

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR
EN EL CONTRATO DE SERVICIO DE MANTENIMIENTO
PREVENTIVO Y DESARROLLO EVOLUTIVO SISTEMA DE
GESTIÓN DE SEGURIDAD DASSNET**

EXPEDIENTE N.º: 50/2026

Área: **Sistemas de Seguridad**

ÍNDICE

1. OBJETO	3
2. ANTECEDENTES.....	3
3. ALCANCE.....	4
3.1 ALCANCE GENERAL	4
3.2 MANTENIMIENTO DE LICENCIAS.....	4
3.3 SOPORTE TÉCNICO	5
3.4 MANTENIMIENTO CORRECTIVO	5
3.5 MANTENIMIENTO PREVENTIVO.....	5
3.6 MANTENIMIENTO EVOLUTIVO.....	6
3.6.1 CREDENCIALES MOVILES. (DORLET MOBILE ACCESS)	6
3.6.2 AUTENTICACIÓN MULTIFACTOR MEDIANTE MICROSOFT ENTRA ID	8
4. REQUISITOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO	8
5. ORGANIZACIÓN DEL SERVICIO	18
6. FORMATO DE LAS ESPECIFICACIONES TÉCNICAS.....	18
7. DESGLOSE DE TRABAJOS POR ANUALIDADES	18

1. OBJETO

El objeto de este documento es la definición de las condiciones técnicas que han de servir para la licitación y posterior ejecución, puesta en marcha y recepción del **MANTENIMIENTO PREVENTIVO Y DESARROLLO EVOLUTIVO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DASSNET**.

Este Pliego de Prescripciones Técnicas servirá de base para la adjudicación de los trabajos. Tendrá carácter contractual para la empresa adjudicataria de los trabajos, regulando las condiciones de ejecución, certificación y recepción de los servicios y obras, así como el resto de los documentos indicados en el Pliego de Condiciones Administrativas Particulares y en el orden de preeminencia declarado en éste en caso de discordancia entre documentos.

2. ANTECEDENTES

Canal de Isabel II, S.A., M.P. (en adelante, "Canal") utiliza como plataforma de control accesos corporativo el Software de Gestión de Seguridad (DassNet) del fabricante Dorlet.

El Área de Sistemas de Seguridad es la responsable de garantizar el correcto funcionamiento, disponibilidad, actualización y continuidad operativa de la plataforma Gestión de Seguridad (DassNet).

Entre sus funciones se incluyen, la administración, mantenimiento preventivo, correctivo y evolutivo de los sistemas, así como la Implementación de medidas de seguridad alineadas con las políticas corporativas.

El Software de Gestión de Seguridad (DassNet) de Canal, está compuesto por:

- Arquitectura centralizada cliente-servidor con servidores «on-premise» virtualizados.
- Servidor «on-premise» de Base de Datos Oracle.
- 70 licencias concurrentes de clientes para la gestión de los sistemas de control de accesos.
- + 600 unidades de control de accesos.
- + 1.000 lectores de tarjetas.
- + 8.000 empleados y colaboradores externos.
- + 5.000.000 de accesos anualmente.

➤ Licencias:

- Integración con CCTV.
- Módulo de gestión de video.
- Licencia lectores ilimitados para DASSnet®.
- Licencia ilimitada de Megáfonos.
- Licencia ilimitada de interfonos.
- Licencia modulo gestión de visitas.
- Licencia LPR lectura de matrículas.

Para garantizar el correcto funcionamiento del SISTEMA DE GESTIÓN DE SEGURIDAD es necesario disponer de un servicio de soporte técnico y funcional que incluya las previsibles actualizaciones y desarrollo evolutivo del software.

3. ALCANCE

Dentro del contrato se incluirá la prestación del servicio de mantenimiento preventivo, correctivo, evolutivo y soporte técnico por el fabricante del SISTEMA DE GESTIÓN DE SEGURIDAD DassNet.

