

ANEXO REQUISITOS DE SEGURIDAD

EXPEDIENTE 97/2025 SERVICIOS DE ATENCIÓN AL CLIENTE Y USUARIOS DE CANAL DE ISABEL II, S.A. M.P.

PARTE I

El licitador cumplirá cada uno de los requisitos de seguridad expuestos a continuación y desarrollados en la PARTE II del presente ANEXO. Se acreditará mediante la cumplimentación de la declaración responsable de acreditación de documentación (ANEXO I del Pliego de Cláusulas Administrativas Particulares):

- El licitador asegura 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), conforme a lo indicado en el punto PS.01 de la PARTE II.
- El licitador asegurará que, en caso de resultar Adjudicatario, informará a Canal de Isabel II, S.A. M.P. 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, S.A. M.P., tanto durante la normal prestación de los Servicios, como en caso de contingencia, conforme a lo indicado en el punto PS.01 de la PARTE II.
- El licitador asegura que, una vez sea Adjudicatario realizará un análisis de riesgos conforme al artículo 14 del ENS según la metodología conforme al ENS, que en particular Canal de Isabel II, S.A. M.P. identifica como MAGERIT (herramienta Pilar). Este Análisis de Riesgos (realizado una vez sea Adjudicatario de los Servicios), será compartido con el Área de Ciberseguridad de Canal de Isabel II, S.A. M.P., conforme a lo indicado en el punto PS.04 de la PARTE II.
- El licitador asegura que, en caso de resultar Adjudicatario, para el alcance del proyecto detallará tanto su estrategia y plan de no obsolescencia, como sus compromisos con la Gestión de las Vulnerabilidades (identificación, remediación, SLA), conforme a lo indicado en el punto PS.07 de la PARTE II.
- El licitador garantiza que, en caso de resultar Adjudicatario, pondrá a disposición de Canal de Isabel II, S.A. M.P. 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, conforme a lo establecido en el punto PS.10.04 de la PARTE II.
- El licitador garantiza que, en caso de resultar Adjudicatario, firmará un Acuerdo de Confidencialidad con Canal de Isabel II, S.A. M.P. y cumplirá los procedimientos de seguridad establecidos para los Adjudicatarios, conforme a lo indicado en el punto PS.13 Concienciación de la PARTE II.
- El licitador asegura que, en caso de resultar Adjudicatario, dispondrá de las siguientes figuras, estando debidamente recogidas y documentadas, y siendo personas distintas; tal y como establece el artículo 13.5 en su apartado 5 del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) conforme a lo indicado en el punto SP de la PARTE II.
 - Responsable de Seguridad
 - Responsable del Proyecto
- El contratista completará el cuestionario de evaluación de seguridad de la cadena de suministro, conforme a lo establecido en la Directiva NIS 2 y a lo indicado en el punto PS.14 de la PARTE II.

Se publica junto con los pliegos del presente procedimiento el citado cuestionario en formato hoja de cálculo a efectos meramente informativos. El cuestionario NO debe ser incluido en la oferta por los licitadores.

- El licitador asegura que, en caso de resultar Adjudicatario, dispondrá de los procesos, normas, procedimientos, recursos, actividades, informaciones, registros, facilidades, herramientas y disposición de colaboración que faciliten al Área de Ciberseguridad de Canal de Isabel II, S.A. M.P., las tareas de supervisión, auditoría, gestión y notificación de incidentes de seguridad que se pudieran producir en relación con el servicio, conforme a lo indicado en el punto SP.04, de la PARTE II.
- El licitador garantiza que el servicio soporta mecanismos de federación de la identidad basado en buenas prácticas y estándares del mercado (SAML v2.0, OAuth, etc.), conforme a lo indicado en el punto GI.05.01 de la PARTE II.
- El licitador asegura que, en caso de resultar Adjudicatario, mantendrá y pondrá a disposición de Canal de Isabel II, S.A. M.P. un inventario actualizado de la totalidad de equipos, conforme a lo indicado en el punto EL.09 y SE.03 de la PARTE II.

PARTE II

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

PS.01 Cumplimiento legal, activo. El licitador 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 y la legislación vigente en materia de protección de datos de carácter personal (RGPD y LOPDGDD), referente a los servicios objeto de contratación por parte de Canal de Isabel II, S.A. M.P.

