



**Pliego de Prescripciones Técnicas para la
Contratación de los Servicios de Alojamiento,
Traslado y Comunicaciones del Centro de
Proceso de Datos de Canal de Isabel II, S.A. M.P.**

166/2024

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Índice

1. Objeto y alcance del servicio	4
1.1. Descripción y ubicación de los CPD	4
1.2. Descripción de la red backbone entre CPDs	4
1.3. Descripción del sistema mainframe	5
1.4. Descripción del sistema open y virtualización	5
1.5. Descripción del sistema de base de datos	5
2. Proyecto de establecimiento de telecomunicaciones	6
2.1. Requisitos de la solución propuesta	6
2.2. Plan de Gestión del proyecto	7
2.3. Características de las líneas y equipos de comunicaciones	8
3. Proyecto de traslado y puesta en marcha de los equipos	10
3.1. Requisitos de la solución propuesta	10
3.2. Plan de Gestión de tiempo y recursos	11
4. Servicio de alojamiento	13
4.1. Características del Datacenter	13
4.2. Energía y climatización	14
4.3. Facilidades de la instalación	14
4.4. Seguridad física y contra incendios	16
4.5. Servicio de manos remotas	16
4.6. Devolución del servicio	17
5. Gestión del servicio de alojamiento	18
5.1. Gestión de Servicios	18
5.2. Gestión de la Relación	19
5.2.1. Modelo de Referencia	20
5.2.2. Comité de Dirección	21
5.2.3. Comité de Seguimiento y control	22
5.2.4. Comité Operacional	23
5.3. Gestión del Servicio	24
5.4. Seguimiento e informes	25
5.5. Acuerdos de nivel de servicio	26
Cálculo de Penalizaciones en Parámetros	¡Error! Marcador no definido.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

6 Auditoría.....	28
6.1 Principios	28
6.2 Procedimientos de auditoría	29
6.2.1 Organización de la auditoría.....	29
6.2.2 Plan de Auditoría	29
6.2.3 Notificación.....	30
6.2.4 Reunión de arranque.....	31
6.2.5 Trabajo de campo.....	31
6.2.6 Informe de auditoría	31
6.2.7 Seguimiento.....	32
6.2.8 Software para la auditoría.....	32
6.2.9 Documentación.....	32
6.2.10Auditorías realizadas por terceros	32
7 Requisitos de Seguridad de obligado cumplimiento	34
ANEXO 1. TABLAS DE ACUERDOS DE NIVEL DE SERVICIO	69

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

1. Objeto y alcance del servicio

El objeto del contrato es el traslado y alojamiento de uno de los dos Centros de Proceso de Datos (CPD) de Canal de Isabel II S.A. M.P. (en adelante Canal) a un “Colocation datacenter”, un espacio que reúna las condiciones técnicas necesarias para alojar con las condiciones adecuadas de disponibilidad y seguridad las infraestructuras TIC que dan soporte a los procesos de negocio de Canal.

Actualmente Canal dispone de dos CPD que funcionan en modo activo-activo localizados en municipios diferentes. El CPD objeto del servicio de alojamiento le denominaremos CPD-A, mientras que el CPD que permanecerá en instalaciones de Canal se nombra por CPD-B.

Ambos CPD están conectados por líneas de fibra óptica propietarias, por dos caminos diferentes para asegurar la redundancia. Todos los datos y servicios están redundando en ambos centros, de forma que la operación de la empresa está asegurada aunque se produzca un fallo que deje uno de ellos fuera de servicio.

El objeto del contrato comprende también los servicios de telecomunicaciones para la interconexión del CPD-B con la nueva ubicación, con prestaciones similares o superiores a las conexiones actuales en términos de velocidad, fiabilidad y redundancia.

Una vez realizado el proyecto de alta de las telecomunicaciones, dentro del ámbito del contrato se producirá el traslado e instalación de los equipos en el datacenter seleccionado y la puesta en marcha del mismo para su funcionamiento conjunto con el CPD-B, de forma que se mantengan los procedimientos de continuidad de negocio actuales.

1.1. Descripción y ubicación de los CPD

Se detalla en el Anexo de Arquitectura.

1.2. Descripción de la red backbone entre CPDs

Se detalla en el Anexo de Arquitectura.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

1.3. Descripción del sistema mainframe

Se detalla en el Anexo de Arquitectura.

1.4. Descripción del sistema open y virtualización

Se detalla en el Anexo de Arquitectura.

1.5. Descripción del sistema de base de datos

Se detalla en el Anexo de Arquitectura.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

2. Proyecto de establecimiento de telecomunicaciones

2.1 Requisitos de la solución propuesta

El proyecto de Telecomunicaciones debe permitir la conexión entre el Collocation y el CPD-B de Canal permitiendo la replicación de datos entre ambos a nivel de red SAN, así como satisfacer las necesidades de interconexión a nivel TCP/IP.

Para garantizar esta conexión entre CPDs, la solución propuesta deberá cumplir:

- Redundancia: La interconexión entre los CPD debe realizarse por dos caminos físicos diferentes, con equipamiento independiente, de forma que la caída de una de las líneas no tenga impacto en el servicio.
- Los circuitos de cada uno de los dos caminos físicos serán de la misma capacidad, debiendo asegurar el siguiente ancho de banda cada uno de ellos:
 - o Capacidad de 8 enlaces LAN 10 GbE
 - o Capacidad de 4 enlaces SAN 8 Gbps para replicación de las cabinas open
 - o Capacidad de 2 enlaces SAN 8 Gbps para replicación de las cabinas mainframe.
- Los circuitos deben tener posibilidad de ampliación de capacidad, bien a través de fibras oscuras adicionales o por mayor aprovechamiento del ancho de banda de las utilizadas, para satisfacer futuras necesidades. A tal efecto, se recogen los precios de ampliaciones de ancho de banda en el cuadro de precios.

La transmisión de paquetes en la red debe cumplir los siguientes requisitos cuantitativos:

- Latencia de red entre CPDs inferior a 3 milisegundos. Se considera este valor de latencia atendiendo a las necesidades de replicación síncrona de las cabinas.
- Jitter inferior a 0,5 ms. Se considera este valor de latencia atendiendo a las necesidades de replicación síncrona de las cabinas.
- Pérdida de paquetes inferior al 0,05%

Adicionalmente, la solución de comunicaciones debe contemplar:

- La interconexión del campus de oficinas centrales que actualmente se realiza a los switch core que van a trasladarse (consultar el apartado de descripción de la red backbone del Anexo de Arquitectura).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Inclusión de todos los elementos de red necesarios para la conexión de los circuitos de telecomunicaciones con el equipamiento de red de Canal (multiplexores, transceptores, adaptadores fibra/cobre, switches específicos, etc.). Esta inclusión se refiere a ambos extremos de la conexión, tanto en el Datacenter donde se ubicará el CPD-A como el equipamiento que sea necesario en el CPD-B.

