



PLIEGO DE PRESCRIPCIONES TÉCNICAS

**SERVICIO DE TELECOMUNICACIONES DE BANDA ANCHA POR SATÉLITE PARA LA CONEXIÓN DE
EMPLAZAMIENTOS AISLADOS DEL CANAL DE ISABEL II, S.A. M.P.**

EXPEDIENTE: Nº: 86/2025

ÍNDICE

1.	Objeto del contrato.....	4
2.	Alcance.....	5
2.1	Fase de Implementación	5
2.1.1	Puesta en Marcha de Estaciones Fijas	5
2.1.2	Puesta en Marcha de Estaciones de Uso Itinerante.....	5
2.1.3	Configuración de Routers Encapsuladores	6
2.2	Fase de Operación y Servicio.....	6
2.2.1	Puesta en Marcha de las Controladoras	6
2.2.2	Accesos de Banda Ancha Terrestre.....	7
2.2.3	Orquestador Central Residente en la Nube	8
2.2.4	Redundancia, Soporte y Escalabilidad	8
2.2.5	Ciberseguridad del servicio.....	9
3.	Especificaciones técnicas de cada subsistema.....	10
3.1	Conectividad Satelital en Estaciones Fijas.....	10
3.1.1	Objetivo y Características Principales	10
3.1.2	Requisitos Mínimos de la Conectividad	10
3.2	Conectividad Satelital Para las Estaciones de Uso Itinerante	10
3.2.1	Objetivo y Características Principales	10
3.3	Conectividad Estaciones Terrestres Gestionables.....	11
3.3.1	Objetivo y Características Principales	11
3.3.2	Requisitos Mínimos de los Dispositivos	11
3.4	Servicio de Conectividad por Fibra Óptica en Sedes Centrales.....	12
3.4.1	Objetivo y Características Principales del Servicio	12
3.4.2	Características Técnicas del Servicio	12
3.4.3	Independencia del Operador de Red	13
3.5	Orquestador Central Residente en la Nube	13
3.5.1	Objetivo y Características Principales del Servicio	13
3.5.2	Requisitos Técnicos Mínimos del Orquestador.....	14
4.	Especificaciones técnicas de los equipos	16
4.1	Routers.....	16
4.1.1	Router Compacto.....	16
4.1.2	Router Ampliado.....	16
4.1.3	Router para Estaciones Terrestres Gestionables	17
4.2	Antena Satelital LEO (+ Router Satelital).....	17
4.2.1	Requisitos Técnicos de la Antena Satelital Estándar	17

4.2.2	Requisitos Técnicos de la Antena Satelital High Performance	18
4.3	Controladoras (Gateways)	18
4.3.1	Características Técnicas Mínimas de las Controladoras.....	18
5.	Mantenimiento y disponibilidad del servicio	20
6.	Formación	22
6.1	Objetivo.....	22
6.2	Temario	22
6.3	Formato y Organización	22
7.	Ejecución del proyecto de puesta en marcha del servicio	23
7.1	Plan General de Proyecto.....	23
7.2	Ejecución de los Trabajos	23
7.2.1	Preparación del Despliegue	23
7.2.2	Suministro.....	23
7.3	Instalación	23
7.3.1	Trabajos Previos a la Instalación	23
7.3.2	Trabajos de Instalación	24
7.4	Aceptación de las Instalaciones	25
7.5	Desinstalación de equipamiento.....	25
7.6	Plan de Seguridad y Salud	25
8.	Gestión del servicio.....	26
8.1	Plan de Gobierno del Servicio	26
8.1.1	Gestión de los Servicios	26
8.1.2	Gestión de la Relación	26
8.1.3	Modelo de Gestión del Servicio	27
9.	Requisitos de seguridad de obligado cumplimiento.	31

1. Objeto del contrato

El objeto del presente contrato es establecer y mantener un servicio integral de conectividad para dotar de acceso a Internet de banda ancha a diversos emplazamientos aislados de Canal de Isabel II, S.A. M.P. en adelante, Canal, mediante tecnologías satelitales en órbita baja (LEO – Low Earth Orbit) y soluciones de conectividad terrestre. El servicio comprenderá los siguientes elementos:

- **Servicio de conectividad de banda ancha vía satélite para estaciones fijas** de Canal, principalmente estaciones depuradoras de aguas residuales (EDAR) y estaciones de bombeo de aguas residuales (EBAR), que carezcan de acceso a redes terrestres de comunicaciones.
- **Servicio de conectividad de banda ancha vía satélite para estaciones móviles o de uso itinerante.** Se habilitarán soluciones de acceso satelital destinadas a:
 - La unidad móvil de emergencias (TETRA).
 - Puntos sin cobertura habitual o afectados por incidencias de red, permitiendo establecer enlaces temporales de comunicaciones de forma ágil y garantizar el acceso a Internet.
- **Integración en la red de transporte propia de Canal de distintos emplazamientos** de Canal mediante el uso de conexiones de banda ancha existentes (no satelitales) proporcionadas por operadores de comunicaciones comerciales, como accesos de fibra óptica o redes móviles 4G/5G, en la plataforma de orquestación enunciada en el siguiente punto. El tráfico de estos emplazamientos será tunelizado hacia la red de datos interna de Canal, garantizando su integración en un entorno unificado de gestión. En el contexto del presente proyecto se denominan estaciones terrestres gestionables.
- **Provisión, integración y mantenimiento de un orquestador central operado en modalidad SaaS**, que permitirá la operación centralizada, gestión, monitorización y control unificado de toda la red de comunicaciones desplegada, incluyendo las estaciones fijas, estaciones terrestres gestionables, estaciones de uso itinerante y controladoras centrales. El orquestador deberá garantizar la visibilidad operativa en tiempo real, la automatización de la gestión de túneles y servicios, y la integración con los sistemas de monitorización de Canal, asegurando una operación flexible, escalable y segura de la infraestructura de conectividad.
- **Conexión de alta capacidad para las sedes centrales:** Se deberá proporcionar una conexión a Internet de alta capacidad, mediante fibra óptica, en las dos sedes centrales de Canal, con el fin de garantizar la conectividad estable y de alto rendimiento con el proveedor del servicio.
- **Evolución y mantenimiento de la solución de conectividad:** El adjudicatario garantizará la ampliación, evolución tecnológica y mantenimiento continuo de la infraestructura de conectividad satelital, cubriendo así las necesidades de comunicación de los distintos emplazamientos de Canal.

2. Alcance

El alcance del contrato comprende los siguientes elementos fundamentales, organizados en dos fases principales: Fase de implementación con la instalación del equipamiento de acceso al servicio de comunicaciones en los emplazamientos remotos y Fase de operación y servicio, sin que ello implique necesariamente un orden secuencial de ejecución.

2.1 Fase de Implementación

La fase de implementación abarca todas las actividades necesarias para la puesta en marcha inicial de la solución. Salvo que se indique lo contrario, todas las actuaciones descritas en esta fase incluyen: la instalación completa de los equipos, suministro de hardware, licenciamiento de software, integración de todos los elementos en el orquestador central residente en la nube, mantenimiento HW/SW y soporte técnico 24x7.

La arquitectura general del servicio demandado, queda representada en el diagrama de la figura 1.

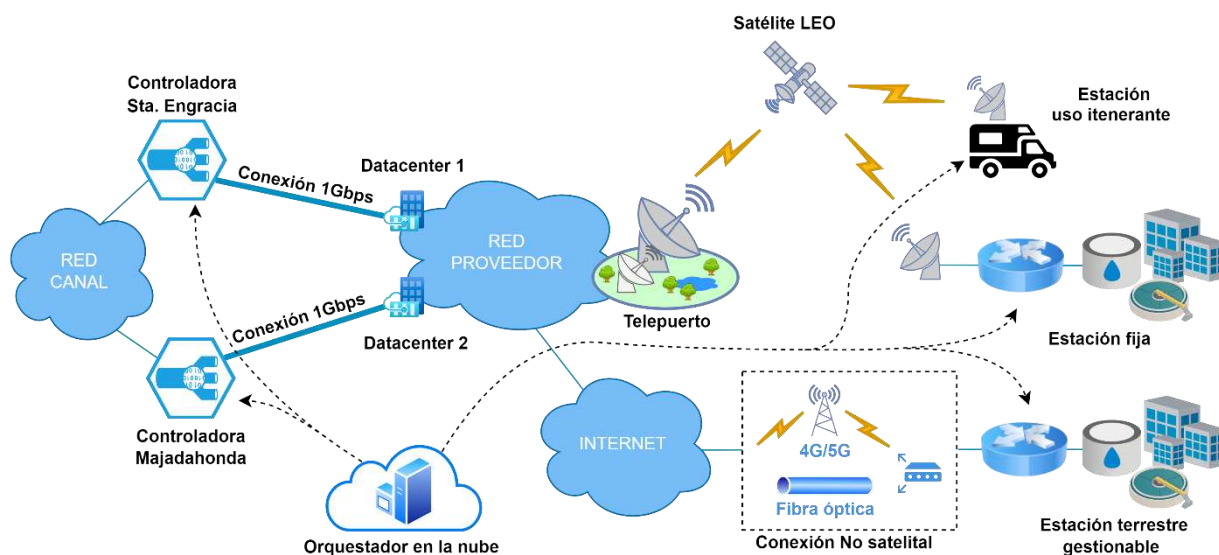


Figura 1: Arquitectura general de la solución

2.1.1 Puesta en Marcha de Estaciones Fijas

Puesta en marcha de emplazamiento de estación estándar y alta de un servicio de datos de banda ancha de acceso a Internet, mediante acceso satelital LEO, para sesenta y tres (63) estaciones fijas.

2.1.2 Puesta en Marcha de Estaciones de Uso Itinerante

Puesta en marcha de estación móvil y alta de un servicio de datos de banda ancha de acceso a Internet mediante acceso satelital LEO, para tres (3) estaciones de uso itinerante, con equipamiento de alto rendimiento (High Performance).

Se requieren dos (2) servicios de este tipo para su instalación en la unidad móvil de emergencias TETRA (principal y backup), más una (1) unidad destinada a la conexión de respaldo en situaciones de incidencias de red en puntos sin cobertura.

Para el servicio de backup de la unidad móvil de emergencias TETRA, el segundo kit satelital deberá garantizar una redundancia completa extremo a extremo, mediante la utilización de un operador satelital diferente al empleado en el servicio principal. El proveedor deberá asegurar que ambos operadores empleen infraestructuras de acceso independientes, con rutas diferenciadas y conexión a través de datacenters distintos de categoría TIER III o superior, situados en ubicaciones geográficas diferentes, con el fin de garantizar la diversidad física y lógica del servicio.

Esta condición será obligatoria para asegurar la continuidad del servicio en caso de fallo o indisponibilidad de uno de los operadores o de sus infraestructuras asociadas.

2.1.3 Configuración de Routers Encapsuladores

Se contempla la incorporación adicional de un conjunto de veinte (20) routers encapsuladores especialmente configurados, en estaciones terrestres gestionables. Esta denominación hace referencia a dispositivos que, si bien aprovechan infraestructura terrestre existente, están plenamente integrados en la lógica operativa y de gestión que los emplazamientos con servicios de conectividad satelital, replicando su comportamiento funcional y de supervisión.

Su función es permitir conectar de forma segura, gestionada y monitorizada estos puntos con la red de datos de Canal, a aquellos emplazamientos donde ya existe una conexión de banda ancha terrestre (como fibra óptica o redes móviles 4G/5G) y no se prevé la instalación de una antena satelital. Además, esta misma arquitectura servirá como respaldo en caso de fallo del enlace satelital principal en cualquier emplazamiento. La estructura general de esta solución se detalla en el diagrama de la figura 2.

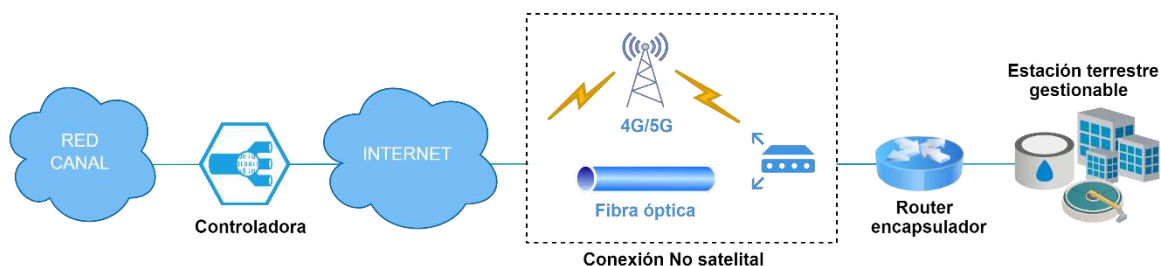


Figura 2: Arquitectura de los routers encapsuladores en estaciones terrestres gestionables

2.2 Fase de Operación y Servicio

2.2.1 Puesta en Marcha de las Controladoras

Se instalará y activará una controladora en cada una de las sedes centrales de Canal. Estas controladoras actuarán como nodo central de agregación y gestión del tráfico proveniente de los distintos emplazamientos conectados por satélite y estarán gestionados por la plataforma de orquestación, bien a través de enlaces terrestres o satelitales.

Cada controladora se encargará de establecer y mantener los túneles seguros de extremo a extremo con los routers desplegados en los emplazamientos remotos, gestionando el tráfico IP de forma centralizada y segura. Asimismo, permitirá aplicar políticas de red, priorización de tráfico, segmentación mediante VLANs/VRFs y asegurar la conectividad con los sistemas internos de Canal.

Además, estas controladoras funcionarán como punto de terminación de los túneles IPSEC y como enlace entre la red satelital y el entorno LAN/WAN de Canal, garantizando un alto nivel de seguridad, fiabilidad y rendimiento. Su despliegue redundado en ambas sedes centrales (Santa Engracia y Majadahonda) en estado Activo-Pasivo, proporciona resiliencia ante posibles fallos o interrupciones.

Se representa el esquema que ilustra el papel de las controladoras dentro del sistema se presenta en el diagrama de la figura 3.

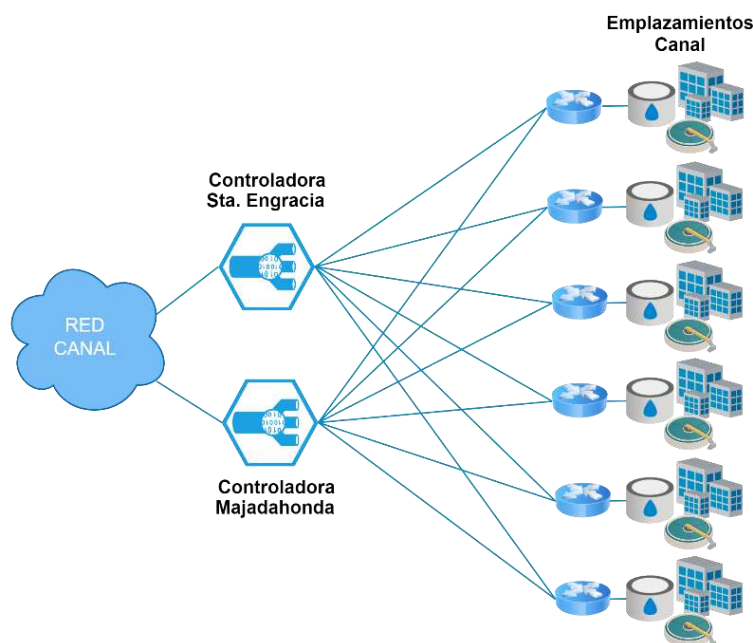


Figura 3: Controladoras en sedes centrales de Canal

2.2.2 Accesos de Banda Ancha Terrestre

Durante la fase de operación, se establecerán dos accesos de banda ancha terrestre mediante fibra óptica dedicada de 1 Gbps simétrico, uno en cada sede central de Canal (Santa Engracia y Majadahonda). Estos accesos constituyen el vínculo principal entre la infraestructura de Canal y el proveedor del servicio, actuando como punto de intercambio de tráfico entre los emplazamientos remotos conectados por satélite y la red de datos interna de Canal.

La provisión dual de accesos garantiza la redundancia y continuidad del servicio, asegurando la conectividad incluso en caso de fallo de uno de los enlaces. Esta diversidad también permite mantener altos niveles de disponibilidad y resiliencia en la comunicación.