El servicio a contratar incluye:

- Actualización de software (Upgrade)
- Mantenimiento de la base de datos
- Carga de parches .BAK y BACK UP local

En general, todas las acciones necesarias para el mantenimiento del núcleo del sistema.

3.1 ALCANCE GENERAL

Atención en un máximo de 8 horas laborables desde la comunicación de la necesidad de soporte técnico, según el calendario laboral.

3.2 MANTENIMIENTO DE LICENCIAS

Dentro del contrato está incluido el mantenimiento de las licencias. El adjudicatario tiene que:

- Proporcionar la última versión liberada del software, y libre de vulnerabilidades conocidas o reportadas.
- Notificar proactivamente a Canal los posibles problemas de seguridad en los productos, así como de la descripción técnica detallada del problema en cuanto tengan conocimiento de ellos.
- Notificar también la disponibilidad de los parches o nuevas versiones que solucionaran los posibles problemas, incluyendo fechas.

3.3 SOPORTE TÉCNICO

Mantenimiento Funcional: Soporte técnico de dudas de funcionamiento de la aplicación (funciones, configuración, ...). Dentro de este soporte técnico, no se incluye la realización de trabajos masivos de alta de datos o parametrizaciones.

3.4 MANTENIMIENTO CORRECTIVO

Soporte a incidencias en la aplicación, resolución de estas, incluido suministro de parche correspondiente en caso de ser necesario y pruebas de que la incidencia ha quedado resuelta.

3.5 MANTENIMIENTO PREVENTIVO

Revisión preventiva anual mediante conexión remota para diagnóstico de BBDD, comprobación de licencias y chequeo de correcto funcionamiento de integraciones, entre otras acciones. Se entregará un informe del estado de la instalación.

- Diagnóstico Bases de Datos (ORACLE)
- Comprobación de Licencias instaladas correctamente
- Revisión de estado equipos (lectores o UCAs averiados, desconectados, etc.)
- Chequeo integraciones (intrusión, incendios, video, etc.)
- Verificación Dorlet Contratas Service
- Verificación Dorlet SDKs Service
- Verificación Dorlet Readers
- Entrega informe estado revisión y proposición de mejoras o incidencias a resolver.

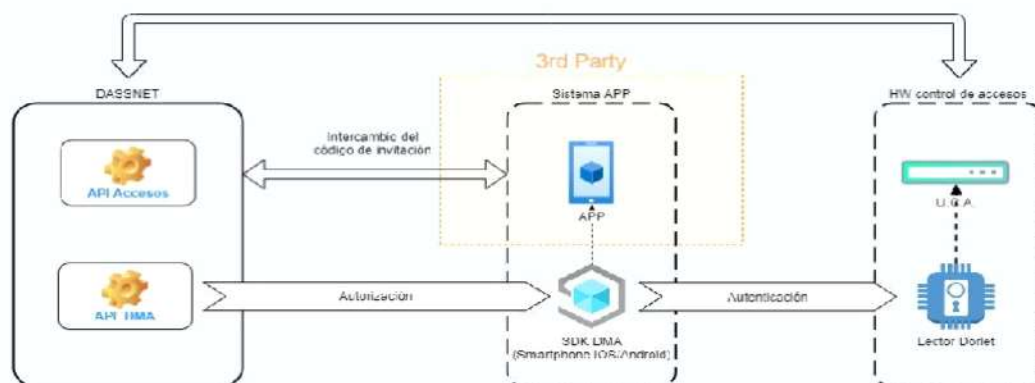
3.6 MANTENIMIENTO EVOLUTIVO.

