

## PLIEGO DE PRESCRIPCIONES TÉCNICAS

### CONTRATO DE SUMINISTRO DE SUSCRIPCIÓN SOLUCIÓN FAX SaaS PARA CANAL DE ISABEL II, S.A., M.P.

EXPEDIENTE N.º: 145/2026

Área: Planificación y Control

## Índice

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>1. Introducción .....</b>                             | <b>3</b>  |
| <b>2. Alcance.....</b>                                   | <b>4</b>  |
| 2.1. Suministros Incluidos en el Contrato .....          | 4         |
| 2.1.1. Fax Entrante y Fax Saliente .....                 | 4         |
| 2.1.2. Email Transaccional .....                         | 4         |
| <b>3. Mantenimiento y Soporte .....</b>                  | <b>5</b>  |
| 3.1. Soporte técnico .....                               | 5         |
| 3.2. Funcionalidades .....                               | 5         |
| 3.3. Servicios Adicionales.....                          | 6         |
| 3.4. Soporte a los servicios.....                        | 6         |
| <b>4. Requisitos de Seguridad .....</b>                  | <b>7</b>  |
| <b>5. Roles y Responsabilidades en el Contrato .....</b> | <b>21</b> |
| <b>6. Formato de las especificaciones técnicas .....</b> | <b>22</b> |

## 1. Introducción

El contrato es el suministro de la suscripción en modalidad SaaS de fax entrante y saliente tanto de aplicaciones como de carácter general (Mail to Fax y Fax to Email) además del servicio de email transaccional (Transactional Email).

Canal de Isabel II, S.A., M.P. (en adelante Canal) tiene en explotación la solución en modalidad software como servicio (en adelante SaaS) del fabricante Retarus consistente en el servicio de fax entrante y saliente tanto de aplicaciones como de carácter general (Mail to Fax y Fax to Email) además del servicio de email transaccional (Transactional Email). A la fecha de finalización de esta suscripción, Canal necesita mantener la continuidad de licenciamiento del software con el fin de mantener el servicio al resto del negocio.

El objeto del contrato es la provisión de un sistema de información en modalidad (SaaS) consistente en el suministro de fax entrante y saliente tanto de aplicaciones como de carácter general (Mail to Fax y Fax to Email) además del suministro de email transaccional (Transactional Email). Así mismo, se ampliará la volumetría máxima de emails/mes y el rendimiento de envío en emails/hora.

Para el cumplimiento de la estrategia de la Subdirección de Sistemas Informáticos, el sistema de información será un sistema comercial llave en mano y en la modalidad de software como servicio (SaaS), con el fin de que sea independiente de la infraestructura informática de Canal.

## 2. Alcance

### 2.1. Suministros Incluidos en el Contrato

Los servicios objeto del contrato son los que se incluyen a continuación:

| Servicio: Fax Entrante y Saliente              |
|------------------------------------------------|
| <b>Concepto</b>                                |
| Tasa mensual (incluye 3.500 páginas mensuales) |
| <b>TOTALES</b>                                 |

| Servicio: Transactional Email                            |
|----------------------------------------------------------|
| <b>Concepto</b>                                          |
| Tasa mensual (incluye 250.000 emails)                    |
| Tráfico Max. mensual adicional estimado (100.000 emails) |
| Soporte Técnico Avanzado                                 |
| <b>TOTALES</b>                                           |

#### 2.1.1. Fax Entrante y Fax Saliente

Suministros que se han de proveer:

- Servicio de Fax entrante y saliente que es gestionado a través de aplicaciones informáticas.
- Servicio de envío y recepción de Fax de carácter general vía email.
- Mantenimiento de Faxes virtuales existentes
- Sustitución de Faxes físicos por Faxes virtuales

#### 2.1.2. Email Transaccional

Servicio de email masivo transaccional.

- Tráfico mensual estimado máximo hasta 350.000 emails/mes y 10.000 emails/hora

### 3. Mantenimiento y Soporte

Al objeto de satisfacer las necesidades de comunicación de los procesos de Canal de Isabel II, S.A., M.P. se requiere de múltiples servicios de comunicación mediante Fax e Email.