Los accesos de fibra serán los encargados de transportar el tráfico tunelizado desde y hacia las estaciones remotas, permitiendo que este llegue a las controladoras ubicadas en las sedes centrales para su procesamiento y entrega al entorno LAN de Canal. Asimismo, estos accesos servirán de canal de comunicación entre el orquestador residente en la nube y los distintos componentes desplegados en el terreno.

Su papel es, por tanto, crítico para la correcta operación del sistema satelital y para el aseguramiento de una conectividad segura, estable y eficiente entre todos los nodos de la red.

En la figura 4 se representa la conectividad de los accesos desde los Datacenters de interconexión con el proveedor, hasta las controladoras ubicadas en cada una de las sedes centrales de Canal.

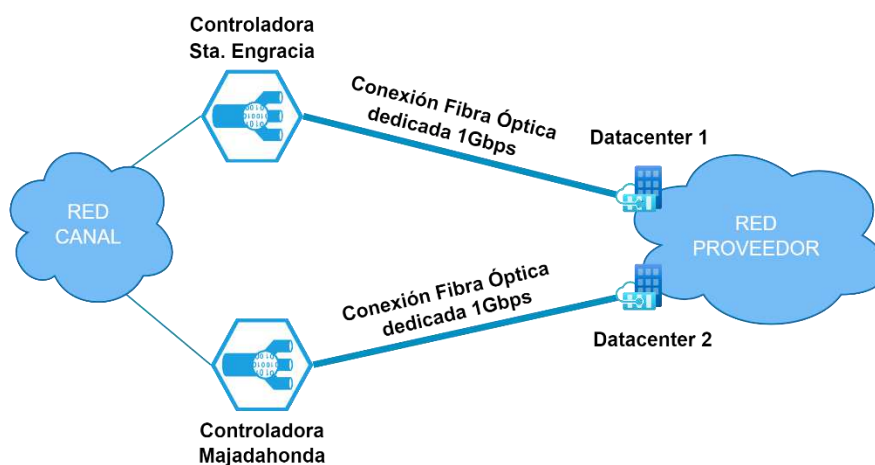


Figura 4: Accesos de banda ancha terrestre

2.2.3 Orquestador Central Residente en la Nube

Servicio de uso y acceso a la plataforma del orquestador central residente en la nube para la operación y control de todas las estaciones y controladoras, monitorización continua, control de redundancia, graficado de transferencia de datos y disponibilidad del servicio en tiempo real, así como la gestión de toda la solución completa. Incluye la implementación y desarrollo de dicho orquestador, así como su mantenimiento, la integración con la red de Canal y su sistema de alarmas SNMP y soporte técnico 24x7. Además, se integrará con el sistema de monitorización de Canal para la gestión de reporte de las incidencias y se proveerá de una herramienta de gestión de tickets para el seguimiento y control de incidencias por ambas partes.

2.2.4 Redundancia, Soporte y Escalabilidad

El adjudicatario deberá implementar soluciones de redundancia automática y manual en el orquestador central residente en la nube, para garantizar la disponibilidad inmediata del servicio en caso de fallo en la sede principal de Canal.

La solución deberá ser escalable tanto en número de emplazamientos como en capacidad de tráfico, permitiendo añadir nuevos nodos y gestionar mayores volúmenes de datos sin afectar al rendimiento,

al menos hasta un total de doscientos (200) emplazamientos. Además, deberá facilitar la evolución tecnológica de Canal, adaptándose fácilmente a nuevas arquitecturas de red o integraciones futuras, gracias a una arquitectura modular y flexible gestionada desde el orquestador.

2.2.5 Ciberseguridad del servicio

La seguridad en la red es un aspecto vital, especialmente para una infraestructura crítica como la de Canal. Alineado con el requerimiento de certificación de la solución en el Esquema Nacional de Seguridad enunciada en el PCAP del contrato, se deben implementar medidas robustas de ciberseguridad para proteger contra amenazas y garantizar la integridad y confidencialidad de los datos. Esto incluye la utilización de encriptación avanzada, firewalls de última generación y sistemas de detección y prevención de intrusiones. Además, se debe asegurar un monitoreo constante y la capacidad de respuesta rápida ante cualquier incidente de seguridad, garantizando así la protección continua de la red y sus usuarios.

2.2.5.1 Presentación de Arquitectura

Al inicio del proyecto y antes de comenzar a implementar la solución, se presentará una arquitectura completa de la misma, que incluirá una descripción detallada de cada componente y los mecanismos de seguridad necesarios para garantizar la confidencialidad, integridad y disponibilidad de los datos gestionados. Esta arquitectura podrá ser revisada por Canal.

2.2.5.2 Sistema de Auditoría Continua

La solución propuesta será incorporada en el sistema de auditoría continua de Canal, para la realización de todas las auditorías de seguridad que se identifiquen como necesarias. El adjudicatario quedará obligado a subsanar todos los problemas de seguridad detectados antes de la puesta en producción de la solución ofertada.

2.2.5.3 Resolución de Problemas de Seguridad

Durante toda la vida del proyecto, el adjudicatario deberá resolver todos los problemas de seguridad que se detecten en la solución, ya sea por organismos oficiales que supervisan a Canal como operador crítico (INCIBE-CERT, CCN-CERT), o por el propio Canal.

3. Especificaciones técnicas de cada subsistema

3.1 Conectividad Satelital en Estaciones Fijas

3.1.1 Objetivo y Características Principales

El servicio satelital cubrirá un total de sesenta y tres (63) emplazamientos fijos, concentrados casi en su totalidad en la Comunidad de Madrid y provincias limítrofes. Actualmente, hay un (1) emplazamiento operativo en la provincia de Cáceres, con la posibilidad de habilitar hasta uno (1) o dos (2) adicionales en función de necesidades futuras, si bien estos casos serán excepcionales.

3.1.2 Requisitos Mínimos de la Conectividad

Por cada uno de los emplazamientos, se requiere un acceso a Internet a través de satélite LEO con las siguientes características:

- **Throughput (pico):** 220 Mbps (download) / 40 Mbps (upload)
- **Latencia:** 20–60 ms
- **Volumen máximo de tráfico de datos mensual:** Datos ilimitados (garantizando velocidad de pico hasta 1TB)
- **Dirección IP:** Una dirección IP pública en cada emplazamiento
- **Prioridad de red y soporte de prioridad**
- **Routing:** Posibilidad de routing nivel 2/3
- **Encriptación:** AES
- **Gestión de redundancia WAN**
- **Encapsulación:** Soporte de tecnologías de encapsulación Ethernet Over IP (como GRE, VxLAN, o soluciones equivalentes)
- **Transmisión segura:** El servicio ofertado debe garantizar la transmisión transparente y segura de todo tipo de tráfico de extremo a extremo, es decir, desde las estaciones fijas hasta la red interna de Canal
- **Gestión de VLANs/VRFs:** de manera automatizada y/o gestionada desde el orquestador central residente en la nube

3.2 Conectividad Satelital Para las Estaciones de Uso Itinerante

3.2.1 Objetivo y Características Principales

Se requiere la puesta en marcha y operación de tres (3) estaciones satelitales de uso itinerante, con equipamiento de alto rendimiento (High Performance) detallado en apartado [4.2.2](#), diseñadas para ofrecer conectividad de banda ancha mediante acceso satelital LEO en escenarios de movilidad y contingencia. Estas estaciones estarán destinadas a los siguientes usos:

- **Unidad móvil de emergencias TETRA:** Dos (2) unidades se instalarán en la unidad móvil de emergencias TETRA de Canal: una como estación principal y otra como sistema de respaldo (backup), ambas estarán plenamente operativas y podrán ser activadas o desactivadas de forma autónoma por el personal de Canal, según las necesidades de operación.
- **Estación de emergencia:** Una tercera unidad (1) estará destinada a prestar conectividad de respaldo en situaciones de incidencias de red en ubicaciones sin cobertura, actuando como estación de emergencia de despliegue ágil.

Estas estaciones proporcionarán acceso a Internet con las mismas características y requisitos técnicos establecidos en el punto 3.1 para las estaciones fijas, garantizando un servicio y gestión unificados.

3.3 Conectividad Estaciones Terrestres Gestionables

3.3.1 Objetivo y Características Principales

En determinados emplazamientos aislados de Canal, donde ya existe una conexión de banda ancha terrestre (fibra óptica o redes móviles 4G/5G) y no se prevé la instalación de antena satelital por razones técnicas, materiales u operativas, se requiere garantizar una conectividad segura, gestionada y monitorizada hacia la red de datos de Canal.

Asimismo, se considera necesario extender esta solución como mecanismo de contingencia aplicable a cualquier emplazamiento (incluidos aquellos con conexión satelital), para garantizar continuidad de servicio en caso de fallo en el enlace principal.

Para ambos escenarios, se requiere la provisión de un subsistema de veinte (20) routers encapsuladores, que reciben la denominación de Estaciones terrestres gestionables dentro del presente proyecto.

3.3.2 Requisitos Mínimos de los Dispositivos

Estos dispositivos deben cumplir los siguientes requerimientos:

- Tunelizar el tráfico IP generado en los emplazamientos, garantizando una transmisión segura y transparente de extremo a extremo hacia la red interna de Canal.
- Estar completamente integrados en la plataforma de gestión, monitorización y control de la red satelital, permitiendo una supervisión unificada.
- Aprovechar las conexiones de banda ancha existentes (no satelitales) existentes para el envío de datos, diferenciándose únicamente del resto de estaciones en el medio de transporte utilizado.
- Mantener una configuración funcional equivalente a la de los routers instalados en las estaciones con conectividad satelital, replicando la misma lógica de encapsulación, políticas de red y gestión remota.

Este subsistema garantiza que todas las estaciones, independientemente del tipo de acceso a Internet utilizado, queden plenamente integradas en el entorno de comunicaciones definido por la solución satelital.

3.4 Servicio de Conectividad por Fibra Óptica en Sedes Centrales

3.4.1 Objetivo y Características Principales del Servicio

Se deberá proporcionar acceso fijo al proveedor de servicio mediante fibra óptica dedicada y garantizada, en las siguientes ubicaciones:

- Oficinas centrales de Canal en Santa Engracia (C/ Santa Engracia, 125)
- Oficinas de respaldo de Canal en Majadahonda (ETAP de Majadahonda)

El servicio deberá reunir, como mínimo, las siguientes condiciones:

- Fibra óptica dedicada empresarial (no se admiten servicios de fibra compartida o FTTH).
- Tráfico entregado mediante conexión directa a nivel de operador.

Estas medidas garantizarán una conectividad estable, segura y de alto rendimiento para la operación de la infraestructura de comunicaciones de Canal.

3.4.2 Características Técnicas del Servicio

El servicio deberá cumplir las siguientes características técnicas:

- Capacidad: Dos conexiones de 1 Gbps simétricos cada una, entre el proveedor de servicio satelital y las sedes centrales de Canal.
- Diversidad geográfica: Cada conexión deberá establecerse a través de Datacenters TIER III distintos, asegurando alta disponibilidad y resiliencia.
- Seguridad de la transmisión: El tráfico IP de los emplazamientos deberá ser tunelizado hacia la red interna de Canal, garantizando su confidencialidad y transparencia extremo a extremo.
- Tráfico ilimitado: No se aceptarán restricciones de volumen de descarga (o cargos adicionales). Se admite la implementación, por parte del proveedor, de una política de uso justo (Fair Use Policy - FUP) a fin de facilitar la gestión de su red en el ámbito de conexiones de tipo empresarial como las demandadas. En todo caso, dicha FUP no deberá ser inferior a un volumen de transferencia mensual de 1 TB por emplazamiento.
- Direcciones IP públicas: Se deberá asignar una IP pública a cada una de las conexiones entregadas.

3.4.3 Independencia del Operador de Red

El adjudicatario será responsable de garantizar un servicio homogéneo, estable y de calidad, independientemente de los operadores de red utilizados para prestar la conectividad. La integración y gestión de las conexiones deberá ser completamente transparente para Canal.

3.5 Orquestador Central Residente en la Nube

3.5.1 Objetivo y Características Principales del Servicio

Como parte fundamental de la solución tecnológica a implantar, se deberá proporcionar, integrar y mantener un sistema orquestador central residente en la nube. Este orquestador actuará como punto único de provisión, despliegue y gestión de los componentes de la red, permitiendo una administración centralizada y unificada de toda la infraestructura.

El sistema deberá ofrecer una visibilidad completa de la red, integrando en una misma interfaz todos los elementos desplegados: desde los routers instalados en estaciones fijas, estaciones terrestres gestionables y unidades móviles, hasta las controladoras ubicadas en las sedes centrales de Canal. Desde este orquestador se gestionarán centralizadamente todas las conexiones de los emplazamientos, así como los enlaces satelitales LEO y las líneas de respaldo por banda ancha terrestre.

El orquestador permitirá:

- Representar gráficamente el estado de la red y de los diferentes emplazamientos sobre un mapa esquemático.
- Visualizar de manera intuitiva el estado operativo de cada nodo mediante un sistema de colores.
- Mostrar bitrate de entrada y salida, tasa de errores, disponibilidad en tiempo real y estadísticas de conectividad para cada emplazamiento.
- Consultar el consumo mensual de datos de cada estación.
- Generar informes periódicos y bajo demanda sobre el estado de los equipos, el rendimiento de la red y las actividades realizadas por los diferentes perfiles de usuario.
- El acceso a la plataforma deberá realizarse a través de una interfaz web segura HTTPS, estando disponible desde cualquier dispositivo con conexión a Internet. El sistema de autenticación se basará en roles, permitiendo configurar perfiles de acceso diferenciados (administrador, supervisor, operador).

Además de las capacidades de supervisión, el orquestador deberá permitir de forma remota:

- Activar y desactivar túneles de comunicación, controlando así la apertura o cierre de servicios en los emplazamientos.
- Configurar las VLANs y asignaciones de red de cada estación.

- Cambiar la controladora activa entre la sede principal y la sede de respaldo (Majadahonda), tanto de forma manual como de manera automática en función de criterios predefinidos.
- Automatizar tareas de gestión de la redundancia y recuperación ante incidencias, asegurando la continuidad operativa.

El orquestador será una herramienta esencial para el control operativo de la red, proporcionando al personal técnico de Canal un entorno flexible, seguro y eficiente para supervisar, gestionar y optimizar toda la infraestructura de comunicaciones desplegada.

3.5.2 Requisitos Técnicos Mínimos del Orquestador

Para asegurar la continuidad del servicio y la escalabilidad del sistema, el orquestador deberá entregarse en modalidad SaaS (Software-as-a-Service), incluyendo todas las licencias necesarias para su funcionamiento y acceso completo durante la vigencia del contrato.

El adjudicatario será responsable de garantizar:

- El mantenimiento, actualizaciones y soporte técnico del orquestador durante toda la duración del servicio.
- El acceso mínimo para al menos 20 usuarios concurrentes, con la posibilidad de asignar distintos perfiles de acceso (administrador, supervisor, operador).
- La disponibilidad de todas las funcionalidades especificadas en este pliego sin restricciones de licencia adicionales.

En caso de que, por causas técnicas, legales o comerciales, no fuera posible mantener operativo el sistema con el fabricante o proveedor inicialmente propuesto (por ejemplo, debido a restricciones de servicio o cambios en las políticas de disponibilidad internacional), el adjudicatario deberá:

- Sustituir el orquestador por una solución equivalente y completamente compatible, que garantice la continuidad del servicio, sin coste adicional para Canal.
- Asegurar que la migración o sustitución de la plataforma no implique pérdida de funcionalidades ni de datos operativos.

La solución ofrecida deberá contemplar mecanismos de continuidad que permitan garantizar el servicio incluso ante eventos de fuerza mayor o restricciones en el acceso a plataformas satelitales LEO específicas, minimizando el riesgo de interrupciones en la operación de la red de Canal.

Los requisitos técnicos mínimos del orquestador son los siguientes:

- Arquitectura nativa residente en la nube (SaaS).
- Alta disponibilidad, con aplicación de políticas de respaldo automático, alta disponibilidad y redundancia geográfica.
- Interfaz web con acceso cifrado mediante HTTPS.
- Compatibilidad con los protocolos VPN IPsec, GRE y SD-WAN con VxLAN.

