Comunidad de Madrid

Dirección General de Salud Digital
CONSEJERÍA DE DIGITALIZACION

[redacted]

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR EN EL CONTRATO DE "OFICINAS DE SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD – 2 LOTES", A CELEBRAR MEDIANTE PROCEDIMIENTO ABIERTO

INDICE

1. INTRODUCCIÓN

La Dirección General de Salud Digital (DGSD), que presta servicios al Servicio Madrileño de Salud (SERMAS), dentro de su estructura organizativa cuenta con un Servicio de Seguridad cuyo cometido es la gestión de la seguridad y la protección de datos de los sistemas de información en el ejercicio de sus competencias. Siendo objeto de este pliego la contratación de dos oficinas técnicas, una denominada Oficina de Seguridad de los Sistemas de Información, y la otra Oficina de Auditoría Interna.

2. OBJETO

El objeto del presente expediente incluye la contratación de:

- Oficina de Seguridad de Sistemas de la Información (OSSI)
- Servicio de cumplimiento normativo en materias de protección de datos y seguridad

que son necesarios para abordar y ejecutar los trabajos destinados a impulsar y adquirir un escenario base que mejore la ciberresilencia global.

El expediente se dividirá en dos lotes, para facilitar la obtención de los objetivos. Se enumeran a continuación:

- **Lote 1**: Oficina de Seguridad de los Sistemas de Información (OSSI).
- **Lote 2**: Oficina de Auditoría Interna.

Incompatibilidades de adjudicación entre lotes

El lote 1, de Oficina de Seguridad de los Sistemas de Información, tendrá incompatibilidad con el lote 2. Por lo que la empresa que resulte adjudicataria de este lote 1, no podrá ser adjudicataria del lote 2, y a la inversa.

3. DESCRIPCIÓN DE LOS SERVICIOS

3.1. Lote 1: Oficina de Seguridad de Sistemas de Información (OSSI)

3.1.1. Alcance del servicio

El presente lote engloba todos los servicios que puedan ser requeridos para las actividades necesarias en la coordinación, planificación, seguimiento y control de las iniciativas de seguridad que se establezcan en la Consejería de Sanidad de la Comunidad de Madrid, dentro de sus competencias. La empresa adjudicataria de este lote será responsable de la gestión del ciclo completo de vida de cada iniciativa, entendiendo la iniciativa desde la necesidad/idea propuesta hasta el soporte en la operación de las soluciones implantadas.

Cabe destacar que el alcance de este pliego abarca los sistemas de información que dan servicio a los tratamientos de datos del SERMAS en su ámbito de actuación, es decir, los sistemas de informática médica, gestión sanitaria y aquellos relativos a las relaciones del sistema sanitario con los ciudadanos, profesionales sanitarios, oficinas de farmacia, sanidad privada y cualesquiera otras personas físicas o jurídicas distintas de la Administración de la Comunidad de Madrid.

El presente lote se centra, no solo en la prestación de servicios técnicos objeto del alcance que se describen a continuación, sino también en labores de gobernanza en materias de seguridad, y apoyo al máximo responsable de la OSSI, su CISO, y al DPD. Así mismo, apoyará al lote 2 mediante la especificación, programación y aporte de evidencias para las auditorías internas que resulten necesarias de acuerdo al cumplimiento de la legislación en materia de seguridad y protección de datos de carácter personal.

La empresa adjudicataria de este lote estructurará sus funciones en torno a las siguientes unidades:

- Oficina de Seguridad, cuya principal misión será la gestión del porfolio de proyectos, definición e implantación del Plan estratégico de seguridad de información (PESI), supervisión de la gobernanza de los servicios, la seguridad, el cumplimiento de estos y el reporte a las diferentes Unidades en la estrategia de la DGSD.
- Gestión de Porfolio de iniciativas. Esta unidad gestionará el ciclo de vida de la necesidad/idea propuesta hasta su concepción como proyecto englobando una gestión de la demanda, desde la definición de una idea hasta la concreción en un caso de uso definido para su automatización.
- Explotación y soporte, esta unidad contempla todos los componentes para proveer soluciones de seguridad estables, sostenibles en el tiempo y alineadas con la calidad requerida desde la DGSD. Entre las funciones de esta unidad está ofrecer apoyo y soporte a las personas usuarias finales en un primer nivel.
- Apoyo al CISO, control y supervisión del servicio, asesoramiento a la Oficina de Seguridad, alineándolo con las decisiones y requisitos de seguridad de la información y de los servicios que así se requieran. Así mismo, apoyo a la revisión de contratos para la adecuación a la normativa de seguridad y privacidad y elaboración de documentación para solicitar fondos, etc.
- Asesoramiento multidisciplinar en materia de seguridad.
- Seguridad en el ciclo de vida de los proyectos de la DGSD.
- Apoyo a los centros sanitarios en materia de seguridad.
- Concienciación en materias de seguridad, dirigida al personal al servicio de la Consejería de Sanidad de la Comunidad de Madrid.

- Apoyo a las auditorías internas en base al cumplimiento de normativas descritas en el pliego, así como RGPD y cumplimiento, que así se requieran.
- Apoyo al resto de lotes en la consecución de los objetivos establecidos por la Oficina de Seguridad de Sistemas de Información.

Hay que indicar que en la actualidad la DGSD ya dispone de la certificación ISO/IEC 27001 para la Oficina de Seguridad de Sistemas de la Información, por lo que el adjudicatario del presente lote deberá mantener dicha certificación.
El detalle de cada una de las actividades está contemplado a continuación en el catálogo de actividades definido para cada unidad.

3.1.2. Actividades generales

A continuación, se identifican las actividades que están contempladas en este lote, enmarcadas en la fase de prestación de los servicios y mejora continua del modelo de gestión de los servicios. Entre las distintas actividades que desarrolla la **OSSI** se contemplan las funciones de gobierno, seguridad, cumplimiento y reporte, la empresa adjudicataria será la responsable de la gestión integral del porfolio de proyectos de seguridad.

Dentro de este alcance se encuentran:

- **Gestión del porfolio y de los proyectos**. En esta función se deben abordar las acciones para garantizar el correcto desarrollo y ejecución de los procesos que cursan ideas, casos de uso, proyectos y operaciones de seguridad. Para ello, el proveedor debe proporcionar mecanismos (procesos y herramientas) de control y monitorización para la gestión del porfolio y de los proyectos.
- **Modelo de gobernanza**. Se establecen los diferentes niveles para el gobierno de los Servicios, así como los procesos para su gobernanza.
- **Seguridad**. En esta actividad se recogen los requisitos necesarios establecidos por el SERMAS en materia de seguridad.
- **Cuadro de mando y reporte**. Esta actividad centraliza el seguimiento y reporte de los datos a través de varios mecanismos de reporte, entre ellos un dashboard centralizado donde se reflejen los distintos indicadores identificados dentro del desarrollo de los servicios.
- Elaboración e implantación del **PESI** (Plan estratégico de seguridad de información).
- Consultoría en administración electrónica. Certificados digitales, eIDAS y firmas electrónicas. Servicios al ciudadano y manejo seguro de documentación digital.
- Mantenimiento y cumplimiento de objetivos en cuanto a marco normativo, dando continuidad a los otros dos lotes del presente expediente.
- Apoyo al CISO, colaborando en las tareas que desde esta figura se requieren y facilitar con ello los objetivos que se le exigen.

- Apoyo al DPD (delegado de protección de datos)
- Asesoramiento multidisciplinar en materia de seguridad.
- Apoyo a la integración en el ciclo de vida de los proyectos de la DGSD
- Apoyo a los centros en materia de seguridad.
- Concienciación en materias de seguridad.
- Apoyo a las auditorías internas en base al cumplimiento de normativas descritas en el pliego, así como RGPD y Compliance que así se requieran.
- Apoyo al resto de lotes en la consecución de los objetivos establecidos por la Oficina de Seguridad.

3.1.2.1. Gestión del porfolio y de los proyectos de ciberseguridad

Esta actividad conlleva la gestión del porfolio y de los proyectos de ciberseguridad. La empresa adjudicataria deberá establecer los mecanismos (procesos y herramientas) adecuados para garantizar la gestión del ciclo completo de la iniciativa:

- Desde su entrada a través del sistema de registro de necesidades/ideas, su valoración, priorización y aprobación de idea y caso de uso.
- Procesos para la gestión de proyectos.
- Seguimiento hasta su certificación final asociada a los procesos de calidad y aseguramiento de la calidad (QA).

La empresa adjudicataria actuará como oficina de control de la cartera de proyectos, coordinándose con los diferentes equipos implicados en las distintas fases del ciclo de vida.
Es por ello, que la empresa adjudicataria ofrecerá un **servicio experto e integral para el seguimiento técnico de cada uno de los proyectos**, y la gestión completa del porfolio de programas o de proyectos que la DGSD quiera abordar. La concepción del proyecto o el programa será responsabilidad del equipo de gestión del porfolio de necesidades/ideas tras estudiar la viabilidad de la iniciativa.

Para la gestión de la cartera de proyectos o programas la empresa adjudicataria deberá realizar un control de costes, de tiempos, evaluación y seguimiento de los beneficios de cada proyecto, así como la identificación de los riesgos asociados a los mismos, proponiendo las actuaciones de mitigación adecuadas para disminuir el impacto del riesgo detalladas en un plan de gestión de riesgos. Esta información quedará registrada en un plan de gestión del porfolio y proyecto e implementada en la herramienta de *Project and Porfolio Management*.

Entre las actividades a realizar se incluye las siguientes:

- Gestión de la cartera de proyectos o programas.
- Gestión y trazabilidad de requisitos desde la Idea hasta el servicio en todo el ciclo de vida.

- Constitución del proyecto o programa, con el lanzamiento de éste.
- Identificación de los responsables del mismo, Product Owner y Scrum Master.
- Aseguramiento del cumplimiento de objetivos y puntos críticos.
- Grado y avance de los proyectos.
- Análisis y gestión de riesgos del proyecto.
- Gestión y control de cambios del proyecto.
- Reporte y elaboración de informes.
- Coordinación de las actividades e interlocución con el resto de los agentes implicados para el desarrollo del servicio.

Con el fin de coordinar y dar seguimiento a cada una de las iniciativas que tengan cabida en los Servicios de Seguridad, la empresa adjudicataria deberá evaluar y establecer los medios metodológicos y operativos a través de la herramienta de Project and Porfolio Management, que será proporcionada por la empresa adjudicataria, que dé soporte al ciclo de vida completo de la iniciativa. La información sobre los requisitos de esta herramienta está en el apartado 3.1.2.6. Cuadro de mando y reporte. Una vez se lleve a cabo la implantación del servicio y finalice la fase de estabilización, se procederá a realizar un Catálogo de Servicios, con el fin de inventariar y gestionar la reutilización de los recursos dentro de la DGSD. Es por ello, que la empresa adjudicataria deberá diseñar, elaborar, publicar y mantener actualizado dicho Catálogo, siendo responsables de la gestión integral del mismo. Los licitadores deberán presentar una propuesta de **gestión de dicho Catálogo de Servicios**.

Este Catálogo de Servicios debe incorporar como mínimo las siguientes características:

- Debe permitir cursar consultas, peticiones preconfiguradas mediante plantilla e incidencias.
- Debe permitir publicación de contenidos comunes sobre servicios de seguridad.
- Compartir información relevante entre órganos y unidades.
- Debe facilitar la reutilización de los elementos generados y buenas prácticas.

Gestión de cambios del porfolio y de los proyectos

Bajo la supervisión de la DGSD la empresa adjudicataria deberá diseñar el **sistema de gestión de cambios del proyecto** que permita llevar a cabo un control y seguimiento de estos que permita asegurar la trazabilidad de todo el ciclo de vida del proyecto.

Se deberá establecer el procedimiento a seguir ante las solicitudes de cambio que se puedan producir en la planificación, ejecución, seguimiento y control del proyecto, y que habrán de formalizarse para su evaluación y resolución. En caso de que se aprobasen las solicitudes de cambio, se llevará a cabo el seguimiento de su implementación, a través de dicha unidad de

gestión. Con este bloque de tareas se dará **soporte a la evaluación de las solicitudes de cambio en cuanto a la naturaleza y el impacto en los objetivos de alcance, tiempo, coste y/o calidad**, para la correspondiente toma de decisiones por parte de la DGSD con los responsables de la solución.

La gestión de cambios en los proyectos deberá considerar la **consistencia de todo el ciclo de vida y especialmente de las aprobaciones de las iniciativas abordadas**.

Identificación, control y seguimiento de riesgos de ciberseguridad

La empresa adjudicataria del presente lote identificará y analizará los riesgos potenciales del servicio cualitativa y cuantitativamente, y elaborará la correspondiente matriz de riesgos, donde se identifique el riesgo, la probabilidad, el impacto, el responsable y las acciones de mitigación del riesgo, poniéndola a disposición de la DGSD para la toma de decisiones.

El **plan de riesgos** deberá incluir al menos información de identificación, categorización, urgencia, impacto, probabilidad de materialización y estrategia a seguir con su correspondiente plan de actuación. La adjudicataria contemplará en el análisis de riesgos información sobre la complejidad de realización, esfuerzo, integraciones a considerar, y aquellas variables que puedan ser motivo de valoración para la adecuada implantación de las acciones resultantes.
Asimismo, la empresa adjudicataria realizará el seguimiento de los riesgos, con la periodicidad establecida en función de la etapa del proyecto.

La adjudicataria debe incluir la información con la evaluación de los riesgos y sus mitigaciones en los correspondientes informes de estado del servicio acordados y solicitados por la DGSD.

