anterior.

Esta "Red de Datos Corporativa" ha de cumplir, al menos, con los requerimientos de la red solicitados de ancho de banda, redundancia y diversificación.

Con el fin de dotar al servicio de la máxima seguridad, los accesos a la red del adjudicatario se efectuarán mediante líneas dedicadas al efecto.

El diseño de la Red cubrirá todas las necesidades actuales, incluyendo las líneas necesarias para interconectar las distintas sedes con los anchos de banda exigidos, todo el equipamiento necesario para la prestación del servicio, la instalación y configuración de todas las infraestructuras, y finalmente la gestión, administración y mantenimiento de toda la Red, durante la vigencia del contrato.

La solución ofertada deberá cumplir las siguientes características:

- Deberá proporcionar toda la estructura de medios físicos que facilite la interconexión entre los centros mencionados.
- Será condición indispensable que los enlaces de datos se realicen mediante medios terrestres y no compartidos con otros usuarios. Se valorará favorablemente la provisión del servicio sobre infraestructura que sea propiedad del operador.

- El centro de gestión global del servicio debe disponer de un ingeniero nominado responsable de la interlocución técnica y asesoramiento con RTVM, responsable técnico de los servicios gestionados. Con funciones de elaboración informes, reuniones de seguimiento mensuales y presenciales e identificación de propuestas de mejora y asesoramiento.

RTVM requiere al adjudicatario la garantía de evolución de la arquitectura de red propuesta, así como su capacidad para soportar los nuevos servicios y aplicaciones que RTVM pueda implementar en un futuro. Desde este punto de vista, se necesita la capacidad de escalar de la red y su capacidad para soportar servicios de VoIP, accesos a redes de nueva generación tanto fijas como móviles, así como las garantías ofrecidas por el licitador para incorporar nuevos tipos de accesos y escalabilidad de ancho de banda a su red.

En caso de que la arquitectura propuesta difiera de la actualmente existente, se valorará especialmente las garantías de bajo impacto sobre los usuarios finales.
Se requiere un acceso redundante, con caminos físicos y equipamiento diferentes, al objeto de evitar puntos únicos de fallo.

El adjudicatario proporcionará a RTVM un caudal inicial de acceso a Internet de al menos 1 Gbps bidireccionales en ambas líneas, si bien, la red debe estar preparada para aumento de caudal a 5 Gbps.

Se demanda que el proveedor disponga de presencia en los principales puntos neutros nacionales e internacionales y acuerdos de "peering" con gran número de operadores. La oferta detallará los puntos neutros en los que el ofertante esté presente y los acuerdos de "peering", lo cual se tendrá en cuenta en el análisis de las ofertas.

Se valorará el uso de infraestructura propia hasta los puntos neutros nacionales e internacionales, por parte del adjudicatario.

Servicio DNS

RTVM dispone en su infraestructura del servicio DNS primario que incluyen todos los registros de recursos de la organización (dominios, zona, etc) y se encarga de atender de forma primaria, las solicitudes DNS para sus dominios.

El adjudicatario debe proporcionar el servicio DNS Secundario, que disponga de la información de todas las zonas corporativas, en modo lectura y que gestione las consultas en caso de indisponibilidad del origen.

Servicio Gestionado

Se requiere una propuesta concreta respecto a la disponibilidad de, como mínimo, un responsable comercial de la cuenta de RTVM, un ingeniero responsable de los nuevos proyectos, y un responsable del seguimiento y la evolución de los servicios contratados.

Asimismo, se describirán todos los sistemas y mecanismos (centros de atención, personal a su disposición, metodología, etc.) a disposición de RTVM, así como de las sedes y los edificios que forman parte de la red de RTVM. Entre estos sistemas, es necesario disponer de un sistema de atención telefónica personalizada ("ventanilla única").
Este sistema de atención al usuario tendrá que ser totalmente flexible para adaptarse a las necesidades de RTVM y deberá funcionar con un horario 24x7.

El adjudicatario deberá mantener reuniones periódicas con los responsables de RTVM para tratar los asuntos de este contrato. La periodicidad de dichas reuniones será definida por RTVM y será mayor durante la implantación del proyecto.

SERVICIOS DE MANTENIMIENTO LAN-WIFI.

RTVM dispone actualmente de una red multiservicio con equipamiento Xtreme de la cual se facilitará a los licitantes a este pliego que así lo requieran el documento de diseño de ALTO NIVEL e inventario de equipos de forma detallada.

Servicio de Mantenimiento LAN-WIFI

El servicio actual finaliza el 10 de octubre de 2024. A partir de esa fecha:

El adjudicatario deberá garantizar el funcionamiento de los productos y servicios objeto de la presente contratación durante todo el contrato, a contar desde la fecha de aceptación, obligándose a la prestación de todos los servicios que para ello sean requeridos, entre ellos:

1. *Mantenimiento integral*
   Afecta a la infraestructura y al software, de los procesos de mantenimientos preventivos (para detectar y evitar/corregir posibles incidencias) como correctivo y evolutivo (reparación/sustitución de componentes físicos, actualización tecnológica y funcional del software, etc.); estarán incluidas en el servicio todas las tareas necesarias para mantener el equipamiento en óptimas condiciones de explotación en todo momento. Se incluirá la gestión con fabricante, gestión de garantías, averías, sustitución de componentes, etc.

2. *Soporte técnico especializado*
   Se requerirá el acceso directo a los técnicos especialistas de segundo nivel LAN del adjudicatario, en el caso de que por incidencias con afectación a los entornos productivos de RTVM.
   Todos los repuestos serán proporcionados en los tiempos establecidos por el proveedor de los servicios, incluyendo el stock y almacenaje de los mismos si procede en función de los tiempos de respuesta.

3. *Servicio de Atención al cliente*
   Con el objeto de facilitar la comunicación y posterior gestión de las posibles incidencias técnicas, el adjudicatario deberá facilitar un **servicio centralizado de atención** de incidencias, que permita la comunicación y consulta de las mismas tanto a través de Internet como telefónicamente.

4. *Mantenimiento preventivo:*
   - Supervisión remota de los equipos (gestión, correcto funcionamiento y detección de anomalías).
   - Pruebas de funcionamiento.
   - Revisión y reparación/sustitución cuando se requiera.
   - Actualización de los niveles de microcódigo, cuando se requiera.
   - Actualización de productos software, cuando se requiera.

5. *Mantenimiento correctivo:*
   El mantenimiento correctivo se aplicará para detectar y solucionar las posibles averías o anomalías que impidan el correcto funcionamiento de equipos y terminales

requeridos, así como sus configuraciones. En el caso de mantenimiento correctivo, es decir incidencias y averías, el horario de atención será de 24x7 (24 horas al día, los siete días de la semana). Los tiempos para la solución de los problemas serán:

- 1 horas máximo si el problema supone una pérdida total del servicio o un servicio tan "degradado" que impide un funcionamiento adecuado de la organización.
- 4 horas máximo si el problema permite un servicio "degradado" pero adecuado (líneas de respaldo o similar)
- Al día siguiente si el problema es "leve" (no afecta al funcionamiento normal de la organización, y no hace falta utilizar las líneas de respaldo)

6. *Mantenimiento adaptativo:*
   Comprende las acciones encaminadas a la optimización de los servicios existentes, así como a la realización de peticiones de actuación sobre dichos servicios. Corresponde a este concepto la actualización tecnológica que se requiera para implantar nuevos servicios, que puedan ser solicitados a lo largo de la duración del contrato. Las propuestas de optimización provendrán tanto del adjudicatario como de RTVM, debiendo ser en todo caso autorizadas por RTVM.

7. *Registro de Incidencias:*
   Se deberá contemplar la existencia de un **registro de incidencias centralizado**, en el que se refleje información correspondiente de:
   - Apertura de la incidencia.
   - Reparación o sustitución del elemento averiado.
   - Restauración del servicio.
   - Comunicación de la restauración del servicio.
   - Cierre de la incidencia.
8. *Informes:*
   Se proporcionarán **informes de monitorización** del tráfico mensuales antes del 5º día de cada mes. En todos los casos, quedan incluidos dentro del servicio de mantenimiento los siguientes conceptos:
   - Desplazamiento de los técnicos al lugar de ubicación del equipo afectado.
   - Mano de obra y servicios correspondientes a la atención de la avería.
   - Gestión y escalado de tercer nivel con el fabricante del equipamiento (Enterasys/Xtreme) ya que el equipamiento actual se encuentra en garantía para los próximos dos años.

Infraestructura LAN

Se adjuntan como información complementaria el inventario objeto del servicio de mantenimiento hardware y software y servicio en:

- **ANEXO INVENTARIO LAN**
- **ANEXO INVENTARIO WIFI**

Cuadro resumen infraestructura LAN.

PART NUMBER	DESCRIPCIÓN	UNIDADES
95507-5420M-48W-4YE	PW 4HR AHR 5420M-48W-4YE	59 Ud
95507-5420M-24W-4YE	PW 4HR AHR 5420M-24W-4YE	15 Ud
95507-5520-24X	PW 4HR AHR 5520-24X	6 Ud
95507-AP4000-WW	PW 4HR AHR AP4000-WW	27 Ud
XIQ-PIL-S-C-PWP	ExtremeCloud IQ Pilot SaaS Subscription and PWP SaaS Support for one (1) devide (1 year) [Term: 2 years]	27 Ud
XIQ-PIL-S-C-PWP-DALAY	ExtremeCloud IQ Pilot SaaS Subscription and PWP SaaS Support for one (1) devide (1 year) [Term: 2 years]	80 Ud
XIQ-NAC-S-1K-PWP	ExtremeNAC SW subscription for 1000 end-systems for 1 Year PartnerWorks Plus [Term: 2 years]	1 Ud

SERVICIOS DE SEGURIDAD EN RED

Actualmente RTVM dispone de una suite de servicios de Seguridad con una serie de características diferencias que permiten disponer en la capa de infraestructura de las herramientas imprescindibles para soportar sus procesos, en un ambiente de máxima automatización y especialización, que incluye procesos de diseño, despliegue, mantenimiento y acciones de mejora continua como soporte a la evolución del Sistema de Gestión de la Seguridad.

Se dispone de los servicios: Tráfico de Correo Limpio, Redes Limpias (Firewall en red, IDS, WebFiltering), QoS.

RTVM requiere del adjudicatario que dote a la organización de un conjunto de servicios en red, en el ámbito del perímetro, que en su conjunto y de forma totalmente gestionada, permitan reducir la superficie de exposición de los procesos de la organización y por lo tanto los riesgos y vectores de ataque, aportando información sobre el tráfico y aplicaciones que atraviesan el perímetro de la organización con el fin de asegurar su integridad.

Por lo tanto, se requiere de los siguientes servicios, gestionados extremo a extremo de acuerdo a las políticas y requerimientos solicitados por RTVM: Firewall en red, Antivirus, Filtrado Web, Anti spam Correo – limpio, Control de Aplicaciones, IDS/IPS, AntiDDos.

Firewall:

El proveedor asegurará el perímetro de la organización con una pareja de WAF de nivel 7 con capacidades de hasta 2GB. El servicio debe disponer de las licencias necesarias para la gestión del proceso de navegación segura.

Anti Virus:

El servicio de Antivirus debe inspeccionar el tráfico que es transmitido por la plataforma de Seguridad, analizándolo con las firmas disponibles en su BBDD, en caso de que exista coincidencia se realiza la acción determinada sobre el archivo (Bloqueo, Aviso…), debe proteger la navegación web, transferencia de ficheros, protocolos de intercambio de correo, mensajería instantánea, etc.

Filtrado Web:

Debido al riesgo que supone la distribución y visualización de contenido no autorizado, se requiere la monitorización del tráfico de navegación y la prevención de la visualización y/o acceso a sitios no autorizados.

El servicio debe permitir el filtrado por categorías en base a contenido, y debe disponer de los módulos de gestión e informes necesarios para su explotación.

Control de Aplicaciones:

El adjudicatario debe proveer de una solución que permita el control de aplicaciones de los clientes internos, para determinar que aplicaciones pueden acceder a la plataforma de seguridad y en caso de ser necesario también permite el filtrado de aplicaciones no deseadas.

El servicio debe analizar el tráfico saliente/entrante y no permitir ni la entrada ni salida de aplicaciones contrarias a las políticas de la empresa

IDS/IPS

El Sistema de Detección y Protección de Intrusión debe funcionar como un sensor de red en tiempo real, basado en firmas, que anticipe la acción de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red.

Debe proveer seguridad hasta la capa de aplicación, sin mermar el rendimiento. La funcionalidad debe prevenir, como mínimo, de los siguientes tipos de ataques: Ataques de Denegación de Servicio (DoS), Ataques de Reconocimiento, Exploits, Ataques de evasión de sondas IDS, botnets.

Servicio Tráfico Limpio de Correo

El adjudicatario debe suministrar como servicio una plataforma que blinde a la organización y ofrezca la máxima protección contra spam, gestión de cuarentena, antivirus, phishing, suplantación de identidad y otras ciberamenazas con múltiples niveles de seguridad y análisis basados en inteligencia artificial.

Debe disponer de capacidad para al menos 20 dominios de la organización y 1100 buzones de correo.

La integración ha de hacerse a través de registros MX de DNS, y habrá un canal de comunicación seguro y único entre la plataforma y RTVM. Además, dispondrá de integración con cuentas de dominio vía LDIF, y servicio de guarda de correo.

La plataforma debe proveer de un portal de gestión de los servicios, así como un motor de informes y estadísticas en tiempo real.

ORGANIZACIÓN DEL SERVICIO

HORARIO-UBICACIÓN

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 en español.
- Horarios de servicio:24x7x365 en dinámica ordinaria.
- El adjudicatario 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 adjudicatario pondrá a disposición del servicio un número de teléfono, una dirección de correo y/o el acceso remoto a través de navegador a una herramienta de gestión de peticiones, con el objetivo de resolver dudas y/o incidencias y/o peticiones de cambio / evolutivos, tanto técnicas como funcionales.

MODELO OPERATIVO

El modelo operativo relaciona todos los servicios que se prestan dentro de este lote, con las operaciones, procesos y procedimientos que las regulan, considerando las herramientas y tecnología que se requieren para su soporte. Es un modelo de Personas, Procesos y Tecnologías interrelacionadas, cuyo objetivo es prestar los servicios de forma eficaz y eficiente.
Todas estas operaciones deben de estar sujetas a la supervisión y control del Responsable del Servicio, responsable de las actividades de gobierno y estrategia de las personas, procesos y tecnologías empleadas, de las relaciones con otras unidades.
En lo que respecta al modelado de operaciones y tecnologías por cada servicio, el modelo operativo deber realiza las siguientes actividades para cada servicio:

- Descripción del servicio: detallando su objetivo, alcance y modelo de servicio.
- Definición de los procesos y procedimientos asociados: se deben documentar los procesos y procedimientos operativos, detallando los requisitos del proceso, responsables, actividades y resultados.
  Esto incluye:

  - Procedimientos de provisión.
  - Procedimientos de operación: gestión de peticiones, consultas e incidencias.
  - Procedimientos de soporte: gestión de cambios, gestión de la configuración, gestión de la capacidad, gestión de problemas, etc.
  - Definición de los niveles de servicio: se deben especificar los diferentes indicadores de riesgo y de rendimiento asociados con cada uno de los servicios, que permita establecer niveles de acuerdo de servicio, ANS.
- Diseño de los interfaces, relaciones entre procesos, entradas salidas de información y flujos de información a integrar.
- Diseño de las herramientas y tecnologías que permitan prestar y gestionar los servicios de forma completa.

MODELO ORGANIZATIVO

El modelo organizativo recoge como deben organizarse los recursos para prestar los servicios de forma eficiente.

Bajo la dirección del Responsable del Servicio de RTVM y su equipo, el adjudicatario deberá nombrar un Responsable único del servicio. Este responsable, organizará los recursos humanos en funciones que se corresponden con los servicios objeto de este lote.

Cada una de estas funciones contará con el equipo de trabajo y al frente de cada una de ellas el adjudicatario pondrá un responsable de función, con el objetivo de facilitar la comunicación con el equipo de RTVM.

Estas funciones son las siguientes:

- Servicio de Internet, WAN y Seguridad en red
- Servicio gestionado de mantenimiento, soporte, operación y administración LAN-WIFI.

Dentro de este modelo organizativo el adjudicatario deberá considerar los requisitos de equipo mínimo que se indican en el apartado **Equipo de trabajo,** y los horarios, ubicación del equipo, indicados en el apartado **Horario-Ubicación** para la prestación del servicio.

EQUIPO DE TRABAJO

La empresa licitadora propondrá 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.

Para garantizar el soporte de calidad en ITIL, el equipo de trabajo debe contar con, al menos, dos personas con titulación Service Manager en ITIL o equivalente que deben pertenecer a la empresa.

Cada licitador 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.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 10 años.
- Responsable del Servicio (tiempo parcial):
  - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 8 años.
- Técnicos de Soporte:
  - Descripción detallada de la misión y funciones a prestar dentro del servicio.
  - Dominio demostrable de las herramientas e infraestructuras para la prestación del servicio.
  - Currículum Vitae. Perfil y certificaciones.
  - Experiencia demostrada de más 4 años.

- Agente Personal:
  - Descripción detallada de la misión y funciones a prestar dentro del servicio requerido.
- 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 6 años en la prestación de servicios similares.

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 y garantizando impacto "cero" en los niveles de servicio.

TECNOLOGÍAS Y HERRAMIENTAS

Todos los servicios de este lote requieren de tecnología y herramientas para cumplir su cometido. Se distinguirán entre herramientas para prestar los servicios y herramientas de gestión y soporte a la operación.
El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para RTVM.

LOTE 3: SERVICIOS DE SEGURIDAD LÓGICA

El Plan Director de Seguridad Lógica de RTVM contempla una serie de iniciativas para un correcto desarrollo de la estrategia corporativa de seguridad.

En función del grado de madurez de estas iniciativas se pueden clasificar en dos grupos:

A. Iniciativas que ya están implantadas y se contempla en el marco de la mejora continua revisarlas y mantenerlas o mejorarlas,
B. Iniciativas que se deben consolidar en tanto que están en proceso de implantación.

En el momento actual RTVM está concentrado en tres líneas de actuación:

1. Garantizar la seguridad de los servicios, los datos y su disponibilidad (ISO 27002).
2. Fortalecer las capacidades de prevención, detección y respuesta ante ciberataques.
3. Sistema de Gestión de la Seguridad (ISO 27001) y Convergencia con la legislación aplicable vigente (RDPD y ENS)

Como desarrollo de la línea 1:

RTVM está rediseñando su estrategia de seguridad para potenciar la definición de arquitecturas más seguras para los sistemas, servicios e infraestructuras de tecnologías de la información y de las comunicaciones (en adelante TIC), para lo cual requiere poner en marcha un servicio de soporte especializado en Diseño Seguro de infraestructuras y tecnologías TIC, (en adelante SDS). Esta iniciativa se engloba dentro del grupo A.

Respecto a la línea 2:

RTVM ha puesto en marcha recientemente un Centro de Operaciones de Seguridad (en adelante SOC– Security Operation Center) con el objetivo de centralizar y mejorar sus capacidades en materia de ciberseguridad, que aglutine y desarrolle las funciones de monitorización de seguridad, detección de incidentes, vigilancia antes nuevas fuentes de amenazas y análisis de vulnerabilidades, optimizando la capacidad de reacción y respuesta ante cualquier ataque. Por su naturaleza centralizada, el SOC facilitará tanto la implantación de las herramientas y/o tecnologías más adecuadas en cada momento, como la adopción de las medidas oportunas para una defensa eficiente. Esta iniciativa se engloba dentro del grupo B.