Configuración y Gestión:

- El orquestador central debe ser capaz de gestionar toda la configuración y administración de la red desde un único punto. Esto incluirá la configuración de routers, protocolos, encapsulación, activación y configuración de puertos, VLANs, entre otros.
- Configuración inicial: El adjudicatario será responsable de realizar la configuración inicial de todo el sistema, incluyendo la instalación de los dispositivos y el despliegue de las estaciones. Esto deberá realizarse conforme a las especificaciones de Canal y tras pruebas exhaustivas para asegurar la correcta puesta en marcha de toda la infraestructura.
- Cambios posteriores:
 - Para modificaciones sencillas, como la adición de VLANs, activación o desactivación de túneles, o ajustes menores, Canal podrá realizar dichos cambios de forma autónoma mediante el orquestador.
 - Para configuraciones más complejas, como la modificación de routers o controladoras, activación y desactivación de puertos o cambio de modo de los puertos, entre otros, el proveedor deberá gestionar las solicitudes de Canal. Estas solicitudes, a efectos de compromiso de ANS demandado al adjudicatario, tendrán el mismo tratamiento y consideración que incidencias de tipo Leve de acuerdo con el ANS que se enuncia en el apartado 9.1 del Anexo I del PCAP.

Requisitos adicionales del Orquestador:

- Capacidad para gestionar al menos 200 nodos simultáneamente.
- Capacidad de integración mediante SNMP y syslog con el sistema de supervisión superior operado por Canal.
- Visualización en tiempo real y generación de alarmas para diferentes parámetros de los equipos, tales como carga de CPU, memoria, voltajes, temperatura del equipo y del procesador, estado incorrecto de la fuente de alimentación, entre otros.
- Escalabilidad y compatibilidad con futuras integraciones tecnológicas, como la adición de nuevos nodos o tecnologías emergentes, como nuevos satélites o redes de telefonía móvil (terrestre y satelital), para ofrecer redundancia y mejorar la cobertura y resiliencia de la infraestructura.

4. Especificaciones técnicas de los equipos

4.1 Routers

En cada una de las estaciones fijas, estaciones terrestres gestionables y estaciones de uso itinerante, se suministrará y configurará un router compatible con las controladoras instaladas en las sedes centrales. Se contemplan tres formatos de routers, cuya elección dependerá del espacio disponible y de la funcionalidad requerida:

- **Router compacto:** utilizado en aproximadamente el 75% de los casos, en emplazamientos con espacio limitado.
- **Router ampliado:** empleado en el 25% restante, en ubicaciones con mayor capacidad de instalación.
- **Router para estaciones terrestres gestionables:** destinado específicamente a este tipo de estaciones, con características adaptadas a sus necesidades operativas.

4.1.1 Router Compacto

Este modelo se utiliza principalmente en emplazamientos con restricciones de espacio, como armarios murales o racks reducidos. Debe cumplir las siguientes características técnicas:

- **Formato:** Tamaño máximo 115 x 90 x 30 mm
- **Rendimiento:** Velocidad igual o superior a 1 Gbps de tráfico de datos
- **Memoria:** RAM superior a 256 MB
- **Alimentación directa AC:** Fuente 100-240 voltios AC
- **Puertos GbE (GigaBit Ethernet):** Al menos 5 puertos GbE (WAN y LAN)
- **POE (Power over Ethernet):** Al menos un puerto con salida POE y un puerto con entrada POE
- **SFP:** Conector para módulo SFP
- **Conectividad:** Soportar SD-WAN, túneles VPN, GRE/IPSEC, y tecnología Ethernet over IP (simultáneo a las dos controladoras)
- **Gestión:** Gestionables y configurables desde el orquestador central residente en la nube

4.1.2 Router Ampliado

Este modelo se instala en ubicaciones con espacio suficiente para equipos de mayor tamaño. Debe cumplir las siguientes características técnicas:

- **Formato:** Tamaño máximo 230 x 120 x 30 mm
- **Kit de enracado:** Posibilidad de montaje en 1U de bastidor
- **Rendimiento:** Velocidad igual o superior a 1 Gbps de tráfico de datos
- **Memoria:** RAM superior a 1 GB

- **Alimentación directa AC:** Fuente 100-240 voltios AC
- **Puertos GbE (GigaBit Ethernet):** Al menos 10 puertos GbE (WAN y LAN)
- **POE (Power over Ethernet):** Al menos un puerto con salida POE y un puerto con entrada POE
- **SFP:** Conector para módulo SFP+
- **Conectividad:** Soportar SD-WAN, túneles VPN, GRE/IPSEC, y tecnología Ethernet over IP (simultáneo a las dos controladoras)
- **Gestión:** Gestionables y configurables desde el orquestador central residente en la nube

4.1.3 Router para Estaciones Terrestres Gestionables

Este tipo de terminales estará destinado al uso de estaciones terrestres gestionables. Estos deben cumplir las siguientes características técnicas:

- **Formato:** Tamaño máximo 115 x 90 x 30 mm
- **Rendimiento:** Velocidad igual o superior a 1 Gbps de tráfico de datos
- **Memoria:** RAM superior a 256 MB
- **Alimentación directa AC:** Fuente 100-240 voltios AC
- **Puertos GbE (GigaBit Ethernet):** Al menos 5 puertos GbE (WAN y LAN)
- **POE (Power over Ethernet):** Al menos un puerto con entrada POE
- **Puerto USB:** USB 2.0.
- **Conectividad:** Soportar SD-WAN, túneles VPN, GRE/IPSEC, y tecnología Ethernet over IP (simultáneo a las dos controladoras)
- **Gestión:** Gestionables y configurables desde el orquestador central residente en la nube
- **Capacitación:** Capacitación del personal de Canal en el uso y gestión de los routers, asegurando que puedan operar y mantener los equipos de manera eficiente, desde el orquestador central residente en la nube.

4.2 Antena Satelital LEO (+ Router Satelital)

En cada una de las estaciones fijas y en las estaciones de uso itinerante, se instalará una antena satelital para satélite LEO, que incluirá su correspondiente router satelital instalado en el interior del emplazamiento o vehículo. Para cada tipo de emplazamiento, las antenas satelitales requerirán unas características específicas mínimas que deben cumplir, determinando dos tipologías: estándar y High Performance.

4.2.1 Requisitos Técnicos de la Antena Satelital Estándar

En el equipamiento requerido para las estas estaciones fijas se debe incluir una antena satelital estándar con las siguientes características técnicas mínimas:

- **Tipo de antena:** Electronic Phase Array (antena de matriz de fase electrónica)
- **Campo de visión:** 110°
- **Orientación:** Manual (asistida por Software)
- **Grado de protección:** IP67 Tipo 4
- **Rango de temperatura:** -30 °C a +50 °C
- **Resistencia al viento:** 96 km/h
- **Capacidad de derretimiento de nieve:** 40 mm/h
- **Consumo eléctrico medio:** 75–100 W

4.2.2 Requisitos Técnicos de la Antena Satelital High Performance

En el equipamiento requerido para las unidades móviles se debe incluir una antena de alto rendimiento (High Performance), diseñada para su instalación permanente en vehículos y con las siguientes características técnicas mínimas:

- **Tipo de antena:** Electronic Phase Array (antena de matriz de fase electrónica)
- **Campo de visión:** 140°
- **Orientación:** Fija
- **Grado de protección:** IP56
- **Rango de temperatura:** -30 °C a +50 °C
- **Resistencia al viento:** 280 km/h
- **Capacidad de derretimiento de nieve:** 75 mm/h
- **Consumo eléctrico medio:** 110–150 W

Para este tipo de antenas, se requerirá un mecanizado del soporte *ad hoc* en el mástil del vehículo móvil, que permita el montaje, anclaje y desmontaje ágil de la antena durante los despliegues. En el replanteo a realizar previo al montaje, entre Canal y el adjudicatario se definirán los detalles de este mecanizado a realizar.

4.3 Controladoras (Gateways)

4.3.1 Características Técnicas Mínimas de las Controladoras

Se suministrará un Gateway por cada sede central de Canal. Estos deben cumplir las siguientes características técnicas:

- **Puertos:** Al menos 13 puertos GbE (WAN y LAN)
- **POE (Power over Ethernet):** Al menos un puerto con salida POE

- **Formato:** Unidad de rack 1U
- **Rendimiento:** Velocidad superior a 7,5 Gbps de tráfico de datos
- **Memoria:** RAM superior a 1 GB
- **Alimentación:** PoE (Power over Ethernet) y fuente redundante (100-240 Vac)
- **Conectividad:** Acceso wireless y cableado, soportar SD-WAN, túneles VPN, GRE/IPSEC, y tecnología Ethernet over IP
- **Seguridad:** Encriptación AES, firewall capa 4-7 (PEF), y solución de seguridad y protección
- **Gestión:** Redundancia WAN, visualización y resolución de problemas de red (MOS, latencia, jitter, pérdida de paquetes), gestionable y configurable desde el orquestador central
- **Capacidad de usuarios:** Hasta 2048 usuarios concurrentes
- **VLAN:** Manejo de hasta 4096 VLAN

5. Mantenimiento y disponibilidad del servicio

El adjudicatario deberá garantizar el mantenimiento continuo de los servicios y equipos detallados en los apartados 3 y 4, así como las actualizaciones de software (SW) que se requieran.

Este mantenimiento incluirá la reparación o sustitución de los equipos instalados en los emplazamientos de Canal, asegurando la disponibilidad continua del servicio conforme a los términos establecidos en el contrato.

El mantenimiento y disponibilidad engloba:

- **Gestión de Servicio E2E:** El servicio debe ser gestionado de forma End-to-End (E2E), asegurando que el adjudicatario se encargue de la totalidad del proceso, desde la provisión de equipos hasta la atención y resolución de incidencias.
- **Mantenimiento Integral:** El servicio debe ofrecer un mantenimiento integral, lo que incluye, sin coste adicional, todas las visitas necesarias a las sedes o emplazamientos de Canal en caso de incidencias o situaciones similares que requieran intervención técnica. A fin de facilitar la valoración del esfuerzo y tiempo que requieren los desplazamientos necesarios, se agrupan en la siguiente tabla el porcentaje de emplazamientos (los puntos de instalación de equipamiento) según su distancia la sede de Oficinas Centrales de Canal, sita en la calle Santa Engracia 125, 28003, Madrid.

Distancia (Km)	%
0-30	29,3%
30-70	47,9%
70-100	19,7%
>100	2,7%

El servicio de mantenimiento incluirá:

- **Operación y mantenimiento del servicio:** mantenimiento continuo tanto del software como del hardware de todos los equipos, asegurando su correcto funcionamiento y actualización. Provisión de soporte técnico especializado disponible las 24 horas del día, los 7 días de la semana, para resolver cualquier incidencia o problema que pueda surgir en la condiciones y compromisos que enuncia el ANS descrito en apartado 9.1 del Anexo I del PCAP del contrato.
- **Herramienta de ticketing:** para la comunicación y seguimiento de incidencias en el servicio.
- **Actualización de Software:** Implementación de actualizaciones de software periódicas para garantizar la seguridad y el rendimiento óptimo de todos los equipos.
- **Monitoreo y gestión proactiva mediante el orquestador central en la nube:** Monitoreo constante del rendimiento de todos los equipos y gestión proactiva para prevenir posibles fallos y optimizar su funcionamiento.

- **ANS:** El adjudicatario deberá garantizar que los tiempos de respuesta y los niveles de servicio cumplan con los Acuerdos de Nivel de Servicio (ANS) establecidos en el Anexo I del PCAP. Será responsable de la reparación, reemplazo o solución de los equipos proporcionados, asegurando que cualquier incidencia se resuelva de forma que se mantenga la disponibilidad del servicio, cumpliendo con los ANS definidos. Todos los equipos son propiedad del adjudicatario, quien se encargará de su mantenimiento y funcionamiento continuo durante la duración del contrato

6. Formación

6.1 Objetivo

El objetivo de la formación es proporcionar a los técnicos del Canal un conocimiento profundo y global de la solución, de modo que puedan asumir la gestión, el control y el mantenimiento de los servicios de manera eficaz y con todas las garantías necesarias. A lo largo del curso, los participantes adquirirán las competencias necesarias para operar y mantener los sistemas de comunicación satelital de manera avanzada, cubriendo tanto los aspectos técnicos como operativos.

6.2 Temario

El temario abordará los siguientes puntos principales, aunque Canal, en conjunto con el adjudicatario, definirá los puntos definitivos y posibles adicionales que puedan considerarse de interés:

- **Introducción a las Tecnologías Satelitales:** Tipos de satélites (Geoestacionarios, LEO, MEO) y comparación entre los diferentes sistemas.
- **Conectividad y Equipos Asociados:** Equipos de conexión satelital (controladoras, equipos remotos, antenas, cableado y conectores) e integración de los sistemas de comunicación vía satélite.
- **Soluciones de Conectividad para Puntos Fijos y Móviles:** Implementación de soluciones para puntos fijos remotos y unidades móviles, continuidad de servicio y posibles soluciones futuras.
- **Gestión y Monitoreo de toda la red implementada mediante el orquestador:**
 - Manejo de la plataforma de orquestación residente en la nube: configuración y activación/desactivación de emplazamientos, gestión de redundancia.
 - Monitorización, configuración de alarmas, visualización de informes y análisis de datos.
 - Gestión de incidencias y herramientas de ticketing.

6.3 Formato y Organización

Se impartirán un curso, en dos turnos, a lo largo de la duración del contrato:

- **Duración total:** Curso impartido en dos turnos de 15 horas cada uno.
- **Duración por curso:** 15 horas (de cada turno) distribuidas en 3-4 jornadas.
- **Asistentes:** 15 personas.
- **Medios y sala:** Aportados por el Canal en modalidad presencial.
- **Fechas:** A determinar según la disponibilidad y necesidades del Canal.

7. Ejecución del proyecto de puesta en marcha del servicio

7.1 Plan General de Proyecto

El adjudicatario deberá facilitar, en el plazo de 1 mes tras la firma del Acta de Inicio de los Trabajos, un Plan General del Proyecto (PGP) donde se describan los plazos de ejecución de las diferentes actividades implicadas, momentos de puesta en operación, interlocutores, herramientas de gestión etc. y otras circunstancias.

7.2 Ejecución de los Trabajos

7.2.1 Preparación del Despliegue

De forma previa se realizarán los trabajos previos de suministro e instalación del equipamiento necesario para la prestación del servicio demandado. La empresa adjudicataria deberá realizar los trabajos de replanteo de emplazamientos que sean necesarios para la ejecución del proyecto cumpliendo las especificaciones aquí descritas. Con relación a este aspecto, el adjudicatario realizará, como mínimo las siguientes tareas:

- Plan de Trabajo Final.
- Obtención del material y maquinaria necesaria para la ejecución del proyecto.
- Selección del equipo humano para la realización de trabajos. Toda la gestión y trámites necesarios para la consecución de los permisos y licencias necesarios correrán a cargo del adjudicatario del proyecto.
- Plan de Seguridad y Salud para los trabajos objeto del contrato.
- Metodología para la supervisión de las instalaciones.
- Plan de Medidas medioambientales de aplicación a los trabajos.

7.2.2 Suministro

Los materiales se protegerán contra la corrosión, humedad, rotura o daños que se puedan producir durante su transporte, almacenamiento o montaje.

Los costes de transporte, almacenamiento, seguros, y otros, correrán a cuenta del adjudicatario, de forma que la entrega final del equipamiento será instalado, configurado y en funcionamiento.

7.3 Instalación

7.3.1 Trabajos Previos a la Instalación

De forma previa a la instalación, se deberá realizar una revisión de los trabajos que es necesario llevar a cabo en cada uno de los emplazamientos considerados, con el fin de adecuarlo a la futura instalación. Esta revisión se realizará de forma conjunta entre el director del contrato y el representante de la empresa adjudicataria designado por ésta.

Como mínimo se deberán considerar los aspectos que se recogen a continuación:

- Se definirán las áreas concretas donde se va a instalar y se realizarán las mediciones oportunas.
- Se comprobará que las áreas donde se va a trabajar cumplen las condiciones de seguridad, higiénicas y ambientales necesarias para la ejecución de los trabajos.
- Se elaborarán las actas de replanteo.
- Se elaborará un documento de replanteo que detalle los trabajos a realizar, el recorrido del cable, la ubicación final de la antena y de los equipos, y consideraciones técnicas y de seguridad para tener en cuenta en la instalación, y que incluya también un fotomontaje en el que se observe la situación actual y futura tras la instalación. Este documento será revisado por Canal y, solamente cuando sea aprobado, se procederá con la instalación.