Las principales requisitos y funcionalidades que estos servicios deben proporcionar son las siguientes:

#### 3.1. Soporte técnico

- Capacidad de procesamiento de emails garantiza contractualmente
- Capacidad de portabilidad de numeración fax
- Lista de bloqueo automática, con borrado automático de hasta 45 días.
- Centros de coste configurables por defecto y por transacción
- Facturación detallada, sin prepago ni “créditos”
- Compatible con Unicode (soporte de juego de caracteres europeos y asiáticos, etc.)
- Personalización automática de portadas de fax
- Envío de múltiples mensajes mediante una única invocación REST
- Mecanismos de integración SMTP y REST.
- Cifrado de las comunicaciones mediante VPN
- Soporte de DKIM y SPF
- Soporte local, en horario oficina, en idioma castellano
- Reporting en tiempo real, con estados de entrega de emails, apertura y clics.
- Informes de transmisión detallados, estadísticas, análisis, informe mensual detallado
- Plataforma de gestión EAS, bajo entorno web seguro, con posibilidad de creación de distintos niveles de acceso y roles.
- Datacenters en Europa, propios, con alta disponibilidad garantizada.

#### 3.2. Funcionalidades

- Configuración de prioridades de transmisión de FAX y programación de entrega hasta el minuto exacto.
- Tecnología NeverBusy
- Procesamiento de emails en paralelo, con múltiples Tokens, mediante la misma integración
- Archivado de FAX (7 días incluidos; opción hasta 120 meses)
- Gestión activa del operador, conexiones redundantes a través de múltiples carriers
- Respuesta Automática de Fax
- Reconocimiento de códigos de barras y OCR.
- Función de comentarios en Fichero PDF.
- Tickets de soporte integrados en herramienta de administración
- Soporte de cabecera “unsubscribe” SMTP
- Mecanismos de gestión de reputación de los dominios de envío SMTP
- SPAM score del email previo al envío masivo
- Soporte de FeedBack Loop (FBL) en envíos SMTP
- Sincronización de directorios

- Personalización del dominio de envío de fax.

### 3.3 Servicios Adicionales

- Facilidad de Trace and Recover.
- Administrador de recepciones, respuestas y rebotes (Bounce and Response Manager)
- Línea de alta disponibilidad (Por Dedicated IP de IPV4) y conexión VPN (conexión alternativa a 2 DCs)
- Setup de los ajustes específicos de Canal
- Capacidad de procesamiento de envíos a 10.000 correos hora

### 3.4 Soporte a los servicios

Por parte del proveedor durante el periodo de vigencia del contrato. Será intrínseco a las suscripciones y cubrirá el diagnóstico y resolución de incidentes de forma remota en horario laborable. El servicio de soporte técnico contemplará los siguientes puntos:

- La provisión, configuración y puesta en marcha de los servicios.
- La resolución de incidencias.
- La atención de dudas, cuestiones o aclaraciones relativas a la configuración y utilización de los servicios, incluso formación en los servicios prestados.
- La indicación de recomendaciones sobre conectividad, integración, seguridad, etc del SaaS en aras a optimizar el aprovechamiento del servicio.
- Paquete de 6 horas/año de soporte técnico avanzado a demanda de Canal de Isabel II, S.A., M.P.

## 4. Requisitos de Seguridad

- **Principios de Seguridad de obligado cumplimiento para la prestación de los servicios objeto del contrato.**

- **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, y sin limitarse a, el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (en adelante, Directiva NIS2), y 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.

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

El licitador 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. Por otro lado, el adjudicatario deberá obtener de Canal de Isabel II autorización para cualquier cambio de ubicación geográfica o de los países desde los que presta el Servicio.

- **Políticas de Seguridad.**

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

- **Responsabilidad.**

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.

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 "roles de seguridad" de estos requisitos de seguridad.

○ **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.

○ **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 frente a 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.

○ **Garantías de supervisión.**

■ **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.

■ **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.

■ **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.

■ **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.

- Disponibilidad, Recuperación, contingencia, crisis, continuidad de negocio y planes de salida.

De entre los diversos escenarios en los que sea necesario aplicar un plan de contingencia o incluso el de salida, por parte de Canal de Isabel II es de particular importancia la necesidad de identificar y retener, a alto nivel, las competencias básicas adecuadas a un nivel operativo dentro de Canal de Isabel II para que, in extremis, pueda tener la capacidad de reanudar el control directo de las actividades objeto del contrato. 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 deberán aportar los certificados de destrucción segura emitidos por un prestador de servicios que acrediten la eliminación completa, irreversible y confidencial de datos o documentos, ya sean físicos o digitales que contengan información propiedad de Canal de Isabel II.