2.2 Plan de Gestión del proyecto

La puesta en marcha de las telecomunicaciones se gestionará como un proyecto cerrado.

El adjudicatario presentará un Plan de Proyecto. Este documento contiene una visión global del Proyecto, definiendo como se ejecuta, supervisa y controla el proyecto.

El **Plan de Proyecto**, debe contener la siguiente información:

- Estructura de Desglose del Trabajo (EDT): descomposición en paquetes de los trabajos a realizar. A su vez estos paquetes se desglosarán de nuevo, hasta llegar a un nivel suficiente de desglose en que quede detallado correctamente el alcance y que éste contemple los requisitos del proyecto.
- Asignación de pesos a cada paquete de trabajo (% en coste o esfuerzo respecto al total del proyecto), junto con su tiempo, fechas de inicio y fin previstas.
- Asignación de recursos humanos, la lista del equipo que realizará los distintos trabajos (gestión y desarrollo). Se detallará la relación entre cada actividad, según la EDT, y los responsables de llevarla a cabo. En el caso de ser necesario, se incluirá también el acopio de material necesario para la realización de la tarea.
- Establecimiento de los tipos, mecanismos y flujos de la información, es decir la comunicación necesaria para el proyecto.
- Para garantizar el éxito de los proyectos es necesario un análisis de las amenazas y oportunidades que se puedan presentar a lo largo del ciclo de vida del proyecto. Para intentar que los riesgos no lleguen a materializarse o que su impacto sea mínimo se establecerá el correspondiente plan de mitigación para cada uno de ellos.
- Entregables del proyecto, en una lista que incluirá los responsables de su elaboración, revisión y aprobación.
- Mecanismos de medición de calidad del producto (planes de prueba, PPI programa de inspección por puntos), de forma que puedan verificarse los requisitos de calidad exigidos.
- El mecanismo de control de las variaciones que se produzcan en el alcance, y la se documentarán y aprobarán en su caso. Estas pueden causar una replanificación completa del proyecto.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

El desglose de tareas se representará en un cronograma en forma de diagrama de Gantt o equivalente, debiendo existir una relación biunívoca entre las actividades de la EDT (Plan de Gestión del Alcance) y las actividades detalladas en el cronograma.

Al comienzo del proyecto se realizará la reunión de lanzamiento (Kick-off) que dará paso a la fase de ejecución. Con esta reunión se pretende que todas las personas que participan en el mismo tengan claro su rol en el proyecto.

Para verificar que el proyecto se desarrolla según este plan, se realizarán reuniones de Seguimiento y Control del mismo.

2.3 Características de las líneas y equipos de comunicaciones

El licitador debe ofertar el establecimiento de líneas de comunicaciones que cumplan los requisitos de ancho de banda, capacidad de ampliación y calidad, bien mediante tecnología DWDM o de otro tipo.

Asimismo, debe incluir todo el equipamiento de comunicaciones necesario para proporcionar la transmisión y conversión de la señal al equipamiento de red de Canal descrito en los anexos, tanto a nivel de cobre LAN como de fibra óptica SAN. Este requerimiento incluye ambos extremos, tanto en el Datacenter donde se alojará el CPD como en las instalaciones de Canal en las que haya que incluir equipamiento (incluyendo los SFP que sean necesario).

Este equipamiento tiene la consideración de parte de la línea de comunicaciones, por lo que la propiedad y mantenimiento del mismo es del adjudicatario y su coste debe estar considerado en la oferta económica bien como parte del proyecto de telecomunicaciones o prorrateado en el alquiler de las líneas.

En la oferta económica del PCAP se recogen posibles ampliaciones de capacidad de las líneas de telecomunicaciones. La revisión de los servicios de telecomunicaciones para su posible ampliación o reducción se realizará dos veces al año.

Canal de Isabel II es operador de telecomunicaciones. En las revisiones semestrales de servicios de comunicaciones se podría solicitar la disminución de los circuitos de comunicaciones al pasar a prestarse por medios propios. La reducción de servicios

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

implicaría una reducción de los servicios facturados de manera análoga a la ampliación de los mismos:

- Inicialmente, se facturarán los servicios de comunicaciones con la configuración inicial de número de circuitos y capacidad solicitada.
- La ampliación del número de circuitos de comunicaciones se producirá al precio ofertado para el añadido de circuito adicional. Este precio corresponde al incremento mensual de precio de los servicios de telecomunicaciones de la línea por cada circuito añadido.
- La ampliación de la capacidad se facturará de acuerdo al precio ofertado, que corresponde al incremento mensual del precio por cada circuito que se migre a una capacidad superior.
- El añadido de un circuito de capacidad superior tendrá el precio correspondiente al circuito de capacidad básica más la ampliación de capacidad.
- La reducción del número de circuitos de comunicaciones implicará una disminución del precio de los servicios de telecomunicaciones equivalente al precio de la adición de un circuito.
- La reducción de la capacidad de un circuito producirá una minoración de la facturación de los servicios de comunicaciones equivalente al precio de ampliación de capacidad.
- En caso de que el servicio de telecomunicaciones de Canal absorba el conjunto completo de servicios de telecomunicaciones correspondientes a uno de los apartados del escenario de valoración (servicios línea primaria LAN, servicios línea primaria SAN, servicios línea secundaria LAN, servicios línea secundaria SAN), dejaría de prestarse y facturarse ese servicio.

El equipamiento debe ser capaz de proporcionar los posibles aumentos de capacidad, siendo responsabilidad del adjudicatario la adaptación o sustitución de los mismos para cubrir las ampliaciones que se soliciten.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

3. Proyecto de traslado y puesta en marcha de los equipos

3.1 Requisitos de la solución propuesta

En paralelo al proyecto de establecimiento de las comunicaciones, se comenzará la preparación del traslado del CPD.

- Diseño del cerramiento. La configuración actual del CPD a trasladar y el equipamiento en el momento de redacción del pliego se detalla en el Anexo de Arquitectura.
- Revisión del equipamiento del CPD y etiquetado de todos los componentes para el traslado.
- Montaje del cerramiento, suministro de racks, cableado y adecuación para la recepción de los equipos.
- Tendido de cableado con la Meet Me Room para la conexión con el equipamiento de telecomunicaciones.
- Desmontaje, embalado, transporte y montaje de los equipos en el Datacenter destino.
- Puesta en marcha de los equipos, en colaboración con los servicios de administración de Canal.
- Certificación post-movimiento del equipamiento de los fabricantes NetApp e IBM. El adjudicatario deberá contratar con dichos fabricantes la certificación del movimiento de su equipamiento.