Gestión del conocimiento

La empresa adjudicataria deberá establecer un modelo de gestión del conocimiento que permita asegurar una adecuada transmisión de la información, experiencias y habilidades entre los equipos de trabajo. Este modelo deberá ser sistemático y eficiente afectando a todas las fases del ciclo de vida de la iniciativa, garantizando que en cada fase se tiene la documentación asociada a cada función: desde la gestión de la demanda, gestión del proyecto (constitución, desarrollo del servicio, calidad y pruebas, transición y estabilización) y durante la operación. Este modelo deberá definir todos los flujos de trabajo establecidos para el desarrollo del servicio y su correspondiente asociación con la documentación requerida en cada uno de ellos.

La empresa adjudicataria desarrollará un modelo donde la información cumpla lo siguiente:

- Su almacenamiento y acceso esté basado en repositorios de fácil acceso, propiciando una transferencia de conocimiento entre los miembros de las distintas empresas adjudicatarias de este expediente y el personal de la DGSD responsable del proyecto.
- Esté clasificada y categorizada, de acuerdo con el tipo de información y fase del ciclo de vida en la que se elabora y/o utiliza.
- Se mantenga actualizada a las últimas versiones.
- Cada activo de información tendrá asignado un responsable durante todas sus fases: creación, aprobación y mantenimiento.

La empresa adjudicataria establecerá los **mecanismos adecuados para establecer el control y traspaso del conocimiento** que se genere por los trabajos de gestión de los servicios demandados.

La documentación principal que deberá ser almacenada y gestionada será:

- Documentación de descripción del servicio.
- Manuales y protocolos de coordinación y gestión.
- Manuales de configuración, casos de pruebas y manuales de usuario/a.
- Materiales didácticos utilizados para las formaciones.
- Documentación de gestión del modelo de operación.

La empresa licitadora deberá aportar una **estrategia de gestión del conocimiento** en todas las fases del porfolio y el proyecto, deberá estar sincronizada con una **herramienta de gestión documental** y del repositorio de contenidos, que será utilizado para el almacenamiento y gestión de archivos electrónicos. Está herramienta tendrá que ser integrada con la herramienta de gestión, *Project and Porfolio Management (PPM)*, por la empresa adjudicataria. Toda la documentación generada será propiedad de la DGSD, la empresa adjudicataria deberá asegurar y garantizar que no se producen fugas de conocimiento.

Por otro lado, se solicita a la empresa adjudicataria una estrategia con el modelo de gestión del conocimiento hacia el exterior. En esta estrategia se plantea la necesidad de integrar en un espacio común diferentes elementos de información:

- **Catálogo de servicios**, que cumpla con los requisitos descritos en el apartado **Gestión del porfolio y de los proyectos**, y permita dar a conocer los servicios y necesidades, fomentando la reutilización de recursos sencillos.
- **Materiales formativos**, estarán accesibles los materiales didácticos necesarios, permitiendo la formación en línea de los mismos.

- **Recursos documentales**, tanto la documentación técnica, operativa, como la documentación funcional, y recursos documentales formativos generados para cada servicio estarán accesibles por la DGSD.
- **Ideas**, aquellas necesidades de seguridad planteadas por la DGSD, donde se podrá registrar y consultar su situación y estado de tramitación.
- **Catálogo de peticiones y consultas frecuentes**, que recoja la información sobre las peticiones y consultas más reiterativas y frecuentes realizadas.
- **Inventario**, con la información y detalle de cada uno de los ítems que se requieran en el servicio.

Este modelo de gestión del conocimiento se desplegará en un Portal de Seguridad que deberá proporcionar el presente lote y ser aprobado por la DGSD, debiendo cumplir las siguientes características:

- **Ser reutilizable y compartible**, este espacio permite el acceso a la información, al inventario de ideas, casos de uso...
- **Ser centralizado**, los tres lotes serán usuarios de dicha herramienta y deberán aportar el seguimiento e información. El lote 1 se asegurará de ofrecer los accesos y capacidad a los usuarios de dichos lotes y que faciliten la centralización de las tareas.
- **Estar accesible y disponible**, debe estar a disposición por la **OSSI**, accesible por perfiles autorizados por la DGSD.
- **Ser estructurado**, toda la información contenida en este espacio debe ser estructurada y categorizada con el fin de facilitar su comprensión y su acceso.
- **Estar integrado con una estructura de CMDB** que sea definida desde la DGSD, contando con la información del inventario de los activos objeto del servicio.
- **Estar integrado con la herramienta de ITSM** de la DGSD permitiendo la apertura de incidencias y peticiones que queden registradas en la herramienta de ticketing.
- **Estar integrado con la herramienta GRC** de la DGSD donde se hará pública la normativa aplicable.
- Deberá contener el catálogo de aplicaciones viables y no viables para la DGSD, con el detalle del alcance para cada una de ellas.
- Disponer de una herramienta de visualización de datos de indicadores de servicio que se actualicen de forma dinámica.
- Se deberán incluir capacidades para poder orquestar y automatizar acciones y flujos de Seguridad (integrados con los sistemas y procesos de la DGSD).

3.1.2.2. Modelo de gobernanza

Con el fin de orquestar y coordinar las funciones y recursos de todos los agentes, así como los órganos de control e intervención que requieran la participación y monitorización de los servicios

ofrecidos, será necesario la definición, organización y establecimiento de un modelo de gobierno centralizado que abarque los siguientes niveles:

- **Nivel estratégico**, por el cual se establecerán las herramientas de análisis y diseño de los mecanismos necesarios para la organización y estructura de gobierno, cuyo objetivo será la racionalización y normalización del uso de las tecnologías en los procesos y servicios afectados, generando un marco de buenas prácticas en el empleo de las mismas.
- **Nivel táctico**, coordinación de actividades e interlocución de agentes, que permitirá establecer un modelo de relación con todos los agentes implicados, tanto con proveedores como terceras partes solicitantes del servicio.
- **Nivel operativo**, a través de las herramientas propuestas se velará y garantizará la adecuada operativa y funcionamiento del ciclo de vida de la iniciativa, asegurando la adecuada transición de la iniciativa a proyecto de operación inteligente, a través de mecanismos de normalización de procedimientos del ciclo de vida de la iniciativa, desde el diseño hasta la mejora continua. Asegurando la monitorización tanto de indicadores de gestión de proyectos y operación, como de los rendimientos del servicio.

3.1.2.3. Metodología de gobierno

El modelo de gobierno se materializará a través de un **Plan de Gobierno**, elaborado por la empresa adjudicataria, consensuado con la DGSD y estructurado en varios documentos que recogerán información sobre los diferentes ámbitos:

- Conjunto de **Procesos de Gobierno** que formalice los mecanismos de normalización de procedimientos, herramientas y supervisión de la observancia. Estos procesos de gobierno deberán organizar los procesos operacionales del servicio en cuanto a la gestión del ciclo de vida de la iniciativa, con especial relevancia en la transferencia de información de gestión de la demanda. La empresa adjudicataria deberá establecer una adecuada metodología de gestión y administración del riesgo para la definición y establecimiento de los mismos.
- Modelo de **Comunicaciones y Relaciones**, que establezca los mecanismos de gobernanza y coordinación entre los distintos equipos y las diferentes unidades organizativas que conforman la DGSD, con la identificación de los Responsables y las comunicaciones, así como la identificación de agentes y órganos consultivos y de control.

3.1.2.4. Estructura de gobierno

La estructura de Gobierno se establece en base a un observatorio tecnológico, liderado por la **OSSI**, y los diferentes **Comités operativos** necesarios para el desarrollo del proyecto.
La definición y creación del Comité o Comités se abordará al comienzo de la ejecución del proyecto. Entre sus funciones se encuentran:

- Asesoramiento para la identificación de nuevas tendencias en tecnologías en materia de seguridad, orientada a la eficiencia operacional.
- Asesoramiento sobre los diferentes itinerarios o *Roadmap* con el fin de adelantar características y capacidades de interés en la DGSD.

El **Comité Director**, será el órgano de consulta, supervisión y control que ponga en valor la misión y visión de los servicios y actuará en todas las fases del ciclo de vida. Estará compuesto por responsables del servicio, tanto de la DGSD, o quienes la DGSD delegue/invite, así como los/as directores/as del servicio de la empresa adjudicataria del Lote 1. Estos comités mantendrán una periodicidad mensual. Entre sus funciones se contemplará:

- **Alineamiento de la estrategia** del servicio de seguridad con las necesidades planteadas, estableciendo la relación e interlocución con los correspondientes responsables.
- **Supervisión de la capacidad** del servicio para absorber la demanda requerida, gestionando los riesgos de capacidad.
- **Supervisión y reporte de la ejecución** del gasto y la optimización de los recursos destinados.
- **Promoción de la mejora continua**, estimulando acciones asociadas a la mitigación de riesgos.
- **Supervisión de la gestión del porfolio de iniciativas y proyectos**, y la validez de la viabilidad de las iniciativas aliándolas a los resultados esperados de la estrategia de la **OSSI**.

Los **Comités Operativos**, se estructuran en base al conjunto de comités necesarios para el adecuado desarrollo del servicio. Estarán compuestos por un grupo de personas mixtas tanto de la DGSD, o quienes la DGSD delegue/invite, como de las empresas adjudicatarias de los servicios, según proceda. La periodicidad de estos comités se establecerá de acuerdo con las necesidades del servicio. Aunque se establece al menos, un comité de seguimiento, con carácter bimensual donde la adjudicataria será la responsable de su organización, estructura y contenido en base a los requerimientos de la DGSD. Estos equipos se sustentarán en el refuerzo de sinergias entre las partes, donde la toma de decisiones se acordará y tratará de manera colegiada, en la medida de lo posible, para ofrecer un servicio de calidad.

Las empresas licitadoras incluirán dentro de su catálogo de productos entregables, una estrategia de modelo de gobierno definiendo las herramientas y mecanismos necesarios para llevar a cabo el seguimiento, monitorización y control de las diferentes dimensiones que conforman el gobierno del Servicio de Seguridad. Además, en la propuesta deberá figurar el detalle de toda la documentación que será generada como consecuencia del gobierno del servicio.

3.1.2.5. Seguridad de la información y el servicio

La adjudicataria garantizará la integridad de los sistemas y se asegurará de que los servicios prestados se realizan de acuerdo con los requisitos establecidos por la DGSD en materia de seguridad, acorde con lo previsto en la Ley 40/2015, de 1 de octubre. La adjudicataria deberá velar porque los servicios implantados cumplen con los requisitos del Esquema Nacional de Seguridad aplicables al SERMAS, y aquella normativa de seguridad que le sea de aplicación obligatoria.

3.1.2.6. Cuadro de mando y reporte

Para la correcta consecución de los trabajos, el adjudicatario deberá proporcionar un cuadro de mando y reporte integrado con el Portal de Seguridad descrito anteriormente y que será propiedad de la DGSD a todos los efectos, y que permita la supervisión, coordinación y obtención de información de la correcta implantación del PESI, los diferentes escenarios normativos existentes en el presente pliego. En definitiva, un cuadro de mando que permita a la OSSI la correcta gobernanza del servicio en tiempo real. Estará ubicado en las instalaciones que la DGSD indique.

En la fase de devolución del servicio, el adjudicatario del presente lote deberá proporcionar los fuentes, documentos y materiales necesarios para la correcta evolución de la herramienta si así fuera necesario por la DGSD.

Dado que se facilita que el adjudicatario proponga la herramienta que ofrece la DGSD y que éste deberá aceptar, ésta deberá ser incorporada en la fase inicial del contrato (primer mes), debiendo ser parametrizada y formar correctamente a todos los actores que intervienen en el proceso del servicio que desde la OSSI se gestiona.

3.1.2.7. Elaboración e implantación del PESI

La empresa adjudicataria del presente lote, junto al resto de tareas solicitadas, deberá proporcionar a la DGSD un **Plan Estratégico de Seguridad de Información** (**PESI**). La necesidad de disponer de dicho **PESI** para su posterior implantación se estima en los 3 primeros meses de contrato, siendo obligación del adjudicatario del presente lote el cumplimiento de dicho plazo.

Deberá al menos incluir:

FASE AS-IS: La presente fase pretende hacer un descubrimiento del punto de partida en el que actualmente se encuentra el SERMAS en materia de seguridad/ciberseguridad. Para ello, se deberán como mínimo obtener:

- **Análisis de situación actual**. Recopilación y análisis del punto de partida y la situación inicial, como condicionantes: escenario, alcance, ubicaciones, etc.
- **Identificación de activos esenciales**. Con frecuencia, el valor del sistema en materia de seguridad se concentra en unos pocos activos que son la esencia y razón de ser del sistema, denominados activos esenciales, y en unas pocas dimensiones. Los trabajos se centrarán en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente pueda ser mayor para el funcionamiento del SERMAS.
- Valoración de las dimensiones de seguridad (DICAT) de los activos esenciales identificados.
- Estudio de la política de gestión de los riesgos actual.
- **Nivel de cumplimiento actual en base a SGSI (ISO 27001)**, aunque se dispone de un lote específico en cumplimiento normativo, surge la necesidad de disponer en el presente lote, y tras el punto de partida inicial, un primer contacto y análisis de nivel de cumplimiento en base al SGSI actual que facilite a la OSSI y a la DGSD conocer el estado de los dominios objeto del alcance y sirva de base al resto de adjudicatarios para establecer puntos de partida de su acción.
- **Nivel de cumplimiento actual en base a ENS, GDPR, ISO 22301 y Ley PIC**, como hemos comentado en el punto anterior, se disponen de 2 lotes específicos que ayudarán al DGSD en el cumplimiento normativo y legislativo en materia de seguridad.