3.6.1 CREDENCIALES MOVILES. (Dorlet Mobile Access)

Dentro de las acciones a realizar en el presente contrato, se incluyen todos los trabajos para poner a disposición de los empleados de Canal la opción del uso de móvil como credenciales de accesos a las instalaciones. Para ello, es necesario implantar en el SISTEMA DE GESTIÓN DE SEGURIDAD DassNet, la plataforma Dorlet Mobile Access (DMA a partir de ahora), que es un conjunto de servicios y apps que provee el fabricante DORLET® y permite, en última instancia, desplegar credenciales o tarjetas de acceso virtuales en los teléfonos móviles del usuario. Desde el punto de vista del usuario, el teléfono móvil pasa a ser el soporte que almacenará sus credenciales de acceso, sustituyendo a las tarjetas físicas de acceso utilizadas normalmente.

Los trabajos incluyen trabajos de coordinación con el Área de Sistemas de Seguridad de Canal, para adaptar la aplicación a los requerimientos exigidos por el Área de Ciberseguridad y el Área de Infraestructura Informática de Canal.

La arquitectura general del sistema se compone de tres bloques principales: DASSnet®, la app móvil y el hardware de control de accesos.



A continuación, se describe brevemente cada uno de ellos: DASSnet®

3.6.1.1 DASSNET

Es el software de control de accesos "on-premise" que incluye el componente API DMA, que son los servicios que dan soporte al sistema DMA. Entre las funciones del API DMA destacan:

- Generar los códigos e invitación necesarios para el despliegue inicial de la credencial DMA del usuario.
- Gobernar y autorizar el proceso de instalación inicial de la credencial DMA del usuario.
- Permitir la sincronización o actualización la credencial DMA del usuario, incluyendo la recepción de los eventos de acceso que se producen en lectores offline, si existen.

3.6.1.2 Sistema APP

Se refiere al conjunto de elementos que conforman la app que se integra en el sistema DMA.

Este sistema se divide en dos bloques:

SDK DMA

Es el componente que incorporará cualquier app que desee integrarse en el sistema DMA. Este componente encapsula completamente la funcionalidad relacionada con la gestión y el uso de las credenciales DMA. Entre sus funcionalidades:

- Instalación y almacenamiento seguro de las credenciales DMA (a partir de código de invitación)
- Sincronización de las credenciales, incluyendo los eventos de acceso resultado de la interacción con lectores offline, si existen.
- Autenticación con los lectores para validar la credencial del usuario
- Provee las interfaces necesarias para que la app interactúe con las credenciales DMA almacenadas.

APP DMA

Es la app propiamente dicha, es decir, la aplicación software que se instala en el móvil del usuario final.

Esta app, además de integrar el SDK DMA, puede disponer de un elemento de servidor con los servicios que necesita para su funcionamiento. En el caso de la app Dorlet Mobile Access este tipo de servicios no son necesarios. La única conectividad necesaria es la del SDK con el API DMA.

3.6.1.3 HW Control de accesos

Son los dispositivos de campo instalados en las instalaciones de Canal que conforman el sistema control de accesos y autentican la credencial DMA del usuario.

3.6.2 AUTENTICACIÓN MULTIFACTOR MEDIANTE MICROSOFT ENTRA ID

Con el despliegue de DMA se requiere implementar un módulo de autenticación multifactor integrado en Microsoft Entra ID (Azure Active Directory) de Canal, con el fin de habilitar mecanismos avanzados de autenticación segura, incluyendo autenticación multifactor (MFA), provisión y gestión de credenciales de acceso, y control de identidad conforme a los estándares corporativos de seguridad.

El módulo deberá proporcionar, las siguientes funcionalidades:

- **Integración con Microsoft Entra ID**
 - Implementación del protocolo de autenticación OAuth 2.0 / OpenID Connect, conforme a las especificaciones oficiales de Microsoft.
 - Compatibilidad con los flujos de autenticación:
 - Authorization Code Flow (con PKCE).
 - Obtención y validación de tokens de acceso, ID tokens y tokens de actualización emitidos por Microsoft Entra ID.
- **Autenticación Multifactor (MFA)**
 - Integración con los métodos de MFA soportados por Microsoft Entra ID, incluyendo:
 - Notificación Push mediante Microsoft Authenticator.
 - Código OTP (One-Time Password).
 - Capacidad de forzar MFA en función de las políticas de acceso condicional definidas por el administrador de la plataforma.

4. REQUISITOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO

➤ 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 adjudicatario asegurará que, en caso de resultar adjudicatario, informará a Canal 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, tanto durante la normal prestación del Servicio, como en caso de contingencia. Por otro lado, el adjudicatario deberá obtener de Canal 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 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, conforme a lo indicado en el Pliego de Cláusulas Administrativas Particulares, 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. 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, en particular, al Área de Ciberseguridad de Canal.

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 y 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 Pliego de Cláusulas Administrativas Particulares y en el presente Pliego de Prescripciones Técnicas. El subcontratista cumplirá totalmente con las obligaciones existentes entre Canal y el adjudicatario, incluidas las obligaciones contraídas frente a las diferentes autoridades de control.

El adjudicatario deberá informar a Canal 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. 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.

▪ **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 Canal 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. Asimismo, el licitador se compromete a facilitar en todo lo posible a la Oficina Técnica de Seguridad (OTS) de Canal 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 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 es de particular importancia la necesidad de identificar y retener, a alto nivel, las competencias básicas adecuadas a un nivel operativo dentro de Canal 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 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.

- Concienciación.

El adjudicatario deberá garantizar la adecuada formación, concienciación y capacitación del personal involucrado en la prestación del Servicio a Canal. 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 Pliego de Cláusulas Administrativas Particulares, el adjudicatario debe contemplar el compromiso de devolución y/o destrucción (a elección de Canal) de toda la información propiedad de Canal recabada durante la ejecución de los Servicios.
- Si por la naturaleza del proyecto, Canal 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 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.
- El adjudicatario debe entender y asumir que la responsabilidad final de la Seguridad de los datos, recae en Canal y, por designación de funciones dentro de ésta, en el Responsable de la Seguridad de Canal, 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, 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 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 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 o a cualquier tercero designado a tal efecto por Canal 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 para dar cumplimiento a las obligaciones internas y externas de auditoría.
 - Canal se encuentra sujeta a diversas auditorías externas, ya sea por requerimientos regulatorios, legales, normativos, sectoriales, contractuales, etc. Es por ello por lo que Canal 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 seguridad de los equipos de usuario propiedad del adjudicatario que vayan a conectarse a las redes o sistemas de información de Canal, o a tratar información de Canal.**

- El adjudicatario deberá contar con un plan de acciones correctivas dentro del proceso de mantenimiento para hacer frente a cualquier incidencia de software y/o hardware que se produzca en los equipos o cualquiera de sus componentes.
- 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.
- 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).
- El adjudicatario deberá mantener y poner a disposición de Canal un inventario actualizado de la totalidad de equipos. Este inventario deberá contener al menos los siguientes campos:
 - Dirección IP del equipo.
 - Nombre del equipo (hostname).
 - Dirección MAC del equipo
 - Inventario actualizado del Software instalado en cada equipo.
 - Modelo del equipo.
 - Versión del sistema operativo instalado.
 - Marca, modelo y Versión de la solución de seguridad XDR instalada.
- En el caso de que los equipos utilicen tecnologías de comunicación inalámbrica, el adjudicatario deberá cumplir con los siguientes requisitos:
 - 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.
 - El adjudicatario deberá proporcionar la documentación detallada sobre los protocolos, alcance, requisitos de alimentación, frecuencias y pruebas de funcionamiento de la red inalámbrica.
 - 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.
 - 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.

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

➤ **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. Cualquier acceso no explícitamente autorizado será prohibido.
- El adjudicatario deberá entregar a Canal 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.
- El adjudicatario deberá garantizar que el servicio cuenta con mecanismos de control en la autenticación.
- Los usuarios del adjudicatario que vayan a hacer uso de redes o sistemas de información propiedad de Canal, y/o vayan a acceder a información propiedad de Canal, deben estar dados de alta en los sistemas de Gestión de Identidad de Canal. Para ello, deberán proporcionar al responsable del proyecto de Canal 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 seguirán en todo momento todas las indicaciones de seguridad que se les transmitan desde Canal 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.
 - 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.).