Los dos servicios, SDS y SOC, permitirán la prevención de incidentes, gracias a la mayor resiliencia de los sistemas, servicios e infraestructuras TIC, debido al aumento de su seguridad desde el diseño, y a la mejora de su capacidad de respuesta y recuperación en caso que se materialice algún incidente de seguridad. El ámbito de aplicación de estos servicios de seguridad se circunscribe a los sistemas, servicios e infraestructuras TIC de RTVM.

Adicionalmente, RTVM ha desplegado recientemente agentes en dispositivos móviles para gestionar amenazas y agentes XDR/EDR en puestos, servidores y cortafuegos. Esta iniciativa se engloba dentro del grupo B.

Respecto a la línea 3:

RTVM cuenta ya con este servicio, necesario para asegurar el alineamiento con la legislación aplicable vigente, con los estándares y buenas prácticas. Esta iniciativa se engloba dentro del grupo B.
Se pretende además potenciar las labores de concienciación que se vienen realizando en materia de seguridad lógica dirigidas a empleados.

MEDIDAS TÉCNICAS: LICENCIAS

- Licencias en 50 móviles (asignado a personal directivo y ciertos responsables de área) de un agente para la defensa contra las amenazas móviles. Esta solución mantendrá la información corporativa a salvo, protegiendo los dispositivos móviles en todos los vectores de ataque: aplicaciones, red y sistema operativo. Se adaptará perfectamente al entorno móvil existente, se desplegará y escalará rápidamente, y protegerá los dispositivos sin afectar a la experiencia del usuario ni a la privacidad.
  Actualmente RTVM tiene desplegada la solución Harmony Mobile de CheckPoint, vigente hasta diciembre de 2024.
  Si la solución propuesta por el adjudicatario fuera otra diferente, debe justificar su propuesta de solución sobre la base del posicionamiento de la misma en los cuadrantes comparativos de referencia y/o ventajas funcionales, operativas, económicas.
  Será responsabilidad del adjudicatario el despliegue en los móviles identificados por RTVM e igualmente si se renueva los móviles donde esté desplegado el agente.

- Licencias de agentes XDR/EDR: para los puestos de usuario, servidores y cortafuegos, que realicen funciones de monitorización, detección, bloqueo de amenazas y operen en diferentes capas del sistema.
  Actualmente RTVM tiene desplegada la solución EDR/XDR Cortex de Palo Alto para la detección y respuesta ante amenazas que estará vigente hasta diciembre de 2024.

Si la solución propuesta por el adjudicatario fuera otra diferente, debe justificar su propuesta de solución sobre la base del posicionamiento de la misma en los cuadrantes comparativos de referencia y/o ventajas funcionales, operativas, económicas.
Será responsabilidad del adjudicatario el despliegue de la misma en los equipos identificados por RTVM.

Ítem	Descripción	Cantidad
PAN-XDR-ADV-EP	Cortex XDR for 1 endpoint, includes 30 days of data retention and standard success	1200
PAN-XDR-HOST-INST	Host Insights add-on for Cortex XDR	1200
PAN-XDR-PRO-GB	Cortex XDR Pro for daily ingested GB. Includes 30 days of ingested data retention, 180 days of alerts and incidents retention and standard success	100

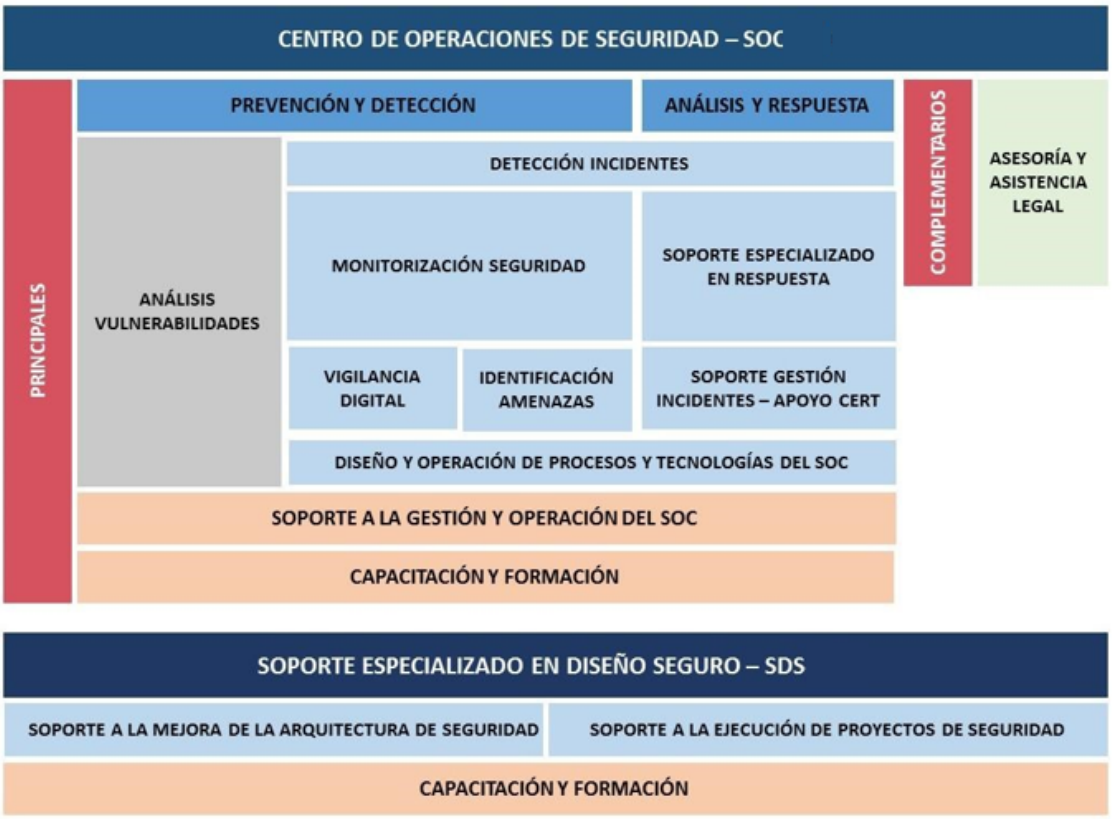
CENTRO DE OPERACIONES DE SEGURIDAD - SOC

Actualmente RTVM dispone de un servicio de SOC soportado sobre la plataforma MonICA vigente hasta diciembre 2024.

Será objeto de este lote la creación de un **Centro de Operaciones de Seguridad, SOC,** que preste los siguientes servicios de ciberseguridad, organizados en 2 bloques, debido a su mayor o menor grado de integración requerido:

- **Servicios PRINCIPALES**:
  - **Servicios de prevención**: consistentes en el análisis de vulnerabilidades de seguridad de los sistemas e infraestructuras TIC.
  - **Servicios de detección**: orientados al desarrollo de monitorización de eventos de seguridad, capacidades de detección temprana de incidentes y amenazas, y vigilancia digital.
  - **Servicios de análisis y respuesta**: orientados a mejorar el proceso de evaluación del impacto y la respuesta de incidentes, a través de un servicio de soporte especializado para la respuesta a incidentes y un servicio de soporte en la gestión de los incidentes.
  - **Servicios de diseño y operación de procesos y tecnologías del SOC**: que facilitarán la definición de los procesos y procedimientos operativos del SOC, las integraciones entre los diferentes servicios y las tecnologías soporte.
  - **Servicios de capacitación y formación en ciberseguridad**, orientados a mejorar la cualificación técnica del personal de seguridad de RTVM.
  - **Servicios de soporte a la gestión y operación del SOC,** de gobierno del SOC, orientados a la definición de cuadros de mando, métricas e indicadores, gestión centralizada de los servicios y gestión del conocimiento.

- **Servicios COMPLEMENTARIOS**:
  - **Servicios de asesoría y asistencia legal**, como apoyo en la ejecución de medidas legales por parte de RTVM en casos de incidentes graves de seguridad o acciones derivadas de obligaciones normativas y/o regulatorias.



El adjudicatario dotará, para la prestación de los mismos, el equipo humano, las capacidades técnicas, herramientas, metodologías y estructuras organizativas necesarias. En el apartado de tecnologías y herramientas propuestas para la prestación de los servicios, los licitadores deberán tener en cuenta la adecuación de las mismas a las herramientas actuales de que disponga RTVM, en caso necesario.

Con carácter general, se considerará dentro del coste de los servicios solicitados todos los gastos derivados de herramientas, desarrollos e integraciones con sistemas ya existentes o similar, propuestos por los licitadores como respuesta técnica a este pliego de prescripciones técnicas y que no estén específicamente presupuestados en la valoración económica de los servicios.

En los siguientes apartados de este pliego se detalla el alcance de cada uno de los servicios demandados.

Servicios de prevención

Se prestarán los siguientes servicios de seguridad, orientados a la prevención de incidentes de seguridad:

Servicio automatizado de análisis de vulnerabilidades

El servicio de análisis de vulnerabilidades facilitará las capacidades técnicas necesarias para el descubrimiento y análisis de vulnerabilidades de seguridad en las infraestructuras TIC, aplicaciones y servicios de RTVM.
Proporcionará una gestión completa del ciclo de vida de las vulnerabilidades, contemplando la planificación y ejecución de las actividades de identificación, el análisis de resultados, la notificación y reporte correspondiente, para su evaluación, priorización y definición de

acciones de remediación por parte de RTVM, y el seguimiento de las acciones correctivas definidas.
El servicio deberá cubrir los siguientes requisitos mínimos:

- Elaborar el inventario de activos y catalogar los mismos, permitiendo así un control de la planta instalada, las vulnerabilidades que afectan a cada activo y su configuración de seguridad**.**
- Identificar las principales fuentes de información y clasificación de vulnerabilidades en base a los activos instalados en RTVM, siguiendo las referencias de vulnerabilidades publicadas por CVE (Common Vulnerabilities and Exposures) o por el NIST (National Institute of Standards and Technology).
- Planificar y ejecutar los análisis de vulnerabilidades, tanto de infraestructura como de sitios web, según las franjas horarias y restricciones trasladadas por RTVM.
- Evaluar y validar los resultados obtenidos, en base a los activos y servicios descubiertos y vulnerabilidades detectadas.
- Explotar, de forma controlada, las vulnerabilidades detectadas, sin comprometer información sensible ni el servicio prestado, para verificar el impacto de la vulnerabilidad.
- Notificar los resultados para su seguimiento y gestión por parte de RTVM.
- Facilitar un soporte técnico experto para la mejor comprensión del impacto de las vulnerabilidades detectadas, su priorización y la definición de plan de acción por parte de RTVM.

El servicio de análisis automatizado de vulnerabilidades descrito se prestará como un servicio continuo, en base a las solicitudes de revisión de infraestructuras o sitios web que solicite RTVM.
El adjudicatario estará obligado a asegurar que las actividades derivadas de este servicio no comprometan la integridad y disponibilidad de las infraestructuras y servicios analizados.
Los licitadores propondrán en su respuesta al apartado **Tecnologías y herramientas del SOC** las herramientas de descubrimiento de activos, base de datos, catalogación, análisis de vulnerabilidades, notificación y gestión del ciclo de vida, que utilizarán para la prestación de este servicio, considerándose dentro del coste del servicio todos los gastos derivados de las mismas (licencias, mantenimientos, actualizaciones, etc.).
Para la prestación de este servicio, el adjudicatario pondrá a disposición de RTVM los recursos recogidos en el apartado **Equipo de trabajo**.

Servicio manual de análisis de vulnerabilidades o pruebas de intrusión.

El servicio manual de análisis de vulnerabilidades o pruebas de intrusión, tendrá como objetivo identificar vulnerabilidades de las aplicaciones en ejecución, desde el punto de vista de un atacante externo, analizando la lógica de negocio de cada aplicación.
Se estudiarán, como mínimo, las siguientes áreas de seguridad:

- Vulnerabilidades del sistema soporte de la aplicación y de la aplicación.
- Vulnerabilidades que permitan la ejecución de código remoto por incorrecta validación de datos.
- Vulnerabilidades relacionadas con la autenticación, autorización y gestión de sesiones.
- Vulnerabilidades derivadas de configuraciones erróneas de seguridad o inadecuada actualización de componentes.
- Vulnerabilidades derivadas de empleo de métodos criptográficos débiles.
- Vulnerabilidades derivadas de incorrecta gestión de errores y logs de eventos de la aplicación (buffer overflow).
- Vulnerabilidades derivadas de ilegitimidad de sites (CSRF).

El adjudicatario elaborará un informe de resultados en cada revisión, donde se describa el alcance, las pruebas realizadas y los resultados obtenidos, categorizados en base a niveles de riesgo e impacto para el servicio.
Los licitadores deberán indicar, en su oferta técnica, el equipo técnico de seguridad que pondrán a disposición de este servicio, así como la metodología de análisis que aplicará, áreas de seguridad a analizar y técnicas y herramientas de explotación de vulnerabilidades utilizadas.
Los análisis manuales de seguridad se realizarán habitualmente en el entorno de producción estando obligado el adjudicatario a asegurar que las actividades no comprometan la integridad de los datos objeto de revisión, la disponibilidad del servicio analizado ni otros servicios ajenos a la aplicación en revisión. De igual forma, por tratarse de aplicaciones en producción, las ventanas horarias de trabajo deberán ser acordadas entre RTVM y el adjudicatario, normalmente fuera del horario de producción, para asegurar el mínimo impacto en el servicio analizado.
Se prestarán servicios de monitorización de eventos de seguridad, vigilancia digital e identificación de amenazas, con los siguientes requisitos:

Servicio de monitorización de eventos de seguridad.

El servicio de monitorización de eventos de seguridad permitirá obtener un conocimiento centralizado del estado de la seguridad, mediante la recolección, procesamiento, explotación y correlación de los eventos o registros de log de las fuentes de información que defina RTVM.
A tal fin, el servicio deberá contemplar la ejecución de las siguientes actividades:

- Suministro, instalación y mantenimiento de un sistema de Gestión de Eventos e Información de Seguridad (SIEM –Security Information and Event Management), incluyendo todos los elementos software y hardware necesarios para la recogida, análisis y almacenamiento de eventos.
  El sistema de gestión de eventos deberá cumplir los requisitos mínimos recogidos en el **ANEXO SIEM - REQUISITOS MÍNIMOS**, de este pliego de prescripciones técnicas.

- Operación del servicio de monitorización, contemplando todas las tareas de mantenimiento y operación de la plataforma como son actualizaciones del sistema, backups, informes de servicio, integraciones de nuevas fuentes de eventos, y monitorización de la plataforma. Esta actividad, a efectos de presupuesto, se recoge como "**Mantenimiento plataforma SIEM"**.

Servicio de vigilancia digital e identificación de amenazas.

El servicio de vigilancia digital e identificación de amenazas se prestará como una solución integral dirigida a la detección temprana de posibles amenazas de seguridad.
Permitirá una valoración del impacto potencial en los servicios TIC prestados por RTVM en caso de materialización de una amenaza de seguridad, y el análisis de las alternativas posibles de mitigación y/o contramedidas de seguridad a implementar.
Se prestará con dos enfoques:

- Uno, orientado a la recopilación y evaluación de amenazas de seguridad publicadas por fuentes externas como SOC's del adjudicatario, fabricantes de tecnología TIC, proveedores de servicios, servicios de alertas tempranas de seguridad, CERTS, etc., que puedan afectar a la seguridad de los servicios, sistemas e infraestructuras TIC gestionados por RTVM.
- Otro, de monitorización de fuentes diversas de información, como redes sociales, sitios web, redes P2P, blogs, foros especializados, etc., que permita detectar:

- publicaciones accidentales o premeditadas de información de servicios TIC de RTVM, que puedan suponer un riesgo o perjuicio a su imagen,
- fugas de información sensible propiedad de RTVM,
- información sobre ataques organizados, suplantación de identidad, o actividades en general fraudulentas, relacionadas con usuarios y/o servicios de RTVM.

El servicio facilitará una gestión completa del ciclo de vida de las amenazas detectadas, contemplando desde la recopilación y almacenamiento centralizado de los datos privados y públicos obtenidos, el procesamiento inteligente de los mismos, su clasificación y evaluación, la generación de alertas e informes, hasta las propuestas para mitigación y/o eliminación de la amenaza.

Servicio de detección de incidentes - Nivel N1

El servicio de detección de incidentes de seguridad de Nivel 1 facilitará una monitorización continua de los eventos y alarmas generadas por el resto de servicios de detección, monitorización, vigilancia digital e identificación de amenazas.

Se realizarán las funciones de identificación, clasificación, categorización, nivel de peligrosidad, impacto potencial, y documentación de los eventos de seguridad, así como un primer nivel de investigación a fin de identificarlo como posible incidente de seguridad, para su análisis por el siguiente nivel de atención.

Servicios de análisis y respuesta

En el apartado de análisis y respuesta frente a incidentes y amenazas de seguridad, se demandarán los siguientes servicios:

Servicio de detección de incidentes nivel N2

El servicio de detección de incidentes de seguridad de Nivel 2 realizará las siguientes funciones:

- Confirmar los incidentes de seguridad, analizando la información recibida del Nivel 1 de detección y la información de vulnerabilidades obtenida del servicio de prevención.
- Estudiar el impacto del incidente, los activos afectados y el nivel de compromiso de los servicios.
- Proponer el plan de mitigación y remediación del incidente, en base a los procedimientos establecidos al efecto.
- Coordinar la ejecución de los planes de mitigación y remediación iniciados, hasta su finalización.
- Escalar si procede a los servicios especializados de respuesta a incidentes el caso detectado, para su evaluación y tratamiento.
- Documentar todos los casos tratados.

Servicio especializado de respuesta a incidentes

El servicio de soporte especializado de respuesta a incidentes de seguridad facilitará capacidades avanzadas de apoyo en la evaluación de incidentes de seguridad graves, la identificación de la causa raíz, su alcance, la relación de activos afectados y el impacto para el negocio, así como el análisis de contexto o análisis forense de los eventos de la red, que permita situar el incidente en el tiempo determinar los orígenes del ataque, los medios utilizados y los objetivos.
El servicio facilitará también capacidades expertas en la definición de las medidas de contención a aplicar, así como las medidas para su eliminación, recuperación del servicio y preservación de evidencias.

Este servicio se prestará con personal del adjudicatario que, bien de forma remota o *in situ*, colabore con el personal de RTVM aportando los procedimientos, procesos y herramientas necesarias en cada escenario.

Servicio de soporte a la gestión de incidentes de seguridad.

El servicio de soporte a la gestión de incidentes de seguridad facilitará capacidades avanzadas de apoyo para la coordinación de la gestión de incidentes críticos, el despliegue de las medidas de contención definidas, y la aplicación de planes de recuperación del servicio, si procede, como complemento y apoyo al equipo de respuesta a incidentes de seguridad de RTVM (CSIRT Computer Security Information Response Team o CERT – Computer Emergency Response Team).

Este servicio se prestará a demanda, con personal del adjudicatario que colabore con el personal de RTVM aportando los procedimientos, procesos y herramientas necesarias en cada escenario.

Servicio de diseño y operación de procesos y tecnologías del SOC

Dentro de este servicio se definirán e implementarán todos los procesos y procedimientos de gobierno y operativos del SOC, se definirán las arquitecturas de las diferentes soluciones para los servicios demandados y se implantarán, adaptarán y evolucionarán los servicios y las herramientas soporte correspondientes.

Serán funciones del servicio, entre otras, la identificación e integración inicial de las fuentes de eventos a monitorizar, y de las sucesivas que RTVM solicite a lo largo del contrato, el modelado de amenazas, la definición y desarrollo de los casos de uso de monitorización, y la prestación en general, de un soporte experto al resto de componentes del SOC de las tecnologías implantadas para el servicio.