FASE TO-BE: La presente fase pretende hacer un descubrimiento de los objetivos a cubrir (GAP) a partir del escenario obtenido en la fase AS-IS en la que se encuentra la DGSD en materia de seguridad/ciberseguridad. Para ello, como mínimo se debe:

- **Realizar un Análisis de Riesgos**, facilitando con ello la identificación de los activos esenciales y la probabilidad de ocurrencia que las amenazas exploten vulnerabilidades sobre los activos identificados o grupo de activos y con ello materialicen un daño en la organización. Su aplicabilidad será siguiendo escenarios como Magerit, Septri, Mosler, Fine o Rachel.

  Se deberá como mínimo cubrir:

  a) Identificación del riesgo: identificación, descripción, fase de aplicabilidad, tipología CIDAT, activo afectado, activos relacionados.
  b) Evaluación, como la probabilidad de ocurrencia, impacto y exposición.
  c) Mitigación, contingencia y estrategia de respuesta.
  d) Propietario o equipo responsable de dicho riesgo.
  e) Escenario de resolución: cuando se revisará, por quien, proceso o procesos que lo sustentan.

Así mismo, además de los riesgos identificados, se deberán proporcionar los riesgos residuales e inherentes que han sido detectados, todo ello, se incorporará al "Mapa de Seguridad".

Entendiéndose por:

a) Riesgo Inherente, aquel intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Propio del trabajo o proceso y que no puede ser eliminado del sistema ya que persiste en la ejecución de la actividad en sí misma.
b) Riesgo Residual, aquel que subsiste después de la implementación de controles que lo mitiguen, en otros términos, el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

- Implementar un sistema de gestión de activos lo cual conduce a una toma de decisiones confiable para el desarrollo, coordinación y control de las actividades relacionadas con el activo. Este sistema de gestión de activos deberá cumplir los requerimientos del Esquema Nacional de Seguridad y estar alienado con los principales objetivos organizacionales.
- El adjudicatario, tras consensuarlo y ser aceptado por el SERMAS, deberá **aplicar un modelo de CMDB**. Es importante a su vez reseñar que se deberá:
  - Generar la interdependencia entre activos.
  - Generar y obtener un mapa de activos que faciliten el mantenimiento y posterior toma de decisiones por la DGSD.
- **Seleccionar las medidas adecuadas** que sean de aplicación al sistema, de acuerdo con los valores máximos de impacto obtenidos en cada una de las dimensiones de seguridad y/o de acuerdo con la categoría del sistema y las medidas de seguridad adicionales resultantes del análisis de riesgos.
- Elaborar un **Plan Estratégico de Seguridad de Información (PESI)** que deberá ser validado por la DGSD o por quien este designe para la aceptación del mismo previo a la implantación.

Objetivos:

- Focalizar esfuerzos donde es necesario.
- Aunar esfuerzos entendiendo los objetivos de las medidas.
- Análisis de riesgos continuo (amenazas y priorización).
- Estrategia alineada siempre con procesos y negocio.

Requerimientos base:

- Un diagnóstico que permita identificar todos los procesos de la organización.

- Análisis de las vulnerabilidades respecto a la infraestructura, el personal, la tecnología y la información.
- Plan de emergencia que defina las acciones que se deben tomar para mitigar los posibles riesgos.
- Manual de seguridad con los respectivos protocolos que se deben seguir ante cualquier emergencia.
- Concienciación por parte de los empleados de la organización.
- Las reglas de seguridad que deben seguirse para generar un entorno más seguro.

Se propondrá un escenario base que deberá ser presentado y aprobado por la DGSD en base a 2 posibles modelos, tras su aprobación se ejecutará el seleccionado o un híbrido de ambos:

- Modelo ENS basado en protección, detección, respuesta y conservación.
- Modelo ISO/IEC 27001, basado en plan-do-Check-Act.

El escenario base para su materialización deberá enfocar:

- Identificación de roles y funciones.
- Procedimientos a aplicar en base al análisis.
- Identificación de medidas.
- Priorización de medidas.
- Modelo y criterio de implantación.
- Aprobación.
- Ejecución y seguimiento del Plan.
- Objetivos que deberá cubrir, entre otros:
    - RESULTADOS
        - Cuantificar el impacto de incidentes de seguridad.
        - Mejora continua del SGSI.
    - SUPERVISIÓN
        - Gestionar los riesgos de Seguridad de Información.
        - Evaluar cambios en la empresa, entorno, tecnología…
        - Aseguramiento de uso y aprobación de aplicaciones móviles corporativas.
        - Aseguramiento del IOTM.
        - Aseguramiento del Servicio digital.
        - Aseguramiento de los entornos Cloud.
        - Aseguramiento y gestión de la calidad de los datos.
        - Aseguramiento de la inteligencia artificial.
        - Aseguramiento en la divulgación de la información.
    - EFICIENCIA
        - Optimizar la gestión de incidentes de Seguridad de Información.
        - Implementar acciones correctivas y de mejora.

- Monitorizar el cumplimiento de los requisitos de Seguridad de Información.
- Ampliar la visibilidad de riesgos y amenazas.

- OBJETIVO
  - Desarrollar cultura de Seguridad de Información.
  - Sensibilizar sobre los riesgos y la privacidad de los datos.
  - Capacitar a las personas (internas y colaboradoras) sobre seguridad de la información.

3.1.2.8. Mantenimiento y cumplimiento de objetivos normativos

Como se ha comentado a lo largo del presente documento, el adjudicatario del Lote 1, tendrá la obligación de dar apoyo al resto de lotes durante el contrato. Además, velará por el correcto cumplimiento de la normativa aplicable en materia de seguridad y protección de datos.

Este servicio está orientado al desarrollo de actividades de asesoría y consultoría para la adecuación a la legislación y normativa relacionada con el cumplimiento del Esquema Nacional de Seguridad (ENS).

Con ese fin, a continuación, se detalla una relación de las actividades que comprenderá el servicio:

- Asesoramiento técnico y consultoría legal y normativa en materia de tecnologías de la información y comunicaciones y seguridad informática.
- Soporte a la DGSD en la interlocución con los agentes implicados en temas de seguridad de la información: Agencia Española de Protección de Datos (AEPD), Centro Criptológico Nacional (CCN), Oficina de Coordinación de Ciberseguridad (OCC), fuerzas de seguridad, juzgados, etc.
- Asesoramiento técnico en la elaboración y actualización de políticas, normas, procedimientos e instrucciones en materia de seguridad (política de contraseñas, acceso remoto, uso del correo electrónico, gestión de la documentación en formato papel, funciones y obligaciones del personal con acceso a datos personales, etc.) de acuerdo con la legislación, normativa estándares y códigos de buenas prácticas.
- Coordinación, dinamización y asesoramiento, tanto técnico, a los comités y comisiones de trabajo en materia de seguridad que pueda necesitar la DGSD.
- Asesoramiento técnico en los procedimientos de contratación de la DGSD que puedan afectar a la disponibilidad, accesibilidad, confidencialidad e integridad de los datos personales de la organización, garantizando el debido respeto de las medidas de seguridad.

- Asesoramiento técnico y apoyo en el uso y custodia de certificados digitales y servicios de firma electrónica, servicios electrónicos al ciudadano y manejo seguro de documentación digital.

Este servicio se apoyará en la herramienta que la DGSD proporcione para la correcta adecuación al ENS, que contemplará las siguientes tareas:

- Proponer un plan de adecuación, con un alcance que tendrá que aprobar la DGSD.
- Proponer las medidas y recomendaciones necesarias para que los Sistemas de Información, cumplan con el ENS.
- Mantener actualizada la categorización de los Sistemas de Información existentes y la identificación y categorización de los nuevos.
- Elaborar y actualizar periódicamente los análisis de riesgos de los diferentes sistemas de información, cumpliendo con los requisitos establecidos en el ENS.
- Mantener actualizada (de manera formal y detallada) la declaración de aplicabilidad en los sistemas de información del sistema sanitario. Se especificará en detalle las medidas técnicas de obligado cumplimiento para cada Sistema de Información identificado.
- Establecer las recomendaciones que se consideren convenientes, para que, dentro del proceso de mejora continua, los sistemas cumplan los objetivos del ENS y se consiga un sistema de gestión de la seguridad de la información que se ajuste a los requisitos exigidos.
- Establecer las recomendaciones en el plan de mejora de la seguridad, que detallará los proyectos y actuaciones destinadas a subsanar las deficiencias detectadas. La OSSI, gestionará y prestará apoyo en la implantación de las medidas recogidas en el plan de mejora de la seguridad.
- Realización y seguimiento del Plan de Acciones Correctivas que surja como resultado de las diferentes auditorias de seguridad que lleve a cabo la DGSD.

3.1.2.9. Apoyo al CISO

Como se ha comentado a lo largo del presente documento, el adjudicatario del Lote 1, tendrá a su vez la obligación de dar apoyo al **CISO (Chief Information Security Officer)** en las tareas requeridas para el correcto desempeño de su labor y los objetivos que persigue, entre otras. Dicho apoyo contará con las siguientes actividades:

- Apoyo en la toma de decisión sobre las acciones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios.
- Asesoramiento en la aprobación de las medidas de seguridad que debe aplicar el sistema de información.
- Análisis de los informes de auditorías de seguridad de la información.

- Establecimiento de medidas de seguridad en el SERMAS y en la DGSD, de acuerdo con la normativa vigente de las actividades de tratamiento que contengan datos de carácter personal, y la realización de auditorías en el ámbito de la protección de datos de carácter personal.
- Establecimiento de mecanismos para garantizar el acceso y la autentificación de los usuarios a los sistemas de información en el SERMAS.
- Definir la normativa de seguridad y velar por su cumplimiento.
- Gestionar los riesgos de seguridad.
- Identificar los requisitos de seguridad.
- Supervisar el cumplimiento de la legislación.
- Apoyo a la interlocución en materia de seguridad con los distintos contactos de interés: la alta dirección, otras CCAA y otras instituciones como CCN-CERT, CNPIC, OCC, Madrid Digital, fuerzas y cuerpos de seguridad… canales de reporte y colaboración con los CERTs.
- Formar, concienciar y sensibilizar en materia de seguridad.
- Gestionar los incidentes de seguridad, en colaboración con el Responsable de Gestión del Incidente designado por el SOC de Madrid Digital.
- Supervisar la continuidad del negocio.
- Dar apoyo a procesos de contratación de la DGSD, si así se requiere.

3.1.2.10. Apoyo al DPD (delegado de protección de datos) de la Consejería de Sanidad de la Comunidad de Madrid.

Como se ha comentado a lo largo del presente documento, el adjudicatario del Lote 1 tendrá a su vez la obligación dar apoyo al DPD (delegado de Protección de Datos de la Consejería de Sanidad) en las tareas requeridas para el correcto desempeño de su labor y los objetivos que persigue. Entre otras, dicho apoyo contará con las siguientes actividades:

- Gestión del registro de operaciones de tratamiento de datos personales.
- Revisar las operaciones de tratamiento de datos personales.
- Registro, mantenimiento y control de actividades de tratamiento.
- Analizar y evaluar los riesgos que implican las operaciones de tratamiento de datos personales.
- Gestionar operaciones que puedan dar lugar a un alto riesgo. Realización de Evaluaciones de Impacto de Protección de Datos (EIPD).
- Supervisión, asesoramiento y seguimiento del cumplimiento normativo.
- Gestionar violaciones de seguridad de datos personales.
- Investigación (incluyendo el tratamiento) de las denuncias internas.
- Proporcionar asesoramiento e información en materia de protección de datos al responsable o al encargado del tratamiento.

- Seguimiento del cumplimiento del RGPD.
- Cooperar con la autoridad de control.
- Asesoramiento normativo en el ámbito de la protección de datos.
- Formación y concienciación a los diferentes interlocutores.
- Plan de formación de protección del dato sanitario en los centros.
- Planes de concienciación para empleados sobre la correcta protección de sus datos.
- Elaboración, supervisión y confección de contratos, convenios y encargos de tratamiento, así como cláusulas legales.
- Estudiar la viabilidad de las iniciativas del SERMAS, proponiendo cambios para el correcto cumplimiento de la legislación en materia de protección de datos y seguridad.
- Identificación correcta de la base de legitimación de los tratamientos de datos de carácter personal.
- Asesoramiento sobre:
    - Marco normativo en el ámbito de la protección de datos.
    - La legitimidad en los accesos a la historia clínica.
    - Los derechos de los pacientes y la gestión de estos.
    - El intercambio y la reutilización de datos con fines de investigación biomédica.
    - Brechas de seguridad.
    - Gestión de derechos de ciudadanos sobre datos personales.
    - Incidencias legales.
    - Procedimientos sancionadores.
- Desarrollo del Marco normativo: Política de privacidad, normativa de atención de los derechos, normativa de identificación e inventariado de los tratamientos, normativa de contratación de encargados de tratamiento, normativa de brechas de seguridad, normativa de seguridad en el diseño, normativa de EIPD, …
- Asesoramiento y soporte en cuestiones de cualquier índole que impliquen a la AEPD, concretamente y sin que sea excluyente, este es el listado de las principales líneas de interrelación con la AEPD:
    - Gestión de comunicaciones realizadas con la AEPD.
    - Generación de los modelos de comunicación.
    - Gestión de brechas de seguridad.
    - Gestión de nombramientos DPO.
    - Consultas previas.
    - Gestión de procedimientos: tutela de derechos, procedimientos sancionadores.