- 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.

- **Cumplimiento normativo.**

- El adjudicatario, de conformidad con la Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, se asegurará de que se satisfarán las obligaciones en relación con los incidentes de seguridad.
- Tal como se recoge en el PCAP, el adjudicatario debe contemplar el compromiso de devolución y/o destrucción (a elección de Canal de Isabel II) de toda la información propiedad de Canal de Isabel II recabada durante la ejecución de los Servicios.
- Si por la naturaleza del proyecto, Canal de Isabel II requiere del borrado y destrucción de cualquier soporte de información englobado dentro del alcance de los Servicios prestados; el adjudicatario deberá aplicar un procedimiento seguro de borrado y destrucción conforme a lo indicado en el Esquema Nacional de Seguridad en lo referente al borrado y destrucción de soportes de información.

- Asimismo, para cada borrado y destrucción realizada, el adjudicatario deberá entregar a Canal de Isabel II un certificado emitido por un prestador de servicios que acredite la eliminación completa, irreversible y confidencial de datos o documentos, ya sean físicos o digitales, que recogerá, al menos, los siguientes campos:
  - Fecha de recogida del material.
  - Personal proveedor encargado de la recogida y transporte.
  - Procedimiento detallado empleado en el borrado y destrucción realizada.
  - Fecha de la destrucción de la información.
- **Roles de seguridad.**
  - **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.
  - **Responsable del Proyecto.**

El adjudicatario debe disponer de un Responsable del Proyecto.
  - **Equipo de seguridad.**

El adjudicatario debe disponer de un completo equipo de seguridad que garantice el diseño, la construcción, configuración, monitorización, operación y administración de los controles de seguridad y privacidad para el correcto mantenimiento del nivel de riesgo aprobado por Canal de Isabel II.
  - 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.
- **En relación con las auditorías.**
  - Canal de Isabel II podrá solicitar informes técnicos de auditorías, o cualquier otro documento relevante para evidenciar que se mantienen en todo momento los niveles de seguridad de los servicios que presta el adjudicatario durante toda la ejecución del contrato (por ejemplo: SSAE16, IASE 3402 SOC 2 Tipo II, etc.)

- Canal de Isabel II podrá realizar revisiones de seguridad y de continuidad de negocio, así como auditar los sistemas de información y procesos que traten, almacenen o gestionen información de su propiedad.
- El adjudicatario deberá proporcionar a Canal de Isabel II o a cualquier tercero designado a tal efecto por Canal de Isabel II y/o Autoridad de Control, acceso completo de la institución a las ubicaciones y centros de trabajo desde los que se presten los Servicios, incluyendo cualquier dispositivo, sistema, red y datos utilizados para la prestación de los Servicios contratados (derecho de acceso).
- La empresa adjudicataria deberá colaborar con Canal de Isabel II para dar cumplimiento a las obligaciones internas y externas de auditoría.
  - Canal de Isabel II se encuentra sujeta a diversas auditorías externas, ya sea por requerimientos regulatorios, legales, normativos, sectoriales, contractuales, etc. Es por ello por lo que Canal de Isabel II podrá solicitar al adjudicatario, sólo si es estrictamente necesario, su colaboración diligente con el fin de entregar las evidencias y participar en las entrevistas de auditoría.
  - Estas auditorías pueden responder a las siguientes necesidades:
    - Auditoría bianual (autoimpuesta).
    - Auditorías de terceros, entre otras, y no excluyentes:
      - IGAE.
      - Tribunal de cuentas.
      - Económico – Financiera.
      - UIC.
      - CNPIC.
      - Auditorías extraordinarias.

- **En relación con la Ciberdefensa.**

- El adjudicatario deberá presentar una descripción detallada de su estrategia de actualización y no obsolescencia de la tecnología, controles o los procesos involucrados en la prestación de los Servicios, incluyendo la frecuencia de las actualizaciones, el ciclo de vida de los componentes que la integran y las medidas previstas para garantizar su vigencia tecnológica. Asimismo, deberá describir su proceso de gestión de vulnerabilidades, indicando los procedimientos de detección, análisis, clasificación, mitigación y corrección, así como los SLA comprometidos para la remediación de vulnerabilidades en función de su criticidad.