El proyecto de traslado debe cumplir con los siguientes requisitos:

- El cerramiento debe tener una capacidad para 20 racks, lo que Canal considera suficiente para el equipamiento actual y posibles ampliaciones. Se puede admitir división en dos cerramientos de 10 racks.
- El suministro de armarios para el montaje del cerramiento corre a cargo del licitador.
- El traslado y puesta en marcha de los equipos debe realizarse en un único fin de semana, con objeto de minimizar el impacto sobre negocio. A efectos de este traslado, se considera que el fin de semana comienza a las 17:00 horas del viernes y termina a las 07:00 horas del lunes.
- El adjudicatario es responsable de la integridad física del equipamiento durante el proyecto de traslado. Se responsabilizará de la reparación o sustitución de cualquier equipo o componente que resulte dañado en el mismo a la mayor brevedad posible.
- El sistema mainframe puede ser objeto de un traslado independiente del sistema open al no compartir equipamiento. Si bien esta separación tiene ventajas desde el punto de vista de prueba de los sistemas y la carga de trabajo del fin de semana, aumenta la complejidad del traslado de los servicios de red.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- La facturación de los servicios de alojamiento comenzará al comienzo del montaje del cerramiento. Este montaje se realizará en paralelo con la última fase del proyecto de establecimiento de las comunicaciones. Con objeto de que Canal no resulte perjudicado por retrasos en la ejecución de los proyectos se establecen en el PCAP las correspondientes penalizaciones por retrasos en los proyectos.

3.2 Plan de Gestión de tiempo y recursos

El traslado y puesta en marcha del CPD se gestionará como un proyecto cerrado.

El adjudicatario presentará un Plan de Proyecto coordinado con el Plan de Proyecto de puesta en marcha de las Telecomunicaciones. Este documento contiene una visión global del Proyecto, definiendo como se ejecuta, supervisa y controla el proyecto.

El **Plan de Proyecto**, debe contener la siguiente información:

- Estructura de Desglose del Trabajo (EDT): descomposición en paquetes de los trabajos a realizar. A su vez estos paquetes se desglosarán de nuevo, hasta llegar a un nivel suficiente de desglose en que quede detallado correctamente el alcance y que éste contemple los requisitos del proyecto.
- Asignación de pesos a cada paquete de trabajo (% en coste o esfuerzo respecto al total del proyecto), junto con su tiempo, fechas de inicio y fin previstas.
- Asignación de recursos humanos, la lista del equipo que realizará los distintos trabajos (gestión y desarrollo). Se detallará la relación entre cada actividad, según la EDT, y los responsables de llevarla a cabo. En el caso de ser necesario, se incluirá también el acopio de material necesario para la realización de la tarea.
- Establecimiento de los tipos, mecanismos y flujos de la información, es decir la comunicación necesaria para el proyecto.
- Para garantizar el éxito de los proyectos es necesario un análisis de las amenazas y oportunidades que se puedan presentar a lo largo del ciclo de vida del proyecto. Para intentar que los riesgos no lleguen a materializarse o que su impacto sea mínimo se establecerá el correspondiente plan de mitigación para cada uno de ellos.
- Entregables del proyecto, en una lista que incluirá los responsables de su elaboración, revisión y aprobación.
- Mecanismos de medición de calidad del producto (planes de prueba, PPI programa de inspección por puntos), de forma que puedan verificarse los requisitos de calidad exigidos.
- El mecanismo de control de las variaciones que se produzcan en el alcance, y la se documentarán y aprobarán en su caso. Estas pueden causar una replanificación completa del proyecto.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

El desglose de tareas se representará en un cronograma en forma de diagrama de Gantt o equivalente, debiendo existir una relación biunívoca entre las actividades de la EDT (Plan de Gestión del Alcance) y las actividades detalladas en el cronograma.

Al comienzo del proyecto se realizará la reunión de lanzamiento (Kick-off) que dará paso a la fase de ejecución. Con esta reunión se pretende que todas las personas que participan en el mismo tengan claro su rol en el proyecto.

Para verificar que el proyecto se desarrolla según este plan, se realizarán reuniones de Seguimiento y Control del mismo. Dada la brevedad del proyecto, las reuniones serán semanales.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

4. Servicio de alojamiento

4.1 Características del Datacenter

El datacenter propuesto para el alojamiento del CPD debe cumplir con las siguientes características:

- **Ubicación:** El datacenter debe estar ubicado a una distancia mínima de 5 kilómetros del CPD-B de Canal (por cuestiones de resiliencia ante desastres), y a un máximo de 50 kilómetros del centro de trabajo de los técnicos, que se encuentra en la actual ubicación del CPD-A (por cuestiones operativas y logísticas). Estas distancias se medirán en línea recta.
- **Disponibilidad:** El datacenter debe cumplir el principio básico de mantenimiento concurrente y tener un nivel de disponibilidad Tier III o equivalente ($\geq 99,982\%$), es decir tiene que cumplir los requisitos exigidos en la modalidad “construcción”, con múltiples sistemas y rutas para energía, refrigeración, conectividad y sistemas redundantes y aisladas entre sí que permitan al personal de operaciones y mantenimiento, trabajar en la configuración garantizando en todo momento la continuidad de los servicios desplegados en el CPD.
- **Redundancia:** Todas las instalaciones y componentes de los sistemas críticos (energía, refrigeración, comunicaciones, etc.) deben tener un nivel de redundancia mínimo de N+1, de forma que se asegure que el fallo en un componente no tiene afección operativa.
- **Tolerante a fallos después de fallo simple:** El datacenter debe asegurar que ante cualquier fallo simple en cualquier punto de la instalación, la operación TI no se resiente. Para justificar esta tolerancia debe indicar las medidas con las que consigue esta tolerancia, como redundancia de componentes, partes de la instalación con redundancias superiores a N+1 (por ejemplo, 2N o 2N+1), vías de distribución (energía, refrigeración, comunicaciones) dobles simultáneamente activas, compartimentación de las vías de distribución, mecanismos de continuidad (sistemas de alimentación ininterrumpida, grupos electrógenos, equipos de refrigeración auxiliares, etc.)
- **Operadores e infraestructura de comunicaciones:** El datacenter debe contar con doble acometida independiente de comunicaciones y disponibilidad de alquiler de fibras oscuras. El datacenter debe tener servicio al menos con 4 operadores diferentes. Asimismo, debe contar con servicios de conexión inalámbrica con disponibilidad para instalar infraestructura de conexión a este tipo de servicios (p.e. Starlink, TETRA, etc.)
- **Servicio de conexión cloud con Azure:** El Datacenter debe prestar servicio de conectividad ExpressRoute con la nube de Azure en alguna de sus modalidades (colocación de CloudExchange, conexión Ethernet punto a punto, conexión IPVPN a través de MPLS, etc).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Servicio de conexión cloud con proveedor alternativo: El Datacenter debe prestar servicio de conectividad con otro cloud alternativo a Azure, por ejemplo Google Cloud Interconnect, AWS Direct Connect o OCI FastConnect.