7.3.2 Trabajos de Instalación

Dentro de los servicios de instalación, el adjudicatario deberá realizar, al menos, los siguientes trabajos:

- Instalación de los equipos en los armarios o en las ubicaciones correspondientes.
- Identificación y etiquetado de los equipos en los armarios donde vayan alojados y de los cables de conexión y de alimentación eléctrica. Todo el cableado será identificado en sus extremos, conexiones y en el armario repartidor de cableado.
- Tendido y conexionado de todos los cables y latiguillos necesarios para la conexión entre los distintos equipos o módulos suministrados. La totalidad del tendido de cableado en el exterior de los emplazamientos deberá realizarse obligatoriamente bajo tubo de acero galvanizado, no siendo válidos los tendidos con tubo de aceroflex o canaleta PVC, evitando así el degradado y corrosión que se pueda producir con el tiempo. Para el cableado interior si se permitirá el uso de canaleta de PVC. Los soportes, mástiles y anclajes necesarios para la sujeción de la antena satelital, también deberán ser de acero galvanizado.
- Con objeto de lograr un alto grado de calidad en el nivel de acabado de la instalación, se contemplarán pequeños remates, tapados de huecos y pintado, tanto de tapas y chapas como de muebles afectados por la instalación, así como la instalación de nuevas cajas de registro en exterior o en interior para el paso de los cables en caso de ser necesarias.
- Para asegurar un correcto funcionamiento y evitar pequeños cortes del servicio que se pudieran producir por cimbres o oscilaciones en la antena satelital debidas al viento, se instalarán, si es preciso, riostras o elementos mecánicos de obra civil para minimizar o tratar de eliminar dicho movimiento.

El transporte, seguros, así como todo el material necesario para la instalación del equipamiento correrá por cuenta del adjudicatario. Las ofertas deberán incluir todos los servicios, materiales y equipos necesarios para la instalación de los equipos suministrados.

El adjudicatario ha de disponer de todas las herramientas, aparatos, equipos de medida, material de seguridad, así como el personal técnico adecuado con la preparación y experiencia necesarias para llevar a cabo las tareas requeridas para la ejecución del contrato.

Asimismo, los trabajos deberán realizarse siguiendo las normas básicas de seguridad e higiene, debiendo quedar las instalaciones, como mínimo, en las mismas condiciones de limpieza en las que se encontraron.

Durante el período de instalación del equipamiento, se interferirá lo menos posible a aquellos servicios e instalaciones existentes en el emplazamiento.

7.4 Aceptación de las Instalaciones

El adjudicatario presentará, con una anticipación no inferior a cinco (5) días de su fecha de finalización, la relación de pruebas de aceptación in situ de la instalación, que se realizarán para comprobar su calidad y operatividad.

Los protocolos de aceptación se someterán a la aprobación de Canal y serán realizados dentro del plazo de ejecución del contrato.

Las pruebas contempladas en los protocolos de aceptación serán realizadas por el adjudicatario, a su cargo, y el personal designado por Canal.

Sí no supera con éxito las pruebas contempladas en los protocolos de aceptación, Canal no dará autorización para la aceptación de la instalación hasta que el problema no se haya superado.

Una vez superadas las pruebas, se entregará la documentación As-built del equipamiento instalado, para que Canal de su aprobación y proceda al acto de recepción, tras haber verificado a su entera satisfacción la corrección de la totalidad de los suministros, instalaciones, y en general el correcto funcionamiento y operación del conjunto de la red implantada.

7.5 Desinstalación de equipamiento

Una vez finalizado el plazo del servicio el adjudicatario tendrá un plazo de 2 meses para la desinstalación y retirada del equipamiento de su propiedad ubicado en instalaciones de Canal y que haya sido necesario para la prestación del servicio.

7.6 Plan de Seguridad y Salud

El adjudicatario deberá realizar un Plan de Seguridad y Salud y entregar a Canal debidamente cumplimentado.

Al inicio del contrato, se realizará una reunión CAE (Coordinación de Actividades Empresariales). En este encuentro, se coordinarán las actividades de las diferentes empresas que comparten un mismo espacio de trabajo, se establecerán protocolos preventivos y de emergencia, y se compartirá información relevante para garantizar la seguridad de todos los trabajadores.

8. Gestión del servicio

8.1 Plan de Gobierno del Servicio

Canal considera que, para el éxito de este proyecto, es imprescindible un Plan de Gobierno del Servicio sólido y consistente, capaz de que los servicios externalizados evolucionen de acuerdo con la evolución del negocio y de la tecnología.

En este apartado se describe el Modelo de Gestión requerido por Canal. El adjudicatario deberá facilitar, en el plazo de 1 mes tras la firma del Acta de Inicio de los Trabajos, un Plan de Gobierno del Servicio que deberá describir con detalle suficiente la organización de su equipo de trabajo, tanto para los servicios centralizados en sus instalaciones, como para aquellos técnicos que deban desplazarse a ubicaciones de Canal. Esta descripción debe incluir el detalle de los procedimientos, políticas, guías y herramientas que utilizará durante la vigencia del contrato para la gestión y supervisión de los servicios, de los equipos de trabajo propios y, en su caso, de los de terceros o subcontratados implicados en la prestación de los servicios.

En su diseño, el proveedor debe adaptarse al Modelo de Gestión que se describe a continuación.

El proveedor debe establecer y detallar en su propuesta, los requerimientos de su modelo organizativo respecto a la participación de personal de Canal.

8.1.1 Gestión de los Servicios

El proveedor será el responsable de la gestión, ejecución, supervisión técnica y control diario de los servicios prestados y de que estos se presten de acuerdo con los niveles de servicio acordados con Canal.

El objetivo que persigue Canal es disponer de un entorno de gestión estándar que permita realizar cambios o incorporaciones durante el contrato o tomar decisiones a su finalización, sin impacto significativo en el usuario de estos.

8.1.2 Gestión de la Relación

Para la gestión de la relación se tendrán presentes los siguientes principios que se consideran clave para el éxito de este proyecto:

- Asegurar que se dispone de la necesaria flexibilidad y agilidad para responder a las necesidades comunicadas desde las Áreas de Canal.
- Asegurar que se puede responder eficientemente a los cambios en el entorno de negocio de Canal.
- Asegurar que la relación definida incluye de forma proactiva la innovación y que esta se traduce en beneficios para Canal.

En el siguiente apartado se describe el Modelo de Relación (Modelo de Referencia de Gestión del Servicio) requerido habitualmente por Canal. No obstante, Canal no precisa de un modelo cerrado por lo que permitirá al adjudicatario, basándose en las principales directrices y niveles de este modelo, diseñar su propio Plan de Gobierno del Servicio.

8.1.3 Modelo de Gestión del Servicio

Canal tiene como objetivo llevar a cabo una gestión activa e integrada de la entrega de los servicios en dos niveles: estratégico y táctico-operativo. Para ello espera que el proveedor implemente un Sistema de Gestión del Servicio que permita a Canal realizar la gestión continua y en todos los niveles.

Nivel Estratégico.

Debe proporcionar una visión global que permita:

- Controlar el cumplimiento del contrato.
- Controlar que los niveles de servicio responden a las necesidades de negocio para mantener la alineación con los objetivos corporativos.
- Controlar el cumplimiento global de los niveles de servicio y que se produce una mejora continua de su calidad.
- Controlar la evolución del consumo de servicio y su coste asociado (ratios de coste).

En el nivel de gestión estratégica se establece el **Comité de Dirección**, en el que participa Canal y el adjudicatario asignando cada uno un Director del Servicio, capaces de asegurar el nivel de decisión y compromiso que requieren las disposiciones estratégicas requeridas a este nivel del modelo. Entre otras, son responsabilidad del Comité de Dirección:

- Aprobar los cambios en el ámbito del Servicio propuestos por el Comité de Seguimiento y Control.
- Aprobar los cambios al Contrato propuestos por el Comité de Seguimiento y Control
- En general, discutir cualquier incidencia o problema surgido durante la ejecución del Servicio.
- Ejecutar cualquier otra actividad relacionada con la dirección estratégica que pueda surgir a lo largo del Servicio.
- Resolver cualquier conflicto continuado entre los participantes en el proyecto, que no haya sido posible resolver tras un periodo de tiempo razonable por otros niveles de gestión subordinados dentro del presente Modelo de Relación.

El Comité de Dirección se reunirá semestralmente o con la frecuencia que razonablemente se considere necesaria o dentro de los 10 días laborables siguientes a una petición por escrito de cualquiera de las partes.

Niveles Táctico y Operativo.

Debe proporcionar una visión de detalle que permita:

- Controlar el cumplimiento de los niveles de servicio.
- Monitorizar y ajustar los niveles de servicio.
- Seguimiento y control de fallos, incidencias y problemas.
- Control y seguimiento de la capacidad.
- Seguimiento, control y ajuste de la asignación de tareas y de recursos.
- Seguimiento y control de la ejecución de tareas y trabajos.

- Maximizar el uso de los servicios del proveedor.
- Conocer el detalle de los consumos y precios de los servicios.

Estos niveles contarán con sendos **Comité de Seguimiento y Control** y **Comité Operacional**.

En un **nivel de gestión táctico**, Canal y el adjudicatario asignarán ambos un Jefe de Proyecto para establecer el Comité de Seguimiento y Control, encargado de dirigir, monitorizar y controlar de la ejecución de todos los servicios. Serán responsabilidades de este Comité, sin limitación:

- Asegurar que se consiguen los niveles de calidad acordados y que, en el caso de deficiencias no resueltas a nivel operativo, se desarrollen e implementen planes de resolución de problemas.
- Monitorizar el estado de los servicios.
- Revisar, actualizar y controlar el cumplimiento de la planificación.
- Coordinar los grupos y personas asignados a la entrega del servicio.
- Discutir nuevos requerimientos o cambios. Revisar y aprobar las Peticiones de Cambio.
- En el caso de que el cambio requiera de cambios en el contrato, deberán revisar el informe de impacto correspondiente. Estos informes deberán ser enviados al Comité de Dirección.
- Asegurar que el personal asignado para la ejecución de los servicios por el adjudicatario está disponible y disponen de los recursos, formación y soporte necesarios para la correcta ejecución de sus tareas.
- Revisar los niveles de servicio medidos en cada periodo, discutir las desviaciones sobre los valores objetivos acordados y calcular, en su caso, las penalizaciones aplicables.
- Servir como punto único de contacto entre las organizaciones de Canal y del adjudicatario para todos los asuntos relacionados nivel de gestión táctico del Servicio.
- Controlar que la facturación se está realizando conforme a los acuerdos y resolver cualquier problema relacionado con el precio o los pagos.
- Revisar y facilitar al Comité de Dirección cualquier información que le sea solicitada.

El Comité de Seguimiento y Control se reunirá al menos mensualmente o con la frecuencia que razonablemente se considere necesaria o después de 1 día laborable tras una petición de cualquiera de los Jefes de Proyecto.

En un nivel de gestión operativo, Canal y el adjudicatario trabajarán en plena coordinación para la consecución de los objetivos de los servicios objeto del contrato. Esta coordinación será asegurada por los Jefes de Proyecto o en quien estos deleguen, abarcando:

- Revisar la lista de tareas pendientes y asignar prioridades
- Revisar y priorizar las peticiones recibidas
- Coordinar los grupos y personas asignados a la entrega del servicio
- Discutir nuevos requerimientos o cambios. Revisar y aprobar las Peticiones de Cambio menores.

- En el caso de que el cambio sea significativo elaborar informe de propuesta para el Comité de Seguimiento y Control.
- Verificar que el personal asignado para la ejecución de los servicios por el adjudicatario está disponible y disponen de los recursos, formación y soporte necesarios para la correcta ejecución de sus tareas.
- Revisar la tendencia de los niveles de servicio y establecer acciones correctoras
- Servir como interlocutor entre las organizaciones de Canal y del adjudicatario para todos los asuntos del día a día relacionados con el Servicio.
- Revisar y facilitar al Comité de Seguimiento y Control cualquier información que le sea solicitada.
- Se establecerán las reuniones de trabajo que se consideren necesarias a petición de cualquiera de las partes.

Cambios del Modelo de Gestión del Servicio

Canal considera como un requerimiento imprescindible contar con estructuras de Gestión del Servicio flexibles, que permitan las modificaciones de aspectos del servicio que sean precisas como consecuencia de cambios en la demanda de servicios de negocio de Canal, o cambios en el entorno de negocio de Canal. Además, debe garantizar que el proyecto se beneficia del avance de la tecnología, tanto en mejoras de calidad de servicio o de la productividad. El licitador debe describir los procedimientos, métodos y herramientas que propone implantar para la gestión de cambios en el Modelo de Servicio planteado. Para ello debe enunciar adecuadamente en su Plan de Gestión del Servicio un Procedimiento de Gestión de Cambios al Modelo de Servicio capaz de gestionar:

- Cambios mayores y menores.
- Cambios en la documentación.
- Cambios en el ámbito de los servicios.
- Cambios como consecuencia de la implantación o ejecución de iniciativas de mejora o de planes de acciones correctoras.
- Cambios en las actividades de negocio (nuevos servicios, abandono de actividades) o en la organización de Canal que impactan en el ámbito, volúmenes o la forma de entrega de los servicios.
- Cualquier otro cambio que pueda afectar a la estructura o contenido del Modelo de Gestión del Servicio que regulan la prestación de los servicios.

Seguimiento e Informes

Se establecen como estándar los informes siguientes:

- Informe mensual: dirigido a los miembros del Comité de Seguimiento y Control para analizar la información requerida en dicho Comité, en especial la actividad del periodo correspondiente (tareas periódicas, tareas bajo demanda e incidencias), el cumplimiento de los indicadores, cuantificando las desviaciones producidas en su caso y la identificación proactiva de problemas en el cumplimiento del Acuerdo de Nivel de Servicio descrito en el Anexo I del PCAP.

- Informe semestral: dirigido a los miembros del Comité de Dirección para analizar la información requerida en dicho comité, en especial recogiendo la evolución de los indicadores de calidad, y la información de los elementos que se consideren más críticos.

Adicionalmente a estos informes, y ante situaciones específicas, el adjudicatario deberá presentar información requerida a demanda de Canal.

9. Requisitos de seguridad de obligado cumplimiento.

Canal de Isabel II, en fase ejecución del contrato, podrá solicitar al adjudicatario el cumplimiento de los siguientes requisitos de seguridad con las evidencias que correspondan para cada uno de ellos (informes, etc.).

PS. Principios de Seguridad de obligado cumplimiento para la prestación de los Servicios:

PS.01 Cumplimiento legal, activo. El adjudicatario debe ser consciente de las obligaciones legales en materia de Tecnologías de la Información (en adelante TI) que adquirirá, en caso de resultar adjudicatario, tales como el Esquema Nacional de Seguridad (ENS) y la Directiva NIS2, referentes a los servicios objeto de contratación por parte de Canal de Isabel II.

Estas obligaciones legales se materializan en obligaciones técnicas tales como la gestión de los incidentes o las evaluaciones, análisis, gestión y tratamiento de riesgos.

El adjudicatario asegurará que, en caso de resultar adjudicatario, informará a Canal de Isabel II de la ubicación geográfica y de los países desde los que presta el Servicio y en los que puede almacenar y tratar la información de Canal de Isabel II, tanto durante la normal prestación de los Servicios, como en caso de contingencia. Además, será obligatorio, salvo que se disponga de autorización expresa, que la prestación de los Servicios se realice desde el Espacio Económico Europeo. Por otro lado, el adjudicatario deberá obtener de Canal de Isabel II autorización para cualquier cambio de ubicación geográfica y de los países.

PS.02 Políticas de Seguridad. El adjudicatario deberá conocer y cumplir las medidas de seguridad recogidas y especificadas y detalladas a continuación. El adjudicatario, deberá tener establecidas Políticas de Seguridad de los Sistemas de Información en su empresa.

PS.03 Responsabilidad. La responsabilidad última de la adecuada gestión de los riesgos asociados con las actividades objeto del contrato recae en la alta dirección de Canal de Isabel II, por lo que la realización de funciones TI por parte de un tercero no debe perjudicar la supervisión de Canal de Isabel II y, por ende, de los servicios que se realicen.