Atendiendo a la siguiente clasificación de priorización, los SLAs no serán mayores en ningún caso que los indicados:

|                                                                  | RIESGO           |                                                                                                                     |                          |
|------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|
| CRITERIO                                                         | BAJO (1 punto)   | MEDIO (2 puntos)                                                                                                    | ALTO (3 puntos)          |
| Gravedad de la vulnerabilidad<br>(según <i>scoring</i> CVSSv4.0) | Baja             | Media                                                                                                               | Alta o Crítica           |
| Probabilidad de explotación                                      | Improbable       | Posible                                                                                                             | Muy probable             |
| Exposición del sistema                                           | Sólo uso interno | Accesible desde redes no confiables (equivalente a la definición de “zona no controlada” según se define en el ENS) | Accesible desde Internet |
| Impacto en el Negocio<br>(según BIA)                             | Muy Bajo o Bajo  | Medio                                                                                                               | Alto o Muy Alto          |

La probabilidad de explotación se evalúa considerando el nivel de exposición del activo, la disponibilidad de mecanismos o métodos conocidos para aprovechar la vulnerabilidad y la complejidad técnica necesaria para hacerlo. Se clasifica como:

- **Improbable** cuando no existen reportes ni evidencia de intentos de explotación y la vulnerabilidad requiere condiciones poco comunes.
- **Posible** cuando se tiene conocimiento de intentos o métodos limitados que demandan condiciones o conocimientos específicos.
- **Muy probable** cuando existen métodos ampliamente conocidos, evidencia de explotación activa o alta exposición del activo a entornos externos o no controlados.

El riesgo final se calcula mediante la siguiente fórmula: **Riesgo = Gravedad × Probabilidad × Exposición × Impacto**

En base al valor obtenido, se establecen los siguientes niveles de prioridad y tiempos máximos de actuación:

- Nivel de Prioridad Alto ( $\geq 28$  puntos):
  - Mitigación temporal (*workaround*): En caso de que exista una medida de mitigación validada por el equipo de Ciberseguridad de Canal de Isabel II, se deberá aplicar en un plazo máximo de 48 horas.
  - Solución definitiva: máximo 15 días naturales a partir de la disponibilidad de la solución definitiva.
- Nivel de Prioridad Medio ( $9 \leq 27$  puntos):

- Mitigación temporal (*workaround*): En caso de que exista una medida de mitigación validada por el equipo de Ciberseguridad de Canal de Isabel II, se deberá aplicar en un plazo máximo de 72 horas.
  - Solución definitiva: máximo 30 días naturales a partir de la disponibilidad de la solución definitiva.
- Nivel de Prioridad Bajo ( $\leq 8$  puntos):
    - Mitigación temporal (*workaround*): En caso de que exista una medida de mitigación validada por el equipo de Ciberseguridad de Canal de Isabel II, se deberá aplicar en un plazo máximo de 5 días naturales.
    - Solución definitiva: máximo 35 días naturales a partir de la disponibilidad de la solución definitiva.
- El adjudicatario deberá disponer de mecanismos, controles y capacidades de seguridad específicamente diseñados para entornos *cloud*, garantizando su integración con arquitecturas virtualizadas, autoescalables y dinámicas. Dichos mecanismos deberán ser compatibles con modelos de infraestructura y despliegue basados en infraestructura como código (IaC), configuración mediante plantillas, microsegmentación, centros de datos definidos por software (SDDC), arquitecturas de microservicios, contenedores, orquestadores, pipelines CI/CD y prácticas DevSecOps.
    - A tal efecto, el adjudicatario deberá describir detalladamente la estrategia, metodologías, procedimientos, herramientas y servicios que empleará para garantizar la seguridad de la solución durante todo su ciclo de vida, incluyendo, al menos, las capacidades de protección, monitorización, detección, respuesta y mejora continua de la seguridad en entornos *cloud*.
  - 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 auditoría 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.
    - 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.
    - Los registros deben incluir al menos los siguientes campos: Actividad, acceso, IP origen, IP destino y usuario.
    - Los registros deben estar normalizados para que su información pueda ser relacionada con otras fuentes e interpretada adecuadamente. Es responsabilidad del adjudicatario realizar estas tareas.
    - Los registros podrán ser entregados 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 registros 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.
- 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.
  - El adjudicatario deberá comunicar al Área de Ciberseguridad de Canal de Isabel II 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 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.
  - 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.
  - 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.).
- El adjudicatario deberá realizar periódicamente pruebas de seguridad sobre las aplicaciones, infraestructuras y demás componentes que soporten la plataforma objeto del contrato, incluyendo, cuando resulte aplicable, pruebas de intrusión (*pentesting*), ejercicios de hacking ético, análisis de vulnerabilidades u otras actividades equivalentes de evaluación de la seguridad.
  - Cuando dichas actuaciones afecten directa o indirectamente a los entornos, sistemas, servicios o datos de Canal de Isabel II y se ejecuten durante la vigencia del contrato, el