4.2 Energía y climatización

El datacenter propuesto para el alojamiento del CPD debe cumplir con las siguientes características relativas a energía y climatización:

- El datacenter debe contar con una política de gestión energética, avalada mediante una certificación independiente (LEED, ISO 50001 o similar).
- El factor PUE (Power Usage Effectiveness) del datacenter debe cumplir con los siguientes valores de referencia. El PUE en diseño y el de carga IT actual deben poder ser acreditados, y este factor será objeto de seguimiento durante la ejecución del contrato:
 - PUE en diseño inferior a 1,35
 - $PUE \leq 1,3$ con carga IT superior al 50%
 - $PUE \leq 1,4$ con carga IT entre el 30 y el 50%
 - $PUE \leq 2,0$ con carga IT inferior al 30%
- Soporte de huellas de distintas densidades, en el rango de 2 a 22 Kw (con una media estimada de 5 Kw por huella).
- Dispositivos de medida de parámetros eléctricos instantáneos y consumo acumulado.
- Rango de temperatura de la sala del CPD adecuado, con una temperatura media en cada periodo de 24 horas de entre 21° y 23°, con una fluctuación entre 18° y 26°.
- Rango de humedad de la sala del CPD adecuado, con una humedad en el rango de entre el 30% y el 60%.
- Sensorización ambiental de la sala del CPD con sensores de temperatura, humedad y detección de fuga de líquidos.

4.3 Facilidades de la instalación

El datacenter propuesto para el alojamiento del CPD debe poner a disposición de Canal las siguientes facilidades:

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Cerramiento securizado exclusivo para el CPD de Canal con capacidad para 20 racks.
- Dos localizaciones en racks separados para comunicaciones en Sala Meet Me Room (MMR). Dado que se requieren comunicaciones separadas para asegurar la continuidad, las entradas de las líneas primaria y secundaria se producirán por acometidas diferentes y tendrán como destino equipos en racks diferentes.
- Sala de almacén compartida para recepción de nuevo material y depósito de material retirado hasta su recogida.
- Gestión de la recepción y entrega a Canal del material.
- Sala de trabajo compartida para su utilización puntual por personal técnico de Canal con derecho de uso de hasta 4 puestos con conectividad de red bajo reserva.
- Derecho de uso de hasta 2 plazas de aparcamiento bajo reserva en el propio datacenter o en aparcamiento concertado en las proximidades, para facilitar el desplazamiento ocasional de los técnicos de Canal.
- Disponibilidad de muelle de carga/descarga con plataformas hidráulicas o rampa niveladora.

En cuanto al servicio de monitorización, siendo posible darlo por diferentes medios (intercambio de ficheros, acceso a herramienta de monitorización del datacenter), la forma preferida por Canal es la integración con su sistema de monitorización basado en Nagios, que es un criterio técnico valorable:

- Servicio de alertas 24x7 con comunicación vocal y avisos por SMS/email al personal designado por Canal para la comunicación de eventos urgentes.
- Recepción de avisos y solicitudes 24x7 por herramienta de ticketing, proporcionando a Canal los mecanismos para la notificación de los mismos.
- Servicio de Monitorización, que permita hacer seguimiento y control del CPD y del uso eficiente de los recursos energéticos. El adjudicatario deberá facilitar como mínimo información con un decalaje máximo de 15 minutos de los siguientes valores:
 - Acceso al cerramiento
 - Temperatura y humedad de la sala del CPD
 - Temperatura y humedad del pasillo frío
 - Temperatura y humedad del pasillo caliente
 - Estado de fuga de líquidos
 - Consumo acumulado del contador eléctrico a través del cual se facture (KWh)
 - Voltaje (V) y Amperaje (A) de las líneas eléctricas
 - Potencia activa instantánea (KW)
 - Potencia aparente instantánea (KVA)

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Alarmas referentes al estado de suministro eléctrico de la red general, los sistemas de alimentación ininterrumpida del datacenter y las líneas eléctricas que alimenten al CPD de Canal.

4.4 Seguridad física y contra incendios

El datacenter propuesto para el alojamiento del CPD debe tener las siguientes medidas de seguridad física:

- Control de acceso a las instalaciones
- Control de acceso al cerramiento privado.
- Acompañamiento, registro, vigilancia y seguridad del personal externo que esté autorizado a entrar a la sala IT de Canal de Isabel II SA
- Servicio de videovigilancia y anti-intrusión de las instalaciones

El datacenter debe contar con medidas anti-incendios que aseguren la integridad de las instalaciones y equipamiento, siendo obligatorias las siguientes.:

- Detectores de humo e incendios en todas las salas TI y “facilities”.
- Sistemas de extinción de incendios mediante agentes limpios que permita la extinción total y eficaz de fuegos de clase A, B y C. Cumplimiento con las normas EN15004-2 y NFPA 2001
- Pulsadores de disparo manual e inhibición de disparo
- Resistencia mínima al fuego de puertas y muros de 120
- Sistema de Extracción Rápida de Humos y/o Agentes Contaminantes

4.5 Servicio de manos remotas

El datacenter propuesto para el alojamiento del CPD debe ofrecer servicio de manos remotas, con personal cualificado para realizar las tareas que se describen a continuación y que podrán ser solicitadas puntualmente y facturadas ad-hoc de acuerdo a los precios ofertados en el escenario de valoración del PCAP:

- Provisión, Instalación/desinstalación y etiquetado de cableado de cobre y fibra
- Instalación/Desinstalación de hardware, racks y etiquetado

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Instalación de periféricos, tales como discos, memoria y dongles USB
- Chequeos visuales de los sistemas instalados
- Reinicio de equipos: Reinicios seguros y ordenados de sistemas y servidores siguiendo procedimiento específico
- Ejecución de comandos desde consola bajo procedimiento específico y a petición de Canal por imposibilidad de acceso remoto al equipo
- Traslados de racks y/o equipos individuales
- Proceso de protección y embalaje del equipamiento
- Cambio y custodia de cintas
- Retirada y achatarramiento de equipamiento obsoletos. Certificado de destrucción/entrega a centro de recepción de residuos.

4.6 Devolución del servicio

Con antelación a la finalización del servicio, Canal solicitará al adjudicatario un plan de devolución de servicio que debe ejecutarse de manera coordinada con Canal para el traslado del CPD o el traspaso del servicio dentro del mismo datacenter a un nuevo adjudicatario.