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 licitador asegurará que, en caso de resultar Adjudicatario, informará a Canal de Isabel II, S.A. M.P. 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, S.A. M.P., tanto durante la normal prestación de los Servicios, como en caso de contingencia. Además, será obligatorio, salvo que se disponga de autorización expresa, que la prestación de los Servicios se realice desde el Espacio Económico Europeo. Por otro lado, el Adjudicatario deberá obtener de Canal de Isabel II, S.A. M.P. 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 en el resto de Requisitos que se detallan 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, S.A. M.P. Por lo que la realización de funciones TI por parte de un tercero no debe perjudicar la supervisión de Canal de Isabel II, S.A. M.P. y, por ende, de los servicios que se realicen.

El Adjudicatario 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 SP (roles de seguridad y privacidad) de este documento.

PS.04 Análisis de Riesgos. El licitador 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 el Canal de Isabel II, S.A. M.P. identifica como MAGERIT (herramienta Pilar), salvo que, por indicación contraria y expresa, del Área de Ciberseguridad de Canal de Isabel II, S.A. M.P. se especifique lo contrario. El análisis de riesgos deberá incluir:

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

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

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

PS.05 Gobierno de la seguridad. Se asegurará de que los servicios prestados en virtud del presente procedimiento de contratación, así como los sistemas de información que los sustentan, se prestan de conformidad a los requisitos de seguridad establecidos en el Esquema Nacional de Seguridad.

PS.06 Clasificación de la información y de activos. El Adjudicatario garantizará la confidencialidad de la información propiedad de Canal de Isabel II, S.A. M.P., 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, S.A. M.P. 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, S.A. M.P., en particular, al Área de Ciberseguridad de Canal de Isabel II, S.A. M.P.

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

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

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

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

PS.09 Control de la cadena de suministro de la tercera parte. El Adjudicatario podrá realizar la subcontratación en los términos y condiciones recogidos en el Pliego de Cláusulas Administrativas Particulares y en el Pliego de Prescripciones Técnicas. El subcontratista cumplirá totalmente con las obligaciones existentes entre Canal de Isabel II, S.A. M.P. y el Adjudicatario, incluidas las obligaciones contraídas a favor de las diferentes autoridades de control.

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

PS.10 Garantías de supervisión.

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

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, S.A. M.P. en caso de ser requeridos, así como debidamente protegidos.

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

PS.10.03 Auditorías. El Adjudicatario de los Servicios deberá permitir y colaborar, en el caso que sea necesario, en las diversas auditorías a las que se encuentra sujeta Canal de Isabel II, S.A. M.P.

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

PS.10.04 Documentación. El licitador garantiza que, en caso de resultar Adjudicatario, pondrá a disposición de Canal de Isabel II, S.A. M.P. 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, S.A. M.P. es de particular importancia la necesidad de identificar y retener, a alto nivel, las competencias básicas adecuadas a un nivel operativo en Canal de Isabel II, S.A. M.P. para que, *in extremis*, pueda tener la capacidad de reanudar el control directo de las actividades subcontratadas. El Adjudicatario debe hacer una propuesta de identificación de dichas competencias y capacidades. Además, el Adjudicatario deberá facilitar el proceso de devolución de la información de Canal de Isabel II, S.A. M.P. 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, S.A. M.P.

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

PS.13 Confidencialidad. El personal del Adjudicatario y el personal de las empresas subcontratadas por el Adjudicatario (en caso de que aplique) deberá firmar un Acuerdo de Confidencialidad con el Canal de Isabel II, S.A. M.P., así como cumplir los procedimientos de seguridad establecidos para los Adjudicatarios.

PS.14 Evaluación de Seguridad de la Cadena de Suministro. El contratista 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 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. En caso de no estar certificada el licitador se comprometerá a solicitar dicha certificación antes de 9 meses a partir del inicio de la Fase de Pleno Servicio de los Servicios objeto de contratación, en caso de resultar Adjudicatario.

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

CN.03 Debe contemplarse el compromiso de devolución/destrucción (a elección de Canal de Isabel II, S.A. M.P.) de toda la información propiedad de Canal de Isabel II, S.A. M.P. recabada durante la ejecución de los Servicios.