El adjudicatario por tanto es responsable directo de los riesgos TI que se derivan de las actividades que se le han contratado, en la medida de que de él depende el diseño, transformación, construcción y operación de los sistemas, servicios y actividades realizadas objeto de la presente licitación.

El licitador deberá asegurar que, en caso de resultar adjudicatario, dispondrá de las figuras que se indican en el punto RS de este documento.

PS.04 Análisis de Riesgos. El adjudicatario que resulte adjudicatario deberá llevar a cabo un análisis de riesgos conforme al artículo 14 del ENS según la metodología conforme al ENS, que en particular Canal de Isabel II identifica como MAGERIT (herramienta Pilar), salvo que, por indicación contraria y expresa, del Área de Ciberseguridad de Canal de Isabel II se especifique lo contrario. El análisis de riesgos deberá incluir:

- Identificación de los activos que forman parte del proyecto (comunicaciones, hardware, software, personal, etc.)
- Valoración de los Servicios.
- Riesgo Inicial acorde a MAGERIT (Alto, Medio o Bajo).
- Amenazas de seguridad.
- Controles de seguridad que mitiguen las amenazas.
- Riesgo Residual obtenido tras aplicar los controles de seguridad, también acorde a MAGERIT (Alto, Medio o Bajo).

Este Análisis de Riesgos cumple con un doble objetivo: por un lado, el adjudicatario es consciente de los riesgos de ciberseguridad que debe tener en cuenta, y, por otro lado, debe ser consciente que la calidad del Análisis de Riesgos realizado, le permitirá responder más adecuadamente las salvaguardas que le sean de aplicación, una vez gestionado y evaluado el riesgo por Canal de Isabel II.

El Análisis (realizado una vez sea adjudicatario de los Servicios), será compartido con el Área de Ciberseguridad de Canal de Isabel II, ya que formará parte de la evaluación del Riesgo que realizará Canal de Isabel II. El adjudicatario deberá colaborar e implementar bajo el alcance del contrato, aquello que le sea de aplicación.

PS.05 Gobierno de la seguridad. El adjudicatario asegurará de que los servicios prestados en virtud del presente procedimiento de contratación, así como los sistemas de información que los sustentan, se prestan de conformidad a los requisitos de seguridad establecidos en el Esquema Nacional de Seguridad (ENS) contemplados en la categoría MEDIA solicitada como solvencia.

PS.06 Clasificación de la información y de activos. El adjudicatario garantizará la confidencialidad de la información propiedad de Canal de Isabel II conforme a lo indicado en el PCAP, así como la información reservada de autenticación, desplegando los mecanismos de control que procedan en cada caso.

El adjudicatario deberá realizar un tratamiento de la Información teniendo en cuenta la clasificación de la Información que haya realizado el Responsable de la Información y del Servicio de Canal de Isabel II. El adjudicatario debe disponer de un inventario de dicha información (activos, clasificación, valoración y riesgos), siendo su responsabilidad mantenerla al día con rigurosidad, exactitud, completitud y calidad. Así mismo, esa información debe ponerse de forma accesible, práctica y segura a Canal de Isabel II, en particular, al Área de Ciberseguridad de Canal de Isabel II.

Los activos de información, en lo referente a elementos de software (Sistemas Operativos, software base, complementos, aplicaciones y servicios), hardware (sistemas informáticos de red y seguridad), así como cualquier otro elemento que tenga valor para el servicio debe estar adecuadamente documentado. Para esto, se deberá incluir fabricante, marca, modelo, versión, parches, configuraciones, usuarios con derechos de acceso, el detalle de los derechos para los mismos, así como cualquier otra información que se requiera necesaria para su operación, administración y gestión de incidentes, supervisión y auditoría.

PS.07 No Obsolescencia y Gestión de Vulnerabilidades. El adjudicatario asegura que, en caso de resultar adjudicatario, para el alcance del proyecto detallará tanto su estrategia y plan de no obsolescencia, como sus compromisos con la Gestión de las Vulnerabilidades (identificación, remediación, SLAs, etc.).

PS.08 Elementos de seguridad adecuados al entorno Cloud. El adjudicatario garantizará que los sistemas de seguridad tendrán una plena integración con las particularidades de los entornos virtuales, autoescalables, temporales, de *delivered* de configuración por plantillas, *cloudtrail* y VPC logs, de microsegmentación, de SDDCs, de desarrollo ágil, de fusión de DevOps, de microservicios, pipelines y orquestación, etc. que vayan asociados a los entornos de nube específicos para el presente contrato.

El adjudicatario, asegura que, en caso de resultar adjudicatario, describirá su estrategia, metodologías y herramientas / soluciones / activos que se plantea utilizar para lograr este objetivo.

PS.09 Control de la cadena de suministro de la tercera parte. El adjudicatario podrá realizar la subcontratación en los términos y condiciones recogidos en el PCAP y en el PPT. El subcontratista cumplirá totalmente con las obligaciones existentes entre Canal de Isabel II y el adjudicatario, incluidas las obligaciones contraídas a favor de las diferentes autoridades de control.

El adjudicatario deberá informar a Canal de Isabel II de la subcontratación de parte de los Servicios, debiendo cumplir los requisitos correspondientes de seguridad en relación con parte del contrato en que intervenga.

PS.10 Garantías de supervisión.

PS.10.01 Supervisión. El adjudicatario deberá habilitar los mecanismos para garantizar la supervisión del nivel de seguridad por parte del Área de Ciberseguridad de Canal de Isabel II. Esta supervisión incluye, aunque no se limita, a la visión no sólo de los registros de auditoría de aplicaciones, servidores y bases de datos, sino al acceso en modo lectura a las consolas de los diferentes sistemas de seguridad, a los usuarios que tienen permisos en los mismos, a los permisos de éstos, a los eventos, configuraciones, reglas, etc.; en suma, a cuantos elementos permitan a los activos de información que recogen, tratan, transmiten, procesan y almacenan la información propiedad de Canal de Isabel II.

PS.10.02 Trazabilidad. El adjudicatario deberá habilitar suficientes mecanismos para garantizar el registro, auditoría y trazabilidad de los eventos, operaciones, acciones y actividades llevados a cabo y/o materializados en las aplicaciones, microservicios, sistemas e infraestructura involucrados en el servicio. Los registros deberán estar accesibles y disponibles para el Canal de Isabel II en caso de ser requeridos, así como debidamente protegidos.

Debe proveerse de los registros necesarios para unir y trazar la información de red con la de Negocio.

PS.10.03 Auditorías. El adjudicatario deberá permitir y colaborar, en el caso que sea necesario, en las diversas auditorías a las que se encuentra sujeta Canal de Isabel II.

Asimismo, el licitador se compromete a facilitar en todo lo posible a la Oficina Técnica de Seguridad (OTS) de Canal de Isabel II la realización de una prueba de penetración del conjunto de la solución ofertada, en caso de resultar adjudicatario.

PS.10.04 Documentación. El adjudicatario pondrá a disposición de Canal de Isabel II la definición, el diseño y esquemas de los elementos, mecanismos y arquitecturas de seguridad y continuidad de negocio desplegadas sobre la infraestructura tecnológica y los procedimientos y procesos que soportan el servicio, incluyendo:

- Activos de información, incluyendo el mapa y dependencias.
- Configuraciones.
- Procesos (conforme al proceso de documentación de procesos).
- Procedimientos técnicos.

PS.11 Disponibilidad, Recuperación, contingencia, crisis, continuidad de negocio y planes de salida. De entre los diversos escenarios en los que sea necesario aplicar un plan de contingencia o incluso el de salida, por parte de Canal de Isabel II es de particular importancia la necesidad de identificar y retener, a alto nivel, las competencias básicas adecuadas a un nivel operativo dentro de Canal de Isabel II para que, *in extremis*, pueda tener la capacidad de reanudar el control directo de las actividades contratadas. El adjudicatario debe por tanto hacer una propuesta de identificación de dichas competencias y capacidades. Además, el adjudicatario deberá facilitar el proceso de devolución de la información propiedad de Canal de Isabel II inherente a un cese o rescisión del contrato. Adicionalmente, se deberá aportar las certificaciones oportunas de destrucción segura de la información propiedad de Canal de Isabel II.

PS.12 Concienciación. El adjudicatario deberá garantizar la adecuada formación, concienciación y capacitación del personal involucrado en la prestación de los Servicios a Canal de Isabel II. Dicho personal deberá contar con formación y conocimientos específicos de las tecnologías involucradas en la prestación de los Servicios, Seguridad de la Información y la legislación aplicable en el contexto de los Servicios.

PS.13 Evaluación de Seguridad de la Cadena de Suministro. El adjudicatario deberá completar el cuestionario de evaluación de seguridad de la cadena de suministro, conforme a lo establecido en la Directiva NIS 2. Este cuestionario deberá ser completado y entregado dentro de los 30 días posteriores al envío de este por parte del Área de Ciberseguridad y actualizado, al menos, una vez al año.

CN Relativo al Cumplimiento Normativo

CN.01 La solución ofertada por el licitador debe estar certificada en el ENS nivel MEDIO, tal y como aparece recogido en el Documento de Seguridad “Obligaciones de los prestadores de servicios a las entidades públicas” del CCN.

CN.02 El adjudicatario, de conformidad con la Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, asegurará que se satisfarán las obligaciones en relación con los incidentes de seguridad.

CN.03 El adjudicatario contemplará el compromiso de devolución/destrucción (a elección de Canal de Isabel II) de toda la información propiedad de Canal de Isabel II recabada durante la ejecución de los Servicios.

CN.03.01 Si por la naturaleza del proyecto, Canal de Isabel II requiere del borrado y destrucción de cualquier soporte de información englobado al alcance de los Servicios prestados; el adjudicatario deberá aplicar un procedimiento seguro de borrado y destrucción conforme a lo indicado en el Esquema Nacional de Seguridad.

CN.03.02 Asimismo, para cada borrado/destrucción realizada, el adjudicatario deberá entregar a Canal de Isabel II un certificado recogiendo al menos los siguientes campos:

- a) Fecha de recogida del material.
- b) Personal proveedor encargado de la recogida y transporte.
- c) Procedimiento detallado empleado en el borrado/destrucción realizada.

SD Relativo a la Seguridad de los Datos,

SD.01 Gobierno del dato: Los datos de Negocio deben ser protegidos conforme a:

SD.01.01 El acceso a la plataforma, y los sistemas y servicios que la soportan, debe ser conforme a los roles y autorizaciones de dichos roles previamente definidos y autorizados por el Responsable de la Información y del Servicio de Canal de Isabel II.

SD.01.02 El adjudicatario pondrá a disposición del Responsable de la Información y del Servicio de Canal de Isabel II los listados nominales de autorizaciones, accesos y modos de acceso.

SD.01.03 El adjudicatario, además de tener un control e inventario de los repositorios de datos estructurados y no estructurados, debe tener una solución comercial de DLP que permita descubrir datos de carácter personal y tarjetas de pago. Al menos cada tres meses, se realizarán procesos de descubrimiento para la revisión del inventario y la toma de acciones.

SD.01.04 El adjudicatario debe contar con mecanismos de respaldo de la información adecuados y contrastados (*backup*, restauración, pruebas, etc.) para garantizar su correcta salvaguarda en caso de contingencia grave.

SD.01.05 El adjudicatario garantizará la integridad de la información propiedad de Canal de Isabel II transmitida, procesada o almacenada en sus sistemas, prestando especial atención a funcionalidades de acceso en modo offline.

SD.02 Trasvase seguro de datos entre entornos:

SD.02.01 El adjudicatario deberá describir su estrategia para evitar fugas de información derivadas del trasvase de datos entre los distintos entornos, así como detectar e inventariar proactivamente la presencia de datos sensibles / regulados en las diferentes bases de datos de los Servicios ofertados. Se deben describir las metodologías y herramientas / soluciones / activos que se plantee utilizar para lograr este objetivo.

SD.03 Cifrado de los datos:

SD.03.01 El adjudicatario deberá proporcionar los oportunos mecanismos de cifrado de información en tránsito (comunicaciones), en uso y almacenada que, según el caso, sean de aplicación, considerando cualquier información sensible que pueda ser intercambiada dentro del contexto de la plataforma y los sistemas y servicios que la soportan. Los datos confidenciales de clientes deben ser cifrados. Para la parte del cifrado de información en tránsito se hará por tanto uso exclusivo de TLS 1.2 o superior, utilizando sólo suites de cifrado robustas (es decir, ni débiles ni vulnerables). Para la parte de información en uso y almacenada, se utilizarán igualmente algoritmos de cifrado robustos (se entiende como cifrado robusto aquél que se ha comprobado que es altamente resistente a ataques de criptoanálisis), prestando especial atención a la información a la seguridad en el almacenamiento de todos los datos de autenticación. En cualquier caso, se pondrá a disposición de Canal de Isabel II información detallada sobre los servicios criptográficos disponibles.

SD.03.02 El adjudicatario debe establecer a qué nivel o niveles protegerá los datos sensibles para cada caso y tipo de información, así como el material criptográfico a utilizar.

SD.03.03 Para los certificados digitales, éstos serán obligatoriamente de tipo cualificado, las suites de cifrado tendrán un algoritmo de intercambio de claves que será, al menos, ECDHE, el algoritmo de autenticación será, al menos, RSA con una longitud de clave mínima de 2048 bits (3072 bits en el caso de que sea de aplicación el estándar PCI-DSS vigente), pero preferiblemente ECDSA, un algoritmo de cifrado simétrico que será, al menos AES con longitud de clave mínima de 128 bits, no utilizando cifrado de bloques (CBC) sino el modo Galois / Counter (GCM) y una función resumen para la comprobación de autenticación del código del mensaje que será, al menos, SHA-256.

SD.03.04 De igual modo, se incluyen la elaboración y ejecución de procedimientos asociados al ciclo de vida del cifrado, con especial atención a los procesos de firma longeva. El adjudicatario deberá explicar la estrategia para dicho ciclo de vida y su grado de automatización.

SD.03.05 La custodia de certificados se realizará por el adjudicatario en contenedores hardware seguros HSM.

SD.04 Protección de Bases de Datos:

SD.04.01 El adjudicatario deberá describir su estrategia para la protección de las diferentes bases de datos (cifrado, ofuscación, pseudo-anonimización, etc.) y persistencias de la plataforma y los sistemas y servicios que la soportan, incluyendo las funciones de auditoría y cifrado de datos sensibles. El adjudicatario debe describir las metodologías y herramientas / soluciones / activos que se plantea utilizar para lograr este objetivo.

SD.04.02 El adjudicatario, en caso de alojar información de Canal de Isabel II en Bases de Datos ajenas al mismo; deberá seguir las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/24 Recomendaciones de seguridad en bases de datos” y todas aquellas guías técnicas adicionales que estén vigentes y sean de aplicación a los sistemas que soportan el Servicio.

RS En cuanto a los Roles de Seguridad

RS.01 Responsable de Seguridad: El adjudicatario debe disponer de un Responsable de Seguridad para el proyecto con la adecuada formación y experiencia en gestionar el servicio tal y como establece el artículo 13 en su apartado 5 del ENS.

RS.02 Equipo de seguridad: El adjudicatario debe disponer de un completo equipo de seguridad que garantice el diseño, la construcción, configuración, monitorización, operación y Administración de los controles de seguridad y privacidad para el correcto mantenimiento del nivel de riesgo aprobado por Canal de Isabel II.

RS.03 El adjudicatario debe entender y asumir que la responsabilidad fina de la seguridad de los datos recae en el Canal de Isabel II y, por designación de funciones dentro de ésta, en el Responsable de la Seguridad de Canal de Isabel II, motivo por el que deberá disponer de los procesos, normas, procedimientos, recursos, actividades, informaciones, registros, facilidades, herramientas y disposición de colaboración que faciliten al Responsable de la Seguridad de Canal de Isabel II, las tareas de supervisión, auditoría, gestión y notificación de incidentes de seguridad que se pudieran producir en relación con el Servicio.

GI Relativo a la Gestión de Identidades y Accesos:

GI.01 El adjudicatario deberá establecer y desplegar mecanismos de control que garanticen el acceso restringido y adecuado (tanto lógico como físico) a la información propiedad de Canal de Isabel II. Cualquier acceso no explícitamente autorizado será prohibido. Se deberá proporcionar a Canal de Isabel II un informe ejecutivo con las medidas de seguridad físicas implementadas para el control de acceso a las instalaciones físicas, a los CPDs, etc., desde donde se presten los Servicios.