3.1.2.11. Servicio multidisciplinar en materia de seguridad

Este asesoramiento tiene como objetivo velar por el adecuado grado de madurez de la seguridad de los sistemas de información de los centros del SERMAS, asegurar la continuidad del servicio y prevenir otros riesgos como pérdida de datos o confidencialidad, mediante la asesoría y

seguimiento de la normativa de seguridad aplicable, así como de estándares y códigos de buenas prácticas, relacionados con la seguridad de los sistemas de información.

Comprende, entre otras, las siguientes actividades:

- Auditorías de controles generales de TI en centros de la CSCM (Indicadores de Contrato Programa y Diagnósticos de Seguridad (ISO 27002)).
- Auditorías de seguridad física y medioambiental de la infraestructura tecnológica (CPDs). (Estándar TIER).
- Asesoría en desarrollo e implantación de medidas de seguridad de TI.
- Aplicación de planes de continuidad de negocio alineados con las tareas definidas.

3.1.2.12. Realización de diagnósticos de seguridad

Se trata de un servicio especializado de seguridad TI que cubra diagnósticos de:

1) Infraestructura, comprende entre otras las siguientes actividades:
   a. Análisis de seguridad perimetral para dar cobertura a posibles incidentes de seguridad.
   b. Análisis de cumplimiento y regulación TIER en línea de las auditorías físicas realizadas en los CPDs de los centros.
   c. Dar apoyo en la realización de planes de contingencia y realizar actividades de gestión de riesgos (planificación, detección, mitigaciones).
   d. Gestionar la seguridad de la información, aplicando las normativas y estándares existentes, guiando en la implementación de políticas de seguridad y en la implementación de controles de seguridad y el Sistema de Gestión de Seguridad de la Información (ITSM), alineando las actividades programadas en el marco de los estándares existentes y aplicables.
   e. Alinear las actividades programadas al marco de los estándares existentes (ISO 27001, ISO 22301, ENS, COBIT, NIST, otras).
2) Comunicaciones:
   a. Desarrollar e implementar las políticas y procedimientos de seguridad. Monitorear su cumplimiento.
   b. Gestionar incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.
   c. Conocimiento y gestión de configuración de cortafuegos (WAF) y Sistemas de protección de aplicaciones en el tiempo de ejecución (RASP).
   d. Realizar análisis de riesgos en nuevas tecnologías. Aplicar metodologías, tecnologías y herramientas, modelos formales, análisis forense, etc. en las áreas implicadas.
   e. Realizar actividades de gestión de riesgos (planificación, detección, mitigaciones).

Siempre que los diagnósticos de seguridad comprendan competencias de Madrid Digital, u otros organismos independientes, habrá que motivar esta necesidad y coordinar los trabajos tras recibir la aprobación oportuna.

En todos los casos se deberá:

1) Proporcionar un informe de resultados y recomendaciones para subsanar las vulnerabilidades y riesgos encontrados. Debiendo justificar debidamente cada vulnerabilidad detectada:
    a. Tipo de vulnerabilidad.
    b. Responsable.
    c. Sistemas afectados.
    d. Impacto.
    e. Valoración CVSS v.3.X o superior si aplicara llegado el caso.
    f. Número de ocurrencias.
    g. Categoría de vulnerabilidad.
    h. Riesgo.
    i. Descripción detallada de la vulnerabilidad, con el fin de que se entienda perfectamente cómo se ha producido y ayude a la persona encargada de corregirla a solucionarla. Inclusión de evidencias, POCs… que faciliten su comprensión.
    j. Recomendaciones que solucionen de una manera correcta y homogénea la vulnerabilidad descrita.
    k. Informe ejecutivo de los resultados, con enfoque claro a la dirección.

2) Opcionalmente, si así fuera requerido, publicar en la herramienta ANA del CCN-CERT o en la herramienta/cuadro de mando que designe la DGSD si fuera necesario.

3) El adjudicatario deberá disponer de los medios necesarios, herramientas y licencias para el correcto desempeño de su labor, basándose en productos licenciados de mercado de calidad reconocida.

3.1.2.13. Integración en el ciclo de vida seguro de los proyectos de la Consejería de Sanidad

Existen diferentes mecanismos que facilitan la protección de los proyectos. Dichos mecanismos pueden en ocasiones resultar ineficaces en la construcción del sistema si no se ha realizado de forma segura desde su desarrollo.

Por ello, tan importante es proteger el entorno donde se ejecutan las aplicaciones, como desarrollar aplicaciones con un nivel de seguridad aceptable, en entornos protegidos y mediante un Ciclo de Vida de Desarrollo Seguro (SDLC) y aplicación de Buenas Prácticas de Desarrollo.

Se requiere dar apoyo a dichas acciones de integración en el ciclo de vida seguro en los siguientes escenarios SDLC:

- Microsoft Security Development Lifecycle: formación, requisitos, diseño, implementación, comprobación, lanzamiento y respuesta.
- OWASP – Software Assurance Maturity Model (SAMM): funciones de negocio (gobierno, construcción, verificación e implementación), prácticas de seguridad, estrategia y métricas, políticas y cumplimientos, educación y orientación, requisitos de seguridad, evaluación de amenaza, arquitectura de seguridad, revisión de diseño, pruebas de seguridad, revisión de código, fortalecimiento del ambiente, administración de vulnerabilidades, habilitación operativa.

Acciones base que se deberán realizar para asegurar dicho ciclo de vida:

- Alinear el desarrollo con la política de seguridad de la Consejería de Sanidad. Dicha política, en revisión periódica, garantizará el alineamiento con las directrices de seguridad.
- Aplicar los procedimientos de seguridad requeridos para cada una de las tecnologías aplicadas.
- Identificación y análisis de casos de abuso y cómo comportarse ante estas circunstancias.
- Analizar los riesgos existentes modelizando las posibles amenazas.
- Supervisión y asesoramiento en el cumplimiento de requisitos legales a tener en cuenta en el desarrollo.
- Marcar las directrices de diseño que faciliten la aplicabilidad de buenas prácticas.
- Marcar las directrices de programación, estableciendo pruebas de seguridad a partir de los requisitos de seguridad establecidos.
- Establecer directrices en los despliegues que nos aseguren que el nivel de riesgo en dicha acción es mínimo.
- Aplicar procesos de auditoría continua que faciliten un óptimo resultado.
- Alineamiento con DevSecOps para integrar la seguridad en la metodología de desarrollo.

Pruebas integradas en el ciclo de desarrollo

La DGSD gestiona una gran cantidad de sistemas de información basados en desarrollos a medida, que debe ser verificados a nivel de seguridad antes de su puesta en operación.

Para ello se requiere de la mayor automatización de tareas, basado en el paradigma DevSecOps. El presente servicio contiene las tareas necesarias para una provisión correcta de los servicios de pruebas de seguridad integradas en el ciclo de desarrollo y que son las que se describen a continuación:

- Servicio de análisis estático de código para la búsqueda de vulnerabilidades en las aplicaciones, realizando tareas de caja blanca, basados en productos licenciados de mercado de calidad reconocida. Integración del servicio dentro de los flujos de trabajo de la DGSD.
- Servicio de análisis dinámico de código para la búsqueda de vulnerabilidades en las aplicaciones, basado en productos licenciados de mercado de calidad reconocida. Integración del servicio dentro de los flujos de trabajo de la DGSD.
- Servicio de análisis SCA (Software Composition Analysis) para los componentes de código abierto utilizados en los desarrollos basados en software comercial o de fuentes abiertas.
- Evaluar, proponer, operar, configurar e integrar herramientas adicionales de realización de pruebas de seguridad, del tipo SAST, SCA, DAST, etc.
- Definir los criterios de aceptación de las pruebas de seguridad sobre aplicativos en auditoría estática y dinámica de código fuente.
- Soporte en el entendimiento y remedio de las vulnerabilidades encontradas, dando apoyo a las áreas de desarrollo sobre la forma de resolver las vulnerabilidades encontradas. Atender consultas relacionadas, y propuesta de soluciones alternativas para la mitigación de las vulnerabilidades detectadas.
- Configurar, operar e informar de los resultados obtenidos en el servicio de análisis de código fuente tanto automatizados como solicitados bajo demanda, donde se indiquen las vulnerabilidades detectadas clasificadas y ponderadas, las evidencias y las recomendaciones de remediación.

Las pruebas integradas en el ciclo de desarrollo se prestarán en modo servicio, sin disponer la DGSD de licencias de las herramientas de pruebas integradas sino utilizando los servicios del adjudicatario.

3.1.2.14. Comunicación, concienciación y formación en seguridad de la información

Debido a la tipología de acciones que se realizan, es necesario orientar los servicios a la concienciación y formación en materia de seguridad de información, y al entendimiento de la legislación y normativa que les aplica a todos los entes del SERMAS. Así mismo, es necesario comunicar, formar y concienciar sobre la seguridad en el uso de nuevas tecnologías y/o herramientas al personal al servicio de la Consejería de Sanidad de la Comunidad de Madrid.

Se debe diseñar y desplegar un **Plan de formación anual**, con un itinerario formativo orientado a:

- una formación presencial por cada centro hospitalario y otra sesión para la atención primaria;

- la concienciación del equipo directivo de la DGSD con las acciones formativas ad-hoc que la DGSD estime oportunas; y
- formación para responsables TI tanto de servicios centrales como de los centros sanitarios.

Las fases que tiene que contemplar el plan son las siguientes:

- Fase 1. Planificación. La información obtenida de la primera fase será un input que ayudará a ajustar las acciones de las siguientes etapas.
    - Análisis e identificación de las necesidades, riesgos y puntos de vulnerabilidad de los colectivos seleccionados.
    - Estudio del modelo de gobierno e identificación de los canales para el lanzamiento de las acciones formativas.
    - Elección de la modalidad que más se adapte a la consecución de los objetivos: charlas presenciales, webinars, ejercicios phishing, contenido gamificado, podcasts, videotutoriales, infografías, píldoras, cursos online…
- Fase 2. Diseño. Definir, crear y desarrollar el contenido de las acciones formativas para cada colectivo.
- Fase 3. Implementación. Se llevarán a cabo las acciones planificadas y diseñadas previamente. Esta etapa estará sujeta a continua evolución, ya que estará sujeta a los cambios de las distintas necesidades que vayan surgiendo.
- Fase 4. Mejora continua.
    - Medición de la evolución de los comportamientos ciberseguros de los colectivos impactados en el Plan bianual de Formación.
    - Creación de informes y/o cuadros de mandos con los resultados de las acciones lanzadas en la Fase de Implementación.

Dentro de estos puntos se abarcarán las siguientes actividades:

- Desarrollo de material de formación relacionado con protección de datos en el ámbito sanitario, legislación y normativa relacionada.
- Impartición de acciones formativas en materia de protección de datos en el ámbito sanitario, normativa, estándares y códigos de buenas prácticas.
- Desarrollo de material de formación relacionado con seguridad de información, legislación y normativa relacionada.
- Impartición de acciones formativas tanto de seguridad de la información, normativa, estándares y códigos de buenas prácticas, así como gestión y asesoría en herramientas (presenciales y online).
- Gestión del contenido del portal intranet de la OSSI, así como la realización de comunicaciones del boletín de seguridad de la DGSD (newsletter bimensual).

- Generación y mantenimiento de canales de comunicación para la concienciación en materias de seguridad de la información.

3.1.2.15. Ciberejercicios

Además, se realizarán ciberejercicios de manera anual, en el que se ponga a prueba la capacidad de respuesta de la DGSD en coordinación con los servicios proporcionados por el SOC de Madrid Digital. La OSSI marcará un calendario de actuación en coordinación con Madrid Digital y teniendo en cuenta el calendario del Plan de formación anual de la OSSI. El propósito de la ejecución de ciberejercicios es aumentar el nivel de madurez en términos de eficacia y eficiencia ante la existencia de un ciberincidente, ante circunstancias que se podrían dar en situaciones reales, con el fin de revisar los procedimientos establecidos y encontrar puntos de mejora.

El objetivo de estos ciberejercicios es poner a prueba la capacidad de respuesta en un entorno controlado. Al igual que se hace con actividades de auditoría para las fases de protección y detección de ataques. Se realizará una planificación y un diseño controlando el impacto en la organización y los objetivos a ser medidos.

Cada año se tendrá en cuenta uno de los siguientes supuestos:

- Roleplay: Persigue entrenar y evaluar la toma de decisiones por parte del comité de crisis ante la existencia de un incidente de alta prioridad e impacto en el negocio. Se basará en casos reales de grandes incidentes.
- Ingeniería Social: Persigue entrenar y evaluar el grado de concienciación de los usuarios de una organización con respecto a ataques dirigidos. Se basarán en técnicas de suplantación para obtener información relevante.
- Simulación: Persigue entrenar y evaluar la capacidad técnica de análisis de un ciberincidente. Se basará en la determinación de un entorno comprometido hasta la formulación del timeline completo de acciones del atacante.

El adjudicatario proporcionará la metodología y herramientas propuestas para estos ensayos, que implicarán a los niveles de la DGSD y del propio adjudicatario que sean necesarios en cada supuesto.

Cualquier herramienta, escenario o simulación necesaria para estos ejercicios será proporcionada por el adjudicatario sin coste adicional.

3.1.2.16. Apoyo a la DGSD en la consecución de los objetivos en materia de seguridad establecidos

Distinguiendo entre otras actividades:

- Identificación de problemas y definición conjunta de soluciones.
- Análisis de alternativas y selección.
- Generación de documentación que sustente el apoyo.
- Registro y comunicación de decisiones con los involucrados.
- Aplicación de la decisión.
- Seguimiento de la decisión.
- Apoyo en la defensa de las auditorías internas.
- Implicación en la gestión de los incidentes de seguridad.