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

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

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

SD Relativo a la Seguridad de los Datos.

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

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

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

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

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

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

SD.01.06 El Adjudicatario debe mantener la acreditación del cumplimiento con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (*Payment Card Industry Data Security Standard*) o PCI-DSS vigente durante toda la vigencia del contrato.

SD.02 Trasvase seguro de datos entre entornos:

SD.02.01 El Adjudicatario deberá describir su estrategia para evitar fugas de información derivadas del trasvase de datos entre los distintos entornos, así como detectar e inventariar proactivamente la presencia de datos sensibles / regulados en las diferentes bases de datos de la plataforma y de los sistemas y servicios que la soportan. 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, S.A. M.P. información detallada sobre los servicios criptográficos disponibles.

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

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

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

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

SD.04 Protección de Bases de Datos:

SD.04.01 El Adjudicatario deberá describir su estrategia para la protección de las diferentes bases de datos (Cifrado, ofuscación, pseudo-anonimización, etc.) y persistencias de la plataforma y los sistemas y servicios que la soportan, incluyendo las funciones de auditoría

y cifrado de datos sensibles. El Adjudicatario debe describir las metodologías y herramientas / soluciones / activos que se plantea utilizar para lograr este objetivo.

SD.04.02 El Adjudicatario, en caso de alojar información de Canal de Isabel II, S.A. M.P. 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”.

- Si la tecnología de las Bases de Datos es DB2, deberá seguir adicionalmente las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/23 Recomendaciones de seguridad para bases de datos DB2”.
- Si la tecnología de las Bases de Datos es Oracle, deberá seguir adicionalmente las recomendaciones de seguridad establecidas en la Guía “CCN-CERT BP/22 Recomendaciones de seguridad para Oracle Database 19C”.

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 Responsable del Proyecto: El Adjudicatario debe disponer de un Responsable del proyecto.

RS.03 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, S.A. M.P.

RS.04 El licitador debe entender y asumir que la responsabilidad fina de la Seguridad de los datos, recae en el Canal de Isabel II, S.A. M.P. y, por designación de funciones dentro de ésta, en el Responsable de la Seguridad de Canal de Isabel II, S.A. M.P., motivo por el que, en caso de resultar Adjudicatario, 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, S.A. M.P., 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, S.A. M.P. Cualquier acceso no explícitamente autorizado será prohibido. Se deberá proporcionar a Canal de Isabel II, S.A. M.P. un informe ejecutivo con las medidas de seguridad físicas implementadas para el control de acceso a las instalaciones físicas, a los CPDs, etc., desde donde se presten los Servicios.

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

GI.03 Los usuarios del Adjudicatario que vayan a hacer uso de redes o sistemas de información propiedad de Canal de Isabel II, S.A. M.P., y/o vayan a acceder a información propiedad de Canal de Isabel II, S.A. M.P., deben estar dados de alta en los sistemas de Gestión de Identidad de Canal

de Isabel II, S.A. M.P. Para ello, deberán proporcionar al responsable del proyecto de Canal de Isabel II, S.A. M.P. los siguientes datos:

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

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

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

GI.04.01 Personal del Adjudicatario.

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

GI.04.03 Personal de Canal de Isabel II, S.A. M.P.

GI.04.04 Clientes finales.

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

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

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

GI.07 La plataforma, y los sistemas y servicios que la soportan, ofertados por el licitador deberán:

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

GI.07.02 Discernir las solicitudes legítimas de las ilegítimas.

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

GI.07.04 Incluir la capacidad para cumplir con las políticas que la Política de Seguridad de Canal de Isabel II, S.A. M.P. 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 redes sociales y con proveedores de identidades, debiendo describirse los mecanismos por medio de los que se propone posibilitar dichas integraciones y el análisis de riesgos correspondiente.

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

GI.07.07 El Adjudicatario deberá dotar a la plataforma, y los sistemas y servicios que la soportan, 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 el criterio de mínimo privilegio.

GI.07.08 El Adjudicatario deberá explicar y documentar los modelos de autorización previstos y cómo se adaptan a cada caso de uso de la plataforma y de los sistemas y servicios que la soportan.