Se definirá y coordinará también dentro de este servicio la implantación de todas las herramientas de gestión del SOC, teniendo en cuenta los requisitos mínimos recogidos en el apartado **Tecnologías y herramientas del SOC**, así como el diseño del portal de ciberseguridad, descrito en el apartado **Servicio de soporte a la gestión y operación del SOC**

Servicio de capacitación y formación en ciberseguridad

Los licitadores deberán incluir en su propuesta un Plan de Formación continuo, sin coste adicional, orientado a la capacitación del personal técnico de RTVM sobre los servicios de seguridad, equipamientos y herramientas de gestión puestas a disposición del contrato.
La propuesta formativa deberá contemplar, como mínimo, lo siguiente:

- Formación en análisis de vulnerabilidades TIC: orientadas a la obtención de conceptos básicos de seguridad en infraestructuras TIC, configuraciones de seguridad, seguridad en entornos web y manejo de las herramientas de análisis automatizados y manuales propuestas para el servicio.
- Formación en administración y operación del sistema de gestión de eventos: Arquitectura del sistema desplegado, funcionalidades de los componentes y administración básica de la plataforma, reglas de detección y correlación, y componentes de recolección de datos.
- Formación en análisis forense: conceptos de la informática forense, técnicas y metodologías de análisis y evidencia digital.

Además, como impulso a las acciones de divulgación y sensibilización en materia de seguridad TIC y orientado al personal técnico de RTVM, se valorará la puesta a disposición

del contrato de contenidos formativos de carácter general, en forma de píldoras formativas, cursos on-line, vídeos divulgativos, o ejecución de campañas de evaluación del grado de concienciación en seguridad.

Servicio de soporte a la gestión y operación del SOC

Como soporte a la gestión y operación del SOC, el adjudicatario del contrato deberá desarrollar y mantener un **Portal de Ciberseguridad TIC** desde el que se facilite un reporte integrado de todos los servicios puestos a disposición del contrato.
Desde el portal se facilitará un acceso integrado a las consolas de gestión de los distintos servicios, las herramientas de seguimiento de vulnerabilidades, las bases de datos de conocimiento y activos, así como a los sistemas de reporting y control del servicio propuestos, procedimientos, cuadros de mando, indicadores, sistemas de alerta, informes de trabajos y, en general, toda la información de seguimiento y control generada.
El portal facilitará una vista pública, orientada a todo el personal de RTVM, de carácter informativo y de divulgación general sobre las actividades del Centro de Operaciones de Seguridad, seguridad, y una vista privada, mediante autenticación y autorización de usuarios, para el seguimiento y control de los servicios, orientada al equipo de seguridad de RTVM.
El portal de gestión será accesible vía web desde la Intranet de RTVM.

Servicios de asesoría y asistencia legal.

Los servicios de asesoría y asistencia legal complementarán el resto de servicios solicitados, facilitando un soporte legal en todas aquellas iniciativas que RTVM deba realizar relativas a lo siguiente:

- La recuperación de información o contenidos publicados, obtenidos de forma fraudulenta y publicados en sitios web, foros o similar, detectados por los servicios de vigilancia digital.
- Asesoría en los procesos legales de respuesta a incidentes de seguridad detectados que puedan iniciarse.
- En general, en el análisis y adecuación de los procesos y procedimientos internos del SOC-MD a las obligaciones derivadas del cumplimiento de la normativa vigente.

Incorporación de otros servicios de seguridad.

La constante y rápida evolución de las amenazas de seguridad, obliga a adaptar al mismo ritmo las capacidades de prevención, detección y respuesta de las organizaciones y sus mecanismos de protección frente a ataques a la seguridad de los sistemas, servicios e infraestructuras TIC.
Por ello, hay que tener en cuenta que en el ámbito de la Ciberseguridad es prácticamente imposible, definir con absoluta precisión el alcance y límites de todos los servicios de seguridad que se puedan requerir durante el periodo de ejecución del contrato, considerando que la tecnología evoluciona y cambia día a día, los ataques se profesionalizan y las TIC están ya presentes en todos los ámbitos.
En consecuencia, se contempla la posibilidad de incorporar, durante la vigencia del contrato, servicios adicionales de seguridad orientados a la prevención, detección, análisis y respuesta de incidentes y amenazas de seguridad, que en el caso de que resulten estrictamente necesarios, se incorporarán de acuerdo con lo establecido para las modificaciones en el Pliego de Cláusulas Administrativas Particulares.

SOPORTE ESPECIALIZADO EN DISEÑO SEGURO - SDS

El objetivo del servicio será proponer, definir y diseñar controles técnicos de seguridad, nativos y complementarios, que mejoren las arquitecturas de los servicios e infraestructuras desde su diseño.
El entorno tecnológico de referencia sobre el que se desarrollarán las actividades de soporte se recoge en el **ANEXO ENTORNO TECNOLÓGICO**.
A continuación, se detallan las actividades a realizar y el equipo de trabajo requerido para la prestación del servicio.
Las actividades a desempeñar con carácter general para este servicio de soporte especializado en diseño seguro, al amparo del servicio son las siguientes:

- Mejora de la seguridad de las arquitecturas técnicas desde el diseño, mediante la definición de las políticas y controles de seguridad en cada escenario, considerando la legislación, normativa de seguridad de RTVM, buenas prácticas y referencias de arquitecturas seguras, como son las del NIST (National Institute of Standards and Technology del gobierno de EEUU), las del CCN (Centro Criptológico Nacional de España) teniendo en cuenta la arquitectura técnica implantada. Básicamente deberán trabajar en la realización de:
  - Procedimientos e instrucciones técnicas de bastionado seguro de componentes de arquitecturas técnicas.
  - Recomendaciones de soluciones y tecnologías adicionales que puedan complementar la seguridad del servicio, sistema y/o infraestructura tecnológica.
  - Guías de mejora de la seguridad de los procedimientos operativos de tecnologías de información. - Revisiones de estado de seguridad y propuesta de mejora.
- La creación de una base de datos de configuraciones de seguridad, que complemente los procesos de gestión de configuraciones existentes en RTVM.
- La definición, creación de scripts y herramientas que sean capaces de detectar y comprobar si los controles de seguridad están aplicados.
- La asistencia técnica en materia de seguridad en las fases de definición y diseño de proyectos tecnológicos y de desarrollo en el ámbito de RTVM.

OFICINA DE GOBIERNO Y DPD

Oficina Técnica de Gobierno (OTG) y DPO con el objetivo de mejorar la madurez de sus procesos relacionados con la Seguridad de la Información

Se ha identificado y valorado, como parte troncal del proyecto de Seguridad Gestionada, la necesidad de contar con servicios de alto valor relativos a la Gestión de Seguridad Lógica, más concretamente entendidos como propios de consultoría de cumplimiento normativo y seguridad: **Oficina Técnica de Gobierno.**

En este marco, y como parte del servicio de **Oficina Técnica de Gobierno**, se habrán de atender como mínimo las siguientes tareas:

- Revisión y mejora del marco normativo de seguridad.
- Revisión y gestión del plan de seguridad.
- Incorporación de acciones de mejora continua del plan de seguridad.
- Definición, creación y puesta en marcha de medidas organizativas.
- Convergencia al ENS
- Cumplimiento de la normativa ISO 270001 en dos ámbitos:
  - Técnico en lo que se refiere a los sistemas.
  - Validación jurídica.
- Servicios de Delegado de Protección de Datos (DPO)
- Auditoría de seguridad de Protección de Datos y ENS con la cadencia, al menos, que requiere la correspondiente Autoridad de Control.

- Servicios de concienciación orientado a todos los empleados.

El seguimiento y actualización del Plan de Seguridad, así como la implantación de las recomendaciones resultado de los análisis, habrá de dar como resultado la implantación de un modelo de gobierno de los servicios TI, que propicie un Sistema de Gestión Unificado de la Seguridad práctico, robusto y en continuo crecimiento. Se requiere de un servicio continuado de soporte en ésta y otras tareas de Gobierno, Riesgo y Cumplimiento, que velen por la mejora continua del proceso, atendiendo tanto aquellas medidas de carácter más técnico/tecnológico, acompañadas del soporte jurídico asociado a las mismas (según establece la **ISO 27001/02 y ENS**, para las medidas organizativas, técnicas y jurídicas dentro del enfoque de la seguridad de las TIC). Asimismo, contemplar los requisitos trasladables desde el Delegado de Protección de Datos (**DPO**) a incluir en la propuesta desde la exigencia y aplicabilidad del Reglamento General de Protección de Datos de la Unión Europea (**RGPD**), y las auditorías pertinentes -en este caso, cada dos años-.

Servicios de Concienciación

RTVM solicita un programa formal de concienciación en materia de seguridad lógica con el objetivo de capacitar a los empleados sobre las posibles amenazas y cómo evitar situaciones que puedan poner en riesgo los datos de la organización.

Los objetivos del programa de concienciación de seguridad informática son:
- Reducir la superficie de ataque de la organización
- Capacitar a los usuarios para que asuman la responsabilidad personal de proteger la información de la organización
- Hacer cumplir las políticas y procedimientos que la organización ha implementado para proteger sus datos

RTVM al menos requiere 5 campañas de concienciación, una al año y dos de ellas, como mínimo, basadas en Tabletop.
El licitador debe proponer un programa de concienciación, justificado y debe presentar el marco metodológico que seguiría de resultar adjudicatario.

ORGANIZACIÓN DEL SERVICIO

HORARIO, UBICACIÓN

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

Para el servicio de SOC:
- Servicio remoto con posibilidad de presencia local.
- Servicio técnico, funcional y de desarrollo en español.
- Horarios de servicio:24x7x365 en dinámica ordinaria.

Para el servicio SDS:
- Este servicio se prestará a demanda de RTVM en horario 8x5 de acuerdo al calendario laboral de la Comunidad de Madrid y fuera de las instalaciones de RTVM, salvo cuando puntualmente haya que realizar sesiones de trabajo que procedan realizarse presencialmente y entonces se llevarán a cabo en las dependencias de RTVM.

Para el servicio de OTG y DPD:

- Este servicio se prestará a demanda de RTVM en horario 8x5 de acuerdo al calendario laboral de la Comunidad de Madrid y fuera de las instalaciones de RTVM, salvo cuando puntualmente haya que realizar sesiones de trabajo que procedan realizarse presencialmente y entonces se llevarán a cabo en las dependencias de RTVM.

Para todos los servicios de este Lote:

- El adjudicatario 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 adjudicatario pondrá a disposición del servicio un número de teléfono, una dirección de correo y/o el acceso remoto a través de navegador a una herramienta de gestión de peticiones, con el objetivo de resolver dudas y/o incidencias y/o peticiones de cambio / evolutivos, tanto técnicas como funcionales.

MODELO OPERATIVO SOC

El modelo operativo relaciona los servicios que se prestan dentro del SOC, con las operaciones, procesos y procedimientos que las regulan, considerando las herramientas y tecnología que se requieren para su soporte. Es un modelo de Personas, Procesos y Tecnologías interrelacionadas, cuyo objetivo es prestar los servicios del SOC de forma eficaz y eficiente.

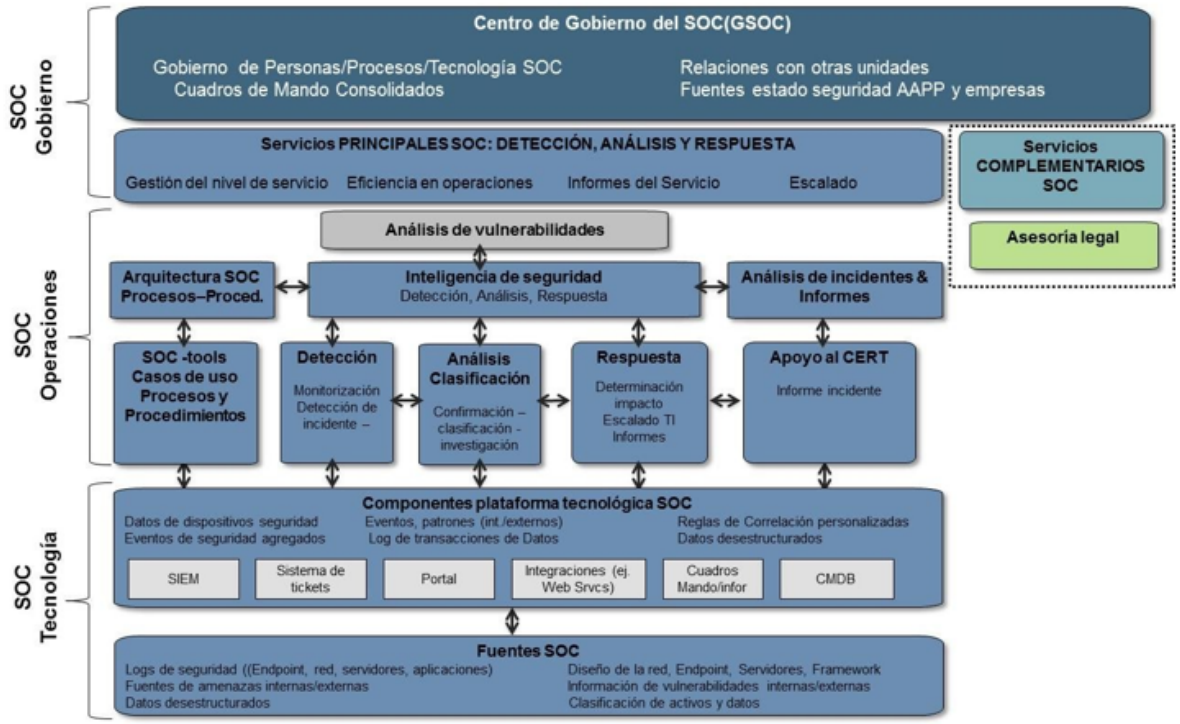
Todas estas operaciones deben de estar sujetas a la supervisión y control del centro de gobierno del SOC.

Por tanto, el modelo operativo incluye su centro de gobierno, responsable de las actividades de gobierno y estrategia de las personas, procesos y tecnologías empleadas en el SOC, de las relaciones con otras unidades y con empresas, organismos de AAPP, etc. en materia de seguridad.

En lo que respecta al modelado de operaciones y tecnologías por cada servicio, el modelo operativo deber realiza las siguientes actividades para cada servicio:

- Descripción del servicio: detallando su objetivo, alcance y modelo de servicio.
- Definición de los procesos y procedimientos asociados: se deben documentar los procesos y procedimientos operativos, detallando los requisitos del proceso, responsables, actividades y resultados. Esto incluye:
  - Procedimientos de provisión.
  - Procedimientos de operación: gestión de peticiones, consultas e incidencias.
  - Procedimientos de soporte: gestión de cambios, gestión de la configuración, gestión de la capacidad, gestión de problemas, etc.
  - Definición de los niveles de servicio: se deben especificar los diferentes indicadores de riesgo y de rendimiento asociados con cada uno de los servicios, que permita establecer niveles de acuerdo de servicio, ANS.

- Diseño de los interfaces, relaciones entre procesos, entradas salidas de información y flujos de información a integrar.
- Diseño de las herramientas y tecnologías que permitan prestar y gestionar los servicios de forma completa. La relación de estas herramientas será desarrollada en su apartado correspondiente.



MODELO ORGANIZATIVO SOC

El modelo organizativo del SOC recoge como deben organizarse los recursos para prestar los servicios de forma eficiente.

Bajo la dirección del responsable del SOC de RTVM y su equipo, el adjudicatario deberá nombrar un responsable único del servicio del SOC, Service Manager.

Este responsable de servicio del SOC, organizará los recursos humanos del SOC en seis funciones que se corresponden con los servicios principales y complementarios del SOC. Cada una de estas funciones contará con el equipo de trabajo y al frente de cada una de ellas el adjudicatario pondrá un responsable de función, con el objetivo de facilitar la comunicación con el equipo de SOC de RTVM.

Estas seis funciones son las siguientes:

- Detección, Monitorización – Nivel N1 de SOC.
- Análisis – Nivel N2 de SOC.
- Respuesta y Soporte a la Gestión de incidentes – Nivel N3 de SOC.
- Procesos & Tecnología de SOC.

- Análisis de vulnerabilidades.
- Asesoría Legal.

Dentro de este modelo organizativo el adjudicatario deberá considerar los requisitos de equipo mínimo que se indican en el apartado **Equipo de trabajo,** y los horarios, ubicación del equipo, indicados en el apartado **Horario y ubicación para la prestación del servicio**.

EQUIPO DE TRABAJO SOC

Los perfiles profesionales, sus funciones y sus requisitos de titulación, formación y experiencia requeridos son los siguientes:

Responsable del Servicio del SOC:

- Responsable del diseño, implantación y operación diaria de los servicios y equipo de trabajo del SOC. Para ello deberá:
  - Coordinar todo el proyecto y ser el responsable, en último término, de la buena marcha de los trabajos.
  - Interlocutor principal del responsable del SOC de RTVM.
  - Ejercer el mando y la responsabilidad sobre el equipo completo del SOC.
  - Realizar la planificación general de los trabajos y de las tareas asociadas.
  - Asegurar la ejecución de las operaciones diarias del SOC según los ANS establecidos.
  - Gestionar problemas e incidencias en las operaciones de seguridad que puedan comprometer el servicio y garantizar que se gestionen adecuadamente.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager,) de la organización ISACA o CISSP (Certified Information Systems Security Professional) de la organización ISC^2, y formación en gestión de proyectos y/o

gestión de servicios TI con certificaciones en ITIL, CoBIT, PRINCE2, PMP o equivalentes.

- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con diez (10) años de experiencia como responsable o gerente de SOC, o bien como jefe de proyecto y/o gerente de operaciones de seguridad TIC.

Arquitecto senior de seguridad de SOC:

- Arquitectos especialistas funcionales y técnicos en la implantación de servicios de SOC, y por consiguiente en su diseño, despliegue de herramientas, procesos y tecnologías. Para ello deberá:
  - Diseñar e implantar la plataforma centralizada de gestión de eventos de seguridad (SIEM), asegurando la integración de las fuentes de datos de eventos necesarias.
  - Automatizar la carga de logs, eventos, modelado de amenazas, etc. en el SIEM
  - Crear y probar los casos de uso de modelado de comportamientos anómalos, probables incidentes, para su implantación en el SOC.
  - Definir y divulgar los procesos y procedimientos de operación del SOC.
  - Diseñar y mantener el portal del SOC, los cuadros de mando, la CMDB y el sistema de ticketing.
  - Detectar, mitigar y/o resolver problemas e incidencias en las operaciones de seguridad que puedan comprometer el servicio y garantizar que se gestionen adecuadamente.
  - Dar soporte técnico a los responsables de las unidades técnicas y de servicios de RTVM, en relación a las integraciones de las fuentes de datos y eventos de seguridad con la plataforma de gestión de la seguridad (SIEM).
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA o OCSP (Offensive Security Certified Professional) de Offensive Security
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con diez (10) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño y operación de sistemas SIEM, arquitectura de sistemas de detección y prevención de intrusión (IDS, IPS) de host y red, arquitectura de sistemas de seguridad perimetrales, cortafuegos de nivel 4 y nivel 7, proxys de control de acceso a Internet y sondas de análisis de seguridad de red.