El adjudicatario está obligado a colaborar con los servicios de traslado incluyendo:

- Documentación de la instalación y configuración del cableado.
- Acceso del personal que determine Canal al cubo privado y las facilidades de la instalación (almacén, muelle de carga, etc.).
- Pruebas de comunicaciones
- Conexión y desconexión de servicios de telecomunicaciones.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

5 Gestión del servicio de alojamiento

Canal considera que, para el éxito de este proyecto, es imprescindible un Modelo de Gestión y de Relación con los Proveedores sólido y consistente, capaz de evolucionar los servicios externalizados de acuerdo con la evolución del negocio y de la tecnología.

En este apartado describiremos el Modelo de Gestión requerido por Canal. El proveedor deberá presentar antes del comienzo del servicio el modelo de gestión que describa con detalle suficiente la organización del servicio y el equipo de trabajo. 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 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.

5.1 Gestión de Servicios

El proveedor es 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 calidad acordados con Canal.

Para completar estas actividades, el proveedor deberá utilizar el modelo **ITIL-ITSM**. El objetivo que persigue Canal es disponer de un entorno de gestión estándar que permita realizar cambios, incorporaciones o bajas en los servicios.

Canal considera como un requerimiento imprescindible contar con estructuras de servicio flexibles, que permitan los cambios en cualquier aspecto del servicio que sea preciso como consecuencia de cambios en la demanda de servicios a los usuarios o áreas de negocio de Canal. Además, debe garantizar que el servicio se beneficia del avance de la tecnología, tanto en mejoras de calidad de servicio o productividad como en su coste.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Un aspecto crítico para el éxito del proyecto y que, por lo tanto, será valorado especialmente, son los mecanismos para gestionar la variabilidad del ámbito de los Servicios a lo largo de la vida del contrato.

El proveedor debe describir los procedimientos, métodos y herramientas que propone implantar para la gestión de cambios en el servicio. El proveedor deberá proponer concretamente un Procedimiento de Gestión de Cambios al Servicio capaz de gestionar:

- Cambios en los procesos del Servicio
- Cambios en los documentos y en los Apéndices
- Cambios en el Ámbito de los servicios contenido en el Contrato
- Cambios en los ANS
- Cambios como consecuencia de la implantación o ejecución de iniciativas de mejora o de los Planes de Transformación
- 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 de los contratos que regulan la prestación de los servicios

5.2 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 para responder a los cada vez más rápidos cambios en el entorno de negocio de Canal.
- Asegurar que la relación definida incluye de forma proactiva la innovación TIC y que esta se traduce en beneficios para Canal.

Dicho modelo está basado en el Modelo de referencia que se expone a continuación.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

5.2.1 Modelo de Referencia

El Modelo requerido se estructura en tres niveles.

- El **nivel estratégico** es el encargado de velar por que la estrategia y objetivos del servicio estén alineados con los corporativos, y de controlar y garantizar que todas las decisiones y operaciones se ajustan a dicha estrategia.
- El **nivel táctico** se encarga de transformar las decisiones estratégicas en planes de operación y acción y de coordinar, dirigir y controlar los esfuerzos necesarios para su ejecución.
- El **nivel operacional** se responsabiliza de la gestión, ejecución, supervisión técnica y control diario de los servicios.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

5.2.2 Comité de Dirección

Frecuencia	Comité	Responsabilidades	Asistentes	
			CANAL	Proveedor
Semestral (o tras 10 días de la petición de cualquiera de las partes)	Dirección	<ul style="list-style-type: none"> Revisar y aprobar los cambios en los servicios de Telecomunicaciones propuestos por el comité de Seguimiento y control Aprobar los cambios en el ámbito del servicio propuestos por el Comité de Seguimiento y Control 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. 	<ul style="list-style-type: none"> Director ejecutivo (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas) (*) 	<ul style="list-style-type: none"> Gestor Estratégico (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas)

(*) Rol que preside el Comité

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

5.2.3 Comité de Seguimiento y control

Frecuencia	Comité	Responsabilidades	Asistentes	
			CANAL	Proveedor
Mensual (o a petición de cualquiera de las partes)	Seguimiento y control	<ul style="list-style-type: none"> ■ 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 ■ Coordinar los grupos y personas asignados a la entrega del Servicio ■ Discutir nuevos requerimientos o cambios en los servicios contratados. ■ Elevar al Comité de Dirección los cambios en los servicios necesarios realizando el informe justificativo correspondiente. ■ Asegurar que el personal asignado para la ejecución de los servicios por el proveedor 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 	<ul style="list-style-type: none"> ■ Jefe de Proyecto / Responsable Operativo (*) 	<ul style="list-style-type: none"> ■ Responsable del Servicio/ Proyecto

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Frecuencia	Comité	Responsabilidades	Asistentes	
			CANAL	Proveedor
		<ul style="list-style-type: none"> Servir como punto único de contacto entre las organizaciones de Canal y del proveedor 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 		

(*) Rol que preside el Comité

5.2.4 Comité Operacional

Frecuencia	Comité	Responsabilidades	Asistentes	
			CANAL	Proveedor
		<ul style="list-style-type: none"> Elaborar planes de detalle de actuación para las modificaciones acordadas en los servicios prestados 	<ul style="list-style-type: none"> Jefe de Proyecto / Responsable Operativo (*) Técnicos 	<ul style="list-style-type: none"> Jefe de Proyecto / Responsable Operativo Técnicos

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Frecuencia	Comité	Responsabilidades	Asistentes	
			CANAL	Proveedor
Semanal / A petición de cualquiera de las partes	Operativo	<ul style="list-style-type: none"> Realizar seguimiento continuo de los servicios contratados y la calidad de los mismos. Revisar la lista de incidencias y tareas pendientes y asignar prioridades. Coordinar los grupos y personas asignados a la entrega del Servicio Detectar necesidades o mejoras necesarias en el servicio y elaborar informe propuesta para el Comité de Seguimiento y Control. Verificar que el personal asignado para la ejecución de los servicios por el Proveedor 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 Revisar y facilitar al Comité de Seguimiento y Control cualquier información que le sea solicitada. 		

(*) Rol que preside el Comité

5.3 Gestión del Servicio

- **Niveles Táctico y Operativo.** Tener una visión detallada que permita:
 - Controlar el cumplimiento de los niveles de servicio
 - Monitorizar y ajustar los niveles de servicio

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- Seguimiento y control de fallos, incidencias y problemas
- Control de las configuraciones y topologías de sistemas y redes
- Control y seguimiento de la capacidad y de los planes e iniciativas relacionadas con 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

El proveedor debe detallar en el Plan de Gestión de la Comunicación dentro del Plan de Gestión del Proyecto las herramientas y procesos que componen el Sistema de Gestión Integrado que propone utilizar. El proveedor incluirá en su descripción ejemplos de interfaces, informes, etc.

5.4 Seguimiento e informes

Se establecen como estándar los informes de seguimiento siguientes, que deberán ser entregados una semana antes de las reuniones:

Informe mensual de seguimiento del servicio

Informe 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, el cumplimiento de los indicadores de nivel de servicio y la identificación proactiva de problemas en el cumplimiento del ANS.