GI.02 El adjudicatario deberá garantizar que el servicio cuenta con mecanismos de control en la autenticación.

GI.03 Los usuarios del adjudicatario que vayan a hacer uso de redes o sistemas de información propiedad de Canal de Isabel II, y/o vayan a acceder a información propiedad de Canal de Isabel II, deben estar dados de alta en los sistemas de Gestión de Identidades de Canal de Isabel II. Para ello, deberán proporcionar al responsable del proyecto de Canal de Isabel II los siguientes datos:

- a. Nombre y dos apellidos.
- b. Cuatro últimos dígitos del DNI/NIE.
- c. Correo electrónico corporativo profesional.

Los usuarios del adjudicatario dados de alta en los sistemas de Gestión de Identidad de Canal de Isabel II seguirán en todo momento todas las indicaciones de seguridad que se les transmitan desde Canal de Isabel II junto con sus credenciales de acceso.

GI.04 El adjudicatario debe identificar los diferentes colectivos que harán uso de los activos de la información objeto del alcance que en principio son:

GI.04.01 Personal del adjudicatario.

GI.04.02 Personal subcontratado (o de la cadena de suministro de las IaaS, PaaS o SaaS).

GI.04.03 Personal de Canal de Isabel II.

GI.04.04 Clientes finales.

GI.04.05 Y dentro de estos colectivos los usuarios privilegiados (administradores, auditores, seguridad, etc.) y los no privilegiados.

GI.05 El adjudicatario informará siempre, y a la mayor brevedad posible, siempre a través del Responsable del Proyecto de Canal de Isabel II, la baja del personal propio asignado a la prestación de los Servicios, una vez que éste deje de formar parte del equipo de trabajo asignado a la prestación de los Servicios.

GI.06 Está terminantemente prohibido la utilización de usuarios genéricos. Se debe proporcionar medios para detectar la creación y utilización de este tipo de usuarios no identificados nominalmente.

GI.07 Los Servicios ofertados por el licitador deberán:

GI.07.01 Validar la identidad de los usuarios cuando acceden a la plataforma y a los sistemas y servicios que la soportan.

GI.07.02 Discernir las solicitudes legítimas de las ilegítimas.

GI.07.03 Asociar a las legítimas un nivel adecuado de privilegios en la plataforma y los sistemas y servicios que la soportan.

GI.07.04 Incluir la capacidad para cumplir con las políticas que la Política de Seguridad de Canal de Isabel II establezca para este contexto y que permita un número máximo de intentos fallidos, o bien que contextualicen los requerimientos en base al riesgo (intentos fallidos previos, origen de las conexiones, etc.).

GI.07.05 Poder integrarse con proveedores de identidades (IdP), debiendo describirse los mecanismos por medio de los que se propone posibilitar dichas integraciones y el análisis de riesgos correspondiente.

GI.07.06 Los intentos de autenticación (fallidos o correctos) deben registrarse, así como con la información necesaria para la investigación de incidentes (dirección IP, información de negocio, etc.).

GI.07.07 El adjudicatario deberá dotar al Servicio ofertado de medios de autorización y gestión de perfiles, y, así, tener la capacidad de dotar a los diferentes usuarios de permisos adecuados para realizar las acciones previstas para sus correspondientes perfiles, aplicando siempre el criterio de mínimo privilegio.

GI.07.08 El adjudicatario deberá explicar y documentar los modelos de autorización previstos y cómo se adaptan a cada caso de uso de los Servicios ofertados.

GI.08 El adjudicatario se compromete a utilizar medios adecuados para la gestión de accesos privilegiados a los sistemas y aplicaciones por parte de los administradores.

GI.09 Los Servicios ofertados por el licitador dispondrán de los recursos hardware, software y procedimentales necesarios para que el acceso de usuarios con privilegios no represente un riesgo. Para ello se impondrán los debidos controles de acceso, control de acciones, trazabilidad, auditoría y escalado de privilegios.

GI.10 Las conexiones de dichos usuarios se deben establecer de forma segura, para al menos, los siguientes tipos de acceso a las redes de sistemas en caso de producirse:

GI.10.01 Locales

GI.10.02 Remotos

GI.10.03 VPN

GI.11 El adjudicatario detallará cómo se proporcionará solución para este tipo de usuarios privilegiados, qué controles aplicará (organizativos, procedimentales) así como las capacidades técnicas (incluidas herramientas) y humanas que se incluyen en la propuesta de gestión segura de acceso de usuarios privilegiados.

GI.12 Debe poderse habilitar al menos un segundo factor de autenticación (2FA) resistente a ataques de *phishing* para garantizar la identidad de los usuarios de los Servicios, ya sea mediante el uso de certificados electrónicos cualificados reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc. La aplicación del 2FA se debe forzar a nivel de administración del aplicativo para que no pueda ser deshabilitado por el propio usuario. En caso de que el 2FA sí pueda ser deshabilitado por el propio usuario, es obligatorio que existan y se implementen, al menos, los siguientes controles compensatorios adicionales:

o Notificación automática de eventos (usuario que deshabilita el 2FA)

- o Notificación de inicio de sesión y de inicios de sesión desde direcciones IP extranjeras y por distintos medios (SMS, correo electrónico, etc.)
- o Posibilidad de generación de informes periódicos con el listado del estado de configuración de los usuarios (por ejemplo, usuarios que tienen habilitado o deshabilitado el 2FA)

Como medida compensatoria a este requisito, debe poderse implementar restricciones de acceso al Servicios objeto de contratación por parte de Canal de Isabel II desde los rangos IP públicos de navegación de Canal de Isabel II.

SE1 En relación con la Seguridad de los Equipos:

SE1.01 El adjudicatario deberá disponer de documentación detallada sobre los protocolos, puertos necesarios, aplicaciones (capa 7), requisitos de alimentación, frecuencias y pruebas de funcionamiento de cada equipo asignado a la prestación de los Servicios objeto de contratación por parte de Canal de Isabel II.

SE1.02 Deberá existir documentación formal detallando las medidas necesarias para la configuración segura de los dispositivos de red y los equipos asignados a la prestación de los Servicios objeto de contratación por parte de Canal de Isabel II. Se deben evitar, entre otras, malas prácticas las configuraciones “de caja” (*out-of-the-box*), las credenciales por defecto, los permisos no ajustados a las necesidades, el uso de credenciales no unipersonales, etc.

SE1.03 El adjudicatario deberá documentar con detalle la configuración de los elementos de información y observar específicamente cualquier medida de seguridad asociada con el sistema (incluidos los dispositivos de cifrado y la protección por contraseña, así como los protocolos o versiones de protocolos a utilizar).

SE1.04 Los equipos deberán estar provistos de métodos de autenticación como contraseñas, u otros mecanismos seguros de autenticación (firmas digitales, entre otros), para estar protegida de modificaciones o usos no autorizados.

SE1.05 El adjudicatario deberá mantener los equipos actualizados a la última versión de software y firmware disponible por el o los fabricantes, según un proceso o política de actualización que deberá ser elaborado por el adjudicatario. Además, no debe estar próxima la fecha de finalización del soporte el software instalado en dichos equipos.

SE.05.01 En caso de que el adjudicatario sea conocedor de que uno de los equipos se encuentre en obsolescencia tecnológica, es decir, cuando no puedan instalarse nuevos parches de seguridad o no estén disponibles a pesar de existir vulnerabilidades que le afecten, ya sea por causa del fabricante, sistema operativo u otra causa relacionada con el equipo, deberá notificárselo a Canal de Isabel II.

SE1.06 El adjudicatario deberá disponer de una política de bastionado de los equipos que soportarán los Servicios. Al menos:

SE1.06.01 El adjudicatario eliminará o inhabilitará en todos los equipos, el software que no sea necesario para la operación y el mantenimiento de dicho equipo antes de ponerlo a disposición de Canal de Isabel II.

SE1.06.02 Todos los nombres de usuario, contraseñas u otros códigos de seguridad configurados por el adjudicatario o por defecto, se cambiarán o eliminarán en el momento de la entrega a Canal de Isabel II.

SE1.06.03 Se adoptará siempre la premisa de menor privilegio y confianza cero (*zero trust*) en todas las configuraciones.

SE1.07 El adjudicatario deberá contar con un plan de acciones correctivas dentro del proceso de mantenimiento para hacer frente a cualquier incidencia software y/o hardware que se produzca en los equipos o cualquiera de sus componentes.

SE1.08 Deberá colaborar con el Canal de Isabel II en lo que este le requiera para la remediación de infecciones que se produzcan en los equipos y responsabilizándose de la efectiva remediación de dichas infecciones. Asimismo, y para minimizar el número de estas posibles acciones, el adjudicatario deberá realizar la instalación y el mantenimiento de actualizaciones de una solución de seguridad con capacidad extendida de detección y respuesta (XDR) en aquellos sistemas de información que den soporte al Servicio ofertado y que permitan su instalación.

SE1.09 El adjudicatario deberá mantener y poner a disposición de Canal de Isabel II de un inventario actualizado de la totalidad de los equipos asignados a la prestación del Servicio ofertado. Este inventario deberá contener al menos los siguientes campos:

- a. Dirección IP del equipo.
- b. Nombre del equipo (*hostname*).
- c. Dirección MAC del equipo
- d. Inventario actualizado del Software instalado en cada equipo.
- e. Modelo del equipo.
- f. Versión del sistema operativo instalado.
- g. Marca, modelo y versión de la solución de seguridad XDR instalada, cuando sea de aplicación.

SE1.10 El adjudicatario deberá proteger la información de los equipos eléctricos y electrónicos frente amenazas de tipo TEMPEST, que pueden llevar a la obtención de información por cauces no previstos.

SE2 En relación con la seguridad de los equipos de usuario propiedad del adjudicatario que vayan a conectarse a las redes o sistemas de información de Canal de Isabel II, o a tratar información de Canal de Isabel II:

SE2.01 El adjudicatario deberá contar con un plan de acciones correctivas dentro del proceso de mantenimiento para hacer frente a cualquier incidencia software y/o hardware que se produzca en los equipos o cualquiera de sus componentes.

SE2.02 El adjudicatario deberá mantener los equipos actualizados a la última versión de Software disponible por el o los fabricantes, según un proceso o política de actualización que deberá ser elaborado por el adjudicatario. Además, no debe estar próxima la fecha de finalización del soporte el software instalado en dichos equipos.

SE2.03 El adjudicatario realizará la remediación de infecciones que se produzcan en los equipos y se responsabilizará de la efectividad de dicha remediación. Asimismo, y para minimizar el número de estas posibles acciones, el adjudicatario deberá realizar la instalación y el mantenimiento de actualizaciones de una solución de seguridad con capacidad extendida de detección y respuesta (XDR).

SE2.04 El Adjudicatario deberá mantener y poner a disposición de Canal de Isabel II de un inventario actualizado de la totalidad de equipos. Este inventario deberá contener al menos los siguientes campos:

- a. Dirección IP del equipo.
- b. Nombre del equipo (*hostname*).
- c. Dirección MAC del equipo
- d. Inventario actualizado del Software instalado en cada equipo.
- e. Modelo del equipo.
- f. Versión del sistema operativo instalado.
- g. Marca, modelo y versión de la solución de seguridad XDR instalada.

SE2.05 El adjudicatario que haga uso de equipos de usuario (Windows 10/11, Linux, etc.) portátiles, sobremesa o cualquier otro tipo de dispositivo (Tablet, Surface, etc.) no gestionado por Canal de Isabel II, en los que se vaya a tratar información de Canal de Isabel II o se vayan a conectar a la red o sistemas de información de Canal de Isabel II (tanto los trabajos que implican accesos de forma remota o bien desde la red de Canal de Isabel II), deberá proporcionar al Jefe de Proyecto la siguiente información para cada uno de los equipos, que será a su vez remitida al Área de Ciberseguridad:

SE2.05.01 Informe agregado de cumplimiento elaborado por el adjudicatario, en el que se debe incluir en el nivel de cumplimiento obtenido en el informe individual, de cada uno de los equipos bajo alcance del proyecto. Este informe debe indicar el valor agregado, que será el valor medio del Informe individual de todos los equipos bajo alcance del proyecto.

SE2.06 En el caso de que los equipos utilicen tecnologías de comunicación inalámbrica, el adjudicatario deberá cumplir con los siguientes requisitos:

SE2.06.01 El adjudicatario debe minimizar, en lo posible, el uso de redes inalámbricas frente a redes cableadas, dado que, por el diseño de especificaciones, son más inseguras.

SE2.06.02 El adjudicatario deberá proporcionar la documentación detallada sobre los protocolos, alcance, requisitos de alimentación, frecuencias y pruebas de funcionamiento de la red inalámbrica.

SE2.06.03 La red inalámbrica proporcionará exclusivamente comunicaciones cifradas con WPA2-EAP o superior. El adjudicatario deberá identificar claramente los métodos de seguridad y capacidades de seguridad, para que las configuraciones por defecto sean modificadas.

SE2.06.04 La red inalámbrica deberá estar provista de métodos de autenticación como contraseñas, u otros mecanismos seguros de autenticación (firmas digitales, entre otros), para estar protegida de accesos, modificaciones y usos no autorizados.

SE2.06.05 El adjudicatario debe incluir este equipamiento inalámbrico dentro de los procesos de gestión del riesgo y gestión de las vulnerabilidades.

DM En relación con los dispositivos móviles del adjudicatario que vayan a conectarse a las redes o sistemas de información de Canal de Isabel II, o a tratar información de Canal de Isabel II:

DM.01 El adjudicatario deberá considerar en obsolescencia tecnológica un dispositivo móvil cuando no puedan instalarse nuevos parches de seguridad o no estén disponibles a pesar de existir vulnerabilidades que le afecten, ya sea por causa del fabricante, sistema operativo u otra causa relacionada con el terminal. En estos casos el adjudicatario deberá sustituir el terminal por otro que no esté obsoleto tecnológicamente. La instalación de parches virtuales en el dispositivo por parte del adjudicatario sería equivalente, si técnicamente es así, a la instalación del parche del fabricante.

DM.02 El adjudicatario deberá mantener los terminales actualizados a la última versión de Software disponible por el fabricante según un proceso o política de actualización que deberá ser elaborado por el adjudicatario.

DM.03 El adjudicatario debido a su condición de encargado de la administración de los dispositivos móviles deberá elaborar una política de bastionado de los dispositivos móviles una vez sea el adjudicatario del proyecto y aplicar dicha política una vez cuente con el visto bueno correspondiente de Canal de Isabel II.

DM.04 Los dispositivos móviles deben verificar en tiempo de arranque que su Sistema Operativo (OS) no ha sido modificado.

DM.05 Los dispositivos móviles deberán disponer de la separación eficaz de entornos entre parte profesional y parte personal. Estos terminales deben permitir el cifrado robusto (es decir, altamente resistente a ataques de criptoanálisis) de la parte profesional por hardware, mediante el suministro de licencias por parte del adjudicatario de soluciones destinadas a este fin.

DM.06 Los dispositivos deben estar gestionados por parte del adjudicatario en una solución MDM. La versión del MDM debe estar actualizada de tal forma que contenga las últimas funcionalidades en materia de seguridad.

DM.07 El adjudicatario debe facilitar a Canal de Isabel II los usuarios de auditoría que le sean requeridos para la solución MDM en la que se administren los dispositivos móviles del

adjudicatario que se utilicen para la prestación de los Servicios objeto de contratación en la presente licitación.

DM.08 La solución MDM desde la que el adjudicatario administrará los dispositivos móviles de su propiedad y que se utilicen para la prestación de los Servicios objeto de contratación en la presente licitación, debe garantizar el cumplimiento de la Política de Seguridad corporativa del adjudicatario, mediante políticas que puedan forzarse de manera automática y centralizada para todos los terminales.

DM.09 El adjudicatario deberá proporcionar los oportunos mecanismos de cifrado de información en tránsito desde los dispositivos móviles a la plataforma y los sistemas y servicios que la soportan.

SI En relación con la Seguridad de la Infraestructura:

SI.01 El adjudicatario debe configurar la plataforma y los sistemas y servicios que la soportan siguiendo estrictos estándares de seguridad para una estrategia de defensa en profundidad y mínima superficie expuesta.