Técnicos de seguridad SOC DETECCIÓN nivel 1:

- Técnicos de seguridad con experiencia en la monitorización de eventos de seguridad y detección de incidentes de seguridad. Realizará las siguientes actividades:
  - Identificar, categorizar, priorizar e investigar eventos de seguridad.
  - Controlar las colas de eventos entrantes para asegurar el procedimiento de detección
  - Realizar la investigación inicial y la clasificación inicial de posibles incidentes, y escalar o cerrar eventos según corresponda.
  - Supervisar la cola del ticket SOC (o correo electrónico) para posibles informes de eventos de entidades externas y usuarios individuales.
  - Mantener registros de cambios de SOC con actividad relevante.
  - Documentar los resultados de la investigación, asegurando que los detalles relevantes se pasen al nivel 2 para el análisis del posible incidente.
  - Actualizar las herramientas de actividad del SOC según sea necesario.

  - Realizar las actividades de vigilancia digital, recopilación información e inteligencia sobre amenazas y exploits emergentes.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: Técnico Superior en Administración de Sistemas Informáticos en red, o cualquier otra titulación de formación profesional de grado superior relacionada con las tecnologías de la información y de las comunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna certificación de fabricantes de soluciones de seguridad, Cisco, Palo Alto, HP Fortify, HP ArcSight, IBM, etc.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con tres (3) o más años de experiencia demostrable en operación y mantenimiento de plataformas de gestión de seguridad SIEM, análisis de logs de seguridad y tratamiento de eventos de redes, hosts, bases de datos, y de infraestructuras de seguridad perimetral, o bien, experiencia en labores de operación de cortafuegos, proxys de acceso a Internet, sistemas IPS, IDS y sistemas antimalware de puestos y servidores.

Analistas de seguridad SOC ANÁLISIS – DETECCIÓN nivel 2:

- Analistas de seguridad con experiencia en la confirmación, clasificación y análisis de incidentes de seguridad, determinando el impacto y proponiendo plan de actuación. Realizará las siguientes actividades:
  - Confirmación del incidente a través del análisis de la información pasada por el nivel 1 del SOC.
  - Análisis en profundidad del incidente, cotejando información de fuentes de amenazas, vulnerabilidades y eventos de seguridad, considerando toda la información recogida por el nivel 1.
  - Determinar el impacto del incidente, identificando activos afectados y nivel de compromiso.
  - Hacer el primer plan de mitigación, remediación del incidente.
  - Ejecutar si procede y según los procedimientos establecidos la mitigación, remediación del incidente.
  - Mantener registros de cambios de SOC con actividad relevante.
  - Documentar los resultados de la investigación, haciendo el informe final en caso de resolución del incidente y cerrando el caso.
  - Escalar a nivel 3 en caso de incidentes que no puedan resolverse en este nivel, asegurando que los detalles relevantes se pasen al nivel 3.
  - Actualizar las herramientas de actividad del SOC según sea necesario.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: Técnico Superior en Administración de Sistemas Informáticos en red, o cualquier otra titulación de formación profesional de grado superior relacionada con las tecnologías de la información y de las comunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA deberá disponer de alguna certificación de fabricantes de soluciones de seguridad, Cisco, Palo Alto, HP Fortify, HP ArcSight, IBM, Fortinet, CheckPoint, etc.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) o más años de experiencia demostrable en administración de plataformas de gestión de seguridad SIEM, modelado de casos de uso, análisis en profundidad de logs de seguridad, detección de amenazas, detección y gestión de incidentes de seguridad, elaboración y ejecución de planes de mitigación de impacto, o bien, experiencia en labores de diseño y administración de cortafuegos, proxys de acceso a Internet, sistemas IPS, IDS y sistemas antimalware de puestos y servidores.

Especialista de seguridad SOC RESPUESTA nivel 3:

- Ingenieros expertos en seguridad TIC con experiencia en resolución o mitigación de incidentes. Realizará las siguientes actividades:

  - Resolución y/o mitigación de incidentes complejos que no puedan ser resueltos en el nivel 2.
  - Análisis en profundidad del incidente escalado, cotejando información de fuentes de amenazas, vulnerabilidades y eventos de seguridad, considerando toda la información recogida por el nivel 1 y nivel 2.
  - Realizar y/o completar el análisis de impacto del incidente, identificando activos afectados y nivel de compromiso.
  - Ejecutar si procede y según los procedimientos establecidos la mitigación, remediación del incidente.
  - Análisis de los resultados de los análisis de vulnerabilidades, de los tests de intrusión realizados a las infraestructuras tecnológicas y aplicaciones ejecutados en RTVM, con el objetivo de prevenir la materialización de incidentes de seguridad, proponiendo los planes de mitigación.
  - Informar y dar soporte al CERT según los procedimientos establecidos.
  - Mantener registros de cambios de SOC con actividad relevante.
  - Documentar los resultados de la investigación, haciendo el informe final y cerrando el caso. Actualizar las herramientas de actividad del SOC según sea necesario.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA o OCSP (Offensive Security Certified Professional) de Offensive Security.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia en correlación avanzada de eventos y logs de seguridad, análisis de incidentes complejos de seguridad, mitigación de incidentes y realización de planes de análisis de impacto, respuesta y recuperación. Experiencia en gestión de incidentes y colaboración con equipos de CERT de comunicación de incidentes. Debe de disponer de experiencia en procesos y tecnologías de análisis de vulnerabilidades y detección de amenazas, con el objetivo de prevenir la materialización de incidentes de seguridad.

Ingenieros, auditores, analistas de seguridad de vulnerabilidades:

- Especialistas con experiencia en la realización de escaneos de vulnerabilidades y test de intrusión a sistemas, BBDD, sistemas operativos, entornos virtuales, redes y aplicaciones.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA, OCSP (Offensive Security Certified Professional) de Offensive Security, o certificaciones de fabricantes de escáneres de vulnerabilidades de Nessus o Qualys.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en técnicas y herramientas de escaneos de vulnerabilidades en sistemas, aplicaciones, hosts y equipos de red, realización de análisis de resultados de escaneos, determinación de impacto y propuesta de mitigación.

Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones (a demanda):

- Expertos en ordenamiento jurídico en materias de derecho de las tecnologías de la información y de las comunicaciones, seguridad de la información y protección de datos.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado en Derecho, Licenciado en Derecho, o equivalente.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de algún postgrado relacionado con derecho de Internet, derecho de las TIC, etc.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia en asesoría legal en empresas y/o AAPP en relación a la legislación vigente en materia de seguridad de la información y protección de datos, aplicada a la protección de información, sistemas, redes e infraestructuras tecnológicas.

TECNOLOGÍAS Y HERRAMIENTAS SOC

Todos los servicios del SOC requieren de tecnología y herramientas para cumplir su cometido. Se distinguirán entre herramientas para prestar los servicios de seguridad y herramientas de gestión y soporte a la operación del SOC.
El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas del SOC y estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para RTVM.

La relación de herramientas MÍNIMAS necesarias (excluido el SIEM) son las siguientes:

- **Herramientas mínimas de prestación de servicios de seguridad del SOC:**
  - **Análisis de vulnerabilidades**: Analizadores de vulnerabilidades de hosts y red. Inspección del estado de seguridad de servicios, sistemas y tecnologías. Herramientas de descubrimiento de activos, base de datos, catalogación y gestión del ciclo de vida de las vulnerabilidades.
  - **Monitorización:** plataforma de monitorización de seguridad SIEM + sondas + integración con fuentes de amenazas externas, cuya funcionalidad es la centralización y correlación de eventos de seguridad.
  - **Vigilancia digital**: Rastreadores, analizadores, agregadores de información en Internet de amenazas y riesgos tecnológicos. Detección de amenazas, riesgos y ataques publicados en Internet contra los servicios TIC de RTVM.

- **Herramientas de gestión y soporte a la operación del SOC:**
  - Sistema integral de CMDB.
  - Sistema de monitorización de salud.
  - Sistema de gestión documental.
  - Cuadros de mando e informes.
  - Software de gestión de contenidos de portales.

EQUIPO DE TRABAJO SDS

Se requerirá el siguiente equipo mínimo de trabajo:

Arquitecto, Ingeniero de seguridad perimetral y de las comunicaciones: expertos en diseño seguro con experiencia en labores de diseño e implantación de tecnologías de seguridad perimetral y de las comunicaciones de voz y datos.

- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, Certificaciones de seguridad de Palo Alto o CheckPoint, o bien CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad perimetral de red datos, con experiencia demostrable en diseño, administración y soporte de seguridad de redes, cortafuegos, gestión de soluciones VPN, y diseño seguro de elementos de comunicaciones de nivel 2, 3 (switches, routers).
  Excepcionalmente, se admitirán perfiles con titulaciones mínimas de formación profesional de grado superior relacionadas con las tecnologías de la información y las comunicaciones, como Técnico Superior en Administración de Sistemas Informáticos, siempre que acrediten una experiencia profesional mínima de diez (10) años en los entornos requeridos para este perfil.

Arquitecto, ingeniero de seguridad de sistemas: expertos en diseño seguro de sistemas operativos de servidor UNIX y Windows, bases de datos Oracle, SQL Server y MySQL.

- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, OCSP (Offensive Security Certified Professional) de Offensive Security, certificaciones de seguridad en sistemas operativos de servidor y bases de datos.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño seguro de servidores y bases de datos.

Arquitectos de seguridad, expertos en seguridad de otras infraestructuras TIC: como pueden ser entornos web y de colaboración, puesto de trabajo ofimático, servicios en cloud, y cualquier otro que RTVM tenga en producción o esté evaluando su implantación.

- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA, OCSP (Offensive Security Certified Professional) de Offensive Security, y certificaciones de seguridad de Microsoft.
- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: debido a que este perfil es a demanda se asume que pueden ser varias personas las que pueden prestar el servicio según su tipología, servicio específico: seguridad en entornos de trabajo, entornos de colaboración, puesto de trabajo ofimático o servicios en cloud. En todo caso la persona que preste el servicio, debe disponer
  de cinco (5) años de experiencia como arquitecto de seguridad en cada servicio de seguridad requerido.

Este servicio se ofrecerá a demanda, en función de las necesidades de RTVM. En todo caso, el licitador deberá acreditar la disponibilidad de personal técnico cualificado, experto en, como mínimo, las siguientes tecnologías:

- Entornos de colaboración.
- Gestores de contenidos.
- Puesto de trabajo ofimático.
- Aplicaciones web, entornos web, y servicios CDN.

MODELO ORGANIZATIVO SDS

Bajo la dirección del responsable del servicio SDS de RTVM y su equipo, el adjudicatario deberá nombrar un Responsable del Servicio por su parte.
Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la Dirección de RTVM designe a los efectos.

El adjudicatario, a través del Responsable del Servicio, y con la periodicidad que RTVM determine, informará sobre la planificación de trabajos, el estado de ejecución y, en su caso, sobre las incidencias producidas.

Este responsable será el interlocutor único entre el adjudicatario y RTVM. Coordinará toda la prestación del servicio y será el responsable, en último término, de la buena marcha de los trabajos. Entre sus tareas principales cabe destacar las siguientes:

- Coordinar la ejecución de los trabajos.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Supervisar y controlar la calidad de las actividades desarrolladas por su equipo.
- Hacer entrega a RTVM de los documentos desarrollados por su equipo.

TECNOLOGÍAS Y HERRAMIENTAS SDS

El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas del servicio SDS, tanto de gestión como de soporte a sus actividades, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para RTVM.

MODELO OPERATIVO OTG Y DPD

RTVM ha previsto un modelo estándar, en el que se define un gobierno, se gestiona el riesgo y cumplimiento normativo, por medio del desarrollo de proyectos adaptativos, de adecuación y definición de políticas.
La Oficina Técnica de Gobierno es la encargada de la coordinación, seguimiento, control y monitorización de los diferentes proyectos o tareas que se lleven a cabo en el ámbito del resto de servicios objeto de este Lote.

- En el ámbito de la Oficina Técnica de Seguridad se contempla la Oficina de Protección de Datos y la figura de Delegado de Protección de Datos. Entre las tareas que realizarán se encuentran:
- Informar y asesorar al responsable y a los empleados que se ocupen del tratamiento, de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación

del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.

- Cooperar con la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Trabajo con proveedores, valoración y evaluación.

MODELO ORGANIZATIVO OTG Y DPD

La gestión de la seguridad lógica, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designen a las entidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito.

El modelo básico de referencia propuesto se basa en tres premisas:
1. Identifica una estructura organizativa de unidades prestadoras de los diferentes servicios de ciberseguridad;
2. Integra los procesos de gestión para la gobernanza de la seguridad lógica, con especial énfasis en los servicios de prevención proactiva que dicho marco debe contemplar;
3. Identifica los servicios aprovisionados por la cadena de suministro de Tecnologías de la Información, así como los requisitos de cumplimiento exigibles a los suministradores.

Entre las competencias de esta Oficina se incluyen la coordinación de los diferentes actores de seguridad de los órganos concernidos y el Centro de Operaciones de Ciberseguridad. Además, tendrá funciones de asesoría legal y normativa, prestando apoyo en la resolución de cuestiones de este ámbito a toda la estructura de seguridad y pudiendo asumir competencias de asesoría legal en materia de ENS, Protección de Datos y otras regulaciones del entorno de la seguridad de las TIC, la resiliencia y la privacidad.

EQUIPO DE TRABAJO OTG Y DPD

La Oficina Técnica de Gobierno lo constituirán los profesionales que, como equipo principal, sean responsables de la ejecución del trabajo, siendo por tanto necesario un equipo multidisplicinar con formación y experiencia en seguridad técnica, organizativa y legal. Deberán disponer de la cualificación, conocimiento y experiencia adecuados a la naturaleza de los trabajos, tal y como se exige en este apartado. Como apoyo al servicio, el adjudicatario deberá contar en su plantilla con un equipo adecuado que actuará como segundo nivel y tercer nivel de soporte.

El número de técnicos adscritos a cada perfil deberá ser suficiente para cubrir con solvencia las ausencias (bajas, vacaciones, etc.).

Se han previsto los siguientes perfiles:

Security Manager

- Titulación universitaria de grado superior en el ámbito de las Tecnologías de la Información, Computación, Telecomunicaciones o Industria.

- Contará con experiencia mínima de seis (6) años en actividades en gestión y coordinación de proyectos relativos a la Seguridad de los Sistemas de Información, Planes Directores de Seguridad, Oficinas Técnicas de Seguridad, Equipos de Respuesta ante ciber-incidentes, Planes Estratégicos de Seguridad de la Información, Planes de Continuidad de Negocio, etc.
- Deberá haber dirigido, al menos, dos (2) proyectos similares o análogos a los del presente contrato en los últimos cinco (5) años.
- Deberá acreditar conocimiento en metodologías de gestión de proyectos (PMI u otras), mediante certificados de formación.
- Deberá estar en posesión de, al menos, dos (2) certificaciones de seguridad de entre las siguientes: CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), CRISC (Certified in Risk and Information Security Control), CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional).

Personal adscrito a la Oficina Técnica de Seguridad de la Información:

Consultor Tecnológico

- Titulación universitaria de grado medio o superior en el ámbito de las Tecnologías de la Información, Computación, Telecomunicaciones o Industria.
- Deberá estar en posesión de, al menos, una (1) certificación de seguridad.
- Con experiencia en:
  - Consultoría tecnológica.
  - Diseño, administración y operación de herramientas de seguridad (NGF, WAF, SIEM, MDM, Antimalware, Antispam, etc.).
  - Realización de auditorías técnicas de Seguridad.
  - Administración y bastionado de equipos y sistemas operativos Windows y Linux.
  - Diseño y administración de redes y hardware de comunicaciones.
  - Programación, administración y bastionado de portales web.
  - Análisis de malware y fraude electrónico.
  - Análisis forense e ingeniería inversa
  - Seguridad en dispositivos móviles (Android e IOS).
  - Lenguajes de programación (SQL, php, Python…).

Consultoría Normativo-legal:

- Planificación de la seguridad y gestión del riesgo (metodologías, elaboración de planes directores de seguridad, etc.). Específicamente, deberá tener conocimiento y experiencia metodología MAGERIT y herramienta PILAR.
- Implantación y/ o auditoría de sistemas de gestión de la seguridad (ISO 27001 y subsiguientes, Esquema Nacional de Seguridad, etc.).
- Diseño y desarrollo de planes de continuidad de negocio.
- Diseño y desarrollo de planes de recuperación ante desastres.
- Gestión del cumplimiento normativo y legal aplicable a la seguridad de la información (RGPD y LOPDGDD, Ley de Firma electrónica, Ley PIC, Ley NIS, LSSI y otras regulaciones en materia de ciberseguridad y protección de datos).
- Elaboración de procedimientos de seguridad de la información.
- Diseño de cuadros de mando, métricas e indicadores de seguridad de la información.
- Diseño de Planes de Concienciación, Formación y capacitación en seguridad de la información para usuarios.

Delegado de Protección de Datos:

- Titulación universitaria: Licenciatura en Derecho,

- Contar con experiencia como responsable en Protección de Datos de al menos, cinco (5) años, buen nivel técnico en el sector y habilidades de comunicación, además de expertise en impartir formación a otros miembros de la compañía.

Es deseable contar con:

Formación complementaria en Protección de Datos - Certificación Bureu Veritas o similar como DPD

TECNOLOGÍAS Y HERRAMIENTAS OTG Y DPD

El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas del servicio, tanto de gestión como de soporte a sus actividades, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para RTVM.

ORGANIZACIÓN DEL CONTRATO Y MODELO DE GOBERNANZA

Para todos los lotes

Los servicios solicitados en los distintos lotes precisan de un estrecho seguimiento en su ejecución por parte de RTVM con objeto de garantizar el correcto desarrollo de los mismos y asegurar la vigencia de los acuerdos como respuesta a las necesidades cambiantes de las TIC.

Para alcanzar estos objetivos se define una estructura de seguimiento de cada uno de los lotes en dos niveles:

- Nivel estratégico, orientado a la evolución del contrato y la mejora de los servicios, que se encargará de velar porque la estrategia y objetivos de la contratación de servicios estén alineados con los de RTVM, así como de controlar y garantizar que todas las decisiones y operaciones se ajusten a dicha estrategia.
- Nivel operativo, ligado a la ejecución concreta de los servicios que se encargará de transformar las decisiones estratégicas en planes de acción y de dirigir y controlar los esfuerzos necesarios para su ejecución. En este nivel el adjudicatario se responsabiliza de la gestión, ejecución, supervisión técnica y control operativo de los servicios.

Atendiendo a la estructura señalada se establecerán Comités diferenciados a dos niveles para el control y la toma de decisiones:

- Nivel Estratégico: Comité de Seguimiento del Contrato (CSC)
- Nivel Operativo: Comité Técnico y Operativo (CTO)

Una vez iniciada la ejecución del contrato, se procederá al nombramiento de un Comité de Seguimiento del Contrato y un Comité Técnico y Operativo que incorporarán personal perteneciente a RTVM y a la empresa adjudicataria.

COMITÉ DE SEGUIMIENTO DEL CONTRATO

El Comité de Seguimiento de Contrato (CSC) podrá estar formado típicamente por personas designadas por RTVM, además del Responsable del Contrato (o responsable del servicio), y, por el adjudicatario, el Responsable Comercial o Responsable del Contrato, el

Responsable del Servicio básicamente por roles con capacidad de movilización y mando sobre todo los recursos dentro de la organización del adjudicatario.