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 La plataforma y los sistemas y servicios que la soportan dispondrá 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 licitador asegura que, en caso de resultar Adjudicatario, detallará cómo se proporcionará solución para este tipo de usuarios, qué controles aplicará (organizativos, procedimentales) así como las capacidades técnicas (incluidas herramientas) y humanas que se incluyen en la propuesta de gestión segura de acceso de usuarios privilegiados.

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

- o Notificación automática de eventos (usuario que deshabilita el 2FA)
- o Notificación de inicio de sesión y de inicios de sesión desde direcciones IP extranjeras y por distintos medios (SMS, correo electrónico, etc.)
- o Posibilidad de generación de informes periódicos con el listado del estado de configuración de los usuarios (por ejemplo, usuarios que tienen habilitado o deshabilitado el 2FA)
- o Restricción de acceso a los servicios objeto de contratación por parte de Canal de Isabel II, S.A. M.P. desde los rangos IP públicos de navegación de Canal de Isabel II, S.A. M.P.

GG Relativo a la gestión de las grabaciones:

GG.01 El Adjudicatario deberá proporcionar un nivel de seguridad adecuado de acceso a las grabaciones, mediante la utilización de un segundo factor de autenticación (2FA), que incluya la verificación de usuario y contraseña, así como la implementación de un factor adicional de autenticación que será resistente a ataques de *phishing*.

GG.02 Los servidores donde se alojen las grabaciones, deben permitir la configuración de diferentes niveles de acceso basados en roles, asegurando que cada usuario solo pueda acceder a las grabaciones que le correspondan según sus responsabilidades y necesidades. Dichos accesos

deben estar aprobados por el Responsable de la Información y del Servicio de Canal de Isabel II, S.A. M.P.

GG.03 Tanto las grabaciones en tránsito como las almacenadas deben estar cifradas para proteger la confidencialidad y la integridad de los datos.

GG.04 Se debe tener la capacidad de registrar todas las actividades relacionadas con las grabaciones, incluyendo quien accedió, qué acciones se realizaron y cuándo. Estos registros deben ser almacenados de manera segura y estar disponibles para su revisión y auditoría.

GG.05 Se deben implementar medidas de seguridad para proteger la infraestructura contra intentos de intrusión. Además, se deben definir y aplicar políticas de seguridad para proteger los servidores físicamente, así como establecer medidas de mitigación.

GG.06 Se debe implementar un mecanismo de respaldo para garantizar la disponibilidad y la integridad de las grabaciones en caso de fallos o incidentes. Además, se debe tener un plan de recuperación de datos establecido para poder restablecer las grabaciones en caso de pérdida o daño.

GG.07 La administración de los servicios de Canal de Isabel II, S.A. M.P. alojados en la infraestructura del Adjudicatario deberá realizarse a través de equipos dedicados exclusivamente a la administración de los servicios de Canal de Isabel II, S.A. M.P.

GG.08 Además, de no especificarse lo contrario, los datos propiedad de Canal de Isabel II, S.A. M.P. 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, S.A. M.P.

SE1 En relación con la Seguridad de los Equipos:

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

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

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

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

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

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

SE1.06 Deberá colaborar en la elaboración por parte de Canal de Isabel II, S.A. M.P., y cuando este lo requiera, de una política de bastionado de los equipos una vez sea el Adjudicatario del proyecto.

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, S.A. M.P.

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, S.A. M.P.

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, S.A. M.P. 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).

SE1.09 Deberá mantener y poner a disposición de Canal de Isabel II, S.A. M.P. de un inventario actualizado de la totalidad de equipos objeto de la presente licitación. Este inventario deberá contener al menos los siguientes campos:

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

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, S.A. M.P., o a tratar información de Canal de Isabel II, S.A. M.P.:

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

SE2.02 El Adjudicatario deberá mantener los equipos actualizados a la última versión de Software disponible por el o los fabricantes, según un proceso o política de actualización que

deberá ser elaborado por el Adjudicatario. Además, no debe estar próxima la fecha de finalización del soporte el software instalado en dichos equipos.

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

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

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

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

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

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

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

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

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

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

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

DM En relación con los dispositivos móviles del Adjudicatario que vayan a conectarse a las redes o sistemas de información de Canal de Isabel II, S.A. M.P., o a tratar información de Canal de Isabel II, S.A. M.P.:

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, S.A. M.P.