➤ **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 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: CONCEPCIÓN/ DISEÑO Y DESARROLLO/ VERIFICACIÓN Y VALIDACIÓN/ DESPLIEGUE/ OPERACIÓN Y MONITORIZACIÓN/ REEVALUACIÓN/ 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. En caso de no aplicar tales técnicas, el adjudicatario garantizará 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 injustificados, 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, 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 asegurará haber establecido un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización del sistema.

5. ORGANIZACIÓN DEL SERVICIO

Responsable del servicio

El adjudicatario nombrará dentro de su organización un *responsable del servicio*, interlocutor válido a efectos de tratamiento con la dirección del contrato de todos los asuntos técnicos, sean sobre mantenimiento de licencias, o mantenimiento evolutivo. Este nombramiento se comunicará *por escrito* al director del contrato por parte del Canal, en fecha previa a la firma del acta de inicio del servicio de mantenimiento. El acta será firmada por ambos.

Acta de Inicio y Datos de Contacto

Antes de comenzar los trabajos, el adjudicatario deberá firmar un Acta de Inicio. Este documento será imprescindible para dar inicio a la ejecución del contrato y para el cómputo de plazos.

En el acta de inicio se deberá incluir, como mínimo:

- Fecha de inicio del servicio de mantenimiento.
- Nombre y cargo del director del contrato por parte del Canal.
- Nombre y cargo del responsable designado por el adjudicatario.
- Datos de contacto de ambos responsables (teléfono y correo electrónico).

6. FORMATO DE LAS ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas se atenderán al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.

7. DESGLOSE DE TRABAJOS POR ANUALIDADES

UD.	CONCEPTO	CTD.
Primera anualidad		
Ud.	Anualidad completa para el Servicio de mantenimiento aplicativo software de gestión de Seguridad Dassnet (DORLET CARE +).	1
Ud.	Soporte técnico para la personalización y despliegue del módulo Dass Mobile Azure (DMA).	1
Ud.	Implantación de autenticación multifactor (MFA), protección de identidad y acceso condicional mediante Microsoft Entra ID para la administración de identidades en DassNet Mobile Access.	1
Ud.	Credenciales para dispositivos móviles Android e iOS compatible para aplicación Dass Mobile Azure	1.000

UD.	CONCEPTO	CTD.
Segunda anualidad		
Ud.	Anualidad completa para el Servicio de mantenimiento aplicativo software de gestión de Seguridad Dassnet (DORLET CARE +).	1
Ud.	Credenciales para dispositivos móviles Android e iOS compatible para aplicación Dass Mobile Azure	1.000
H.	Mantenimiento correctivo / evolutivo	20

UD.	CONCEPTO	CTD.
Tercera anualidad		
Ud.	Anualidad completa para el Servicio de mantenimiento aplicativo software de gestión de Seguridad Dassnet (DORLET CARE+).	1
Ud.	Credenciales para dispositivos móviles Android e iOS compatible para aplicación Dass Mobilre Azure	1.000
H.	Mantenimiento correctivo / evolutivo	20

UD.	CONCEPTO	CTD.
Cuarta anualidad		
Ud.	Anualidad completa para el Servicio de mantenimiento aplicativo software de gestión de Seguridad Dassnet (DORLET CARE+).	1
H.	Mantenimiento correctivo / evolutivo	20

Jefe de Área Sistemas de
Seguridad

Conforme:
El Director de Seguridad

Firmado por
COLMENAREJO GARCÍA
ROQUE - ***4235**
FIRMA el día
07/04/2026 con un
Roque Colmenarejo García

Firmado electrónicamente
por: RICARDO LLORENTE
HERNÁN-GÓMEZ
En la fecha y hora
07.04.2026 10:08:01 CEST
Ricardo Llorente Hernán-Gómez