Las funciones de este Comité serán, entre otras, las siguientes:

- A propuesta del Responsable del Contrato de RTVM, determinación y calificación sobre el grado de incumplimiento, en cada caso concreto, al objeto de aplicar la correspondiente penalización, según la forma prevista en el *Pliego de Cláusulas Administrativas Particulares*.
- La aprobación de medidas correctivas destinadas a la mejora del servicio y/o corrección de desviaciones respecto a los ANS establecidos, como resultado de la aplicación de políticas de gestión de la Calidad de los Servicios.
- La aprobación de notas técnicas de instalación o metodologías de prestación de los servicios.
- La solicitud de ampliación de recursos para la ejecución de las actividades y servicios, objeto de este contrato, a instancias del Responsable del Contrato, si se considera insuficiente el número existente para el cumplimiento de los niveles de calidad exigidos.
- La solicitud de ampliación en funcionalidad del Portal de Gestión, con respecto a los requerimientos recogidos en este Pliego.
- Las altas, modificaciones y/o bajas de productos y servicios asociados a los ítems recogidos en el Catálogo de Productos y Servicios, siempre que no afecten a los precios unitarios de adjudicación.
- La aprobación del Catálogo de Productos y Servicios, como concreción a los requerimientos del contrato y de sus posibles posteriores modificaciones.
- La presentación ejecutiva de los proyectos en curso.
- La revisión de la facturación si procede.
- En el caso que se observare la necesidad de incorporaciones al Catálogo de Productos y Servicios de nuevos elementos que supongan nuevas unidades facturables con nuevos precios unitarios, proponer la modificación de contrato necesaria.
- Cualquier otro asunto que el propio Comité considere de interés.

Cada adjudicatario presentará con la periodicidad que RTVM determine para cada LOTE, y como máximo semestralmente, su propuesta de grado de incumplimiento y ANS mensual.

El incumplimiento de este plazo tendrá las penalizaciones contempladas en el *NIVELES DE SERVICIO Y PENALIZACIONES*. RTVM revisará y cotejará con sus propias mediciones y cálculos, determinando el Responsable del Contrato de RTVM la calificación definitiva.
Las decisiones adoptadas en el seno del CSC deberán ser de mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones.

COMITÉ TÉCNICO Y OPERATIVO

El Comité Técnico y Operativo (CTO) estará formado por personal de las áreas técnicas de RTVM por los responsables del servicio que designe el adjudicatario. Su principal objetivo será el seguimiento de la implantación y explotación de los servicios.
Su principal objetivo será el seguimiento de la implantación y explotación de los servicios.

Las funciones de este Comité serán, entre otras, las siguientes:

- Seguimiento y evaluación del progreso de las tareas y plazos planificados para la implantación y prestación de los Servicios.

- Seguimiento y análisis de incidencias complejas y/o escaladas.
- Seguimiento y análisis del cumplimiento de los Niveles y Calidad del Servicio.
- Coordinación de las reuniones e informes del proyecto.
- Verificación del cumplimiento de las especificaciones técnicas y administrativas solicitadas para el servicio.
- Planificación de los trabajos programados y proyectos especiales.
- Elaboración y definición de los procedimientos de funcionamiento entre RTVM y el adjudicatario para actividades concretas de provisión, mantenimiento y operación.

El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en las cuarenta y ocho (48) horas siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva. El incumplimiento de este plazo tendrá las penalizaciones contempladas en el *NIVELES DE SERVICIO Y PENALIZACIONES*.

PLAZOS, DURACIÓN Y ETAPAS DEL SERVICIO

Con el fin de garantizar la transición ordenada desde la situación actual al nuevo contrato, que ha de asumir el adjudicatario, se ha divido la prestación del servicio en tres fases:

- Fase de Implantación del Servicio (Transición de entrada)
- Fase de Operación o Pleno Servicio
- Transición de Salida

La definición de las fases para el servicio contratado tiene por objetivo garantizar la correcta asunción y ejecución del servicio por el nuevo adjudicatario.
Cada una de las fases tiene definido un principio y un fin en la escala temporal y un conjunto de resultados e hitos que deben ser aprobados por RTVM y que se especifican en cada una de ellas.
Todos los plazos especificados en este apartado, expresados en días, se deben considerar días naturales.

FASE DE IMPLANTACIÓN (TRANSICIÓN DE ENTRADA)

La fase de implantación (Transición de Entrada) comprende desde el inicio del contrato hasta el comienzo de prestación completa del servicio por parte del nuevo adjudicatario; tendrá una **duración máxima de CINCO (5) mes**. Será responsabilidad del adjudicatario garantizar la continuidad de todos los servicios durante este periodo sin coste adicional a RTVM.

Esta fase contempla los siguientes hitos:

1. Reunión de Lanzamiento del Servicio

En esta reunión, el adjudicatario debe entregar la siguiente documentación:

- **Composición del Equipo de Trabajo propuesto**. Se verificará el grupo de profesionales propuesto que componen el equipo, los requerimientos mínimos exigidos y cualquier aspecto adicional añadido en la oferta del adjudicatario. Éste entregará toda la información que solicite RTVM para verificar el cumplimiento de la propuesta.
  En dicha reunión RTVM comprobará que el equipo propuesto consiste en el 100% de perfiles requeridos y que se corresponden exactamente, en aquéllos casos que aplique,

con los candidatos cuyos *Currículos* hayan sido aportados y aceptados previamente de conformidad con el *Pliego de Cláusulas Administrativas Particulares*. En caso de que no coincidan por una causa justificada, o que RTVM no encuentre satisfactorio alguno de los presentados en base a los requerimientos de este Pliego (experiencia, certificaciones específicas requeridas, etc.), el adjudicatario deberá proponer candidatos alternativos con curriculum similar o superior. Dado que existe un periodo de transición desde la adjudicación al pleno servicio, el adjudicatario podrá plantear a RTVM un plazo adicional para la conformación del 100% del equipo de trabajo. En ese caso, el adjudicatario planteará la nueva fecha de presentación del equipo al completo, el cual deberá estar conformado, inexcusablemente, quince (15) días antes del inicio de la Fase de pleno servicio, que se describe más adelante.

- **Planificación de implantación**. El adjudicatario deberá entregar la planificación detallada de la implantación que debe describir con detalle, al menos, las siguientes actividades:
  - Definición de la transferencia de responsabilidad en los servicios, en el que se deberá detallar qué servicios se transfieren, cómo y cuándo se transfieren, qué controles se van a realizar para verificar que cada servicio se ha asumido correctamente, responsables, fechas, etc. Asimismo, se incluirá un estudio de riesgos que deberá acompañarse de un plan de contingencia para la minimización del impacto de la toma del servicio por parte del nuevo prestatario.
  - **Especificación de las herramientas e integraciones** necesarias para la prestación y gestión del servicio.
  - Identificación de los elementos funcionales y físicos vinculados a la prestación del servicio.
  - Recopilación de la documentación de los procesos, procedimientos y tareas operacionales del servicio.
  - Transferencia del Conocimiento al nuevo adjudicatario; para ello, durante la fase de implantación, RTVM, o quien RTVM designe, participará en sesiones de transferencia de información al equipo que designe el adjudicatario. El adjudicatario es responsable de trasladar esta formación a todo el equipo prestador; para ello, el adjudicatario deberá realizar un **Plan de Formación** detallando contenidos, fechas, asistentes, pruebas a realizar para verificar el conocimiento por cada perfil del equipo, etc. **Plan de activación de las garantías, licencias y mantenimientos de fabricante.** El adjudicatario deberá presentar el plan para la activación de las garantías de fabricante establecidas, las cuales deberán estar en vigor, **el día primero del inicio del contrato**.

- Creación del **Comité de Seguimiento del Contrato (CSC) y el Comité Técnico y Operativo (CTO)**. Definición de los puntos clave a contemplar en el Plan de Implantación y en el Plan de Activación de Garantías de Fabricante según las pautas dadas por RTVM.

Cualquier incumplimiento por parte de adjudicatario supondrá una penalización según lo indicado en el apartado Niveles de Servicio y Penalizaciones de este pliego.

2. Plan de implantación.

Será responsabilidad del adjudicatario la realización de las gestiones y acuerdos de continuidad del servicio necesarios con los **actuales adjudicatarios**, a fin de minimizar el impacto del cambio.
RTVM no asumirá ningún coste adicional como consecuencia del proceso de implantación de los servicios requeridos.

La implantación de los servicios/sistemas se abordará de forma paralela según los diferentes tipos, de acuerdo con las siguientes fases:

- Elaboración por parte del adjudicatario. El adjudicatario dispondrá de un máximo de 5 días para elaborar el correspondiente plan que incluirá todos los aspectos técnicos y de explotación sobre los servicios y sistemas a implantar con el máximo detalle, en base a la propuesta presentada. En este periodo se podrán realizar reuniones a petición del adjudicatario o de RTVM para poner en común los aspectos que se consideren necesarios. Incluirá:
  - Solución técnica: solución final de diseño (arquitectura, tecnología, dimensionado, esquemas), normativas de seguridad en la implantación, plan de implantación, plan de pruebas, plan de formación, plan de emergencia, etc.
  - Solución de explotación: planes de explotación, que incluirán los procedimientos y protocolos, aplicativos, formados de datos, etc., para la provisión de los servicios asociados a la explotación.
- Aprobación por parte de RTVM. Una vez recibido RTVM dispondrá de 5 días para su análisis y elaborará sus propuestas de modificación. El adjudicatario dispondrá de 5 días adicionales para entregar el plan definitivo.
- Ejecución y puesta en marcha. Una vez entregado el plan definitivo se iniciarán los procesos de ejecución y puesta en marcha.
- Test y pruebas. El adjudicatario realizará los test necesarios de acuerdo con el plan de pruebas presentado. RTVM podrá realizar pruebas adicionales, con el apoyo del personal y medios del adjudicatario, sin ningún coste.
- Formación. El adjudicatario se responsabilizará de la formación de los usuarios y/o personal técnico de RTVM.
- Aceptación. Realizadas con éxito las pruebas y entregada toda la documentación de las instalaciones y procesos, RTVM procederá a la aceptación de las instalaciones con lo que se arrancará el inicio de la operación y explotación de los servicios y sistemas.
- La documentación, que se entregará en papel y en formato electrónico, incluirá las versiones finales con los resultados de las pruebas de test realizadas.

Para la elaboración del Plan de implantación, los licitadores tendrán en cuenta que:

- Aquellas tareas que tengan impacto en la continuidad de los servicios actuales se tendrán que llevar a cabo en ventana nocturna y/o fines de semana o festivos y teniendo en cuenta los requerimientos de los servicios críticos que RTVM determine en cada momento.

El objetivo de este Plan es asegurar que se describen, detallan y ejecutan todas las acciones necesarias para garantizar el éxito de la Transferencia y Puesta en marcha del Servicio por parte del adjudicatario sin merma de calidad respecto de la situación de partida.

Éste será entregado por el adjudicatario, para su aprobación por RTVM, **a los siete (7) días** desde la Reunión de Lanzamiento del Servicio. Si se incumple la fecha de entrega o el Plan no cubre los aspectos definidos, se penalizará según lo indicado en el apartado Niveles de Servicio y Penalizaciones de este Pliego.

La Planificación de Implantación debe describir con detalle, al menos, las siguientes actividades:

- Definición de la transferencia de responsabilidad en los servicios, en el que se deberá detallar qué servicios se transfieren, cómo y cuándo se transfieren, qué

controles se van a realizar para verificar que cada servicio se ha asumido correctamente, responsables, fechas, etc. Asimismo, se incluirá un estudio de riesgos que deberá acompañarse de un plan de contingencia para la minimización del impacto de la toma del servicio por parte del nuevo prestatario.

- **Especificación de las herramientas e integraciones** necesarias para la prestación y gestión del servicio.
- Identificación de los elementos funcionales y físicos vinculados a la prestación del servicio.
- Recopilación de la documentación de los procesos, procedimientos y tareas operacionales del servicio.
- Transferencia del Conocimiento al nuevo adjudicatario; para ello, durante la fase de implantación del Contrato, Madrid Digital, o quien Madrid Digital designe, formará a los recursos del adjudicatario desplazados en sus dependencias o en las dependencias de Madrid Digital junto con el Coordinador del Centro de Gestión y Monitorización y a los formadores que el adjudicatario designe, en lo necesario para prestar el servicio. El adjudicatario es responsable de trasladar esta formación a todo el equipo prestador; para ello, el adjudicatario deberá realizar un **Plan de Formación** detallando contenidos, fechas, asistentes, pruebas a realizar para verificar el conocimiento por cada perfil del equipo, etc. El adjudicatario, si Madrid Digital lo considera necesario, dedicará esfuerzos a completar la documentación de los servicios que no estén adecuadamente documentados. Se entregará una propuesta identificando la documentación a modificar, planificación, personal que lo realiza, etc.; esta propuesta formará parte del **Plan de Gestión del Conocimiento**, el cual deberá ser entregado junto con el Plan de Formación. Madrid Digital validará el Plan y la documentación generada y el adjudicatario la publicará en el repositorio que Madrid Digital determine.

3. Ejecución de la Implantación

Se deberá garantizar la ejecución exitosa de las tareas definidas en la planificación de implantación, en particular:

- Transferencia de todo el conocimiento al adjudicatario. La transferencia hará hincapié en el desarrollo y ejecución de todas las actividades relacionadas con la implantación y puesta en marcha del Servicio.
- Validación de la infraestructura asociada a la futura prestación del servicio, incluidas las instalaciones del adjudicatario.
- Garantizar el funcionamiento del plan de contingencia de la puesta en marcha del Servicio.
- Asegurar que están descritas las tareas de transferencia de actividad en el momento de recibir el servicio por parte del adjudicatario.

Durante esta etapa, RTVM trabajará en estrecha relación con todos los proveedores, entrante y saliente, con el fin de dar consistencia y conformidad a lo descrito.
En caso de necesidad, el Comité Técnico y Operativo podrá proponer la modificación de alcance, fechas, duración y contenidos de cada una de las etapas y fases referidas en el presente documento. Dicha propuesta deberá ser ratificada por el Comité de Seguimiento de Contrato.
Conforme se vaya haciendo la transferencia de cada uno de los servicios, deberá hacerse entrega de un documento donde el adjudicatario indique el servicio traspasado, con las tareas y fechas ejecutadas, responsables que han participado y riesgos y propuestas de mejora identificadas. El cumplimiento de cada uno de estos hitos deberá quedar documentado y aprobado formalmente por RTVM.

Los conjuntos de estos documentos conformarán el **documento de Puesta en Marcha del Servicio**. Su entregará en su versión definitiva se realizará como máximo a los **6 meses** del inicio del contrato.

Los **entregables** de la Fase de Implantación se relacionan a continuación:

- Acta de inicio de la Fase de Transición.
- Plan de Transición.
- Roles y Responsabilidades en el Servicio. Composición del equipo de trabajo y centro de gestión y monitorización propuesto. Modelo de relación.
- Equipo Base: identificación de cada miembro y su función. Modelo de relación.
- Plan de Traslado.
- Plan de Contingencia.
- Plan de Formación.
- Documentación de los servicios documentados en la Fase de Implantación.
- Plan de Gestión del Conocimiento.
- Puesta en marcha del servicio.
- Informe del estado de los contratos de mantenimiento con fabricante derivado de la ejecución del Plan de garantías de fabricante.
- Documento de Cierre de la Fase de Implantación.

Finalizada la Fase de Implantación, el Comité de Seguimiento del Contrato se reunirá para evaluar los entregables y resultados de dicha fase.

En caso de que la entrega no se haga en la fecha estipulada o no contemple los aspectos pactados, se penalizará según el apartado Niveles de Servicio y Penalizaciones del presente Pliego.

Una vez completada la fase de Implantación será responsabilidad exclusiva del adjudicatario la Prestación del Servicio.

FASE DE PLENO SERVICIO

La etapa de Pleno Servicio tendrá lugar a la finalización de la Fase de Implantación, es decir, como máximo **comienza a los 5 meses del inicio del contrato**. La duración de esta etapa llega hasta la finalización del contrato.
El adjudicatario asumirá la responsabilidad de la prestación integral del servicio ajustándose a los requisitos de calidad exigidos por RTVM.

FASE DE TRANSICIÓN DE SALIDA

Durante el periodo final de vigencia del contrato, RTVM podrá establecer un periodo transitorio de ejecución en condiciones especiales, de modo que se garantice la prestación del servicio de forma ininterrumpida, comprometiéndose el adjudicatario a colaborar, en su caso, con el o los nuevos adjudicatarios en aquellas actividades necesarias, encaminadas a la planificación y ejecución del cambio y la transferencia de conocimiento.

Los servicios descritos en cada lote en "situación actual" deberán tener continuidad desde el primer día del plazo de implantación, fecha en la que empieza a proveer los servicios el adjudicatario de cada lote, hasta finalizada la migración a los nuevos servicios. Será responsabilidad de cada adjudicatario llegar a los acuerdos pertinentes con los proveedores anteriores de los servicios para lograr esta continuidad, o tener disponible su servicio desde el primer día del plazo de implantación

Si fuera necesario para garantizar la continuidad del servicio, el operador saliente tendrá obligación de llegar a acuerdo con en el operador entrante en las mismas condiciones técnicas y económicas que tiene con RTVM.

Al objeto de garantizar una adecuada transición de salida, el adjudicatario, durante ese periodo de transición establecido deberá **seguir garantizando la completa y correcta operatividad de todos los servicios prestados** al amparo del contrato, comprometiéndose además a facilitar el traspaso de conocimiento al prestador entrante.

El adjudicatario se compromete a ejecutar durante los tres últimos meses del contrato el Plan de Transición de Salida que implicará, entre otras cosas:

- Transmisión del conocimiento al nuevo prestador del servicio (y/o a la propia RTVM) de cara a garantizar la prestación futura del servicio.
- Compromiso para poner los medios que minimicen el impacto en el servicio debido a las actividades de esta fase.
- Entrega a RTVM de la totalidad de herramientas, configuraciones y actualizaciones realizadas durante la prestación del contrato. Esto incluirá la documentación actualizada de soporte (documentación de diseño, programas, manuales, etc.).
- Entrega de todos los datos que obren en su poder relativos a la prestación del servicio.
- Entrega de toda la documentación asociada a la formación impartida durante la ejecución del contrato.
- Cualquier otra información requerida por RTVM.

Una vez finalizada la Etapa de Pleno Servicio, se reunirá el Comité de Seguimiento del Contrato para evaluar los entregables y resultados, dando por finalizados los servicios y verificando el correcto traspaso al nuevo prestador.

La Fase de Transición de Salida como tal tendrá una duración mínima de tres (3) meses.

Esta fase convive con la Fase de Pleno Servicio.

Los **entregables** de la Fase de Transición de Salida se relacionan a continuación:

- Documento de Cierre de la Fase de Transición de Salida.
- Actualización del Plan de Gestión del Conocimiento.
- Actualización del Plan de Formación

En caso de que la entrega no se haga en la fecha estipulada o no contemple los aspectos pactados, se penalizará según el apartado Niveles de Servicio y Penalizaciones del presente Pliego.

GARANTÍA: PLAZOS Y CONDICIONES

Para cada uno de los lotes se establece un plazo de garantía de **seis meses,** cuyo cómputo se iniciará desde la fecha de finalización del contrato.

Hasta que no tenga lugar la finalización del periodo de garantía, el adjudicatario responderá de la correcta realización de los trabajos contratados, de los equipamientos instalados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de RTVM los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o

recepciones parciales, e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

NIVELES DE SERVICIO Y PENALIZACIONES

Los acuerdos de nivel de servicio (en adelante ANS) constituirán el mecanismo cuantitativo y cualitativo básico de seguimiento y control de la calidad de los servicios, sin que ello suponga perjuicio alguno en el establecimiento de otros mecanismos de control periódicos o extraordinarios con el objetivo de asegurar que el compromiso de calidad se cumpla en la práctica.

A continuación, se exponen los parámetros de control que forman parte de los ANS, con su definición y el umbral de cada parámetro, al que los licitadores se comprometen por el hecho de presentar la oferta, ya que constituye un requisito mínimo del servicio.