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 de la parte profesional por hardware, mediante el suministro de licencias por parte del Adjudicatario de soluciones destinadas a este fin.

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

DM.07 El Adjudicatario debe facilitar a Canal de Isabel II, S.A. M.P. los usuarios de auditoría que le sean requeridos para la solución MDM en la que se administren los dispositivos móviles del Adjudicatario que se utilicen para la prestación de los Servicios objeto de contratación en la presente licitación.

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

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

SI En relación con la Seguridad de la Infraestructura:

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

SI.02 Cuando existan para el entorno, deben seguirse las guías de configuración del CCN. En caso de existir la guía y que el Adjudicatario entienda que no puede o no debe seguir la correspondiente guía, deberá pedir autorización expresa a Canal de Isabel II, S.A. M.P.

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

SI.04 Nunca pueden existir usuarios por defecto.

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

SI.06 El Adjudicatario deberá exponer su metodología, activos y enfoque para abordar este proceso y cómo se adapta a los diferentes casos de uso de la plataforma y de los sistemas y servicios que la soportan. Si la solución propuesta se basa en el uso de uno o varios proveedores de Cloud Pública, se requiere el cumplimiento de estándares /normativas como el ENS.

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

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

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

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

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

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

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

SI.14 Además, de no especificarse lo contrario, los datos propiedad de Canal de Isabel II, S.A. M.P. 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, S.A. M.P.

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

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

SI.16.01 Protección por reputación

SI.16.02 Creación de Sinkhole

SI.16.03 Protección de exfiltración mediante paquetes DNS.

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

Debe describirse el enfoque, la metodología para su gestión y su integración en la estrategia propuesta de monitorización de seguridad de la plataforma y de los sistemas y servicios que la soportan.

SI.17 Todos los sistemas y micro-servicios de la plataforma y de los sistemas y servicios que la soportan 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 El Adjudicatario deberá, para los accesos del personal y terceros de Canal de Isabel II, S.A. M.P., así como para el personal del Adjudicatario que trabaje en los servicios de Canal de Isabel II, S.A. M.P., dotar de herramientas específicas a Canal de Isabel II, S.A. M.P. y a los terceros citados, de tal manera que se garantice la confidencialidad del tráfico generado en dichos procesos a través de protocolos considerados como seguros o soluciones específicas destinadas a tal efecto. De la misma forma, la gestión y administración interna de los elementos involucrados en la provisión de los Servicios deberán contar con dichas garantías.

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

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

CD En relación con la CiberDefensa:

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

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

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

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

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

CD.03.02 Protecciones IDS e IPS.

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

CD.03.04 UEBA, UBA o SUBA.

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

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

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

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

CD.03.09 Cuando la naturaleza de la solución del Adjudicatario requiera navegación web, de usuarios o aplicaciones, se requerirá una solución de protección de la navegación vía proxy de navegación o a través de la categorización de las URLs, que incluirá además la categorización por nivel de riesgo (bajo, medio o alto). Se revisará con Canal de Isabel II, S.A. M.P. 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, S.A. M.P. previo a su autorización.

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

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

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

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

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

En relación con estos productos, el Adjudicatario deberá alinearse con los fabricante y modelos que actualmente están en explotación en la infraestructura de Canal de Isabel II, S.A. M.P. 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, S.A. M.P., el Adjudicatario garantizará la no obsolescencia de la tecnología, controles o los procesos involucrados en la prestación de los Servicios, llevando a cabo, y bajo autorización expresa de Canal de Isabel II, S.A. M.P., procesos de renovación y actualización de los sistemas y procesos según se determine necesario.

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

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

- I. El sistema objeto de este procedimiento de contratación será objeto de escaneos de vulnerabilidades, bien por parte del Adjudicatario o bien por parte del Canal de Isabel II, S.A. M.P., ya que ésta aplica actualmente un proceso continuo de gestión de vulnerabilidades de su infraestructura IT, debiendo para ello el Adjudicatario habilitar en las políticas de red los correspondientes accesos para los escaneos periódicos.
 - a. En el caso de que el Adjudicatario cuente con informes/reportes de escaneo de vulnerabilidades de la plataforma y de los sistemas y servicios que la soportan, realizados por un tercero, y una vez que sean analizados por el Área de Ciberseguridad de Canal de Isabel II, S.A. M.P., 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 Área de Ciberseguridad de Canal de Isabel II, S.A. M.P.
- III. Además, el Adjudicatario deberá resolver las vulnerabilidades detectadas en los escaneos en los plazos establecidos en las políticas de Canal de Isabel II, S.A. M.P., de acuerdo con su criticidad.