adjudicatario deberá comunicarlo previamente al Jefe de Proyecto designado por Canal de Isabel II y obtener su autorización expresa antes de su realización.

- La solicitud de autorización deberá incluir, al menos, la identificación de las personas y organizaciones que participarán en las pruebas, el alcance previsto, la metodología a emplear, las ventanas de ejecución, los posibles impactos esperados, así como los acuerdos de confidencialidad, privacidad y demás garantías legales aplicables.
  - Una vez realizadas las pruebas, el adjudicatario deberá poner a disposición de Canal de Isabel II los informes completos de resultados, incluyendo las vulnerabilidades identificadas, su clasificación por criticidad, el análisis de impacto, las recomendaciones de mitigación y, en su caso, el plan de remediación correspondiente. Dichos informes deberán ser compartidos con el Área de Ciberseguridad de Canal de Isabel II.
  - El adjudicatario deberá describir las metodologías, procedimientos, herramientas, soluciones y demás activos que prevé utilizar y la justificación de su idoneidad para garantizar el correcto funcionamiento, seguridad, rendimiento y evolución de la plataforma, así como de 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).
  - La realización de estas pruebas no eximirá al adjudicatario de su obligación de corregir las vulnerabilidades identificadas dentro de los plazos comprometidos en los acuerdos de nivel de servicio (SLA) establecidos para la gestión de vulnerabilidades.
- 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 o los sistemas corporativos de Canal de Isabel II disponibles para ello, y asegurar así la autenticidad de los dominios de Canal de Isabel II, o aquellos que se autoricen expresamente por Canal de Isabel II según el procedimiento existente.
- **Gestión de identidades y accesos.**
    - 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.
    - El adjudicatario deberá entregar a Canal de Isabel II un informe ejecutivo que describa las medidas de seguridad física implementadas para garantizar el control de acceso a las instalaciones (incluyendo CPDs u otras dependencias) desde las cuales se preste el servicio objeto del contrato.
    - 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

datos de alta en los sistemas de Gestión de Identidad 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 profesional.
- Los usuarios del adjudicatario dados de alta en los sistemas de Gestión de Identidad de Canal de Isabel II seguirán en todo momento todas las indicaciones de seguridad que se les transmitan desde Canal de Isabel II junto con sus credenciales de acceso.
  - El adjudicatario deberá identificar los diferentes colectivos que harán uso de los activos de la información objeto del alcance del contrato que en principio son:
    - Personal del adjudicatario.
    - Personal subcontratado (o de la cadena de suministro de las IaaS, PaaS o SaaS).
    - Personal de Canal de Isabel II.
    - Clientes finales.
    - Dentro de estos colectivos se identificarán los usuarios privilegiados (administradores, auditores, seguridad, etc.) y los no privilegiados.
  - El adjudicatario notificará con la mayor diligencia, y siempre por conducto del Responsable del Proyecto designado por la empresa, la desvinculación del personal propio previamente asignado a la prestación de los servicios, tan pronto dicho personal deje de formar parte del equipo de trabajo.
  - Se prohíbe el uso de cuentas genéricas o compartidas. El adjudicatario deberá implementar controles técnicos y procedimientos de monitorización que permitan la detección, registro y notificación de la creación y utilización de credenciales no asociadas de manera individualizada a un único usuario, para garantizar los principios básicos de acceso, la confidencialidad, la integridad y la trazabilidad establecidos en el Esquema Nacional de Seguridad y en otras normativas internacionales de seguridad de referencia (ISO/IEC 27001, etc.).
  - Debe poderse habilitar al menos un segundo factor de autenticación (2FA) resistente a ataques de phishing para garantizar la identidad de los usuarios de los servicios, ya sea mediante el uso de certificados electrónicos cualificados reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.
  - La aplicación del 2FA se debe forzar a nivel de administración del aplicativo para que no pueda ser deshabilitado por el propio usuario. En caso de que el 2FA sí pueda ser deshabilitado por el propio usuario, es obligatorio que existan y se implementen, al menos, los siguientes controles compensatorios adicionales:
    - Notificación automática de eventos (usuario que deshabilita el 2FA).
    - Notificación de inicio de sesión y de inicios de sesión desde direcciones IP extranjeras y por distintos medios (SMS, correo electrónico, etc.).