En todos los casos en los que el cumplimiento de los acuerdos de nivel de servicio dependa de terceros suministradores, el adjudicatario será el responsable ante RTVM del cumplimiento de los acuerdos establecidos, no siendo motivo de exención de esta responsabilidad el posible incumplimiento por parte de terceros de los acuerdos de nivel de servicio que el adjudicatario haya contraído con los citados terceros.

Los activos, ubicaciones y servicios se enumeran en este pliego, aunque de cara a los ANS se consideran incluidos los cambios en los mismos que se implanten en el marco del presente contrato, y que sean manifestados expresamente por RTVM a lo largo de su ciclo de vida.

LOTE 1: SERVICIOS DE VOZ FIJA Y VOZ Y DATOS MÓVILES

El adjudicatario se compromete como mínimo a mantener los siguientes niveles de servicio y prestaciones, corriendo de su cuenta toda adecuación y actuación sobre los sistemas de comunicaciones destinadas a cumplir estos requisitos.

Incidencias y Peticiones:

Para cualquier tipo de incidencia en los servicios, el adjudicatario debe entregar al personal responsable de RTVM, un informe detallado de la incidencia/avería/gestión de cambios, etc. en un plazo no superior a 24 horas.

En todos los casos se entiende:

- Por tiempo de respuesta 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.

El horario de atención será de 24 horas x 365 días al año.
El tiempo de respuesta/el tiempo de resolución ante incidencias será:

Masivas:
- dentro del horario laboral: 30 minutos/ 2 horas.
  - 95% de los casos.
- fuera del horario laboral: 30 minutos / 6 horas.
  - 95% de los casos.

Individuales:
- Antes de finalizar el siguiente día laborable al de presentación de la reclamación.
  - 95 % de los casos.

Usuarios clave:
- Tiempo de respuesta/resolución 30 minutos/1 hora.

Disponibilidad:

En fase de pleno servicio:
Se define como el porcentaje de tiempo al mes en el que los servicios están disponibles, calculándose de la siguiente forma:

$$Disponibilidad = ((T_{tot} - T_{indisponibilidad}) / T_{tot)}) * 100\ (\%)$$

Dónde:

- D = disponibilidad
- T_{tot} = tiempo total del periodo considerado.
- T_{nodisp} = tiempo de no disponibilidad del servicio dentro del intervalo T_{tot} considerado.
- No se computarán los tiempos de mantenimiento programado debidamente comunicados y autorizados por RTVM dentro del plazo fijado.

El SLA objetivo relativo a la disponibilidad del servicio de Telefonía será de **99,9%.**

Tipo de SLA	SLA	Valor	% Penalización
Implantación del Servicio	100% Equipo de trabajo conformado	Menos de 15 días naturales de la fecha máxima de inicio de la fase de pleno servicio	10% por cada día de retraso con un máximo de 1 mensualidad
	Entrega Plan de Implantación	Más de 7 días desde naturales desde la Reunión de Lanzamiento del Servicio	10% por cada día de retraso con un máximo de 1 mensualidad
	Entrega Documentación definitiva generada en fase de implantación del servicio	Más de 1 mes desde la finalización de la fase de implantación del servicio	3% por cada día de retraso con un máximo de 1 mensualidad
	Desviación en la implantación de los servicios del LOTE	En el caso de incumplimiento del tiempo de implantación, se aplicará la siguiente penalización: Por cada 7 días naturales de desviación: 5 %	5% cada 7 días naturales con el máximo de 1 mensualidad
Disponibilidad Servicio	Disponibilidad de servicio	<0,3%	3%
		>0,3% y <1%	6%
		> 1%	12%
Gestión de Incidencias	Tiempo de respuesta en todos los casos <30 minutos	>30	2%
	Averías Masivas (Será menor de 2 horas en el 95% de los casos)	> 95 %	2% por cada hora de retraso con un máximo de un 10% de una mensualidad del servicio afectado
	Averías Individuales (Será menor de 24 horas en el 95% de los casos)	> 95 %	2% por cada hora de retraso con un máximo de un 10% de una mensualidad del servicio afectado
	Averías Usuarios Clave	> 1 h	1% por cada hora de retraso con un máximo de un 10% de una mensualidad del servicio afectado
	Informe de la incidencia	>24 h	5%
Gestión de peticiones	Provisión de nuevos Servicios o Terminales Usuarios	> 48 horas	50 € por día de retraso
Transición de Salida	Entregables disponibles en la fecha estipulada o no contemple los aspectos pactados.	No Cumplimiento	10% por cada semana de retraso

Servicio Gestionado:

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:

Gobierno Indicador de servicio	Valor objetivo	Porcentaje de cumplimiento mínimo	Penalización - % importe facturación mensual
Reunión de Seguimiento	<10º día del mes	100%	2%
Entrega de Informes	<5º día del mes	100%	2%
Documentación en fase de pleno servicio: guías, procedimientos etc.	0	100%	2%
Incidencias generadas por el servicio	0	100%	2%
Reaperturas de solicitudes cerradas	0	100%	2%
Valoración semestral de calidad	Mejora continua	100%	2%

Observaciones:

- Los valores están expresados en períodos laborables.
- La periodicidad se considera mensual.
- 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.
- Valoración semestral de la calidad del servicio con los usuarios clave, proceso que permita medir el porcentaje (%) de mejora del servicio y a la eficiencia del mismo.

- En la reunión de arranque del servicio, se consensuarán algunos aspectos cualitativos con el objetivo de cuantificar los SLAs de manera objetiva.

Los SLAs propuestos tendrán una vigencia no superior a 7 meses tras la finalización del plan de implementación. Con dicha periodicidad, dentro de los **planes de mejora continua** que debe regir el servicio, se valorarán, conjuntamente, los indicadores y los umbrales de servicio comprometidos, estableciéndose nuevos objetivos de mejora y, en consecuencia, se podrían incluir o retirar SLAs. En el caso de incorporar nuevos SLAs se consensuará el esquema de penalización correspondiente que, aplicará, en caso de no cumplimiento.

Las 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 las penalizaciones se realizará mensualmente y en el informe de cierre del servicio.

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:

Nº SLA incumplidos	Penalización - % importe facturación mensual
Menos de 3 SLA	2% por SLAs/mes
Entre 3 y 5 SLA	5% por SLA/mes
Más de 5 SLA	8% SLA /mes

Esta penalización no se aplica de forma escalonada, sino para todos los SLA.

El % de importe de facturación mensual correspondiente a penalizaciones no superará el 50% del importe total de facturación mensual.

El incumplimiento prolongado durante más de 3 meses de dos o más niveles de servicio (SLA) podrá ser causa de rescisión del contrato.

LOTE 2: SERVICIOS DE INTERNET, WAN, LAN

A continuación, se describen los SLA para los cuales RTVM considera necesario realizar un seguimiento mensual:

Incidencias y Peticiones:

Para cualquier tipo de incidencia en los servicios, el adjudicatario debe entregar al personal responsable de RTVM, un informe detallado de la incidencia/avería/gestión de cambios, etc. en un plazo no superior a 24 horas.

En todos los casos se entiende:

- Por tiempo de respuesta 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.

El horario de atención será de 24 horas x 365 días al año.

El tiempo de respuesta/resolución ante incidencias será:

Masivas:

- Reclamaciones dentro del horario laboral: 30 minutos/ 2 horas.

- 95% de los casos.

- Reclamaciones fuera del horario laboral: 30 minutos / 6 horas.
  - 95% de los casos.

Individuales:

- Antes de finalizar el siguiente día laborable al de presentación de la reclamación.
  - 95 % de los casos.

Disponibilidad:

En fase de pleno servicio:
Se define como el porcentaje de tiempo al mes en el que los servicios están disponibles, calculándose de la siguiente forma:

$$Disponibilidad = ((T_{tot} - T_{indisponibilidad}) / T_{tot)}) * 100\ (\%)$$

Dónde:

- D = disponibilidad
- T_{tot} = tiempo total del periodo considerado.
- T_{nodisp} = tiempo de no disponibilidad del servicio dentro del intervalo T_{tot} considerado.
- No se computarán los tiempos de mantenimiento programado debidamente comunicados y autorizados por RTVM dentro del plazo fijado.

El SLA objetivo relativo a la disponibilidad del servicio de Telefonía será de **99,9%**

Tiempo medio de configuración de nuevos servicios:

Se define como el plazo transcurrido desde la solicitud de nueva configuración de servicio o modificación de un servicio existente hasta la entrega del servicio por parte del proveedor. Este cálculo se realizará de forma mensual.
El SLA objetivo relativo al tiempo medio de configuración de servicios será de **24 horas.**

Mantenimiento Preventivo:

El adjudicatario realizará el mantenimiento preventivo de acuerdo a la cadencia establecida en dinámica ordinaria y excepcionalmente, como consecuencia de incidencias o d intervenciones programadas.

El cumplimiento de este indicador será del 100% si se realizan todos los mantenimientos en tiempo y forma durante el mes objeto del seguimiento.
El SLA objetivo relativo al mantenimiento preventivo será del **98%**.

Configuración y Actualizaciones:

El adjudicatario realizará las tareas relativas a cambios de configuración y actualizaciones de parches.
El cumplimiento de este indicador será del 100% si se realizan en tiempo y forma durante el mes objeto del seguimiento de acuerdo a la política consensuada con RTVM.
El SLA objetivo relativo al mantenimiento preventivo será del **98%.**
Estas acciones se realizarán al menos una vez al año siempre que no se justifiquen como consecuencia de incidencias.

Tipo de SLA	SLA	Valor	% Penalización
Implantación del Servicio	100% Equipo de trabajo conformado	Menos de 15 días naturales de la fecha máxima de inicio de la fase de pleno servicio	10% por cada día de retraso con un máximo de 1 mensualidad
	Entrega Plan de Implantación	Más de 7 días desde naturales desde la Reunión de Lanzamiento del Servicio	10% por cada día de retraso con un máximo de 1 mensualidad
	Entrega Documentación definitiva generada en fase de implantación del servicio	Más de 1 mes desde la finalización de la fase de implantación del servicio	3% por cada día de retraso con un máximo de 1 mensualidad
	Desviación en la implantación de los servicios del LOTE	En el caso de incumplimiento del tiempo de implantación, se aplicará la siguiente penalización: Por cada 7 días naturales de desviación : 5 %	5% cada 7 días naturales con un máximo de 1 mensualidad
Disponibilidad Servicio	Disponibilidad de servicio	<0,3%	3%
		>0,3% y <1%	6%
		> 1%	12%
Gestión de Incidencias	Tiempo de respuesta en todos los casos <30 minutos	>30	2%
	Averías Masivas (Será menor de 2 horas en el 95% de los casos)	> 95 %	2% por cada hora de retraso con un máximo de 10% de una mensualidad del servicio afectado
	Averías Individuales (Será menor de 24 horas en el 95% de los casos)	> 95 %	2% por cada hora de retraso con un máximo de 10% de una mensualidad del servicio afectado
	Averías Usuarios Clave	> 1 h	1% por cada hora de retraso con un máximo de 10% de una mensualidad del servicio afectado
	Informe de la incidencia	>24 h	5%
Gestión de peticiones	Provisión de nuevos Servicios (a excepción de servicios que impliquen suministro/obras)	> 24 horas	0,5% por cada hora de desviación
Pérdida de paquetes	Valor de pérdida de paquetes se encuentra por debajo de un valor máximo	<=0,7%	2% con un máximo de 10% de una mensualidad del servicio afectado

Tipo de SLA	SLA	Valor	% Penalización
Retardo de Tránsito en RED IP	El retardo en red IP es el tiempo de transmisión medio en milisegundos entre los nodos de la red. Se considera tiempo de transmisión, el tiempo de ida y vuelta de un paquete de prueba	25 ms	2% con un máximo de 10% de una mensualidad del servicio afectado
Jitter en RED IPP	El Jitter en RED IP se define como la diferencia de retardo entre un paquete y el siguiente en la transmisión de la comunicación.	2 ms	2% con un máximo de 10% de una mensualidad del servicio afectado
Mantenimiento Preventivo	Cumplimiento de calendario de mantenimiento preventivo (semanal en dinámica ordinaria y cuando se programe como consecuencia de incidencias/intervenciones programadas)	>98%	2% con un máximo de 10% de una mensualidad del servicio afectado
Configuración Actualizaciones Parches.	% Cumplimiento política actualización parches. (De manera reactiva cuando se programe de manera proactiva al menos 1 vez al año)	>98 %	2%
Transición de Salida	Entregables disponibles en la fecha estipulada o no contemple los aspectos pactados.	No Cumplimiento	10% por cada semana de retraso
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	2%
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	2%

Servicio Gestionado:

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:

Gobierno Indicador de servicio	Valor objetivo	Porcentaje de cumplimiento mínimo	Penalización - % importe facturación mensual
Reunión de Seguimiento	<10º día del mes	100%	2%

Entrega de Informes	<5º día del mes	100%	2%
Documentación en fase de pleno servicio: guías, procedimientos etc.	0	100%	2%
Incidencias generadas por el servicio	0	100%	2%
Reaperturas de solicitudes cerradas	0	100%	2%
Valoración semestral de calidad	Mejora continua	100%	2%

Observaciones:

- Los valores están expresados en períodos laborables.
- La periodicidad se considera mensual.
- 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.
- Valoración semestral de la calidad del servicio con los usuarios clave, proceso que permita medir el porcentaje (%) de mejora del servicio y a la eficiencia del mismo.

- En la reunión de arranque del servicio, se consensuarán algunos aspectos cualitativos con el objetivo de cuantificar los SLAs de manera objetiva.

Los SLAs propuestos tendrán una vigencia no superior a 7 meses tras la finalización del plan de implementación. Con dicha periodicidad, dentro de los **planes de mejora continua** que debe regir el servicio, se valorarán, conjuntamente, los indicadores y los umbrales de servicio comprometidos, estableciéndose nuevos objetivos de mejora y, en consecuencia, se podrían incluir o retirar SLAs. En el caso de incorporar nuevos SLAs se consensuará el esquema de penalización correspondiente que, aplicará, en caso de no cumplimiento.

Las 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 las penalizaciones se realizará mensualmente y en el informe de cierre del servicio.

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:

Nº SLA incumplidos	Penalización - % importe facturación mensual
Menos de 3 SLA	2% por SLAs/mes
Entre 3 y 5 SLA	5% por SLA/mes
Más de 5 SLA	8% SLA /mes

Esta penalización no se aplica de forma escalonada, sino para todos los SLA.

El % de importe de facturación mensual correspondiente a penalizaciones no superará el 50% del importe total de facturación mensual.

El incumplimiento prolongado durante más de 3 meses de dos o más niveles de servicio (SLA) podrá ser causa de rescisión del contrato.

LOTE 3: SERVICIOS SEGURIDAD LÓGICA

CENTRO DE OPERACIONES DE SEGURIDAD – SOC

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Servicio automatizado de análisis de vulnerabilidades	Implantación del servicio	T. Máximo = 30 días naturales	2%
Servicio manual de análisis de vulnerabilidades	Implantación del servicio	T. Máximo = 30 días naturales	2%
Servicio de monitorización de eventos	Implantación del servicio	T. Máximo = 90 días naturales	2%
	Disponibilidad de la plataforma de monitorización y sus elementos	Disponibilidad ≥ 95%	2%
	Tiempo de respuesta ante una incidencia del sistema	T. Máximo = 1 hora	
	Tiempo de resolución ante una incidencia en el sistema	T. Máximo = 48 horas	
	Incorporación de nuevas fuentes de eventos de seguridad	T. Máximo = 30 días naturales	2%
Servicio de detección de amenazas y vigilancia digital	Implantación del servicio	T. Máximo = 60 días naturales	2%
Servicio de detección de incidentes Nivel 1 y Nivel 2	Implantación del servicio	T. Máximo = 60 días naturales	2%
	Tiempo de notificación de actividades sospechosas desde su detección	T. Máximo ≤ 30 minutos	2%
	Tiempo de emisión de dictamen sobre actividad sospechosa detectada y acciones a realizar	T. Máximo ≤ 90 minutos	2%
	Eficacia de la detección	Nº Eventos sospechosos no descubiertos ≤ 0	1.000 € por cada evento sospechoso no descubierto
Servicio especializado de respuesta a incidentes	Implantación del servicio	T. Máximo = 15 días naturales	2%
	Tiempo de entrega de informes de impacto	T. Máximo = 24 horas	2%

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Servicio de soporte a la gestión de incidentes de seguridad	Implantación del servicio	T. Máximo = 15 días naturales	2%
	Tiempo de asignación de recursos desde solicitud	T. Máximo = 4 horas	2%
Servicio de diseño y operación de procesos y tecnologías del SOC	Implantación del servicio	T. Máximo = 15 días naturales	2%
Servicio de soporte a la gestión y operación del SOC	Implantación del servicio	T. Máximo = 5 meses	2%
	Disponibilidad del portal	Disponibilidad ≥ 95%	2%
Servicio de asesoría y asistencia legal	Implantación del servicio	T. Máximo = 15 días naturales	2%
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	2%
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	2%

Para todos aquellos ANS asociados al cálculo de disponibilidad, ésta se calculará, por periodos de 1 mes aplicando la siguiente fórmula:

$$Disponibilidad = ((T_{tot} - T_{indisponibilidad}) / T_{tot)}) * 100\ (\%)$$

Dónde:

- D = disponibilidad
- T_{tot} = tiempo total del periodo considerado.
- T_{nodisp} = tiempo de no disponibilidad del servicio dentro del intervalo T_{tot} considerado.
- No se computarán los tiempos de mantenimiento programado debidamente comunicados y autorizados por RTVM dentro del plazo fijado.

SOPORTE ESPECIALIZADO EN DISEÑO SEGURO – SDS

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	2%
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	2%

OFICINA TÉCNICA DE SEGURIDAD (OTG) Y DPD

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	2%
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	2%
Auditorías	Cadencia exigida por Autoridad de Control(APDE, ENS)	100%	2%

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

Servicio Gestionado:

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:

Gobierno Indicador de servicio	Valor objetivo	Porcentaje de cumplimiento mínimo	Penalización - % importe facturación mensual
Reunión de Seguimiento	<10º día del mes	100%	2%
Entrega de Informes	<5º día del mes	100%	2%
Documentación en fase de pleno servicio: guías, procedimientos etc.	0	100%	2%
Incidencias generadas por el servicio	0	100%	2%
Reaperturas de solicitudes cerradas	0	100%	2%
Valoración semestral de calidad	Mejora continua	100%	2%

Observaciones:

- Los valores están expresados en períodos laborables.
- La periodicidad se considera mensual.
- 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.
- Valoración semestral de la calidad del servicio con los usuarios clave, proceso que permita medir el porcentaje (%) de mejora del servicio y a la eficiencia del mismo.

- En la reunión de arranque del servicio, se consensuarán algunos aspectos cualitativos con el objetivo de cuantificar los SLAs de manera objetiva.

Los SLAs propuestos tendrán una vigencia no superior a 7 meses tras la finalización del plan de implementación. Con dicha periodicidad, dentro de los **planes de mejora continua** que debe regir el servicio, se valorarán, conjuntamente, los indicadores y los umbrales de servicio comprometidos, estableciéndose nuevos objetivos de mejora y, en consecuencia, se podrían incluir o retirar SLAs. En el caso de incorporar nuevos SLAs se consensuará el esquema de penalización correspondiente que, aplicará, en caso de no cumplimiento.

Las 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 las penalizaciones se realizará mensualmente y en el informe de cierre del servicio.

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:

Nº SLA incumplidos	Penalización - % importe facturación mensual
Menos de 3 SLA	2% por SLAs/mes
Entre 3 y 5 SLA	5% por SLA/mes
Más de 5 SLA	8% SLA /mes

Esta penalización no se aplica de forma escalonada, sino para todos los SLA.
El % de importe de facturación mensual correspondiente a penalizaciones no superará el 50% del importe total de facturación mensual.