SI.02 Cuando existan para el entorno, deben seguirse las guías de configuración del CCN que sean de aplicación. En caso de existir la guía y que el adjudicatario entienda que no puede o no debe seguir la correspondiente guía, deberá justificarlo técnicamente y pedir autorización expresa a Canal de Isabel II.

SI.03 El adjudicatario no debe mantener configuraciones por defecto.

SI.04 Nunca pueden existir usuarios por defecto.

SI.05 Siempre que se puedan modificar, los *path* se deben modificar y no deben estar las configuraciones que vienen por defecto.

SI.06 El adjudicatario deberá exponer su metodología, activos y enfoque para abordar este proceso y cómo se adapta a los diferentes casos de uso de los Servicios ofertados. Si la solución propuesta se basa en el uso de uno o varios proveedores de Cloud Pública, se requiere el cumplimiento de estándares /normativas de seguridad (como mínimo, lo indicado en las medidas de seguridad del ENS).

SI.07 La plataforma y los sistemas y servicios que la soportan deben contar con la capacidad para controlar que los diferentes elementos que los componen cumplen en todo momento con las políticas de configuración segura y que se detectan cambios en las configuraciones que puedan afectar a la seguridad, de manera que se pueda evaluar su impacto cuando se produzcan.

SI.08 Se deben guardar de forma trazable las configuraciones de seguridad para detectar modificaciones en las mismas.

SI.09 Se debe describir las metodologías y herramientas / soluciones que se plantea utilizar, con qué frecuencia, en qué momentos y por qué se consideran idóneas estas opciones para una plataforma, y para los sistemas y servicios que la soportan, de este tipo.

SI.10 El adjudicatario debe incluir en la plataforma y en los sistemas y servicios que la soportan, mecanismos para la detección de comportamientos sospechosos en la infraestructura, que pudieran ser indicativos de una brecha de seguridad. Se incluirán productos comerciales del tipo UEBA, UBA o SUBA.

SI.11 Las soluciones que se pretendan utilizar para la detección de comportamientos sospechosos se deben describir y por qué se consideran adecuadas estas opciones para la plataforma y para los sistemas y servicios que la soportan en sus diferentes escenarios.

SI.12 El adjudicatario debe describir la estrategia propuesta para la seguridad de las comunicaciones, incluyendo la segregación de redes por zonas de confianza, el filtrado de tráfico de red y el manejo del cifrado en los segmentos en que se requiera. Debe describirse las soluciones que se plantea utilizar y por qué se consideran adecuadas estas opciones para la plataforma y para los sistemas y servicios que la soportan en sus diferentes escenarios.

SI.13 De no especificarse lo contrario por parte de Canal de Isabel II, el adjudicatario deberá garantizar la segregación para el *tenant* que utilizará Canal de Isabel II en el ámbito del presente contrato, donde se van a alojar los elementos e infraestructura y la aplicación que soportan la prestación de los Servicios.

SI.14 Los datos propiedad de Canal de Isabel II almacenados en los sistemas del adjudicatario deberán estar segregados de forma física y/o lógica de los de cualquier otro cliente, no siendo accesibles más que por el personal autorizado expresamente por Canal de Isabel II.

SI.15 La administración de los servicios prestados a Canal de Isabel II en el ámbito de este contrato y alojados en la infraestructura del adjudicatario deberá realizarse a través de equipos dedicados exclusivamente a la administración de los servicios de Canal de Isabel II.

SI.16 El adjudicatario deberá dotar a los servicios de DNS específicos para la plataforma y para los sistemas y servicios que la soportan de, al menos, los siguientes mecanismos:

SI.16.01 Protección por reputación

SI.16.02 Creación de Sinkhole

SI.16.03 Protección de exfiltración mediante paquetes DNS.

El adjudicatario debe proveer de la infraestructura necesaria para la provisión, operación y administración de DNS seguros, con las funcionalidades descritas.

Debe describirse el enfoque, la metodología para su gestión y su integración en la estrategia propuesta de monitorización de seguridad de los Servicios ofertados.

SI.17 Todos los sistemas y micro-servicios de los Servicios ofertados deberán tener la misma referencia horaria, que se tomará como estrato principal la del servidor de tiempo del Real Observatorio de la Armada (ROA).

SI.18 Para los posibles accesos del personal y terceros de Canal de Isabel II, así como para el personal del adjudicatario que trabaje en los servicios de Canal de Isabel II, el adjudicatario

deberá dotar de herramientas específicas a Canal de Isabel II y a los terceros citados, de tal manera que se garantice la confidencialidad del tráfico generado en dichos procesos a través de protocolos considerados como seguros o soluciones específicas destinadas a tal efecto. De la misma forma, la gestión y administración interna de los elementos involucrados en la provisión de los Servicios deberán contar con dichas garantías.

SI.19 El adjudicatario debe indicar, para todos los servicios en la nube objeto de la presente licitación, los siguientes datos:

- a. Empresa proveedora encargada de alojar el servicio en la nube.
- b. Direccionamiento IP.
- c. Puertos requeridos para la provisión de los Servicios.
- d. Geolocalización de cada uno de los servicios prestados.

CD En relación con la CiberDefensa:

CD.00 Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN para seleccionar los productos o servicios suministrados por un tercero que formen parte de los productos de seguridad y aquellos que se referencien expresamente en las medidas de seguridad del ENS. En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19 del ENS.

CD.01 Las líneas de comunicación expuestas a internet, deben tener mecanismos de protección frente ataques distribuidos de Denegación de Servicio (DDoS).

CD.02 El adjudicatario contará con todas las licencias necesarias relativas a cualquier herramienta necesaria para garantizar la seguridad integral de los Servicios.

CD.03 Los productos de seguridad deben ser comerciales para las áreas de:

CD.03.01 Defensa perimetral, perímetro virtual, segmentación (NGFW, etc.).

CD.03.02 Protecciones IDS e IPS.

CD.03.03 Solución de seguridad con capacidad extendida de detección y respuesta (XDR).

CD.03.04 UEBA, UBA o SUBA.

CD.03.05 Solución de Seguridad de filtrado a nivel de aplicación.

CD.03.06 Cuando la naturaleza de la solución del adjudicatario incorpore servicios web, el adjudicatario deberá incorporar: Protección de aplicaciones (WAF/AWAF).

CD.03.07 Cuando la naturaleza de la solución del adjudicatario incorpore información sensible o confidencial, por ejemplo, datos de carácter personal, se requerirá de una solución de tipo DLP.

CD.03.08 Cuando la arquitectura de la solución del adjudicatario requiera procesamiento multitenant se requerirá una solución de protección de cargas de trabajo en la nube (CWPP).

CD.03.09 Cuando la naturaleza de la solución del adjudicatario requiera navegación web, de usuarios o aplicaciones, se requerirá una solución de protección de la navegación vía proxy de navegación o a través de la categorización de las URLs, que incluirá además la categorización por nivel de riesgo (bajo, medio o alto). Se revisará con Canal de Isabel II las categorías de navegación permitidas y denegadas. Para el uso de Proxys de entrada (proxys inversos) se requerirá el estudio de viabilidad y seguridad juntamente con Canal de Isabel II previo a su autorización.

CD.03.10 Cuando la naturaleza de la solución del adjudicatario incorpore envío y recepción de correo electrónico se requerirán medidas de protección de correo (ATP, antimalware, antispam, reputación, vínculos seguros, etc.)

CD.03.11 Será obligatorio un segundo factor de autenticación (2FA) resistente a *phishing*, para aquellos servicios expuestos a Internet que requieran autenticación.

CD.04 Todos los formularios sin excepción tienen que estar protegidos contra ataques de fuerza bruta (por ejemplo, uso de CAPTCHA/reCAPTCHA, disociación de los campos “usuario” y “contraseña” en pasos de distintos, pero dependientes y controlados, dentro del proceso de inicio de sesión, etc.) y tienen que controlar completamente los caracteres introducidos por el usuario para evitar ataques de tipo Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI), Remote Code Execution (RCE), Inyección SQL, etc.

CD.05 Cuando la naturaleza de la solución del adjudicatario requiera del uso de servicios web (WS) se requerirá que estén securizados a nivel de mensaje, especificando la forma de firmar y el cifrado de los mensajes de tipo SOAP, a través de la especificación WS-Security. Por tanto:

- o Los servicios deben estar autenticados, preferentemente con WS-Security Tokens.
- o Los usuarios deben ser autenticados vía SAML 2.0.
- o La integridad de la información ha de estar garantizada a través del uso de protocolos seguros (TLS 1.2 o superior y suites de cifrado robustas (ni débiles ni vulnerables)) o vía WS-Signature.
- o El no repudio debe estar garantizado a través del uso de WS-Signature o WS-Addressing.
- o La confidencialidad de la información ha de estar garantizada a través del uso de protocolos seguros (TLS 1.2 o superior y suites de cifrado robustas (ni débiles ni vulnerables)) o vía WS-Encryption.
- o Debe hacerse uso de una política de seguridad (WS-Policy).

En relación con estos productos, el adjudicatario deberá alinearse con los fabricante y modelos que actualmente están en explotación en la infraestructura de Canal de Isabel II. En caso contrario, deberá argumentar técnicamente que cuenta con soluciones de seguridad más adecuadas que las expuestas anteriormente.

CD.06 De no especificarse lo contrario formalmente y de forma autorizada por Canal de Isabel II, el adjudicatario garantizará la no obsolescencia de la tecnología, controles o los procesos involucrados en la prestación de los Servicios, llevando a cabo, y bajo autorización expresa de Canal de Isabel II, procesos de renovación y actualización de los sistemas y procesos según se determine necesario.

CD.06.01 El adjudicatario deberá contar con un proceso formal de Gestión de vulnerabilidades y parcheo de elementos de la plataforma y de toda la infraestructura, sistemas y servicios involucrados en la prestación de los Servicios, que garantice la correcta configuración y actualización de estos.

CD.06.02 Como parte de dicho proceso de Gestión de vulnerabilidades:

- I. El sistema objeto de este procedimiento de contratación será objeto de escaneos de vulnerabilidades, bien por parte del adjudicatario o bien por parte del Canal de Isabel II, ya que ésta aplica actualmente un proceso continuo de gestión de vulnerabilidades de su infraestructura IT, debiendo para ello el adjudicatario habilitar en las políticas de red los correspondientes accesos para los escaneos periódicos.
 - a. En el caso de que el adjudicatario cuente con informes/reportes de escaneo de vulnerabilidades de los Servicios ofertados, realizados por un tercero, y una vez que sean analizados por el Área de Ciberseguridad de Canal de Isabel II, podrán ser aceptados como equivalentes a lo indicado en el párrafo anterior.
- II. Los informes de los escaneos realizados por el adjudicatario deberán entregarse al Jefe de Proyecto que a su vez lo remitirá, sin demora justificada, al Área de Ciberseguridad de Canal de Isabel II.
- III. Además, el adjudicatario deberá resolver las vulnerabilidades detectadas en los escaneos en los plazos establecidos en las políticas de Canal de Isabel II, de acuerdo con su criticidad.

CD.06.03 El adjudicatario describirá las metodologías para la gestión del ciclo de vida de vulnerabilidades y su integración de la gestión de los Servicios ofertados.

CD.07 En el caso de que el adjudicatario hiciese uso de una suscripción en un Cloud público, Canal de Isabel II se reserva el derecho de solicitar capacidades de auditoria haciendo uso de su solución corporativa CNAPP. El adjudicatario facilitará los datos de integración necesarios para realizar dicha integración con objetivo de verificar la postura de seguridad de las configuraciones aplicadas.

CD.08 El adjudicatario deberá habilitar los mecanismos de configuración, generación, almacenamiento, custodia y entrega de registros de trazabilidad de acceso y uso a los activos de información bajo su alcance. Estos, deben incluir al menos los siguientes campos:

- a. Actividad
- b. Acceso
- c. IP origen

- d. IP destino
- e. Usuario

Los logs deben estar normalizados y aplicado el *parseo* correcto para que su información pueda ser relacionada con otras fuentes e interpretada adecuadamente. Es responsabilidad del adjudicatario realizar estas tareas.

Los logs se podrán entregar al SIEM corporativo de Canal de Isabel II bien en las instalaciones de Canal de Isabel II o, en su defecto, y si Canal de Isabel II lo autoriza, a través de una API que el adjudicatario pondría a disposición de Canal de Isabel II para la captura de los logs por parte del SIEM corporativo de Canal de Isabel II. Es responsabilidad del adjudicatario garantizar que la ingesta en el SIEM de Canal de Isabel II se realiza de forma correcta.

El adjudicatario custodiará una copia de dichos registros por el periodo de retención que el Canal de Isabel II especifique para cada fuente.

CD.09 El adjudicatario como parte de su provisión de servicios de seguridad debe monitorizar la infraestructura para detectar incidencias e incidentes en la plataforma propuesta por el adjudicatario y en los sistemas y servicios que la soportan, en formato 24x7.

CD.10 El adjudicatario deberá comunicar directamente al Área de Ciberseguridad de Canal de Isabel II, y en copia al Jefe de Proyecto, los incidentes de seguridad categorizados con un Nivel de Impacto Medio, Alto, Muy Alto y Críticos, según las directrices y criterios de determinación del nivel de impacto de los Ciberincidentes recogido en la Guía de Seguridad de las TIC CCN-STIC 817.

Una vez identificado como posible incidente, la gestión de este se trasladará al SOC de Canal de Isabel II (miembro de la red internacional FIRST y de la red Nacional de CERTS públicos y privados CSIRT.ES), colaborando el adjudicatario en aquellas actividades que el SOC y la Oficina Técnica de Seguridad (OTS) de Canal de Isabel II solicite para la correcta valoración, remediación, documentación y notificación del incidente.

El adjudicatario debe evitar la destrucción de pruebas tanto como consecuencia de acciones internas o externas, intencionadas o no. En especial, en la fase inicial (*triage*) bajo su responsabilidad, en las tareas de recuperación (si procede), así como una vez que razonablemente se haya identificado como posible incidente, la Gestión del incidente y su responsabilidad haya sido transferida a Canal de Isabel II.

El adjudicatario guardará la máxima confidencialidad en todas aquellas actuaciones que se deriven de la gestión del incidente y le sean encargadas por el SOC de Canal de Isabel II.

CD.11 Canal de Isabel II dispone de capacidades de análisis forense, encuadradas en los servicios proporcionados por el SOC de Canal de Isabel II. La empresa adjudicataria debe describir cómo colaborará con dichas capacidades en la plataforma propuesta y en los sistemas y servicios que la soportan, así como el proceso que propone a la hora de gestionar las solicitudes de análisis forense, y en el caso de pruebas de ámbito judicial, cómo garantizará la cadena de custodia (norma nacional / internacional, metodología propia, etc.).

CD.12 El adjudicatario realizará pruebas de seguridad (*pentesting*, hacking ético) ya sea de las aplicaciones y/o infraestructuras que afecten a la plataforma y a los sistemas y servicios que la soportan. En caso de realizarse durante la prestación de los Servicios, debe notificarlo al jefe de Proyecto de Canal de Isabel II. Dado que los datos son propiedad de Canal de Isabel II, debe pedir autorización a dicho Jefe de Proyecto, aportando la información de personas, empresa, ventana, alcance, acuerdos legales, acuerdos de privacidad, etc. Si se autorizase y se realizasen dichas pruebas por el adjudicatario, los resultados de estas deben ser obligatoriamente compartidos con el Área de Ciberseguridad de Canal de Isabel II.

Se deben describir las metodologías y herramientas / soluciones / activos que se plantea utilizar, con qué frecuencia, en qué momentos y por qué se consideran idóneas estas opciones para la plataforma y para los sistemas y servicios que la soportan.

En cualquier caso, Canal de Isabel II se reserva el derecho de ejercer actividades sobre el entorno del contrato: Hacking puntual o en modo continuo (Modalidad *Purple Team*).

CD.13 En el caso de que la solución requiera el envío de correos electrónicos, se deberán llevar a cabo conforme a las medidas de seguridad indicadas por Canal de Isabel II. Todos los correos electrónicos enviados y recibidos deben configurarse para que empleen los sistemas de Canal de Isabel II disponibles para ello, y asegurar la autenticidad de los dominios de Canal de Isabel II.