Informe para el Comité de Dirección

Informe 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Adicionalmente a estos informes, y ante situaciones específicas, el Proveedor deberá presentar información requerida bajo demanda y en particular para cubrir los puntos descritos en el Comité Operacional.

5.5 Acuerdos de nivel de servicio

Se entiende por Acuerdos Nivel de Servicio (ANS), los parámetros que, inicialmente será necesario cumplir para considerar que el Proveedor cumple con sus compromisos. El proveedor puede proponer valores diferentes o parámetros adicionales, justificando convenientemente su inclusión y con un detalle similar al menos al que se marcan los aquí descritos. Canal, a su único criterio, podrá considerar o no los cambios sugeridos por el Proveedor.

La calidad y el compromiso mostrado a través de este acuerdo son un criterio para valorar la oferta del proveedor.

El ANS acordado y el procedimiento para su gestión, tendrán carácter contractual.

Para la medición de los niveles de servicio se establecen los indicadores de objetivo que se indican en este apartado. Adicionalmente se establecen otros indicadores (indicadores de rendimiento) para realizar un seguimiento de la actividad.

El Proveedor deberá satisfacer los niveles de servicio establecidos según los indicadores de objetivo. Si al finalizar un periodo de monitorización no se ha cumplido un indicador el Proveedor deberá establecer medidas correctoras.

El Proveedor proporcionará mensualmente un informe a Canal para verificar el cumplimiento del Proveedor con los niveles de servicio establecidos a través de los indicadores de objetivo. Este informe podrá ser publicado en panel electrónico propiedad del proveedor. El proveedor, en este caso, dará acceso a este panel a Canal mediante usuario y contraseña.

Canal valorará especialmente las herramientas que el Proveedor propone implantar para facilitar la monitorización activa de ANS. La funcionalidad y alcance de tales herramientas deberán ser detallados en su propuesta (incluyendo ejemplos ilustrativos).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Canal podrá en todo momento auditar la información facilitada por el Proveedor, así como las fuentes de datos.

En caso de fallo en la provisión de los Servicios de acuerdo con los requerimientos de calidad acordados, el Proveedor incurrirá en una penalización, que tiene como objetivo una compensación económica que refleje que ha entregado los Servicios con un nivel de calidad inferior al comprometido.

Las penalizaciones aplicables así como el método de cálculo de las mismas se encuentran recogidas en el apartado 9.1 del anexo I del PCAP.

En el Anexo 1 Tablas de Acuerdos de Nivel de Servicio se indican los ANS de este servicio.

Independientemente de las Penalizaciones que sean de aplicación, el Proveedor deberá elaborar e implementar sin coste adicional para Canal un **Plan de Acciones Correctivas** ("PAC") para todos los incumplimientos de los Parámetros de control del ANS.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

6 Auditoría

Se definen los principios y procedimientos aplicables a las actividades de auditoría de Canal y terceros (auditores externos, reguladores, etc.) en los servicios proporcionados por el Proveedor.

6.1 Principios

Canal tendrá derecho a auditar los servicios prestados por el Proveedor durante la vigencia del presente contrato con el fin de determinar:

- El cumplimiento de los servicios según lo especificado en este pliego.
- El cumplimiento de los Acuerdos de Nivel de Servicio
- La integridad y exactitud de los informes.
- La exactitud de los costes facturados.

Canal tiene derecho a llevar a cabo una auditoría en cualquiera de los siguientes momentos:

- Una vez al año.
- Durante la ejecución del proyecto de establecimiento de las telecomunicaciones o del proyecto de traslado.
- A la finalización del proyecto de establecimiento de las telecomunicaciones o del proyecto de traslado.
- Cuando circunstancias específicas den a Canal motivos razonables para el supuesto de que el Proveedor no cumple con sus obligaciones contractuales.

Los costes facturados por un auditor externo elegido por Canal serán pagados por Canal. Cualquier gasto razonable incurrido por el Proveedor con respecto a la auditoría correrá a cargo del Proveedor.

Si el resultado de la auditoría demuestra que el Proveedor ha facturado sus servicios a Canal con un sobrecoste con respecto a los cargos acordados, el Proveedor reembolsará

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

con prontitud las cantidades cobradas de más, más un 5% de penalización sobre dichas cantidades. Si el importe cobrado excede el 5% de los cargos correctos, el Proveedor además correrá a cargo con los costes de la auditoría a Canal.

Sin perjuicio de cualquier otro derecho de Canal, si el resultado de la auditoría demuestra que el rendimiento real de Proveedor no cumple con la oferta, los niveles de servicio o si la auditoría revela cualquier otro rendimiento insuficiente o falta de cumplimiento, el Proveedor definirá, planificará e implementará las mejoras necesarias para subsanar tal incumplimiento que serán autorizadas por Canal. Se hará un Plan de Mejora de la auditoría como se describe en este documento.

6.2 Procedimientos de auditoría

6.2.1 Organización de la auditoría

Canal y el Proveedor asignarán un coordinador de auditoría en el Cliente y en el Proveedor.

6.2.2 Plan de Auditoría

No existe una planificación fija acordada para las auditorías. Cada año Canal preparará un Plan de Auditoría que refleje, al menos, lo siguiente:

- Universo de auditoría (en términos de potenciales objetos de auditoría).
- Lista no limitativa de auditorías que Canal llevará a cabo en el año en curso.
- Calendario previsto.
- Seguimiento de Auditorías.

Canal puede cambiar el Plan de Auditoría durante el año cuando Canal identifica la necesidad de hacerlo. Los cambios en el Plan de Auditoría se comunicarán al coordinador de auditoría del Proveedor.

El coordinador de auditoría de Canal gestionará el Plan de Auditoría y mantendrá relaciones con las otras partes pertinentes de auditoría (auditores externos, reguladores, etc.), coordinará y supervisará las iniciativas de auditoría y actualizará los requisitos de auditoría y Plan de Auditoría con respecto a los servicios proporcionados por el Proveedor

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

cuando sea necesario. El Coordinador de Auditoría de Canal comunicará el Plan de Auditoría anual al Coordinador de Auditoría del Proveedor.

6.2.3 Notificación

Canal notificará al Coordinador de Auditoría del Proveedor de una próxima auditoría con un mes de antelación. Dicha comunicación contendrá información sobre los requisitos de auditoría en los siguientes términos:

- Los objetivos de la auditoría.
- Alcance de la auditoría.
- Duración de la auditoría.
- Listado de información necesaria que debe estar disponible (este listado puede ser modificado durante la auditoría).
- Actividades especiales que los auditores necesiten realizar (ejecución de software de auditoría o scripts).
- Ubicación(es) de auditoría.
- Roles implicados y fechas en las que deben estar disponibles.
- Nombres de los auditores.