El incumplimiento prolongado durante más de 3 meses de dos o más niveles de servicio (SLA) podrá ser causa de rescisión del contrato.

CONTENIDO DE LAS OFERTAS TÉCNICAS

En este capítulo se describe la **estructura y el contenido de la documentación** que debe contener la propuesta técnica que las empresas licitadoras deben presentar y que se incluirá en el ***Sobre B*** de cada lote.

Dentro de este sobre no se deberá incluir ninguna información sobre precios o criterios cualitativos evaluables por fórmulas, la cual deberá entregarse exclusivamente en el ***Sobre C*** según se especifica en el Pliego de Cláusulas Administrativas.
Resulta obligatorio, para facilitar la valoración de las ofertas, que la documentación presentada en el ***Sobre B***, se ajuste al índice que se especifica a continuación y específicamente se señalicen los aspectos implicados en los criterios cualitativos cuya cuantificación depende de un juicio de valor. Los licitadores podrán incluir documentación adicional en anexos si lo consideran necesario.

Adicionalmente, junto a la documentación anteriormente citada, los licitadores adjuntarán un resumen ejecutivo en el que, de forma esquemática y comprensible, recojan el contenido técnico de ese sobre.

En todo caso, cada licitador deberá ajustarse especialmente a lo indicado en este punto, y circunscribir su propuesta exclusivamente a lo demandado en el pliego, separando claramente en la documentación que entregue lo aplicable íntegramente como respuesta tecnológica, evaluable, de la información sobre servicios o productos comerciales que pueda tener en su catálogo comercial, no evaluable.

Las propuestas técnicas presentadas por cada licitador deberán justificar el cumplimiento de todos los requisitos solicitados en este Pliego de Prescripciones Técnicas, no teniéndose en cuenta aquellas ofertas que no cumplan dichos requisitos.

LOTE 1: SERVICIOS DE VOZ FIJA, MÓVIL Y DATOS MÓVILES

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 50 páginas**, incluidos los anexos, ni contener referencias a documentos externos o anexos no incluidos cuando éstos sean puntos clave en la valoración de la propuesta.

Resumen ejecutivo
Definirá los objetivos y el alcance, así como los aspectos relevantes de la oferta y del licitador. El número máximo de páginas previsto para este apartado es de ocho (8) páginas.

Solución técnica propuesta para los servicios requeridos.
Los licitadores propondrán el modelo de servicio propuesto para dar cobertura al objeto del contrato:

- Terminales propuestos
- Solución técnica aportada para el Portal de Gestión
- Solución y accesibilidad de la herramienta de Autoprovisión y Autogestión para los usuarios
- Herramienta de control de llamadas y medidas de uso
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación.
- Oficina Técnica

La solución propuesta para cada servicio deberá contener la configuración de las infraestructuras y sistemas soporte, las especificaciones técnicas básicas de todos los elementos que lo componen, y las características de cada uno de ellos, de modo que cumplan los requerimientos descritos en el presente pliego.

Planes operativos
En este apartado, los licitadores presentarán los planes operativos propuestos para la prestación de los servicios requeridos, con detalle de todas las tareas y actividades implicadas, indicando los plazos previstos de cada una de ellas, los recursos materiales y humanos necesarios por parte del licitador, los hitos de interés, etc.

Deberán contemplarse como mínimo los siguientes planes operativos:

Plan de implantación de los servicios.
Los licitadores deberán presentar un Plan de Implantación de los servicios, en donde se recojan las distintas fases propuestas del proyecto en base a actividades, procesos y recursos, para la puesta en marcha de los servicios demandados.

El Plan de Implantación, que en todo caso deberá ser consensuado y aprobado por RTVM al inicio del contrato, deberá recoger al menos los siguientes aspectos:

- Identificación de datos necesarios.
- Definición de los procesos operativos.
- Organización en niveles de atención, actividades y recursos técnicos.
- Organización de recursos operativos para prestación del servicio, organización del soporte 24x7 y distribución de recursos propuesta.
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación.

El Plan de Implantación, detallará claramente para cada fase propuesta, el calendario de actividades asociado, plazos estimados y los medios técnicos y humanos dedicados.

Plan de operación y devolución de los servicios.

En este apartado se describirá el modelo de gestión propuesto para la operación de los servicios, contemplando como mínimo los siguientes aspectos:

- Metodología propuesta para la operación del servicio.
- Propuesta de mecanismos de control y seguimiento
- Procedimientos operativos de notificación de incidencias y peticiones.
- Procedimientos operativos de escalado de incidentes y relación entre los distintos niveles de soporte (1, 2, y 3).
- Propuesta de métricas (KPI's) e indicadores del servicio y mecanismos de obtención y seguimiento.
- Plan de devolución de servicios que garantice la transferencia de conocimiento a la finalización del contrato, recogiendo la documentación mínima a entregar: documentación de procesos, de instalación de herramientas, de gestión del servicio, etc.

Plan de Calidad

Los licitadores deberán presentar un Plan de Calidad y especificar los parámetros de medición propuestos para asegurar el cumplimiento de los niveles de calidad requeridos.

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS, así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

Plan de Formación

Los licitadores deberán presentar un Plan de Formación.

Con el objetivo de obtener las habilidades necesarias para operar con la solución instalada, el adjudicatario deberá desarrollar, planificar e impartir los cursos de formación de los sistemas instalados para el personal de RTVM, atendiendo a los siguientes criterios:

- Será obligación del adjudicatario el suministro de toda la documentación y material necesario para la realización de los mismos.
- El lugar de impartición de los cursos serán las instalaciones de RTVM.
- La realización de dicho plan de formación se deberá realizar previo a la puesta en producción del servicio objeto de este contrato.
- Los cursos de formación se impartirán por personal con la experiencia, conocimientos y titulaciones requeridas para una actividad de este tipo.
- Se deben contemplar diferentes sesiones para dar cobertura a los diferentes turnos de trabajo asignados al personal de RTVM.

La formación que debe impartirse contemplará como mínimo los siguientes contenidos:

- Formación en el uso de los diferentes módulos de la aplicación para la operación diaria.
- Formación específica para la parametrización de los diferentes módulos para los diferentes administradores de la plataforma.
- Formación para la explotación y consulta de la plataforma técnica de sistemas y de los módulos implantados.

LOTE 2: SERVICIOS DE INTERNET, LAN Y WAN

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 50 páginas**, incluidos los anexos, ni contener referencias a documentos externos o anexos no incluidos cuando éstos sean puntos clave en la valoración de la propuesta.

Resumen ejecutivo
Definirá los objetivos y el alcance, así como los aspectos relevantes de la oferta y del licitador. El número máximo de páginas previsto para este apartado es de ocho (8) páginas.

Solución técnica propuesta para los servicios requeridos.
Los licitadores propondrán el modelo de servicio propuesto para dar cobertura al objeto del contrato:

- Servicio gestionado de mantenimiento, soporte, operación y administración de comunicaciones desde/hacia Internet
- Servicio gestionado de mantenimiento, soporte, operación y administración LAN-WIFI
- Servicio gestionado de mantenimiento, soporte, operación y administración WAN
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación.
- Oficina Técnica

La solución propuesta para cada servicio deberá contener la configuración de las infraestructuras y sistemas soporte, las especificaciones técnicas básicas de todos los elementos que lo componen, y las características de cada uno de ellos, de modo que cumplan los requerimientos descritos en el presente pliego.

Planes operativos
En este apartado, los licitadores presentarán los planes operativos propuestos para la prestación de los servicios requeridos, con detalle de todas las tareas y actividades implicadas, indicando los plazos previstos de cada una de ellas, los recursos materiales y humanos necesarios por parte del licitador, los hitos de interés, etc.

Deberán contemplarse como mínimo los siguientes planes operativos:

Plan de implantación de los servicios.

Los licitadores deberán presentar un Plan de Implantación de los servicios, en donde se recojan las distintas fases propuestas del proyecto en base a actividades, procesos y recursos, para la puesta en marcha de los servicios demandados.

El Plan de Implantación, que en todo caso deberá ser consensuado y aprobado por RTVM al inicio del contrato, deberá recoger al menos los siguientes aspectos:

- Identificación de datos necesarios.

- Definición de los procesos operativos.
- Organización en niveles de atención, actividades y recursos técnicos.
- Organización de recursos operativos para prestación del servicio, organización del soporte 24x7 y distribución de recursos propuesta.
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación.

El Plan de Implantación, detallará claramente para cada fase propuesta, el calendario de actividades asociado, plazos estimados y los medios técnicos y humanos dedicados.

Plan de operación y devolución de los servicios.

En este apartado se describirá el modelo de gestión propuesto para la operación de los servicios, contemplando como mínimo los siguientes aspectos:

- Metodología propuesta para la operación del servicio.
- Propuesta de mecanismos de control y seguimiento
- Procedimientos operativos de notificación de incidencias y peticiones.
- Procedimientos operativos de escalado de incidentes y relación entre los distintos niveles de soporte (1, 2, y 3).
- Propuesta de métricas (KPI's) e indicadores del servicio y mecanismos de obtención y seguimiento.
- Plan de devolución de servicios que garantice la transferencia de conocimiento a la finalización del contrato, recogiendo la documentación mínima a entregar: documentación de procesos, de instalación de herramientas, de gestión del servicio, etc.

Plan de Calidad

Los licitadores deberán presentar un Plan de Calidad y especificar los parámetros de medición propuestos para asegurar el cumplimiento de los niveles de calidad requeridos.

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS, así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

LOTE-3: SERVICIOS DE SEGURIDAD LÓGICA

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 80 páginas**, incluidos los anexos, ni contener referencias a documentos externos o anexos no incluidos cuando éstos sean puntos clave en la valoración de la propuesta.

Resumen ejecutivo

Definirá los objetivos y el alcance, así como los aspectos relevantes de la oferta y del licitador. El número máximo de páginas previsto para este apartado es de ocho (8) páginas.

Solución técnica propuesta para los servicios requeridos.

Los licitadores propondrán las diferentes soluciones para los servicios objeto del contrato:

- Servicio automatizado de análisis de vulnerabilidades.
- Servicio manual de análisis de vulnerabilidades.

- Servicio de monitorización de eventos de seguridad.
- Servicio de vigilancia digital e identificación de amenazas.
- Servicio de detección de incidentes, nivel 1 y nivel 2.
- Servicio especializado de respuesta a incidentes.
- Servicio de soporte a la gestión de incidentes.
- Servicio de diseño y operación de procesos y tecnologías del SOC.
- Servicio de capacitación y formación en ciberseguridad.
- Servicio de soporte a la gestión y operación del SOC.
- Servicio especializado de diseño seguro.

La solución propuesta para cada servicio deberá contener la configuración de las infraestructuras y sistemas soporte, las especificaciones técnicas básicas de todos los elementos que lo componen, y las características de cada uno de ellos, de modo que cumplan los requerimientos descritos en el presente pliego.

Planes operativos

En este apartado, los licitadores presentarán los planes operativos propuestos para la prestación de los servicios requeridos, con detalle de todas las tareas y actividades implicadas, indicando los plazos previstos de cada una de ellas, los recursos materiales y humanos necesarios por parte del licitador, los hitos de interés, etc.

Deberán contemplarse como mínimo los siguientes planes operativos:

Plan de implantación de los servicios.

Los licitadores deberán presentar un Plan de Implantación de los servicios, en donde se recojan las distintas fases propuestas del proyecto en base a actividades, procesos y recursos, para la puesta en marcha de los servicios demandados.

El Plan de Implantación, que en todo caso deberá ser consensuado y aprobado por RTVM al inicio del contrato, deberá recoger al menos los siguientes aspectos:

- Identificación de datos necesarios para el diseño del SOC, como datos críticos, capacidades de seguridad actuales en RTVM o procedimientos operativos vigentes para la gestión de la seguridad.
- Definición de los procesos operativos del SOC para la monitorización de la seguridad y la respuesta a incidentes, y relaciones con otras áreas de RTVM.
- Organización del SOC en niveles de atención, actividades y recursos técnicos.
- Organización de recursos operativos para prestación del servicio, organización del soporte 24x7 y distribución de recursos propuesta.
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación (SIEM, detección de vulnerabilidades, ticketing, etc.)
- Desarrollo del portal de gestión.

El Plan de Implantación, detallará claramente para cada fase propuesta, el calendario de actividades asociado, plazos estimados y los medios técnicos y humanos dedicados.

Plan de operación y devolución de los servicios.

En este apartado se describirá el modelo de gestión propuesto para la operación de los servicios, contemplando como mínimo los siguientes aspectos:

- Metodología propuesta para la operación del servicio.
- Propuesta de mecanismos de control y seguimiento de los eventos de seguridad en sus distintas fases: triaje, clasificación, análisis y tratamiento.
- Mecanismos de control y seguimiento de eventos detectados.
- Procedimientos operativos de notificación de incidencias y peticiones al SOC.
- Procedimientos operativos de escalado de incidentes y relación entre los distintos niveles de soporte (1, 2, y 3), resto de equipos del SOC, y otras áreas de RTVM.

- Propuesta de métricas (KPI's y KRI's) e indicadores del servicio y mecanismos de obtención y seguimiento.
- Plan de devolución de servicios que garantice la transferencia de conocimiento a la finalización del contrato, recogiendo la documentación mínima a entregar: documentación de procesos, de instalación de herramientas, de gestión del servicio, etc.

Plan de Calidad

Los licitadores deberán presentar un Plan de Calidad y especificar los parámetros de medición propuestos para asegurar el cumplimiento de los niveles de calidad requeridos.

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS, así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

ANEXO ENTORNOS TECNOLÓGICOS

El entorno tecnológico sobre el que se prestarán los servicios recogidos en el LOTE 3 será el siguiente:

SISTEMAS OPERATIVOS	
Servidor:	BladeCenter de Lenovo Flex, con tecnología de virtualización ESX Server de Vmware, Red Hat, SUSE, CenTOS, Windows
Puesto ofimático:	Windows, Android, iOS
SERVIDORES	
Web:	Apache,IIS
Aplicaciones:	Tomcat, Jboss
BASES DE DATOS	
	Microsoft SQL Server, MySQL ,MariaDB, Oracle
SEGURIDAD PERIMETRAL	
Cortafuegos:	FortiNet, Palo Alto
COMUNICACIONES	
Routers:	Extreme Networks
Switches:	Extreme Networks
WIFI:	Extrema Networks
DNS, DHCP:	Microsoft
Balanceadores:	Radware
VPN, Acceso Remoto:	FortiClient, ANYDESK,RADIUS
SOFTWARE NEGOCIO	
Gestión documental:	Documentum
ERP's:	SAP, Meta4
Gestores de contenido:	Drupal, Bitban
Correo electrónico:	MS Exchange
Servicios de autenticación:	Active directory

ANEXO INVENTARIO WIFI

ACCESS POINTS			
Extreme	AP4000-WW	4002210180761	10.6.5.0
Extreme	AP4000-WW	4002210180857	10.6.5.0
Extreme	AP4000-WW	4002210180909	10.6.5.0
Extreme	AP4000-WW	4002210180780	10.6.5.0
Extreme	AP4000-WW	4002210180859	10.6.5.0
Extreme	AP4000-WW	4002210180878	10.6.5.0
Extreme	AP4000-WW	4002210181030	10.6.5.0
Extreme	AP4000-WW	4002210180802	10.6.5.0
Extreme	AP4000-WW	4002210180782	10.6.5.0
Extreme	AP4000-WW	4002210180858	10.6.5.0
Extreme	AP4000-WW	4002210180960	10.6.5.0
Extreme	AP4000-WW	4002210180927	10.6.5.0
Extreme	AP4000-WW	4002210181114	10.6.5.0
Extreme	AP4000-WW	4002210180834	10.6.5.0
Extreme	AP4000-WW	4002210180875	10.6.5.0
Extreme	AP4000-WW	4002210180961	10.6.5.0
Extreme	AP4000-WW	4002210180870	10.6.5.0
Extreme	AP4000-WW	4002210180869	10.6.5.0
Extreme	AP4000-WW	4002210180810	10.6.5.0
Extreme	AP4000-WW	4002210181088	10.6.5.0
Extreme	AP4000-WW	4002210180991	10.6.5.0
Extreme	AP4000-WW	4002210180616	10.6.5.0
Extreme	AP4000-WW	4002210180962	10.6.5.0
Extreme	AP4000-WW	4002210180948	10.6.5.0
Extreme	AP4000-WW	4002303020188	10.6.5.0
Extreme	AP4000-WW	4002303020178	10.6.5.0
Extreme	AP4000-WW	4002303020241	10.6.5.0
Extreme	AP4000-WW	4002304130302	10.6.5.0
Extreme	AP4000-WW	4002304130292	10.6.5.0
Extreme	AP4000-WW	4002304130306	10.6.5.0
Extreme	AP4000-WW	4002304130312	10.6.5.0

ANEXO INVENTARIO LAN

Fabricante	Modelo	S/N
Extreme	5520-24X	SB072203G-00069
Extreme	5520-24X	SB072203G-00090
Extreme	5520-24X	SB072203G-00096
Extreme	5520-24X	SB072203G-00169
Extreme	5520-24X	SB072203G-00081
Extreme	5520-24X	SB072203G-00052
Extreme	5420M-24W-4	JA102229G-00005
Extreme	5420M-24W-4	JA102215G-00225
Extreme	5420M-24W-4	JA102229G-00008
Extreme	5420M-24W-4	JA102229G-00077
Extreme	5420M-24W-4	JA102229G-00035
Extreme	5420M-24W-4	JA102229G-00068
Extreme	5420M-24W-4	JA102229G-00014
Extreme	5420M-24W-4	JA102229G-00055
Extreme	5420M-48W-4	JA122301G-00401
Extreme	5420M-48W-4	JA122301G-00429
Extreme	5420M-48W-4	JA122301G-00128
Extreme	5420M-48W-4	JA122301G-00189
Extreme	5420M-48W-4	JA122301G-00408
Extreme	5420M-48W-4	JA122301G-00387
Extreme	5420M-24W-4	JA102240G-00162
Extreme	5420M-24W-4	JA102241G-00060
Extreme	5420M-24W-4	JA102241G-00079
Extreme	5420M-24W-4	JA102241G-00057
Extreme	5420M-24W-4	JA102241G-00072
Extreme	5420M-48W-4	JA122312G-00378
Extreme	5420M-48W-4	JA122312G-01546
Extreme	5420M-48W-4	JA122312G-01493
Extreme	5420M-48W-4	JA122311G-02027
Extreme	5420M-48W-4	JA122312G-00220

Fabricante	Modelo	S/N
Extreme	5420M-48W-4	JA122312G-00678
Extreme	5420M-48W-4	JA122312G-00646
Extreme	5420M-48W-4	JA122312G-00643
Extreme	5420M-48W-4	JA122312G-00082
Extreme	5420M-48W-4	JA122312G-00043
Extreme	5420M-48W-4	JA122311G-01658
Extreme	5420M-48W-4	JA122311G-01464
Extreme	5420M-48W-4	JA122312G-00926
Extreme	5420M-48W-4	JA122312G-01347
Extreme	5420M-48W-4	JA122312G-00541
Extreme	5420M-48W-4	JA122312G-00217
Extreme	5420M-48W-4	JA122311G-02036
Extreme	5420M-48W-4	JA122311G-02042
Extreme	5420M-48W-4	JA122311G-00250
Extreme	5420M-48W-4	JA122311G-00110
Extreme	5420M-48W-4	JA122311G-00261
Extreme	5420M-48W-4	JA122311G-00097
Extreme	5420M-48W-4	JA122312G-01028
Extreme	5420M-48W-4	JA122312G-01376
Extreme	5420M-48W-4	JA122312G-00426
Extreme	5420M-48W-4	JA122312G-01012
Extreme	5420M-48W-4	JA122312G-00203
Extreme	5420M-48W-4	JA122312G-00781
Extreme	5420M-48W-4	JA122312G-00450
Extreme	5420M-48W-4	JA122312G-01135
Extreme	5420M-48W-4	JA122312G-00652
Extreme	5420M-48W-4	JA122311G-02029
Extreme	5420M-48W-4	JA122312G-00225
Extreme	5420M-48W-4	JA122312G-01485
Extreme	5420M-48W-4	JA122311G-01015
Extreme	5420M-48W-4	JA122312G-01105
Extreme	5420M-48W-4	JA122312G-01068
Extreme	5420M-48W-4	JA122311G-02039
Extreme	5420M-48W-4	JA122311G-00737
Extreme	5420M-48W-4	JA122312G-00674

Fabricante	Modelo	S/N
Extreme	5420M-48W-4	JA122312G-00100
Extreme	5420M-48W-4	JA122312G-00537
Extreme	5420M-48W-4	JA122311G-02031
Extreme	5420M-48W-4	JA122312G-00041
Extreme	5420M-48W-4	JA122311G-01343
Extreme	5420M-48W-4	JA122312G-00650
Extreme	5420M-48W-4	JA122312G-01086
Extreme	5420M-48W-4	JA122311G-00159
Extreme	5420M-48W-4	JA122312G-01269
Extreme	5420M-48W-4	JA122311G-00108
Extreme	5420M-48W-4	JA122301G-00402
Extreme	5420M-24W-4	JA102229G-00019
Extreme	5420M-24W-4	JA102215G-00501
Extreme	5420M-48W-4	JA122312G-00241
Extreme	5420M-48W-4	JA122312G-00680

ANEXO SIEM-REQUISITOS MÍNIMOS

Las características funcionales y técnicas mínimas que debe cumplir el suministro del sistema de gestión de eventos e información de seguridad, el SIEM, son las siguientes:

1. Arquitectura del sistema y dimensionamiento

Módulos principales

El sistema de gestión de eventos de seguridad debe contar con, al menos, los siguientes elementos conceptuales, no debiendo identificarse éstos con dispositivos físicos o módulos software:

- Recolector de logs: encargado de recoger la información de las diferentes fuentes de información, y consolidar y normalizar los eventos recogidos.
- Procesador de eventos con funciones de correlación, que se encargará de tareas como normalizar, priorizar, recolectar, evaluar el riesgo y ejecutar el motor de correlación.
- Base de datos, para el almacenamiento de los eventos recogidos, alertas generadas, informes, inventario de activos e información útil para la gestión del sistema.
- Consola de administración y operación centralizada, para la administración unificada de la plataforma.