AU En relación con las auditorías:

AU.01 Canal de Isabel II podrá solicitar informes técnicos, de auditorías, o cualquier otro documento relevante, para acreditar el nivel de seguridad del adjudicatario. Por ejemplo: SSAE16, IASE 3402 SOC 2 Tipo II, etc.

AU.02 Canal de Isabel II podrá realizar revisiones de seguridad, continuidad de negocio y auditar los sistemas de información que traten, almacenen o gestionen información de su propiedad, incluidos los procesos que soporten dichos tratamientos, almacenamiento y gestión de la plataforma, y de los sistemas y servicios que la soportan.

AU.03 El adjudicatario deberá proporcionar a Canal de Isabel II o a cualquier tercero designado a tal efecto por Canal de Isabel II y/o Autoridad de Control, acceso completo de la institución a las ubicaciones y centros de trabajo desde los que se presten los Servicios, incluyendo cualquier dispositivo, sistema, red y datos utilizados para la prestación de los Servicios contratados (derecho de acceso).

AU.04 Canal de Isabel II se encuentra sujeta a diversas auditorías externas, ya sea por requerimientos regulatorios, legales, normativos, sectoriales, contractuales, etc. Estas necesidades son por las que las auditorías que Canal de Isabel II puede solicitar si es estrictamente necesario al adjudicatario, el cual en ese supuesto debe colaborar diligentemente, a fin de entregar las evidencias y participar en las entrevistas de auditoría. Estas auditorías pueden responder a las siguientes necesidades:

AU.04.01 Auditoría anual (autoimpuesta).

AU.04.02 Auditorías de terceros, entre otras, y no excluyentes:**AU.04.02.01** IGAE**AU.04.02.02** Tribunal de cuentas.**AU.04.02.03** Económico – Financiera.**AU.04.02.04** UIC.**AU.04.02.05** CNPIC**AU.04.02.06** Auditorías extraordinarias

Esto, entre otros motivos, hace que la plataforma, los sistemas y servicios que la soportan y los equipos que la construyen y operan sean objeto de auditorías periódicas. La empresa adjudicataria deberá por tanto colaborar con Canal de Isabel II para dar cumplimiento a las obligaciones internas y externas de auditoría.

DS En relación con la Disponibilidad, Recuperación, Contingencia, Crisis, Continuidad de Negocio y los Planes de salida.

DS.01 A los sistemas soportan los Servicios le serán de aplicación los requisitos establecidos por ENS. Este alto nivel de exigencia, junto con el que Canal de Isabel II se impone a sí misma, establece la necesidad de que el adjudicatario deba:

DS.01.01 Disponer de una o más localizaciones en las que poder mantener la provisión de los Servicios en caso de contingencia, crisis o continuidad.

DS.01.02 Proveer a los sistemas que soportan los Servicios de arquitecturas de seguridad redundadas y balanceadas.

DS.01.03 Contar con mecanismos de respaldo de la información adecuados y contrastados (procesos de *backup*, restauración, pruebas de restauración, etc.) para garantizar su correcta salvaguarda en caso de contingencia grave.

DS.01.04 Disponer de planes y medios de actuación para situaciones de contingencia.

DS.01.05 Disponer de un plan de crisis.

DS.01.06 Disponer de un Plan que permita disponer de un Plan de Continuidad del Negocio, para las contingencias que puedan producirse en la prestación de los Servicios al amparo del presente contrato.

DS.01.07 Disponer de un Plan de Salida programada que, entre otras muchas cuestiones, debe detallar cómo la información será devuelta a Canal de Isabel II y destruida de forma segura, completa y veraz de los sistemas del adjudicatario.

DS.01.08 Disponer de un Plan de Salida sobrevenida que, recoja entre otras muchas cuestiones cómo la información será devuelta a Canal de Isabel II y destruida de forma segura, completa y veraz de los sistemas del adjudicatario.

DS.02 Se deben describir las metodologías y herramientas / activos que se plantea utilizar, en qué momentos y por qué se consideran idóneas estas opciones para los sistemas que soportan los Servicios.

DS.03 Adicionalmente, deberá elaborar planes de contingencia que permitan hacer frente a situaciones que pudieran afectar a la disponibilidad de los Servicios ofertados.

RIA Cumplimiento del Reglamento Europeo de Inteligencia Artificial

RIA.01. Si el producto o servicio contratado implica la utilización de sistemas o modelos de Inteligencia Artificial, el adjudicatario deberá cumplir con lo dispuesto en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, y normativa de desarrollo, tanto la vigente en el momento del contrato como la que pudiera ser de aplicación durante la duración del mismo y, en todo caso, deberá cumplir con los siguientes requisitos:

- Asignará e indicará a Canal de Isabel II quien tiene las funciones y responsabilidades técnicas y operativas y proporcionará la dirección y apoyo claros sobre el uso de los sistemas de IA y la aplicación de la ley de protección de datos.
- En el caso de que se traten datos de categoría especial, en aplicación del art. 10.5 letra f) del RIA, "los registros de las actividades de tratamiento de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, deben incluir las razones por las que el tratamiento de categorías especiales de datos personales es estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no puede alcanzarse mediante el tratamiento de otros datos. Se solicita al proveedor explicación de tales razones.
- Documentará las finalidades para el uso de datos personales en cada etapa del ciclo de vida de la IA, y en caso de que se utilizaran para otras finalidades distintas a las originalmente definidas, aportará evaluación analizando si son compatibles con la finalidad originalmente perseguida. Cada una de dichas etapas, en su consideración individualizada, deberá cumplir con los requisitos del RGPD en materia de privacidad. A modo de ejemplo, para facilitar esta información, el adjudicatario puede utilizar la tabla del ciclo de vida del dato de la ISO 29134:2017.

Fase del ciclo de IA: [CONCEPCIÓN/ DISEÑO Y DESARROLLO/ VERIFICACIÓN Y VALIDACIÓN/ DESPLIEGUE/ OPERACIÓN Y MONITORIZACIÓN/ REEVALUACIÓN/ RETIRADA]				
	Interesado	Responsable	Encargado	Tercero
Recogida				
Almacenamiento				
Uso				
Transferencia				
Eliminación				

- d) El adjudicatario garantizará que cuenta con una base de legitimación válida para tratar datos personales en cada una de las fases.
- e) El adjudicatario garantizará que se han aplicado técnicas de desidentificación a los datos de entrenamiento antes de extraerlos de su fuente y compartirlos con Canal de Isabel II. En caso de no aplicar tales técnicas, el adjudicatario garantiza que dichos datos han sido obtenidos lícitamente.
- f) El adjudicatario entregará, mediante una evaluación de impacto (EIPD), las diferentes formas en que el sistema de IA podría generar resultados discriminatorios, erróneos o injustificado, incluyendo en ese caso medidas técnicas y organizativas adecuadas para mitigar o gestionar esos riesgos de manera continua.
- g) El adjudicatario documentará y evaluará los requisitos de explicabilidad y transparencia, considerando el sector o caso de uso en el que vaya a desplegarse el sistema de IA.
- h) El adjudicatario documentará y evaluará qué datos se consideran necesarios para asegurar un conjunto de datos de entrenamiento representativo, confiable y relevante. El proveedor se compromete a informar a Canal de Isabel II, y en su caso, corregir, cualquier característica del conjunto de datos del entrenamiento que requiera ajustar el sistema con suficientes casos de uso.
- i) El adjudicatario deberá entregar descripción de cómo pueden facilitarse las solicitudes de derechos de los interesados en materia de protección de datos a lo largo del ciclo de vida del sistema de IA donde se traten datos personales.
- j) El adjudicatario documentará y evaluará cuándo ha previsto una revisión humana significativa en la cadena de decisiones, quién realizará dicha revisión y qué información adicional tendrá en cuenta a la hora de tomar la decisión final.
- k) El adjudicatario asegura haber establecido un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización del sistema.

CC. Condiciones para la conexión a la red corporativa de datos de Canal de Isabel II

El adjudicatario queda obligado a realizar una conexión privada a la Red Corporativa de Datos (en adelante, RCD) de Canal de Isabel II para la realización de aquellos trabajos contemplados dentro del alcance del presente contrato que lo requieran. El adjudicatario, por tanto, deberá asignar un recurso técnico especializado sin dedicación exclusiva en redes de datos y comunicaciones, que se responsabilice, en el ámbito de la prestación de los Servicios, de la configuración y mantenimiento de la parte de la infraestructura de comunicaciones entre el adjudicatario y Canal de Isabel II que sea responsabilidad del adjudicatario, al objeto de garantizar el cumplimiento de estas condiciones de conexión, la cual se realizará bajo los siguientes condicionantes obligatorios:

CC.01. Conexión única del operador de comunicaciones con la RCD de Canal de Isabel II.

El operador de comunicaciones elegido por el adjudicatario para la puesta en marcha de la conexión con Canal de Isabel II entregará en un único punto tanto la totalidad del tráfico gestionado del propio adjudicatario como el de las otras empresas colaboradoras o contratas que conecten a través de dicho único punto con Canal de Isabel II. Esto es, si el operador de comunicaciones elegido por el adjudicatario ya presta servicio a alguna otra empresa colaboradora o contrata de Canal de Isabel II, la nueva conexión deberá utilizar la infraestructura física existente en Canal de Isabel II para generar la nueva conexión, sin que sea necesaria la instalación de nuevo equipamiento físico ni la realización de ninguna actividad en las dependencias de Canal de Isabel II. La utilización de infraestructura común por parte de las distintas empresas colaboradoras no supone la disponibilidad de conexión entre las mismas, siendo el objeto la conexión privada uno a uno de cada una de las empresas colaboradoras con Canal de Isabel II. En caso de que el operador no preste en la actualidad este servicio a ninguna empresa colaboradora, podrá realizar la conexión a la RCD de Canal de Isabel II, teniendo en cuenta la casuística expuesta para futuras conexiones de otras posibles empresas colaboradoras. El operador de comunicaciones preservará la privacidad de las comunicaciones con la RCD de Canal de Isabel II y, en especial, entre las diferentes empresas colaboradoras a las que pudiera dar servicio con la misma infraestructura.

En caso de que el contrato sea adjudicado a una Unión Temporal de Empresas (UTE), se presentará igualmente una única conexión a Canal de Isabel II, y serán las empresas que forman la UTE las que deberán coordinarse entre ellas y realizar las acciones que sean necesarias para garantizar que la prestación de los servicios contratados por parte de Canal de Isabel II se realice exclusivamente a través de dicha conexión única.

Cada conexión única a Canal de Isabel II va ligada a un único contrato. No se permitirá que un contratista con más de un contrato con Canal de Isabel II comparta una misma conexión para contratos distintos, salvo autorización expresa de los responsables en Canal de Isabel II de cada uno de los contratos y la presentación de un informe que garantice que las características de la línea (ancho de banda, latencias etc.) y que las características de conexión de las operativas de los distintos contratos hacen que no haya afección posible entre los mismos.

La conexión única principal con Canal de Isabel II deberá entregar el tráfico a la RCD de Canal de Isabel II en la siguiente dirección:

Oficinas Centrales Canal de Isabel II, Sociedad Anónima, M.P.

C/ Santa Engracia 125

Edificio 4

CC.02. Conexión de *backup*, contingencia o respaldo con la RCD de Canal de Isabel II.

Si por parte del servicio de Canal de Isabel II responsable del adjudicatario se identificara que el servicio contratado es crítico, o tuviera unos requisitos de disponibilidad altos (por ejemplo, 24x7), el adjudicatario quedará obligado a provisionar una segunda línea de comunicación con Canal de Isabel II a través de otro operador de comunicaciones distinto del seleccionado para la línea de comunicación principal, y en los mismos términos identificados en el punto 1. “Conexión única del operador de comunicaciones con la RCD de Canal de Isabel II”, con el objeto de disponer de una línea adicional de *backup*, contingencia o respaldo, y poder así garantizar la disponibilidad de las comunicaciones.

La conexión de *backup* con Canal de Isabel II deberá entregar el tráfico a la RCD de Canal de Isabel II en la siguiente dirección:

Polígono Industrial El Carralero (Majadahonda)

ETAP Majadahonda

Edificio Espejo

CC.03. Direccionamiento IPv4.

El adjudicatario se adecuará a los rangos de direccionamiento IPv4 privados establecidos por Canal de Isabel II. Se establecerá por parte de Canal de Isabel II un rango IPv4 compatible, en el que el adjudicatario se integrará en la RCD de Canal de Isabel II. Si fuera necesaria la aplicación de traducción de direcciones (NAT) ésta será responsabilidad exclusiva del adjudicatario, bien con medios propios o bien a través de la capacidad de la línea contratada con el operador de comunicaciones elegido por el adjudicatario.

CC.04. Monitorización de la conexión.

La línea de comunicaciones deberá estar dimensionada conforme a los trabajos y servicios que se prestan en el alcance del contrato, permitiendo una prestación eficiente de los mismos. El adjudicatario deberá facilitar la información básica del dimensionamiento y de los requisitos de las conexiones: N.º de conexiones, ancho de banda, latencia, errores físicos de red, etc.

El cumplimiento de estos parámetros de dimensionamiento deberá ser monitorizado por el adjudicatario y, como parte de los informes de servicio mensuales, el adjudicatario deberá facilitar un informe de uso de las conexiones que incluya, al menos, las siguientes gráficas de uso de la red a lo largo del mes:

- N.º de conexiones establecidas (entrante/saliente)
- Ancho de banda consumido (entrante/saliente)
- Latencias
- Errores de red (físicos)

Adicionalmente se deberá hacer una auditoría de forma periódica (al menos, 2 veces al año) donde se compruebe el cumplimiento efectivo de los requisitos de conectividad en base al dimensionamiento realizado en el proyecto, tanto en la línea principal como en las de *backup*, en caso de existir. El adjudicatario deberá facilitar un informe con los resultados de la auditoría en el que se compruebe el cumplimiento de los parámetros del dimensionamiento y de los requisitos de las conexiones.

El adjudicatario tiene la obligación de asegurar el correcto estado de la conexión por parte del operador de telecomunicaciones en todas sus líneas de comunicación (principal y de *backup*, en caso de existir). El adjudicatario está obligado a realizar las comprobaciones oportunas con el operador ante cualquier posible problema de acceso a los sistemas de Canal de Isabel II, proporcionando las evidencias de que el tráfico se entrega en el extremo de Canal de Isabel II y que parte de la interfaz del *router* de operador que conecta con el extremo de Canal de Isabel II. Solo si tras las pruebas realizadas hay evidencia de que no es un problema del operador, se trasladará la incidencia a los técnicos de Servicios de Red y Accesos de Canal de Isabel II, y siempre a través del responsable de contrato en Canal de Isabel II.

Canal de Isabel II se reserva el derecho de monitorizar la línea de comunicaciones solicitada por el adjudicatario. Para ello se debe garantizar el acceso de consulta SNMP a los *routers* en extremos (no a los *routers* que pudieran componer la propia red del operador de telecomunicaciones) dedicados a la conexión con Canal de Isabel II.

CC.05. Contacto.

En caso de duda sobre alguna de las condiciones reflejadas en este documento, el adjudicatario puede dirigir sus consultas o dudas, haciendo referencia a los apartados de este documento, exclusivamente al Jefe de Proyecto en Canal de Isabel II, quien se encargará de tramitarlas de forma interna.

Una vez finalizada las prestaciones del contrato, el adjudicatario estará obligado a solicitar la baja del servicio con el operador de telecomunicaciones, y ha de informar al Jefe de Proyecto en Canal de Isabel II una vez se haya producido la baja efectiva del servicio, quien a su vez informará internamente a las unidades organizativas de Canal de Isabel II afectadas o involucradas en la prestación del servicio.

Firmado electronicamente por: Rafael Martín Espiga
En la fecha y hora 16.07.2025 08:17:15 CEST

Rafael Martín Espiga
Jefe de Área de Telecomunicaciones

Firmado electronicamente por: CESAR MARTÍN MEGÍAS
Por delegación de FRANCISCO JAVIER FERNÁNDEZ
DELGADO

Francisco Javier Fernández Delgado
Subdirector de Telecontrol

Firmado electronicamente por: JUAN SÁNCHEZ GARCÍA
En la fecha y hora 16.07.2025 15:55:53 CEST

Juan Sánchez García
Director de Innovación e Ingeniería