3.1.2.17. Apoyo ante incidentes de alto impacto o cibercrisis

El servicio de gestión de incidentes de alto impacto o gestión de crisis, consistirá en una colaboración de alto nivel de especialización para gestionar los incidentes de seguridad que, por su peligrosidad o impacto, complejidad para su mitigación, alcance o relevancia para la organización, necesiten de una intervención reforzada y/o urgente por parte de un equipo de alta especialización. Se trata de incidentes que deben ser tratados con máxima prioridad, para que el SERMAS pueda realizar sus funciones con total normalidad. Se recogen como cibercrisis potenciales todos los incidentes de ciberseguridad categorizados como MUY ALTO o CRÍTICO de acuerdo con norma STIC 817 del CCN.

Una vez se haya activado la gestión de incidentes de alto impacto, con el Equipo de Respuesta a Incidentes (CSIRT) según los procedimientos establecidos por la DGSD y el SOC de Madrid Digital, la OSSI dará apoyo legal y técnico a la DGSD en todo momento durante la gestión del incidente. La asistencia será en remoto, o in situ, si la DGSD así lo requiere.

3.1.2.18. Supervisión y análisis funcional de la monitorización y vigilancia del entorno sanitario

La OSSI debe coordinar los trabajos de monitorización del SOC. En los cuales se establecen dos niveles diferentes para constituir un trabajo híbrido operativo entre la OSSI y el SOC de MD:

- Supervisar las operaciones del Centro de Operaciones de Seguridad de MD. Supervisará el trabajo del SOC en los procesos de recolección de registros de actividad, la operación de la información recolectada y los procesos dependiente de la operación de seguridad de los sistemas de la información.
- Dentro de la OSSI, se constituirá un equipo de analistas encargados de la reevaluación de las alertas, definición de las reglas basada en negocio y la definición funcional de los casos de uso. Esta información revertirá en el SOC de tal forma que la inteligencia generada será implementada como reglas de correlación.

3.1.2.19. Otras tareas

Además de los servicios encuadrados en los puntos anteriores, se realizarán las siguientes actividades:

- Análisis de activos y de riesgos periódicos, que permitan identificar riesgos relevantes y medidas de seguridad implementadas para mitigarlos.
- Coordinación en la implementación de medidas para permitir la máxima homogeneidad posible en los centros dependientes del SERMAS.
- Control, alimentación y mejora constante del cuadro de mando integral de seguridad.
- Soporte a la gestión de identidades.
- Mantenimiento del Portal institucional de Seguridad.
- Soporte a la implantación de las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público en materia de seguridad y privacidad de la información y los servicios.
- Soporte a la implantación tecnológica del uso del DNIe y otros certificados digitales u otros sistemas de identificación y firma electrónica, por los ciudadanos y profesionales.
- Soporte para el cumplimiento del conjunto de normas para la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado único europeo (eIDAS).
- Soporte a los centros en la realización de las auditorías.
- Validación de requisitos de seguridad en sistemas en producción y en sistemas de nueva creación, colaborando en su ciclo de vida completo.
- Soporte en el tratamiento y resolución de incidencias de seguridad, pruebas de intrusión, hacking ético, etc.
- Formación y concienciación constante a los profesionales, para incorporar buenas prácticas en seguridad.
- Formación en las aplicaciones que se desarrollen como consecuencia de este contrato, a los integrantes de la OSSI, pertenecientes a la DGSD y resto de lotes de este pliego.

3.2. Lote 2: Oficina de Auditoría Interna

3.2.1. Alcance del servicio

El objeto de este lote engloba:

1. El servicio de apoyo a la realización de las auditorías para el cumplimiento del RGPD y LOPDGDD en lo referido a la protección de datos personales para los tratamientos de datos realizados en el SERMAS.
2. La realización de una auditoría regular ordinaria, de las aplicaciones del SERMAS, con los objetivos señalados en el Anexo III del RD 311/2022 que regula el Esquema Nacional de Seguridad, incluyendo sus revisiones posteriores.

Cabe destacar que el alcance de este pliego abarca los sistemas de información que dan servicio a los tratamientos de datos del SERMAS en su ámbito de actuación, es decir, los sistemas de informática médica, gestión sanitaria y aquellos relativos a las relaciones del sistema sanitario con los ciudadanos, profesionales sanitarios, oficinas de farmacia, sanidad privada y cualesquiera otras personas físicas o jurídicas distintas de la Administración de la Comunidad de Madrid.

3.2.2. Actividades a realizar

3.2.2.1. Auditoría en Protección de Datos de Carácter Personal

El contratista elaborará un formulario con un cuestionario inicial de cumplimiento de las medidas técnicas legales y organizativas de seguridad en el tratamiento de datos de carácter personal, incluyendo una lista de puntos de comprobación. Lo remitirá a los Centros y unidades organizativas para realizar una recogida preliminar de información de forma previa a la visita de los auditores.

Recabada esta información, el adjudicatario establecerá la planificación de las entrevistas con el responsable de tratamiento y/o encargado de tratamiento, a las que puede asistir su Comité Delegado de Protección de Datos o DPD como asesor, o aquellas personas en quien estos deleguen. Considerando el elevado número de tratamientos auditables en algunos Centros, se podrá exigir por la DGSD la realización de más de una entrevista en dichos Centros, con el fin de asegurar la calidad de la auditoría. Siempre se efectuarán las entrevistas en cada uno de los Centros.

El auditor deberá realizar la entrevista constatando el estado de cada uno de los epígrafes aplicables y exigibles por el contexto legal, y requiriendo y evaluando las evidencias necesarias para asegurar el cumplimiento. Se deben minimizar las necesidades de recopilación de información y el tiempo necesario por parte de los responsables de tratamiento o de seguridad. El auditor deberá recoger evidencias de cada medida de seguridad auditada, las cuales deberán constar en el informe y ser adjuntadas en la documentación final.
En cada informe de auditoría se debe reflejar el historial de cambios de estado del tratamiento o de la aplicación: por alta nueva, modificación, supresión realizada y prevista próximamente, así como por inclusión del tratamiento en otro existente.

Realizadas las entrevistas, el auditor de la empresa adjudicataria procederá a la elaboración de los informes borradores de auditoría. Estos serán remitidos a los Responsables de Tratamiento de los Centros para la presentación de alegaciones si las hubiese y, una vez solventadas las discrepancias, se procederá a la entrega de los informes finales a cada uno de los Centros,

donde se informará de las deficiencias y de las recomendaciones de mejora. Existirá un informe de auditoría por cada tratamiento auditado en el Centro o unidad organizativa.

Asimismo, el auditor de la empresa adjudicataria elaborará un informe genérico por Centro o unidad organizativa de la CSCM, de cumplimiento de la normativa sobre protección de datos, donde se tengan en cuenta los artículos 4 al 43 de la LOPDGDD (derechos de los ciudadanos, de información, consentimientos, comunicación, cláusulas, formularios, modelos, etc.).

Tras la entrega de los documentos a los Responsables de Tratamiento de cada Centro o unidad organizativa, se evaluarán y aprobarán formalmente con cada Responsable de Tratamiento con el fin de asegurar y verificar el cumplimiento de cada apartado, e informar de las recomendaciones que apliquen para la mejora futura de la seguridad del Centro.

Debe tenerse en cuenta para el informe final de auditoría y para el resto de entregables, los formatos que la CSCM proporcione, o bien acordarse con ésta formatos propios que el contratista pueda proporcionar. Dichos informes serán remitidos a la CSCM y a los Centros y unidades.

El contratista elaborará un informe ejecutivo y específico por Centro y unidad organizativa, así como un informe final con carácter general a partir de los informes detallados de todos los Centros analizados conjuntamente, ambos en el formato y presentación que le sean indicados. El objetivo de estos informes es facilitar la tarea de comparar de forma transversal resultados y medidas correctoras; las especificaciones exactas de este informe se entregarán al contratista al inicio de los trabajos. Se incidirá en las medidas correctoras detectadas y en las líneas de mejoras o complementarias más generales, explicando alcances y plazos futuros. Para las mejoras propuestas, se deberá concretar y motivar el beneficio que se pretende alcanzar con cada mejora.

Será obligatorio que se aplique un tratamiento estadístico a los resultados, elaborando planes cuantificados de mejora, debiendo aportar los documentos con las fuentes a partir de las cuales se hayan obtenido los citados datos. También se entregarán los datos en un formato definido por la DGSD, y del que entregará una plantilla al contratista, compatible con el Cuadro de Mando existente, y que incluirá, al menos los conceptos siguientes:

- Tratamiento, centro, año y tipo de tratamiento.
- Artículo afectado y apartado.
- Grado de incumplimiento, grado de infracción, nota de evaluación.
- Evidencia, medida correctora, observaciones.

Se deberá hacer mención en los datos entregados, a las aplicaciones que se basan en cada uno de los tratamientos y el grado de cumplimiento o nivel de seguridad que alcanzan.

Se efectuará una reunión anual con representantes de la DGSD, o de la OSSI y quien considere oportuno la CSCM, en la que se difundirán los resultados finales ya descritos.

El contratista realizará un plan de trabajo, donde se detalle el procedimiento a seguir durante la ejecución de los trabajos para asegurar la calidad final del servicio ofertado, así como el alineamiento a los objetivos del proyecto y la estrategia marcada por la DGSD.

En el caso de proponer mejoras a la metodología indicada, se deberá concretar y motivar el beneficio que se pretende alcanzar con cada mejora.

Alcance y condiciones de la Auditoria Protección de Datos

El adjudicatario realizará auditorías a un mínimo de 51 centros, organismos y unidades organizativas dependientes de la Consejería de Sanidad que a su vez engloban al menos 430 tratamientos a auditar.

Las auditorías se realizarán de manera que cada dos años queden todos los tratamientos auditados. Fases:

Fase I (CSCM). Una vez hayan sido determinados los centros y unidades cuyos ficheros vayan a ser objeto de auditoría, se llevarán a cabo las siguientes tareas:

- Elaboración de plantillas para entregables.
- Contacto inicial con los centros bajo las premisas concretas que decida la DGSD.

Fase II. El contratista llevará a cabo las auditorías en función de la planificación e información recibidas. Podrá proponer sub-fases dentro de la planificación, dedicadas a los diferentes entornos de la CSCM:

- Atención Hospitalaria
- Atención Primaria
- Servicios Centrales

3.2.2.2. Esquema Nacional de Seguridad (RD 311/2022)

El adjudicatario deberá:

1. Realizar y obtener un informe del estado detallado de los sistemas de información recogidos en el alcance respecto a su estado de cumplimiento del ENS.
2. Elaborar un documento de diagnóstico de situación de cumplimiento del ENS de los sistemas objeto del alcance, que incluya un análisis GAP entre la situación inicial y la objetivo o esperada, así como un análisis de riesgos que demuestre que, tras el

cumplimiento de las medidas definidas de la situación objetivo, se ha alcanzado un nivel de seguridad adecuado y solo se ha obtenido un riesgo residual asumible por el SERMAS.

3. Elaboración de un plan global, de alto nivel, con las acciones de cumplimiento por orden de prioridad (Plan de implantación global) y que esté alineado con las directrices establecidas por la OSSI.
4. A la vista de todas las acciones a abordar, realizar una priorización de las mismas y elaborar un Plan de Implantación detallado que distinga entre acciones transversales y acciones específicas.
5. Realizar el seguimiento del Plan de Implantación:
    a. Asesoramiento y supervisión de Políticas y normativas comunes.
    b. Asesoramiento y supervisión de Políticas y normativas relativas a Servicios de uso común (Servicios horizontales y compartidos).
    c. Elaboración de una hoja de ruta detallada para la implantación de las medidas de seguridad para los Servicios horizontales y compartidos.
    d. Elaboración de una hoja de ruta detallada para la implantación de las medidas de seguridad específicas para cada escenario.
    e. Prestar un servicio de apoyo y orientación que conlleve la implantación y certificación.
6. Seguimiento periódico y ajustes del plan. Ciclos de revisión con frecuencia de, al menos, cada 3 meses.
7. Informe final de auditoría para comprobar el estado de cumplimiento y posibilidad de obtención de certificaciones / declaraciones de conformidad.

Las fases del contrato son:

- Durante la Fase de Implantación, se realizarán las acciones indicadas en los puntos 1 al 4 del epígrafe anterior.
- Durante la Fase de Extensión, se realizarán las acciones indicadas en los puntos 5 y 6 del epígrafe anterior.
- Durante la Fase de Finalización, se realizarán las acciones indicadas en el punto 7 del epígrafe anterior, además de continuar realizándose las indicadas en los puntos 5 y 6.

Alcance y condiciones de las Auditorías de seguridad

A partir de todo el escenario normativo aplicable y descrito en el presente documento, y conjugando las políticas y procedimientos establecidos, se requiere la realización de una auditoria regular ordinaria, que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad.

Se realizará en función de la categoría del sistema, determinado según lo dispuesto en el Anexo I y de acuerdo con lo previsto en el Anexo III.

La adjudicataria hará una propuesta de sistemas de información, con subsistemas, si es necesario, que serán sometidos a la auditoría, con indicación del personal responsable de las mismas, que tendrá que validar la DGSD.

En la realización de la auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocida, así como la normalización nacional e internacional aplicables a este tipo de auditorías. Se indican a continuación las metodologías a seguir:

- CCN-STIC 802 - Guía de Auditoría.
- CCN-STIC 808 - Guía de Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad.
- CCN-STIC 824 - Información del estado de la Seguridad.
- CCN-STIC 805 - Política de Seguridad.
- UNE-ISO/IEC 27001:2007 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005).
- UNE-ISO/IEC 27002:2009 Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.