Los diferentes componentes del sistema se desplegarán en el centro de proceso de datos (CPD) de RTVM.

Módulos adicionales

Adicionalmente, el sistema dispondrá también de:

- Recolectores y analizadores de seguridad de tráfico de red, que podrá ser provisto en dos modalidades alternativas: o sondas de red, encargados de analizar y detectar el tráfico de red malicioso de forma pasiva, incluye las funciones propias de un sistema de detección de intrusión de red (NIDS). Deberán instalarse recolectores de tráfico de red en cada CPD para el análisis del tráfico de salida a Internet y el tráfico interno de entrada a los CPDs.
  - analizadores de flujos de red enriquecidos, que permita inspeccionar en profundidad los paquetes de red y extraer como mínimo datos de identificación de aplicación, login de usuario, email, URLs y DNS queries y responses. Estos analizadores de flujo deberán ser capaces de definir reglas para identificar y alertar sobre tráfico sospechoso y ser gestionados de forma centralizada desde la consola principal. Se prevé la necesidad de analizar un millón de flujos de red por minuto (FPM).
- Pantallas de monitorización de eventos de seguridad detectados, a instalar en la sede de RTVM, donde residirán los servicios de SOC.
- Dimensionamiento
  El sistema de gestión de eventos deberá estar dimensionado y correctamente licenciado durante el periodo de ejecución del contrato para:
  - Recolectar y analizar al menos 10 Gbit/s de tráfico de red por CPD y flujo, flujo de tráfico de salida a Internet y flujo de tráfico interno de entrada a cada CPD.
  - Recolectar un volumen mínimo de 5.000 eventos por segundo (EPS) de media al día en cada CPD, de las distintas fuentes de eventos.
  - Procesar y correlar un mínimo de 5.000 eventos por segundo (EPS) en tiempo real y sin descarte de eventos.
- Almacenar toda la información de eventos y correlación de forma on-line durante un periodo mínimo de seis meses, y un periodo mínimo de retención de eventos off-line de 24 meses.

2. Fuentes de eventos.
La plataforma de gestión de eventos recibirá y almacenará los eventos de fuentes diversas, por lo que deberá tener la funcionalidad para procesar de forma nativa eventos de las siguientes fuentes:

- Cortafuegos de red.
- Balanceadores de tráfico
- Routers.
- Switches.
- Pasarelas de navegación web y pasarelas inversas.
- Servicios de nombres de dominio (DNS).
- Servicios de acceso remoto.
- Servicios de directorio LDAP y DA.
- Servicios de redes privadas VPN.
- Servidores web.
- Servidores de aplicaciones.
- Bases de datos.
- Sistemas operativos.

En el **ANEXO ENTORNO TECNOLÓGICO** se facilita detalle de fabricantes principales.
Deberá disponer del mayor número de analizadores sintácticos (parsers) para otros sistemas de terceros, siendo imprescindible que todos ellos estén completamente documentados, incluyendo las tareas requeridas sobre los sistemas de terceros para su correcta integración en la plataforma.
Permitirá también el desarrollo de nuevos analizadores mediante expresiones regulares estándar o un interfaz de programación (API).

3. Protocolos de intercambio de eventos.
La plataforma debe permitir, al menos, los siguientes protocolos de intercambio de eventos entre las fuentes y el sistema de recolección:
- Protocolos SNMP (en todas sus versiones), SYSLOG y SYSLOG-NG (UDP/TCP/TLS).
- Flujos de red en formato NetFlow o IPFIX (en todas sus versiones tanto para IPv4 como IPv6).
- Push/Pull de ficheros en texto y descarga de información desde URL.
- Fuentes de información externas en formatos XML, TXT, y CSV.

4. Características generales a cumplir.
El sistema de gestión de eventos propuesto por el licitador deberá cumplir los siguientes requisitos funcionales mínimos:

- **Recolectores de logs:**
  Actualización de los interfaces/plugin para asegurar la integración de la plataforma con las evoluciones del software de los dispositivos y sistemas externos.
  - Posibilidad de modificación de firmas de detección existentes y creación de firmas nuevas, personalizadas.
  - Posibilidad de detección de eventos basada en reputación (de direccionamiento, URLs, geolocalización, etc.).
  - Correlación básica.
  - Envío cifrado de eventos desde el equipo recolector al correlador.
  - Reducción de falsos positivos mediante ajuste de umbrales de detección.
  - Mecanismos disponibles para evitar la pérdida de eventos en caso de superación puntual de límite de la capacidad máxima soportada o licenciada.
  - Posibilidad de configuración independiente de detección en cada sensor.
  - Capacidad de almacenamiento local temporal de los eventos procesados.

- Capacidad de integración con fuentes externas de inteligencia.

- **Procesador de eventos con capacidad de correlación:**
  - Actualización de los formatos de eventos y bases de datos de eventos, para asegurar la integración de la plataforma con las evoluciones del software de los dispositivos y sistemas externos.
  - Disponibilidad de reglas de correlación actualizadas, durante la vigencia del contrato.
  - Posibilidad de agregación y normalización de las distintas fuentes de datos monitorizadas y detectadas.
  - Posibilidad de correlación empleando operaciones lógicas sobre los eventos detectados.
  - Posibilidad de correlación relacionando los eventos detectados y la información contenida en la base de datos de conocimiento, como inventario de activos o información sobre los mismos.
  - Posibilidad de correlación de fuentes de flujos de red.
  - Posibilidad de correlación basada en datos históricos.
  - Posibilidad de correlación basada en vulnerabilidades.
  - Posibilidad de detección por anomalías.
  - Posibilidad de detección por analítica de comportamiento.
  - Posibilidad de priorización de eventos según distintos criterios como valoración de activos, tipo de evento, etc.
  - Posibilidad de priorización de eventos basada en reputación de IP.
  - Posibilidad de priorización de eventos basada en taxonomías personalizables.
  - Posibilidad de asignación de políticas de filtrado de eventos a grupos de activos.
  - Posibilidad de filtrado y aplicación de políticas en la detección de eventos según las necesidades del entorno (modificación de la prioridad, eliminación del panel de eventos, notificación de eventos, activación/desactivación de la opción de correlación, etc.) que se den en ciertos activos.
  - Capacidad de que no se produzcan pérdidas de eventos en caso de superación puntual del límite de la capacidad máxima soportada o licenciada.
  - Posibilidad de visualización del contenido de los paquetes de red (payload) de los eventos de red para análisis forense.
  - Posibilidad de modificación y ajuste de las reglas de correlación existentes y creación de reglas de correlación nuevas a medida.
  - Posibilidad de reducción en la detección de falsos positivos mediante ajuste de los umbrales de detección.
  - Posibilidad de ofrecer información de contexto (información histórica de DNS, país, reputación IP,) durante el análisis del evento.
  - Capacidad de integración con fuentes de inteligencia basadas en estándares STIX/TAXII.

- **Base de datos:**
  - Posibilidad de registro de activos manual y masiva, e información sobre los mismos en la base de datos conocimiento, especialmente el valor del activo.
  - Posibilidad de registro, actualización y eliminación masiva de activos. Posibilidad de exportación/importación de base de datos de activos en diferentes formatos de salida/entrada que facilite su tratamiento.
  - Posibilidad de registro de otra información útil para la detección, correlación y gestión de los incidentes detectados (vulnerabilidades conocidas, amenazas actuales, geolocalización de orígenes, reputación, etc.).
  - Posibilidad de almacenar los datos por niveles, de tal manera que el primer nivel será el año, el segundo el mes, días, y que resulte posible hacer copias de estos en almacenamiento externo organizados por periodos de tiempo.

- Funcionalidad de configurar múltiples periodos de retención de logs para eventos y flujos basados en filtros sobre los eventos y flujos.
- Funcionalidad de archivado de aquellos logs/eventos que sobrepasen el periodo de retención determinado.
- Capacidad de firma y sellado de tiempo de los logs y eventos almacenados en formato original.
- Capacidad de integridad de los datos almacenados mediante algoritmos de HASH (SHA2-256 o superior).
- Compresión de datos de al menos de 10 a 1.

- **Gestión de la plataforma:**
  - Acceso de usuarios a la plataforma mediante protocolo HTTPS.
  - Control de acceso basado en usuario y contraseña.
  - Control de acceso y autenticación de usuarios mediante base de datos externa LDAP.
  - Asignación de privilegios a usuarios basada en roles que permitan asignar diferentes niveles de permisos en la plataforma, así como la creación de grupos de usuarios.
  - Acceso a las distintas funcionalidades e información de la plataforma basado en roles. Posibilidad de restringir el acceso a ciertas secciones de la herramienta a roles, usuarios o grupos de usuarios.
  - Funcionalidades de registro de actividad de usuarios.
  - Configuración y gestión de realización de copias de seguridad de la información albergada en la solución.
  - Gestión centralizada de todos los elementos: sensores, fuentes de datos de monitorización, motores de correlación, interfaces de gestión o consulta, etc.
  - Gestión centralizada de políticas de detección y correlación, firmas, orígenes de firmas, inventario, base de datos de conocimiento, etc...
  - Actualización automática de la solución y/o los elementos que la componen (corrección de bugs, implementación de mejoras en las funcionalidades, etc.…).
  - Posibilidad de integración con herramientas externas de análisis de vulnerabilidades y amenazas.
  - Integración con soluciones de ticketing externas mediante servicios web, especialmente LUCIA (herramienta de ticketing definida por el CCN-CERT).
  - Generación de informes personalizados según distintos criterios (sensor, activo y/o grupo de activos, propietario de activos, geolocalización, etc.).
  - Funcionalidad para exportar datos en diferentes formatos de salida, al menos CSV, XML, PDF y HTML.
  - Funcionalidad para configurar paneles informativos personalizados con datos estadísticos de los eventos y demás información relevante proporcionada por la plataforma.
  - Generación de mapas de riesgo en tiempo real.
  - Notificación automática de alertas de seguridad a través de diferentes medios, tales como correo electrónico, consola de operación, servicio web configurable, etc.
  - Definición de políticas de notificación de alertas en base a criterios personalizables como grupo de activos, propietario de activos, sensores de detección, etc.

- **Recolectores de tráfico de red:**
  - Disponibilidad de firmas de detección de patrones actualizadas.
  - Monitorización de tráfico de red de interfaz de 10 Gbps (incluyendo capa 7).
  - Capacidad de generar flujos de red de interfaz de 10 Gbps (incluyendo capa 7).
  - Capacidad de modificación de firmas de detección existentes y creación de nuevas firmas personalizadas.
  - Envío cifrado de eventos desde el equipo sensor al correlador.
  - Reducción de falsos positivos mediante ajuste de los umbrales de detección.

- Mecanismos disponibles para evitar la pérdida de eventos en caso de superación puntual de límite de la capacidad máxima soportada o licenciada.
- Posibilidad de configuración independiente de detección en cada sensor.
- Posibilidad de captura de paquetes de red (payload) que generan los eventos para análisis forense.
- Capacidad de integración con fuentes de inteligencia externas.

- **Seguridad:**
  - La solución SIEM debe permitir cifrar todas las comunicaciones entre sus componentes.
  - La solución SIEM debe permitir la configuración en HA sin componentes adicionales (balanceadores, etc.).
  - La solución SIEM debe permitir autenticar mediante LDAP, Directorio Activo, RADIUS y TACACS.
  - La solución SIEM debe permitir autenticar utilizando Single Sign-On.
  - La solución SIEM deben disponer de una interfaz SNMP para monitorización de los componentes.
  - La solución SIEM debe permitir ofuscar campos o parte del log para evitar que los analistas vean ciertos datos en claro.
  - La solución SIEM debe auditar todas las acciones realizadas por el usuario tanto en la interfaz web como vía línea de comandos en los appliances.
  - La solución SIEM debe permitir definir accesos basados en roles para limitar el acceso a ciertos logs y flujos dependiendo del rol.
  - La solución SIEM debe permitir definir accesos basados en roles para limitar el acceso a las funcionalidades como la administración, informes, filtrados, correlación y/o cuadros de mando.

- **Correlación y Casos de Uso**
  - La solución SIEM debe permitir correlacionar información de Logs, Flujos y vulnerabilidades en tiempo real.
  - La solución SIEM debe permitir correlacionar entre sí la información de Logs, Flujos y vulnerabilidades.
  - La solución SIEM debe permitir la correlación histórica de Logs y Flujos (correlación de una selección de eventos pasados contra Indicadores de Compromiso (IoCs) y Reglas actuales).
  - La solución SIEM debe proporcionar casos de uso por defecto, documentados y mantenidos por el propio fabricante.
    La solución SIEM debe proporcionar Informes por defecto, documentados y mantenidos por el propio fabricante.
  - La solución SIEM debe permitir definir de reglas de anomalía evaluados en tiempo real que detecten cambios repentinos de un valor o suceso (por ejemplo: incremento repentino del volumen de tráfico).
  - La solución SIEM debe permitir definir reglas de anomalía estacionales que detecten desviaciones en un valor o suceso (como el volumen de tráfico o número de logins fallidos) en comparación al mismo día de la semana anterior.
  - La solución SIEM debe incorporar algoritmos de Machine Learning para modelar el comportamiento habitual de usuarios y detectar desviaciones.
  - La solución SIEM debe agrupar y encadenar eventos relacionados (con el mismo host atacante, mismo usuario, misma víctima, etc.) en un único incidente, aunque los eventos sucedan de forma separada en el tiempo (a lo largo de varias horas o días) para detectar patrones “Low and Slow”.
  - La solución SIEM debe tener la capacidad de detectar en tiempo real el uso de una nueva IP o puerto en una subred.

  - La solución SIEM debe tener la capacidad de detectar en tiempo real el uso de un nuevo nombre de usuario en el entorno.
  - La solución SIEM debe tener la capacidad de integrarse con el directorio activo y utilizar esta información en las reglas de correlación (por ejemplo, para detectar que un usuario no está registrado en el DA).

- **Flexibilidad y Colaboración:**
  - La solución SIEM debe incorporar un feed de inteligencia con clasificación de IPs y URLs.
  - La solución SIEM debe soportar la integración de IoCs mediante estándares tipo STIX/TAXII para importar IoCs como para exportarlos.
  - La solución SIEM debe permitir la colaboración mediante la creación de colecciones (públicas o privadas) para compartir IoCs.

5. Instalación y aceptación del sistema.
El sistema de gestión de eventos se instalará en el CPD de RTVM.

Para la instalación y aceptación del sistema, el adjudicatario deberá realizar las siguientes actividades mínimas:

- **Diseño detallado de la solución**: junto con RTVM, el adjudicatario elaborará el Plan Detallado de Instalación, en donde se definirá la arquitectura final del sistema, en base a la situación de partida y las necesidades específicas de RTVM. El plan de instalación incluirá el diseño final de la arquitectura a desplegar, el plan de puesta en marcha con detalle de tareas concretas y tiempos estimados de ejecución, requerimientos de la instalación (espacio en racks, conectividad de red, energía, direccionamiento IP, etc.), la propuesta de integración con los sistemas externos identificados, las políticas generales de configuración y alarmas, y el plan de pruebas.
- **Instalación del todo el equipamiento**: el adjudicatario deberá respetar toda la normativa interna de aplicación para el suministro e instalación del equipamiento en RTVM, como son procedimientos de acceso a los centros, etiquetado patrimonial de componentes, normativa técnica de instalación, etc., que será facilitada al inicio del contrato.
- **Configuración básica del sistema**, necesaria para operar la plataforma y poder comenzar a recoger eventos, fuentes de logs y tráfico de red. El sistema deberá optimizarse para que sólo almacene los datos de interés.
- **Integración de fuentes y otros sistemas:**
  - Elementos de red: configuración y captura de los eventos generados por los sistemas de detección de intrusión ofertados (Recolectores de tráfico de red).
  - Elementos de seguridad: captura de logs generados por los sistemas de seguridad perimetral de los CPDs.
  - Integración de las fuentes de inteligencia de amenazas propuestas por el adjudicatario.

  Y en general la integración con todas las fuentes y sistemas descritos en este anexo.
- **Configuración de casos de uso de monitorización:** el sistema deberá quedar configurado al menos con los siguientes casos de uso:
  - Detección de tráfico de red de código malicioso.
  - Detección de ataques por denegación de servicio.
  - Detección de ataques por explotación de vulnerabilidades.
  - Detección de sistemas pertenecientes a botnets.
  - Detección de accesos sospechosos a dispositivos, sistemas y aplicaciones.

- **Optimización, pruebas y aceptación del sistema:** tras la integración de fuentes y configuración de casos de uso, el adjudicatario establecerá un periodo de optimización

del sistema para reducir el porcentaje de falsos positivos y falsos negativos. Finalizado este periodo, se ejecutará el plan de pruebas aprobado y la aceptación del sistema.

Firmado digitalmente por
SUDIRECTORA - RTVM22597 -
RADIO TELEVISION MADRID.
Fecha: 21/02/2024.