- Generación de informes periódicos con el listado del estado de configuración de los usuarios (por ejemplo, usuarios que tienen habilitado o deshabilitado el 2FA).
- Restricción de acceso al Servicio objeto de contratación por parte de Canal de Isabel II exclusivamente desde los rangos IP públicos de navegación de Canal de Isabel II.
- **Seguridad de los datos.**
  - Gobierno del dato: Los datos de negocio deben ser protegidos conforme a:
    - El acceso a la plataforma, y los sistemas y servicios que la soportan, debe ser conforme a los roles y autorizaciones de dichos roles previamente definidos y autorizados por el Responsable de la Información y del Servicio de Canal de Isabel II.
    - 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.
  - Cifrado de los datos:
    - 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.
    - Para la parte del cifrado de información en tránsito se hará por tanto uso exclusivo de TLS 1.2 y/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.
    - 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.

• **Cumplimiento del Reglamento Europeo de Inteligencia Artificial.**

- Si el producto o servicio contratado implica la utilización de sistemas o modelos de Inteligencia Artificial, el adjudicatario deberá cumplir con lo dispuesto en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, y normativa de desarrollo, tanto la vigente en el momento del contrato como la que pudiera ser de aplicación durante la duración del mismo y, en todo caso, deberá cumplir con los siguientes requisitos:
  - Asignará e indicará a Canal de Isabel II quien tiene las funciones y responsabilidades técnicas y operativas y proporcionará la dirección y apoyo claros sobre el uso de los sistemas de IA y la aplicación de la ley de protección de datos.
  - En el caso de que se traten datos de categoría especial, en aplicación del art. 10.5 letra f) del RIA, "los registros de las actividades de tratamiento de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, deben incluir las razones por las que el tratamiento de categorías especiales de datos personales es estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no puede alcanzarse mediante el tratamiento de otros datos". Se solicitará 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:<br>[CONCEPCIÓN/ DISEÑO Y DESARROLLO/<br>VERIFICACIÓN Y VALIDACIÓN/ DESPLIEGUE/<br>OPERACIÓN Y MONITORIZACIÓN/ REEVALUACIÓN/<br>RETIRADA] |             |           |         |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------|---------|
|                | Interesado                                                                                                                                                     | Responsable | Encargado | Tercero |
| Recogida       |                                                                                                                                                                |             |           |         |
| Almacenamiento |                                                                                                                                                                |             |           |         |
| Uso            |                                                                                                                                                                |             |           |         |
| Transferencia  |                                                                                                                                                                |             |           |         |
| Eliminación    |                                                                                                                                                                |             |           |         |

- El adjudicatario garantizará que cuenta con una base de legitimación válida para tratar datos personales en cada una de las fases.
  - 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.
  - 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.
  - 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.
  - 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.
  - 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.
  - 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.
  - El adjudicatario asegura haber establecido un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización del sistema.
- Con el objeto de acreditar de manera fidedigna el estado de cumplimiento de todos los requisitos de ciberseguridad establecidos en el presente pliego, el adjudicatario será responsable de revisar y mantener actualizadas, de forma periódica y durante toda la vigencia del contrato, todas las evidencias, informes, registros, certificaciones, etc., especialmente tras cualquier cambio significativo en la infraestructura, el software, los servicios subcontratados o los marcos normativos aplicables, garantizando así, y en todo momento, la vigencia y trazabilidad de la información, que deberá aportar en las reuniones de seguimiento del contrato y estar disponible para su revisión por parte de Canal de Isabel II.