CD.06.03 El Adjudicatario describirá las metodologías para la gestión del ciclo de vida de vulnerabilidades y su integración de la gestión de la plataforma y de los sistemas y servicios que la soportan.

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

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

- a. Actividad
- b. Acceso
- c. IP origen
- d. IP destino
- e. Usuario

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

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

El Adjudicatario custodiará una copia de dichos registros por el periodo de retención que el Canal de Isabel II, S.A. M.P. 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 al Área de Ciberseguridad de Canal de Isabel II, S.A. M.P. 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, S.A. M.P. (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, S.A. M.P. 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, S.A. M.P.

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, S.A. M.P.

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

CD.12 El Adjudicatario realizará pruebas de seguridad (*pentesting*, *hacking* ético) ya sea de las aplicaciones y/o infraestructuras que afecten a la plataforma y a los sistemas y servicios que la soportan. En caso de realizarse durante la prestación de los Servicios, debe notificarlo al jefe de Proyecto de Canal de Isabel II, S.A. M.P. Dado que los datos son propiedad de Canal de Isabel II, S.A. M.P., 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, S.A. M.P.

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, S.A. M.P. 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, S.A. M.P. Todos los correos electrónicos enviados y recibidos deben configurarse para que empleen los sistemas de Canal de Isabel II, S.A. M.P. disponibles para ello, y asegurar la autenticidad de los dominios de Canal de Isabel II, S.A. M.P.

AU En relación con las auditorías:

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

AU.02 Canal de Isabel II, S.A. M.P. 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, S.A. M.P. o a cualquier tercero designado a tal efecto por Canal de Isabel II, S.A. M.P. y/o Autoridad de Control, acceso completo de la institución a las ubicaciones y centros de trabajo desde los que se presten los Servicios, incluyendo cualquier dispositivo, sistema, red y datos utilizados para la prestación de los Servicios contratados (derecho de acceso).

AU.04 Canal de Isabel II, S.A. M.P. 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, S.A. M.P. 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 bi-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 colaborar con Canal de Isabel II, S.A. M.P. para dar cumplimiento a las obligaciones internas y externas de auditoría.

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

DS.01 A la plataforma y a los sistemas y servicios que la soportan objeto del presente procedimiento de contratación le serán de aplicación los requisitos establecidos por ENS. Este alto nivel de exigencia, junto con el que Canal de Isabel II, S.A. M.P. se impone a sí misma, establece la necesidad de que el Adjudicatario deba:

DS.01.01 Disponer de una o más localizaciones en las que poder mantener la provisión de servicios en caso de Contingencia, Crisis o Continuidad.

DS.01.02 Proveer a la plataforma y a los sistemas y servicios que la soportan de arquitecturas de seguridad redundadas y balanceadas.

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

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

DS.01.05 Disponer de un plan de crisis.

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

DS.01.07 Disponer de un Plan de Salida programada que, entre otras muchas cuestiones, debe detallar cómo la información será devuelta a Canal de Isabel II, S.A. M.P. 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, S.A. M.P. 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 una plataforma, y para los sistemas y servicios que la soportan, de este tipo.

DS.03 Adicionalmente, deberá elaborar planes de contingencia que permitan hacer frente a situaciones que pudieran afectar a la disponibilidad de la plataforma y de los sistemas y servicios que la soportan.

RIA Cumplimiento del Reglamento Europeo de Inteligencia Artificial

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

- a) Asignará e indicará a Canal de Isabel II, S.A. M.P. 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.
- b) 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.

- c) Documentará las finalidades para el uso de datos personales en cada etapa del ciclo de vida de la IA, y en caso de que se utilizaran para otras finalidades distintas a las originalmente definidas, aportará evaluación analizando si son compatibles con la finalidad originalmente perseguida. Cada una de dichas etapas, en su consideración individualizada, deberá cumplir con los requisitos del RGPD en materia de privacidad. A modo de ejemplo, para facilitar esta información, el Adjudicatario puede utilizar la tabla del ciclo de vida del dato de la ISO 29134:2017.