La auditoría se realizará en los siguientes términos (RD 311/2022 Anexo III):

- Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.
- Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- Documentación de los procedimientos.
- Registro de incidentes.
- Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

- Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

El informe de la auditoría deberá dictaminar sobre:

- El grado de cumplimiento.
- Identificar sus deficiencias.
- Sugerir las posibles medidas correctoras o complementarias necesarias.
- Las recomendaciones que se consideren oportunas.
- Los criterios metodológicos de auditoría utilizados.
- El alcance y el objetivo de la auditoría.
- Los datos, hechos y observaciones en que se basen las conclusiones formuladas.

A nivel de ciclo de vida, como mínimo, se:

- Comunicará y planificará las revisiones, involucrando a todos los stakeholders requeridos.
- Se revisarán todos los procesos y productos de trabajo mediante checklist de revisión de procesos, productos y servicios.
- Se evaluarán las evidencias proporcionadas evitando apreciaciones que no se puedan verificar. Estableciendo oportunidades de mejora, lecciones aprendidas, no conformidades.
- Estableciendo y aplicando un proceso formal de registro y procesamiento de la no conformidad en las revisiones de aseguramiento de calidad.
- Comunicación de resultados.
- Seguimiento del cumplimiento de acciones correctivas que faciliten la mejora continua.
- Facilitar la corrección de las no conformidades detectadas. Seguimiento de las mismas.
- Escalado y difusión de las no conformidades.
- Análisis y retroalimentación (documentación, datos obtenidos, históricos).
- Detección de procesos de mejora.
- Difusión de indicadores generados, niveles y frecuencia.
- Incorporación y mantenimiento en el cuadro de mando.

Las fases del contrato son:

- Durante la Fase de Implantación, se acordarán con la OSSI y su responsable los intervinientes de cada auditoría.
- Durante la Fase de Extensión, se llevará a cabo una auditoría de seguridad al año. Con un informe de auditoría en el que se reflejarán las posibles observaciones, mejoras y no conformidades, debidamente justificadas.
- Durante la Fase de Finalización, se entregarán todos los recursos generados a la DGSD.

3.2.3. Requisitos generales del lote 2

El adjudicatario deberá coordinarse con el adjudicatario del lote 1, con el fin de maximizar el uso de los servicios prestados y directrices estratégicas definidas en el alcance definido por el SERMAS para facilitar el cumplimiento de la normativa de protección de datos y del ENS en aquellos aspectos donde dichos servicios sean de aplicación.

El adjudicatario del lote 2 deberá aportar toda la documentación y justificaciones de los trabajos realizados y sus importes asociados que en el alcance definido por la DGSD requiera en el contexto del Mecanismo Europeo de Recuperación y Resiliencia o cualquier otro marco similar de nivel europeo o nacional.

El adjudicatario deberá maximizar el uso de las herramientas que pone a disposición la DGSD y el CCN para facilitar el cumplimiento del RGPD y la implantación del ENS (INES – con el Asistente de Plan de Adecuación, Asistentes de Implantación y Gestión de la Conformidad de AMPARO, Análisis de Riesgos según la metodología MAGERIT con PILAR, herramientas de configuración segura, etc.), y tendrá acceso a la información del alcance buscado que contiene el sistema de información de la DGSD. A su vez, proveerá los mecanismos necesarios para que dicho sistema de información presente información sobre el cumplimiento del ENS en el alcance definido por la DGSD, lo que puede requerir integraciones con las herramientas del CCN anteriormente citadas o las propias de la DGSD.

La empresa adjudicataria aportará y distribuirá los perfiles diferentes para desarrollar las auditorías de los centros Hospitalarios, Centros de Atención Primaria, u órganos de gestión, de forma que se especialice el conocimiento en las particularidades de cada tipo de centro.

El contratista deberá ser flexible en su horario y calendario con el fin de resolver y agilizar las visitas que se plantean con los Responsables de Tratamiento y/o Seguridad de los Centros. La Comunidad de Madrid no asume ningún tipo de gasto o coste producido por la compensación horaria del personal del adjudicatario, ni de los gastos provocados por la revisión o modificación de las fechas de reunión o planteamiento de nuevos calendarios.

El personal del adjudicatario deberá desplazarse a instalaciones de las entidades en territorio nacional en el caso de que resulte necesario para la realización de los trabajos objeto del lote. Los centros poseen una elevada dispersión geográfica, por lo que la empresa adjudicataria deberá asumir cualquier tipo de gasto producido directa o indirectamente por dicha dispersión (dietas, gastos de desplazamientos, etc.).

La información de las entidades relativa al ENS debe estar relacionada con la información de activos contenida en la CMDB de la DGSD.

Los planes detallados de implantación deben contemplar información con un nivel de detalle suficiente como para permitir a la DGSD abordar la implantación de las medidas de forma inmediata:

- Documento de análisis de la medida a implantar en el contexto de los S.I. concreto.
- Documento de diseño de la medida a implantar.

Dentro del plan de acción se podrán contemplar acciones que faciliten la implantación, como puede ser la elaboración de perfiles específicos, o la adaptación del conjunto de políticas y normativas comunes a grupos de entidades de características similares.
En caso de que se requieran evidencias, datos de sistemas, competencias de Madrid Digital, durante el proceso de auditoría, el adjudicatario deberá seguir el protocolo establecido en Madrid Digital, protocolo que se ha formalizado y publicado internamente dentro de la Agencia que permite recabar todas las autorizaciones formales necesarias del interesado, del responsable de la información, responsable del tratamiento (si procede) y del propio titular de Madrid Digital, para iniciar las actuaciones, establecer el alcance de los trabajos a realizar así como de los activos de la Agencia afectados y salvaguardar toda la confidencialidad necesaria respecto de la información que se pudiera requerir.

4. CARACTERÍSTICAS GENERALES DEL SERVICIO

4.1. Lugar de prestación del servicio

Lote 1 - Oficina de Seguridad de Sistemas de la Información (OSSI)

Por la naturaleza de los trabajos objeto del contrato, el desarrollo de las actividades afectadas al presente pliego técnico se llevará a cabo preferentemente en las instalaciones de la DGSD, sitas en Madrid. Pudiéndose realizar los trabajos en remoto accediendo a los entornos que se precise mediante mecanismos seguros, en caso de que el DGSD así lo requiera. La decisión será comunicada por el DGSD a la empresa adjudicataria con el suficiente tiempo de antelación.
En ambas situaciones, el personal de la adjudicataria deberá tener disponibilidad para la celebración de reuniones de seguimiento del proyecto, así como para procedimientos de toma de datos, validación y pruebas en instalaciones de la DGSD afectados por los resultados del contrato.

Lote 2 - Oficina de Auditoría Interna

Por la naturaleza de los trabajos objeto del contrato, el desarrollo de las actividades afectadas al presente pliego técnico se llevará a cabo preferentemente en remoto, accediendo a los entornos que se precise mediante mecanismos seguros que la DGSD establecerá al efecto, a excepción del responsable/coordinador del lote.

El personal de la adjudicataria deberá tener disponibilidad, tanto en presencial como en remoto, para la celebración de reuniones de seguimiento del proyecto, así como para procedimientos de toma de datos, validación y pruebas en instalaciones de la DGSD afectados por los resultados del contrato.

Habrá un responsable/coordinador del lote que tendrá dedicación exclusiva al servicio, que trabajará de forma presencial en las oficinas de la DGSD o del SERMAS, con posibilidad de teletrabajo con un máximo de 3 días por semana, y en función de las necesidades del servicio.

4.2. Equipamiento del personal de oficina

Los empleados de los adjudicatarios que ejecuten por cuenta de éste trabajos directamente relacionados con el objeto del presente contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por su propia organización, entendiendo como tal ordenador personal, teléfonos móviles, tablets, licencias software ofimático, etc., siguiendo los estándares de la política de seguridad del DGSD.

El adjudicatario debe proveer a su personal de teléfonos móviles o aquel mecanismo que la DGSD estime oportuno para implementar el acceso a los sistemas de la DGSD con múltiple factor de autenticación.

4.3. Horario de prestación de servicio.

Lotes 1 y 2

Se considera horario de servicio a la franja horaria diaria en la que la empresa adjudicataria está en disposición tanto de recibir una comunicación como de acometer la resolución de la misma. La adjudicataria estará obligada a contemplar un horario de servicio mínimo que comprenderá de 8:00 h. a 18:00 h. de lunes a jueves y de 8:00 h. a 15:00 h. los viernes.

La realización del trabajo fuera del horario habitual, en festivos o fines de semana, si los servicios así lo requirieran de forma puntual no tendrá un coste adicional para la DGSD. En caso de ser necesario, esta circunstancia será comunicada con antelación suficiente por parte del responsable de la DGSD. Tampoco supondrá un coste adicional para la DGSD los desplazamientos que tengan lugar para el cumplimiento de los objetivos del presente lote.

5. EQUIPO DE TRABAJO Y CUALIFICACIÓN

5.1. Organización general

Los servicios descritos en los apartados anteriores para cada uno de los lotes deberán ser prestados por un equipo mínimo organizado como se describe en este punto.

Todo el personal propuesto en el equipo base presentado deberá tener dedicación exclusiva del 100% a este contrato, excepto el Responsable/Coordinador del lote 1 que tendrá una dedicación en torno al 50 %. No se considerarán, para la estimación de recursos mínimos exigidos, la participación de personal con servicio parcial o dedicación compartida con otras responsabilidades.

El equipo de trabajo ofertado por cada lote se incorporará tras la formalización del contrato para la ejecución de los trabajos, y deberá estar formado por los componentes relacionados en la oferta de cada uno de los contratistas adjudicatarios. Los cambios de composición del equipo deberán estar correctamente justificados, con la explicación que suscita el cambio y deberán ser aprobados por la DGSD.

Los adjudicatarios deben facilitar la relación nominal de personas que conforman el equipo de trabajo especificando los roles que desempeñaran en la prestación del servicio. Durante la ejecución del contrato deberá mantener dicha relación actualizada.

Dada la criticidad del servicio y con el fin de garantizar su continuidad respecto a la situación actual, el contratista adjudicatario deberá asegurar que asigna los recursos con la suficiente experiencia y conocimiento de los entornos funcionales y tecnológicos objeto de este contrato, especialmente en la fase de planificación.

La gestión de la carga de trabajo durante las épocas vacacionales será la misma que para el resto del periodo del contrato y estará sujeta a la planificación acordada con la DGSD. Los contratistas adjudicatarios deberán garantizar la disponibilidad de los recursos con los conocimientos requeridos para cumplir con dicha planificación, así como con los niveles de servicio establecidos. No podrán reducir unilateralmente la carga de trabajo durante las épocas vacacionales.

5.2. Equipos de prestación de los servicios y requisitos de cualificación y experiencia para los perfiles profesionales

5.2.1. Equipo del lote 1: Oficina de Seguridad de los Sistemas de Información (OSSI)

El equipo mínimo para la prestación del servicio estará compuesto por **19 personas con dedicación exclusiva al servicio**, que será prestado de forma presencial, con posibilidad de teletrabajo con un máximo de 3 días por semana, y en función de las necesidades del servicio.

Para la correcta consecución de los trabajos, el adjudicatario del presente lote deberá al menos incorporar en el servicio los siguientes perfiles:

- 1 Responsable/Coordinador del lote
- 2 Auditor/Consultor de seguridad senior
- 3 Auditor/Consultor legal senior
- 4 Consultor legal junior
- 3 Auditor/Consultor TIC
- 2 Analista de seguridad senior
- 2 Ingeniero de seguridad senior
- 1 Arquitecto de seguridad
- 1 Documentalista/Administrativo

A continuación, se detallan los requisitos de experiencia de cada perfil:

Responsable/Coordinador del lote

Áreas de conocimiento:

- Coordinación de equipos de trabajo, planificación, seguimiento y control de actividades y Acuerdos de Nivel de Servicio.
- Gestión de proveedores de servicios de ciberseguridad.
- Cumplimiento de leyes y normas de ciberseguridad, privacidad, conservación de información etc. aplicables.
- Diseño y mejora de procesos, aplicación de modelos de madurez.
- Gestión de relaciones con clientes y proveedores.

Titulación requerida:

- Grado, licenciado o ingeniero o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima requerida.

Certificaciones (al menos 1):

- Project Management Professional (PMP) de PMI

- Risk Management Professional (RMP) de PMI
- Certified in the Governance of Enterprise IT (CGEIT) de ISACA
- Certified Information Security Manager (CISM) de ISACA
- Information Systems Security Management Professional (ISSMP) de ISC2
- Certificaciones ITIL v4 Management, Professional v3 Expert o superiores.

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 8 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.
- Eperiencia de al menos 6 años trabajando en el entorno de la salud.

Auditor/Consultor de seguridad senior

Áreas de conocimiento:

- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Implantación de Esquema Nacional de Seguridad y guías STIC
- Implantación de Ley PIC (elaboración de PSO, PPE, PAO)
- Diseño e implantación de Sistemas de Gestión de Seguridad de la Información.
- Realización de análisis de riesgos de sistemas de información según ENS.
- Realización de análisis de riesgos de sistemas de información según Normativa de protección de datos, LOPD, Reglamento General de Protección de Datos, etc.
- Propuesta de soluciones y mejoras en materia de seguridad de la información.
- Análisis y gestión de riesgos convergente y uso de herramienta PILAR
- Metodología MAGERIT, MOSLER, FINE…
- Sistemas de gestión de continuidad del negocio.