## 5. Roles y Responsabilidades en el Contrato

El contrato se registrará desde su firma y para el plazo estipulado en el mismo a través de unas figuras, tanto de Canal como del Adjudicatario, con sus respectivas responsabilidades que se detallan a continuación. Estas figuras se deben concretar en personas o equipos de personas tanto para Canal de Isabel II, SA, MP como en personas o equipos equivalentes del Adjudicatario del contrato:

### Responsable del Contrato:

El responsable del Contrato por parte de Canal de Isabel II, S.A., M.P. a efectos de lo establecido en el artículo 62 de la LCSP, es el referido en el apartado 10.8 del Anexo I del PCAP.

Sin perjuicio de lo dispuesto en el art 62 el responsable del contrato tendrá las siguientes funciones:

Cumplimiento del contrato en alcance: supervisará que, durante la ejecución del contrato, todos los servicios y suministros que se realicen estén dentro del alcance de este. Gestiona la provisión de suministros y servicios de acuerdo con el contrato, tanto al inicio de este, como para las necesidades contempladas en el contrato que vayan surgiendo durante su ciclo de vida.

Cumplimiento del contrato en coste: supervisará que el coste de los suministros y servicios sea el contratado y que nunca se excederá del precio del contrato.

Cumplimiento del contrato en tiempo: supervisará que se cumplan los plazos acordados y que el contrato no exceda el plazo de ejecución previsto.

### Responsable del Contrato del adjudicatario:

El contratista designará igualmente un responsable del Contrato con las siguientes funciones:

Cumplimiento del contrato en alcance: supervisará que, durante la ejecución del contrato, todos los servicios y suministros que se realicen estén dentro del alcance de este. Gestiona la provisión de suministros y servicios de acuerdo con el contrato, tanto al inicio del mismo, como para las necesidades contempladas en el contrato que vayan surgiendo durante su ciclo de vida.

Cumplimiento del contrato en coste: supervisará que el coste de los suministros y servicios sea el contratado y que nunca se excederá del precio del contrato.

Cumplimiento del contrato en tiempo: supervisará que se cumplan los plazos acordados y que el contrato no exceda el plazo de ejecución previsto.

### Unidad encargada de la ejecución del contrato:

Será la unidad de Canal de Isabel II, S.A., M.P. encargada del seguimiento y ejecución ordinaria del contrato a la que van dirigidos los suministros y/o servicios objeto del mismo y estará en relación directa con el Responsable del Contrato de Canal de Isabel II, S.A., M.P.

### Comunicación de incidencias en materia de Protección de Datos de Canal de Isabel, S.A., M.P.:

Para cualquier cuestión o incidencia en materia de Protección de Datos será de aplicación lo establecido en la Cláusula 29 y en el apartado 11 "Protección de Datos de carácter personal" del Anexo I al PCAP. En el caso de que se produzca un incidente que comprometa o pudiera comprometer los datos de Canal deberá comunicarlo a las direcciones de correo electrónico siguientes: [protecciondatos@canal.madrid](mailto:protecciondatos@canal.madrid) y [ds.ciberseguridad@canal.madrid](mailto:ds.ciberseguridad@canal.madrid) informando al Responsable del Contrato de Canal, independientemente de las acciones que deba ejecutar para subsanar el incidente.

### Comunicación de incidencias en materia de Ciberseguridad

Para cualquier cuestión o incidencia en materia de Ciberseguridad el adjudicatario deberá comunicarlo a la dirección de correo electrónico de contacto de Canal de Isabel II, S.A., M.P. [ds.ciberseguridad@canal.madrid](mailto:ds.ciberseguridad@canal.madrid) informando al Responsable del Contrato de Canal, independientemente de las acciones que deba ejecutar para subsanar el incidente. El adjudicatario del contrato deberá proporcionar a Canal de Isabel II, S.A., M.P. al inicio del contrato, la identificación y/o cargo y forma de contacto (correos electrónicos y teléfonos) del personal responsable en materia de protección de datos y en materia de ciberseguridad.

## 6. Formato de las especificaciones técnicas

La oferta técnica se atenderá al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas Particulares del presente procedimiento.

Firmado electronicamente por: Jesus Plaza Rubio  
En la fecha y hora 16.09.2026 12:52:50 CEST

JEFE DE ÁREA DE PLANIFICACIÓN Y CONTROL

Firmado electronicamente por: Ángel Rodríguez García

SUBDIRECTOR DE SISTEMAS INFORMÁTICOS

Firmado electronicamente por: JUAN SÁNCHEZ GARCÍA

DIRECTOR DE INNOVACIÓN E INGENIERIA