El Coordinador de Auditoría del Proveedor evaluará los requisitos de auditoría e informará al Coordinador de Auditoría de Canal sobre cualquier conflicto que afecte a la auditoría.

Para las auditorías causadas por circunstancias específicas que den a Canal motivos razonables para el supuesto de que el Proveedor no cumple con sus obligaciones contractuales, se notificará al Coordinador de Auditoría del Proveedor tan pronto como sea razonablemente posible. Si no hay tiempo para definir los requisitos de auditoría, la notificación puede ser informal.

En estos casos, el Proveedor proporcionará la información solicitada y el acceso a los datos con alta prioridad.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

6.2.4 Reunión de arranque

La reunión de arranque se llevará a cabo el primer día de la auditoría, con el Proveedor, Canal y los auditores para comunicar a los participantes los requisitos de la auditoría a fin de eliminar cualquier confusión.

6.2.5 Trabajo de campo

El Coordinador de Auditoría del Proveedor facilita el trabajo de auditoría, poniendo a disposición del equipo auditor los distintos elementos expuestos en los requisitos de auditoría y haciendo que los roles implicados estén disponibles y con el propósito de acelerar el proceso de auditoría. Aquellos que participen en alguna reunión durante el proceso de auditoría resolverán la solicitud de información adicional (documentación, datos, procedimientos, etc.) y verificarán que las actas de las reuniones reflejan los puntos tratados y resultados obtenidos.

El Coordinador de Auditoría del Proveedor podrá asistir a cualquier reunión de trabajo de campo durante el proceso de auditoría.

El trabajo de campo incluye:

- Entrevistas con empleados del Proveedor o con terceros contratados por el Proveedor.
- Consulta de documentación.
- Pruebas de los procedimientos tomando muestras.
- Otras actividades que se requieran para ofrecer garantías suficientes sobre la calidad de los procesos y datos.

6.2.6 Informe de auditoría

Cada auditoría se traduce en un informe de auditoría donde se refleja el cumplimiento del servicio según el alcance establecido. El informe de auditoría se presentará en una reunión a la que asistirán el Coordinador de Auditoría de Canal y el Coordinador de Auditoría del Proveedor.

El Coordinador de Auditoría del Proveedor elaborará un Plan de Mejora para solventar las posibles no conformidades expuestas en el informe. En dicho Plan de Mejora se indicará,

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

para cada no conformidad, las acciones a tomar, la fecha en la que acción será completada y la persona responsable de realizar la acción. El Plan de Mejora se entregará a Canal no más tarde de un mes después de la fecha del informe de auditoría. Canal aprobará el Plan de Mejora y lo remitirá al equipo auditor para su aprobación final.

6.2.7 Seguimiento

Se realizará un seguimiento del cumplimiento de las acciones del Plan de Mejora debido a la auditoría. Dicho seguimiento se realizará en las reuniones de seguimiento del servicio establecidas mensualmente según se indica en el Modelo de Gobierno.

6.2.8 Software para la auditoría

Con el fin de acelerar el proceso de auditoría mediante la automatización de actividades, el equipo auditor podrá solicitar la instalación y ejecución de cierto software de auditoría o de scripts relacionados. En ese caso se seguirá el proceso de Gestión de Cambios acordado. El software de auditoría y los scripts pueden incluir descarga de datos de Canal o del Proveedor o la extracción de la configuración de equipos. El Proveedor facilitará la implantación del software de auditoría o scripts.

6.2.9 Documentación

Canal puede acceder a toda la documentación necesaria que mantiene el Proveedor que está relacionada con los servicios. El Proveedor entregará una copia (electrónica) de la documentación pertinente si es necesario. Canal y el equipo auditor tratarán toda la documentación suministrada por el Proveedor con carácter confidencial,

6.2.10 Auditorías realizadas por terceros

Canal puede decidir delegar las actividades de auditoría a auditores independientes. El Proveedor tratará estos auditores independientes de manera similar a lo descrito en este documento y los considerará como si fueran empleados de Canal. En los casos auditorías realizadas por terceros, Canal seguirá siendo responsable de la Auditoría. La auditoría realizada por terceros nunca será realizada por un competidor en el ámbito de los servicios del Proveedor.

Canal puede decidir contratar a expertos en la materia para delegar actividades de auditoría específicas. El Proveedor podrá rechazar a estos expertos en la materia si

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

concurrirán motivos razonables. Si el Proveedor rechaza el experto en la materia, propondrá un experto en la materia alternativo comparable al presentado por Canal. Estos expertos firmarán un acuerdo de confidencialidad aceptable para el Proveedor.

Canal será responsable de las acciones u omisiones de estos auditores independientes y asegurará que se adhieran a las obligaciones derivadas del Acuerdo Marco de Servicios, como si fueran parte del mismo (por ejemplo, en temas de confidencialidad), sin obstáculos o impedimentos.

El Coordinador de Auditoría del Proveedor y el Coordinador de Auditoría de Canal se mantendrán mutuamente informados acerca de las actividades previstas por el auditor independiente.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

7 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 del Servicio:

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 del Servicio, como en caso de contingencia. Además, será obligatorio, salvo que se disponga de autorización expresa, que la prestación del Servicio 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, del Servicio que se realicen.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio.
- 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 del Servicio), 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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. El adjudicatario asegura que, en caso de resultar adjudicatario, para el alcance del proyecto detallará su estrategia y plan de no obsolescencia.

PS.08 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 del Servicio, debiendo cumplir los requisitos correspondientes de seguridad en relación con parte del contrato en que intervenga.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 de Canal de Isabel II. Esta supervisión incluye, aunque no se limita, a la visión y acceso en modo sólo lectura a las consolas de los diferentes sistemas de seguridad que soporten el Servicio, los usuarios que tienen acceso, los permisos de éstos, los eventos, configuraciones, reglas, etc.; en suma, a cuantos elementos recojan, traten, transmitan, procesen y almacenen información relativa a los sistemas 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.

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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio a Canal de Isabel II. Dicho personal deberá contar con formación y conocimientos específicos de las tecnologías involucradas en la prestación del Servicio, Seguridad de la Información y la legislación aplicable en el contexto del Servicio.

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 ALTO, 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 del Servicio.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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:

- Fecha de recogida del material.
- Personal proveedor encargado de la recogida y transporte.
- 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 las plataformas, sistemas y servicios que soportan el Servicio, debe ser conforme a los roles y autorizaciones de dichos roles previamente definidos y autorizados por los Responsables de la Información y del Servicio de Canal de Isabel II y el Responsable del Sistema.