Titulación requerida:

- Grado, licenciado o ingeniero o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- Certified Information Systems Auditor (CISA) de ISACA
- Certified in Risk and Information Systems Control (CRISC) de ISACA
- Certified Data Privacy Solutions Engineer (CDPSE) de ISACA

- Certified Information Systems Security Professional (CISSP) de ISC2
- Information Systems Security Management Professional (ISSMP) de ISC2
- Security Assessment and Authorization Certification (CAP) de ISC2
- Certified Chief Information Security Officer (CCISO) de ECCouncil
- Cisco Certified Networking Associate (CCNA) de CISCO

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 5 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Auditor/Consultor TIC

Áreas de conocimiento:

- Amplio conocimiento metodológico en normativas y legislación de seguridad (GDPR, ENS, ISO 27001, ISO 22301, Ley PIC).
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Auditoría de sistemas TIC.
- Auditoría de sistemas de gestión de costes operativos, medida de actividad, facturación o similares.
- Análisis y evaluación de procesos y metodologías.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de derecho, ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- Certificación profesional Certified Information Systems Auditor (CISA) de ISACA
- Certified Information Security Manager (CISM) de ISACA
- Certified Information Systems Security Professional (CISSP) de ISC2

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 4 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Analista de seguridad senior

Áreas de conocimiento:

- Experto en análisis de eventos de seguridad y sistemas de correlación de logs, SIEMs, herramientas de detección de anomalías, etc.
- Experto en la gestión de incidentes de ciberseguridad.
    - Detección y respuesta a ciberincidentes.
    - Contención de ciberincidentes.
    - Coordinación de gabinete de crisis.
- Experto en análisis forense y recolección de evidencias:
    - Sistemas Linux y Windows.
    - Servidores web y de aplicaciones.
    - Servidores de BBDD.
    - Equipos de Comunicaciones.
    - Sistemas de seguridad.
- Experto en tareas de "Threat Hunting", análisis y revisión proactiva de logs, detección de anomalías, potenciales vulnerabilidades de los sistemas TIC, etc., orientados a la detección proactiva de intrusiones en fases preliminares o de amenazas persistentes avanzadas (APTs).
- Experto en tareas de vigilancia digital, inteligencia de fuentes abiertas, detección de amenazas y posibles riesgos a partir del análisis de información pública y restringida de ciberseguridad.
- Capacitación y concienciación, elaboración de itinerarios de formación, material de formación e impartición de cursos en materia de ciberseguridad.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- GIAC Certified Incident Handler (GCIH) de SANS
- GIAC Certified Forensics Examiner (GCFE) de SANS
- GIAC Certified Forensics Analyst (GCFA) de SANS

- GIAC Network Forensics Analyst (GNFA) de SANS
- GIAC Certified Intrusion Analyst (GCIA) de SANS
- GIAC Cyber Threat Intelligence (GCTI) de SANS
- Certified Threat Intelligence Analyst (CTIA) de ECCouncil
- Certified Incident Handler de ECCouncil
- Computer Hacking Forensics Investigator de ECCouncil
- Certified COCS Analyst (CSA) de ECCouncil
- Cisco Certified Networking Associate (CCNA) de CISCO

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 4 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Ingeniero de seguridad senior

Áreas de conocimiento:

- Experto en instalación, configuración y mantenimiento de herramientas de ciberseguridad:
  - Análisis automático de vulnerabilidades.
  - Análisis automático de seguridad de código fuente.
  - Gestión y correlación de logs, SIEMs, sistemas de "Threat Hunting".
  - Antivirus, EDR.
  - Herramientas de análisis forense, obtención y conservación de evidencias.
- Experto en instalación, configuración y mantenimiento de sistemas de ciberseguridad:
  - Firewalls
  - WAF
  - IDS
  - IPS
- Experto en análisis y diseño de arquitecturas de ciberseguridad, selección de fuentes de eventos, evolución y rediseño de arquitecturas de seguridad.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- GIAC Certified Incident Handler (GCIH) de SANS
- GIAC Certified Forensics Examiner (GCFE) de SANS
- GIAC Certified Forensics Analyst (GCFA) de SANS
- GIAC Network Forensics Analyst (GNFA) de SANS
- GIAC Certified Intrusion Analyst (GCIA) de SANS
- GIAC Cyber Threat Intelligence (GCTI) de SANS
- Certified Threat Intelligence Analyst (CTIA) de ECCouncil
- Certified Incident Handler de ECCouncil
- Computer Hacking Forensics Investigator de ECCouncil
- Certified COCS Analyst (CSA) de ECCouncil
- Cisco Certified Networking Associate (CCNA) de CISCO

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 5 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Arquitecto de seguridad

Áreas de conocimiento:

- Experto en integración, instalación, configuración y mantenimiento de soluciones de ciberseguridad:
  - Análisis automático de vulnerabilidades
  - Análisis automático de seguridad de código fuente
  - Gestión y correlación de logs, SIEMs, sistemas de "Threat Hunting"
  - Antivirus, EDR, Firewalls, WAF, IDS, IPS…
- Experto en análisis, diseño e implantación de arquitecturas de ciberseguridad, selección de fuentes de eventos, evolución y rediseño de arquitecturas de seguridad.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- GIAC Certified Incident Handler (GCIH) de SANS
- GIAC Certified Forensics Examiner (GCFE) de SANS
- GIAC Certified Forensics Analyst (GCFA) de SANS
- GIAC Network Forensics Analyst (GNFA) de SANS
- GIAC Certified Intrusion Analyst (GCIA) de SANS
- GIAC Cyber Threat Intelligence (GCTI) de SANS
- Certified Threat Intelligence Analyst (CTIA) de ECCouncil
- Certified Incident Handler de ECCouncil
- Computer Hacking Forensics Investigator de ECCouncil
- Certified COCS Analyst (CSA) de ECCouncil
- Cisco Certified Networking Associate (CCNA) de CISCO

Experiencia profesional mínima:

- Más de 5 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Auditor/Consultor legal senior

Áreas de conocimiento:

- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Implantación de Esquema Nacional de Seguridad y guías STIC.
- Diseño e implantación de Sistemas de Gestión de Seguridad de la Información.
- Realización de análisis de riesgos de sistemas de información según ENS.
- Realización de análisis de riesgos de sistemas de información según Normativa de protección de datos, LOPD, Reglamento General de Protección de Datos, etc.
- Propuesta de soluciones y mejoras en materia de seguridad y privacidad de la información.
- Análisis y gestión de riesgos convergente y uso de herramienta PILAR.
- Metodología MAGERIT, MOSLER, FINE…
- Sistemas de gestión de continuidad del negocio.
- Conocimientos en la protección de datos específica del entorno sanitario.

Titulación requerida:

- Titulación mínima universitaria MECES Nivel 2 o 3 en Derecho.
- Estudios de postgrado en Derecho de las Tecnologías o similar.

Experiencia profesional mínima:

- 5 años como especialistas en ámbito de asesoría legal en protección de datos.
- Al menos 3 años de experiencia en proyectos de seguridad de las tecnologías de la información.
- Acreditación al menos, de 3 años de experiencia en el sector público sanitario.

Auditor/Consultor legal junior

Áreas de conocimiento:

- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Implantación de Esquema Nacional de Seguridad y guías STIC.
- Implantación de Ley PIC (elaboración de PSO, PPE, PAO).
- Diseño e implantación de Sistemas de Gestión de Seguridad de la Información.
- Realización de análisis de riesgos de sistemas de información según ENS.
- Realización de análisis de riesgos de sistemas de información según Normativa de protección de datos, LOPD, Reglamento General de Protección de Datos, etc.
- Propuesta de soluciones y mejoras en materia de seguridad y privacidad de la información.
- Análisis y gestión de riesgos convergente y uso de herramienta PILAR.
- Metodología MAGERIT, MOSLER, FINE…
- Sistemas de gestión de continuidad del negocio.

Titulación requerida:

- Titulación mínima universitaria MECES Nivel 2 o 3 en Derecho.
- Estudios de postgrado en Derecho de las Tecnologías o similar.

Experiencia profesional mínima:

- 2 años como especialistas en ámbito de asesoría legal en protección de datos.
- Al menos 1 año de experiencia en proyectos de seguridad de las tecnologías de la información.

Documentalista/Administrativo

- Grado universitario (MECES 2).
- Experiencia en Gestión Documental.
- Conocimiento de Gestores Documentales.
- Experiencia en herramientas office.

- Experiencia mínima de 2 años en entornos TIC.

El equipo de trabajo, en su conjunto, debe reunir conocimientos en las siguientes materias:

- En relación a las actuaciones derivadas de la aplicación del Esquema Nacional de Seguridad, aplicación de los fundamentos para la determinación de la categoría de un sistema, así como de la selección y aplicación de medidas de seguridad, de acuerdo a lo que establece el ENS.
- Certificación de Delegado de Protección de Datos, según el esquema de la Agencia de Protección de Datos.
- Metodologías para el análisis de riesgos en el ámbito de la Seguridad de la Información y de las TIC.
- Herramientas de apoyo al análisis de riesgos (herramienta PILAR de la Administración Pública o equivalente).
- Familia de normas ISO/IEC 27000, para la Gestión de la Seguridad de la Información y las buenas prácticas en la materia, así como los específicos para el ámbito de la Sanidad que puedan publicarse.
- Realización de auditorías técnicas, basadas en los estándares al respecto, como la ISO 17021 y la ISO 27015.
- Familia de normas ISO/IEC 22301, para la Gestión de la Continuidad de Negocio.
- Tecnologías y soluciones de firma electrónica.
- Conocimientos generales en materia de Derecho aplicado a las TIC.
- Normativa para la protección de infraestructuras críticas.
- Conocimientos avanzados sobre la seguridad y protección de datos en el ámbito sanitario.
- Conocimientos avanzados en inglés técnico y legal, tanto hablado como escrito.

5.2.2. Equipo del lote 2: Oficina de Auditoría Interna

El equipo mínimo para la prestación del servicio estará compuesto por 6 personas con dedicación exclusiva al servicio.

Para la correcta consecución de los trabajos, el adjudicatario del presente lote deberá al menos incorporar en el servicio los siguientes perfiles:

- 1 Responsable/Coordinador del lote
- 2 Auditor/Consultor de Seguridad
- 1 Auditor/Consultor TIC

- 2 Auditor/Consultor GRC Protección de datos

A continuación, se detallan los requisitos de experiencia de cada perfil:

Responsable/Coordinador del lote

Tendrá dedicación exclusiva al servicio, que será prestado de forma presencial en las oficinas de la DGSD, con posibilidad de teletrabajo con un máximo de 3 días por semana, y siempre en función de las necesidades del servicio.

Áreas de conocimiento:

- Coordinación de equipos de trabajo, planificación, seguimiento y control de actividades y Acuerdos de Nivel de Servicio.
- Gestión de proveedores de servicios de ciberseguridad
- Cumplimiento de leyes y normas de ciberseguridad, privacidad, conservación de información etc. aplicables.
- Diseño y mejora de procesos, aplicación de modelos de madurez.
- Gestión de relaciones con clientes y proveedores.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima requerida.

Certificaciones (al menos 2):

- Project Management Professional (PMP) de PMI.
- Risk Management Professional (RMP) de PMI.
- Certified in the Governance of Enterprise IT (CGEIT) de ISACA.
- Certified Information Security Manager (CISM) de ISACA.
- Information Systems Security Management Professional (ISSMP) de ISC2.
- Certificaciones ITIL v4 Management, Professional v3 Expert o superiores.

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 8 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Auditor/Consultor de Seguridad

Áreas de conocimiento:

- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Implantación de Esquema Nacional de Seguridad y guías STIC.
- Diseño e implantación de Sistemas de Gestión de Seguridad de la Información, ISO 27000.
- Realización de análisis de riesgos de sistemas de información según ENS.
- Realización de análisis de riesgos de sistemas de información según Normativa de protección de datos, LOPD, Reglamento General de Protección de Datos, etc.
- Propuesta de soluciones y mejoras en materia de seguridad de la información.
- Análisis y gestión de riesgos, herramienta PILAR.
- Metodología MAGERIT.
- Sistemas de gestión de continuidad del negocio ISO 22301.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima requerida.

Certificaciones (al menos 1):

- Certified Information Systems Auditor (CISA) de ISACA
- Certified in Risk and Information Systems Control (CRISC) de ISACA
- Certified Data Privacy Solutions Engineer (CDPSE) de ISACA
- Certified Information Systems Security Professional (CISSP) de ISC2
- Information Systems Security Management Professional (ISSMP) de ISC2
- Security Assessment and Authorization Certification (CAP) de ISC2
- Certified Chief Information Security Officer (CCISO) de ECCouncil

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 4 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Auditor/Consultor TIC

Áreas de conocimiento:

- Amplio conocimiento metodológico en normativas y legislación de seguridad (ISO 27001, ENS, NIST).
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Auditoría de sistemas TIC.
- Auditoría de sistemas de gestión de costes operativos, medida de actividad, facturación o similares.
- Análisis y evaluación de procesos y metodologías.

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima Requerida.

Certificaciones (al menos 1):

- Certificación profesional Certified Information Systems Auditor (CISA) de ISACA
- Certified Information Security Manager (CISM) de ISACA
- Certified Information Systems Security Professional (CISSP) de ISC2

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 4 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

Auditor/Consultor GRC Protección de datos

Áreas de conocimiento:

- Amplio conocimiento metodológico en normativas y legislación de seguridad.
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de protección de datos.
- Auditoria de protección de datos y respaldo a las diferentes Unidades.
- Análisis y evaluación de procesos y metodologías relativas a GRC, normativas de protección de datos.
- Soporte y respaldo a los diferentes perfiles (responsable del tratamiento, delegado...).