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

- d) El Adjudicatario garantizará que cuenta con una base de legitimación válida para tratar datos personales en cada una de las fases.
- e) El Adjudicatario garantizará que se han aplicado técnicas de desidentificación a los datos de entrenamiento antes de extraerlos de su fuente y compartirlos con Canal de Isabel II, S.A. M.P. 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, S.A. M.P., 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, S.A. M.P.

El Adjudicatario queda obligado a realizar una conexión privada a la Red Corporativa de Datos (en adelante, RCD) de Canal de Isabel II, S.A. M.P. para la realización de aquellos trabajos contemplados dentro del alcance del presente contrato que lo requieran. El Adjudicatario, por tanto, deberá asignar un recurso técnico especializado sin dedicación exclusiva en redes de datos y comunicaciones, que se responsabilice, en el ámbito de la prestación de los Servicios, de la configuración y mantenimiento de la parte de la infraestructura de comunicaciones entre el Adjudicatario y Canal de Isabel II, S.A. M.P. 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, S.A. M.P.

El operador de comunicaciones elegido por el Adjudicatario para la puesta en marcha de la conexión con Canal de Isabel II, S.A. M.P. entregará en un único punto tanto la totalidad del tráfico gestionado del propio Adjudicatario como el de las otras empresas colaboradoras o contratas que conecten a través de dicho único punto con Canal de Isabel II, S.A. M.P. Esto es, si el operador de comunicaciones elegido por el Adjudicatario ya presta servicio a alguna otra empresa colaboradora o contrata de Canal de Isabel II, S.A. M.P., la nueva conexión deberá utilizar la infraestructura física existente en Canal de Isabel II, S.A. M.P. 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, S.A. M.P.

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, S.A. M.P. 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, S.A. M.P., 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, S.A. M.P. y, en especial, entre las diferentes empresas colaboradoras a las que pudiera dar servicio con la misma infraestructura.

En caso de que el contrato sea adjudicado a una Unión Temporal de Empresas (UTE), se presentará igualmente una única conexión a Canal de Isabel II, S.A. M.P., y serán las empresas que forman la UTE las que deberán coordinarse entre ellas y realizar las acciones que sean necesarias para garantizar que

la prestación de los servicios contratados por parte de Canal de Isabel II, S.A. M.P. se realice exclusivamente a través de dicha conexión única.

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

La conexión única principal con Canal de Isabel II, S.A. M.P. deberá entregar el tráfico a la RCD de Canal de Isabel II, S.A. M.P. en la siguiente dirección:

Oficinas Centrales Canal de Isabel II, S.A. M.P.
C/ Santa Engracia 125
Edificio 4

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

Si por parte del servicio de Canal de Isabel II, S.A. M.P. 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, S.A. M.P. 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, S.A. M.P.", con el objeto de disponer de una línea adicional de *backup*, contingencia o respaldo, y poder así garantizar la disponibilidad de las comunicaciones.

La conexión de *backup* con Canal de Isabel II, S.A. M.P. deberá entregar el tráfico a la RCD de Canal de Isabel II, S.A. M.P. en la siguiente dirección:

Polígono Industrial El Carralero (Majadahonda)
ETAP Majadahonda
Edificio Espejo

CC.03. Direccionamiento IPv4.

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

CC.04. Monitorización de la conexión.

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

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

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

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

El Adjudicatario tiene la obligación de asegurar el correcto estado de la conexión por parte del operador de telecomunicaciones en todas sus líneas de comunicación (principal y de *backup*, en caso de existir). El Adjudicatario está obligado a realizar las comprobaciones oportunas con el operador ante cualquier posible problema de acceso a los sistemas de Canal de Isabel II, S.A. M.P., proporcionando las evidencias de que el tráfico se entrega en el extremo de Canal de Isabel II, S.A. M.P. y que parte de la interfaz del *router* de operador que conecta con el extremo de Canal de Isabel II, S.A. M.P. 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, S.A. M.P., y siempre a través del responsable de contrato en Canal de Isabel II, S.A. M.P.

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

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, S.A. M.P., 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, S.A. M.P. 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, S.A. M.P. afectadas o involucradas en la prestación del servicio.