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

SD.01.03 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.01.04 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 Traspase seguro de datos entre entornos:

SD.02.01 El adjudicatario deberá describir su estrategia para evitar fugas de información derivadas del traspase de datos entre los distintos entornos, así como detectar e inventariar proactivamente la presencia de datos sensibles / regulados en

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

las diferentes bases de datos del Servicio 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 las 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, los sistemas y servicios que soportan el Servicio, 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 se apliquen 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,

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 Centros de Datos, etc., desde donde se presten el Servicio.

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:

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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 prestarán o que harán uso del Servicio, 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 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 del Servicio, una vez que éste deje de formar parte del equipo de trabajo asignado a la prestación del Servicio.

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 El Servicio ofertado por el licitador deberá:

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

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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 El Servicio ofertado 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 del Servicio, 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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 del Servicio 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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:

- Dirección IP del equipo.
- Nombre del equipo (*hostname*).
- Dirección MAC del equipo
- Inventario actualizado del Software instalado en cada equipo.
- Modelo del equipo.
- Versión del sistema operativo instalado.
- 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).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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:

- Dirección IP del equipo.
- Nombre del equipo (*hostname*).
- Dirección MAC del equipo
- Inventario actualizado del Software instalado en cada equipo.
- Modelo del equipo.
- Versión del sistema operativo instalado.
- 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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,

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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 del Servicio 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio ofertado. 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, 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 cualquiera de los elementos que soporten la prestación del Servicio prestado a Canal de Isabel II.

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 del Servicio 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 del Servicio prestado a 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 del Servicio ofertados.

SI.17 Todos los sistemas y micro-servicios del Servicio 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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:

- Empresa proveedora encargada de alojar el servicio en la nube.
- Direccionamiento IP.
- Puertos requeridos para la provisión del Servicio.
- Geolocalización de cada uno del Servicio 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 del Servicio.

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).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- 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 del Servicio, 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 parchado de elementos de la plataforma y de toda las infraestructura, sistemas y servicios involucrados en la prestación del Servicio, 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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 del Servicio 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio, 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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 del Servicio 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 del Servicio 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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				

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio, 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 contratadas 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 contratada 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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 del Servicio 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.

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

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:

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

- 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

(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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Firmado electronicamente por: Elías Manrique
Rojo
En la fecha y hora 01.10.2025 10:55:10 CEST

Firma: Elías Manrique Rojo
ÁREA INFRAESTRUCTURA INFORMÁTICA

Firmado electronicamente por: Ángel Rodríguez
García
En la fecha y hora 01.10.2025 11:02:41 CEST

Firma: Ángel Rodríguez García
SUBDIRECCIÓN DE SISTEMAS INFORMÁTICOS

Firmado electronicamente por: JUAN
SÁNCHEZ GARCÍA
En la fecha y hora 01.10.2025 20:30:34 CEST

Firma: Juan Sánchez García
DIRECCIÓN INNOVACIÓN E INGENIERÍA

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

ANEXO 1. TABLAS DE ACUERDOS DE NIVEL DE SERVICIO

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
CPD01	Indisponibilidad del CPD	Porcentaje de tiempo en el que se ha producido una indisponibilidad del servicio de alojamiento.	100 – (Tiempo total disponible/Tiempo total)	100 – Valor ofertado en A)2.3	100 - (Valor ofertado + 0.001)	0,018	10
CPD02	Temperatura del CPD	Número de incumplimientos de las condiciones de temperatura indicadas en el apartado 4.2	Conteo a partir de las alertas del sistema de monitorización requerido en el apartado 4.3	0	1	4	5

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
CPD03	Humedad del CPD	Número de incumplimientos de las condiciones de humedad indicadas en el apartado 4.2	Conteo a partir de las alertas del sistema de monitorización requerido en el apartado 4.3	0	1	4	2
CPD04	Seguridad de accesos	Número de incumplimientos de las condiciones de seguridad de accesos indicadas en el apartado 4.4	Conteo a partir de las alertas del sistema de monitorización requerido en el apartado 4.3	0	1	2	1
COM01	Indisponibilidad de las comunicaciones	Porcentaje de tiempo en el que se ha producido una indisponibilidad de los servicios de telecomunicaciones	100 – (Tiempo total disponible/Tiempo total)	0	0,001	0,018	10

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
COM02	Latencia de red	Tiempo en milisegundos de transmisión de paquetes de datos entre CPD on-prem y el datacenter..	Test periódicos de red. Se tomará el valor más alto recogido en cada test.	3	3.2	4	6
COM03	Jitter de red	Variabilidad en milisegundos en el tiempo de llegada de los paquetes de datos entre CPD on-prem y datacenter.	Test periódicos de red. Se tomará el valor más alto recogido en cada test.	0.5	0.6	1	3
COM04	Pérdida de paquetes	Porcentaje de paquetes perdidos en la transmisión entre CPD on-prem y datacenter.e	Test periódicos de red. Se tomará el valor más alto recogido en cada test.	0.05	0.06	0.10	4

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
MON01	Fallos de monitorización	Número de caídas del sistema de monitorización o falta de ficheros de datos	Conteo de los fallos	0	1	4	2
FAC01	Indisponibilidad de las facilidades auxiliares	Número de ocasiones en las que se ha requerido el uso de las facilidades especificadas en el apartado 4.3 y no han estado disponibles	Conteo de los fallos	0	1	2	1
MAN01	Tiempo de respuesta del servicio de manos remotas en incidentes críticos	Tiempo en horas desde que se comunica el incidente hasta que el servicio de manos remotas inicia las actuaciones para resolverlo.	Tiempos registrados en el sistema de ticketing	0.5	1	2	2

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
MAN02	Tiempo de respuesta del servicio de manos remotas en incidentes no críticos	Tiempo en horas desde que se comunica el incidente hasta que el servicio de manos remotas inicia las actuaciones para resolverlo	Tiempos registrados en el sistema de ticketing	2	4	24	1
MAN03	Tiempo de respuesta del servicio de manos remotas en solicitudes	Tiempo en horas desde que se comunica la solicitud hasta que el servicio de manos remotas inicia las actuaciones para resolverla	Tiempos registrados en el sistema de ticketing	8	24	72	1
SRV01	Fiabilidad información	Fiabilidad de la información facilitada. Ausencia de información requerida, errores en las medidas o en el cálculo de los KPI.	Errores o falta de información detectados en los informes. Errores en los datos de disponibilidad del hosting, de disponibilidad de las comunicaciones o de cualquier actividad en el ámbito del contrato.	0	1	2	1

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A. M.P.	Alojamiento CPD	Sept. 2025
Elaborado por	Documento	Versión
Área de Infraestructura Informática	Pliego de Prescripciones Técnicas	V1.0

Código	Parámetro	Descripción	Cálculo	Vc	Va	Vi	Peso
SRV02	Retrasos en la entrega de los informes de servicio	Retrasos en la entrega de los Informes según las especificaciones establecidas	Total de días de retraso en la entrega de los informes de ANS respecto a los plazos acordados	0	2	7	1