Titulación requerida:

- Grado, licenciado o ingeniero superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o telecomunicaciones.

  Alternativa: Ciclo Formativo de Grado Superior o equivalente, siempre y cuando se acrediten 24 meses de experiencia adicional a la solicitada en la Experiencia Profesional Mínima requerida.

Certificaciones (al menos 1):

- Certificación profesional Certified Information Systems Auditor (CISA) de ISACA
- Certified Information Security Manager (CISM) de ISACA
- Certified Information Systems Security Professional (CISSP) de ISC2
- Certificaciones de legislación de protección de datos, Compliance, grc.

Experiencia profesional mínima:

- Para cada recurso asociado al perfil, más de 4 años de experiencia en los puntos recogidos en el apartado correspondiente a áreas de conocimiento del presente lote.

5.3. Modificaciones en la constitución del equipo de prestación del servicio

La incorporación o sustitución de personas en los equipos de cualquiera de los lotes, deberá mantener los requisitos establecidos como mínimos para cada perfil. La DGSD podrá solicitar el cambio de cualquiera de los componentes del equipo, con un preaviso de un mes, por otro de igual categoría, si existen razones justificadas que lo aconsejen.

Si es el contratista adjudicatario el que propone el cambio de una de las personas del equipo mínimo (rotación planificada) deberá solicitarlo con al menos quince días de antelación, acompañándose de un solapamiento del recurso saliente con el entrante para la adecuada transferencia de conocimiento durante al menos 15 días y cumplir los siguientes requisitos:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de posibles candidatos para un perfil cuya cualificación técnica sea igual o superior al de la persona que se pretende sustituir.
- Aceptación por la DGSD de los candidatos propuestos.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones en los componentes del equipo, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario.

El contratista adjudicatario deberá asegurar en todo caso la transferencia de conocimiento del recurso sustituido hacia el equipo de trabajo.

5.4. Capacitación del equipo del contrato

La adjudicataria se compromete a mantener formado al personal por él asignado a los servicios y proyectos objeto de esta licitación durante toda la vida del contrato, con el fin de mantener un equipo de servicio con los conocimientos plenamente actualizados y alineados con los servicios a los que específicamente se oriente.

6. PLANIFICACIÓN

Las empresas adjudicatarias proporcionarán a la DGSD una gestión integral de los servicios detallados en el PPT, configurados de acuerdo al mismo. Para la prestación de los servicios objeto del presente contrato, se han definido las siguientes fases para la ejecución, aplicables de manera independiente a cada lote:

Fase de planificación o arranque: Se inicia con la entrada en vigor del contrato y tiene un plazo estimado de un mes en los cuales se realizarán los preparativos para la **prestación de los servicios**. Durante esta fase la empresa adjudicataria del lote 1 no podrá cobrar por sus servicios.

Fase de prestación de los servicios: Se inicia con el comienzo de los trabajos de consultoría y ejecución de las empresas adjudicatarias, tras el periodo de la fase de planificación.

Fase de devolución: Un mes antes de la terminación del contrato, se inicia la fase de devolución. En esta fase se realizarán los trabajos necesarios para la transición del servicio a la DGSD o a otra empresa proveedora de servicios, además de realizar la prestación de los servicios del mismo modo que durante la fase de prestación de servicios.

Para cada fase del contrato las empresas adjudicatarias deberán definir un plan asociado que describa los procedimientos propuestos para su consecución exitosa, alineados con los procesos existentes o planteados por la DGSD. Las empresas adjudicatarias tendrán que definir la gestión de las fases con recursos dedicados, las reuniones, la documentación y todo aquello que la DGSD considere oportuno para la gestión de las fases de forma independiente y coordinada.

La implantación de los servicios se gestionará con metodología de gestión de porfolio y proyectos tecnológicos basada en las principales metodologías: PMI, SCRUM e ITIL.

La gestión integral de los servicios ofertados, en sus aspectos técnicos y de facturación, es un factor determinante a la hora de obtener un rendimiento óptimo y mantener un control de la ejecución de unos servicios como los solicitados por la DGSD en esta licitación. Por ello la

empresa adjudicataria asegurará que el modelo de gestión propuesto cumple los requisitos de gestión establecidos en este PPT.

6.1. Fase de planificación

En el caso de servicios que se prestan total o parcialmente actualmente, se realizará el traspaso de los elementos básicos e imprescindibles para la prestación del servicio, entre los prestadores que viniera suministrando los servicios, en el periodo anterior a la entrada en vigor del presente contrato y los contratistas adjudicatarios. Para ello, el contratista deberá realizar, entre sus primeras tareas, las relacionadas con la adquisición de conocimiento y las de formación que considere necesaria.

Esa transferencia de conocimientos será responsabilidad de los contratistas adjudicatarios. Por parte de la DGSD se supervisarán los procesos de transferencia, con el objetivo de la máxima colaboración de las partes durante todo el proceso.

Esta fase se iniciará con la celebración de una sesión de lanzamiento (kick-off), cuya preparación será responsabilidad de la empresa adjudicataria con la información necesaria para la realización de los servicios.

Las empresas adjudicatarias deberán elaborar en esta fase un **Plan de Prestación del Servicio**, que contendrá las tareas y trabajos necesarios para la adecuada ejecución de los servicios a prestar, a partir de la fecha de entrada en vigor del contrato. Corresponderá al DGSD la supervisión y validación de las propuestas para la ejecución de los trabajos, y la posterior aceptación de los trabajos realizados. Se establece que un máximo para esta fase de un mes.

El Plan de Prestación del Servicio incluirá un calendario de los trabajos a realizar. Deberá contemplar la totalidad de los servicios a entregar al inicio de la prestación de los servicios y describirá cómo se llevarán a cabo. De este modo el plan recogerá los procesos, procedimientos, actividades y responsabilidades encaminadas a asegurar el correcto y continuo funcionamiento de todos los servicios demandados.

La adjudicataria deberá definir un completo **Plan de Riesgos** asociado a las actividades de prestación de servicios, donde deberán quedar claramente reseñados los riesgos, amenazas y mitigaciones que propone.

Las empresas adjudicatarias deberán ajustarse a los procesos que proponga a la DGSD pudiendo esta proponer o presentar procesos o mejoras a los existentes en la fase de lanzamiento, para su aprobación por parte de la DGSD.

Asimismo, la DGSD definirá unos flujos de trabajo iniciales basados en tareas, hitos y puntos de control. Estos flujos se definirán al principio del proyecto y contendrán las tareas a realizar por las empresas adjudicatarias. Si la DGSD considerase necesario algún cambio en estos flujos, estos podrán revisarse a lo largo de la vigencia del contrato.

El Plan de Prestación del Servicio contendrá, al menos, los siguientes apartados: Lanzamiento del proyecto, equipo de trabajo, tareas a ejecutar, responsables, planificación y coordinación, y por último aceptación con los mecanismos y procedimientos requeridos por la DGSD. También deberá especificar la documentación y entregables a suministrar durante la prestación del contrato.

El plan deberá tener en cuenta diferentes requisitos que serán definidos por parte de la DGSD:

- El proceso de generación, aprobación y actualización de soluciones técnicas.
- El proceso de aceptación de los servicios prestados.
- El proceso de entrega de documentación.
- Puntos de control de servicios para realizar el seguimiento de su prestación.
- El cumplimiento de ANS de acuerdo a las condiciones establecidas en el apartado 13. ACUERDOS DE NIVEL DE SERVICIO.
- Descripción de los medios materiales y humanos puestos a disposición del contrato, incluyendo el detalle de las personas de la adjudicataria que participarán en el contrato y las responsabilidades que asumirán.

Para la gestión durante esta fase las empresas adjudicatarias asignarán un Coordinador de Ejecución del Contrato para la correcta gestión y comunicación con la DGSD. El coordinador de ejecución del contrato designado será el interlocutor único con la DGSD, siendo el responsable de realizar y gestionar el **Plan de Prestación del Servicio**, debiendo gestionar la entrega de documentación, los plazos acordados y la calidad de los procesos y entregables, es decir, cuidando de cumplir los procesos de seguimiento y aceptación definidos por parte de la DGSD.

La empresa adjudicataria de cada lote, a través de un proceso de colaboración permanente y obligatoria con la DGSD, el CGSI y con las empresas adjudicatarias de los otros lotes, deberá sincronizar acciones para la búsqueda de una mejora global el proceso de despliegue de los servicios.

Se establecerán reuniones periódicas de seguimiento de los proyectos de implantación entre la empresa adjudicataria de cada lote y los representantes designados por la DGSD y el CGSI. La periodicidad de estas reuniones será establecida por la DGSD en el arranque del proyecto, pudiendo ser modificada su frecuencia a lo largo del periodo adjudicado si así se requiriese.

6.2. Fase de prestación de los servicios

La fase de prestación del servicio comenzará tras el cumplimiento de la fase de planificación y durará desde ese momento hasta la finalización del contrato.

En esta fase de desarrollarán los servicios para cada uno de los lotes, de acuerdo al detalle establecido en el apartado **3. Descripción de los Servicios**. Así en el marco de esta fase, se desarrollarán, de forma general las siguientes actuaciones de coordinación:

- Coordinación de todos los actores para la necesaria sincronización de los requisitos técnicos resultantes ofertados y validados, así como de las actividades y tareas del proceso de prestación de los servicios.
- Planificación global y específica de cada servicio.
- Validación de las planificaciones por parte de la DGSD.
- Documentación, según se establezca, de cada una de las planificaciones.

En esta fase las empresas adjudicatarias de los lotes deberán mantener actualizado un **Plan de Mejora** que presentará propuestas para evolucionar y mejorar el servicio durante el periodo de ejecución del contrato y un periodo posterior a su finalización, de acuerdo a las condiciones establecidas en el presente PPT.

Las empresas adjudicatarias deberán trabajar en base a una metodología de mejora iterativa de los servicios la cual debe recoger y aplicar de forma precisa los requerimientos relativos a la gestión del conocimiento, la gestión de riesgos, evolución del servicio y aseguramiento de la calidad, descritos de forma específica para cada lote en el apartado **3. Descripción de los Servicios**.

Si durante el período de vigencia del contrato se introdujesen en el mercado nuevas funcionalidades tecnológicas o normativas solicitadas que impliquen, a juicio de la DGSD, una mejora en las funcionalidades del servicio inicialmente contratado, la DGSD se reserva la decisión de introducir dicho alcance, previo acuerdo con la empresa adjudicataria y en base a la oferta económica aportada.

En cualquier caso, a la finalización del contrato todos los entregables (aportados por parte de la empresa adjudicataria y que pasan a ser propiedad de la DGSD) deberán quedar actualizados a la última versión liberada.

6.3. Fase de devolución del servicio

Se definirá un Plan de Devolución del servicio que comenzará un mes antes de la finalización del contrato. La empresa adjudicataria deberá facilitar el cambio de prestador de servicios realizando las actividades necesarias acordadas con la DGSD. Su objetivo es garantizar la transferencia del conocimiento adquirido o generado durante la prestación del servicio por parte de la empresa adjudicataria hacia la DGSD, o hacia la tercera parte que la DGSD, designe, sin que ello repercuta en una pérdida del control o del nivel de calidad del servicio.

Durante esta fase, la prestación del servicio sigue siendo responsabilidad de la empresa adjudicataria, por lo que las actividades se desarrollarán teniendo en cuenta la prioridad del servicio sobre cualquier otra circunstancia. Durante esta fase, la DGSD, reducirá el número de cambios y nuevas iniciativas al mínimo posible, para reducir la complejidad de la gestión del servicio, en estas circunstancias.

En caso de cese o finalización de contrato, la empresa adjudicataria estará obligada a devolver el control de los servicios objeto del contrato, simultaneándose los trabajos de devolución con los de prestación del servicio, sin coste adicional.

La empresa adjudicataria elaborará los procedimientos de transferencia a aplicar dentro del Plan de Devolución, con el fin de que en dicha transferencia se minimice el impacto en la continuidad y calidad de los servicios y facilite la transición a la DGSD.

Al inicio de la fase de devolución del servicio, la empresa adjudicataria hará una evaluación y planificación de todas las actividades necesarias, que plasmará en el plan de devolución. Dicho Plan se realizará en un plazo máximo de 15 días naturales desde la notificación del inicio de esta fase. El plan deberá contener, como mínimo:

- Metodología de traspaso de conocimiento de los aspectos fundamentales de los servicios.
- Formación y documentación sobre los servicios prestados, dirigida a personal de la DGSD, o terceras partes que esta designe.
- Mecanismos de traspaso de programas e información utilizados para la provisión del servicio y que quedarán en propiedad de la DGSD, en los términos que establezca el contrato.

La empresa adjudicataria trasladará a la DGSD,, o a una tercera que esta establezca, la lista de servicios que formen parte del backlog en ese momento, así como una versión actualizada de toda la documentación e información manejada para la prestación del servicio, antes de la finalización del contrato.

El cumplimiento del hito de devolución del servicio deberá quedar formalmente documentado mediante actas y deberá ser aceptado tanto por parte de la empresa adjudicataria, como por parte de la DGSD.

7. MODELO DE RELACIÓN

El modelo de relación tiene como objetivo asegurar la coordinación e integración eficiente de los proveedores asignatarios de los Lotes con las diferentes áreas de la organización en la DGSD. El Modelo de Relación debe cubrir todos los niveles de información y decisión, desde el nivel operativo hasta el estratégico, facilitando la toma de decisiones, el seguimiento de los objetivos globales y la resolución de potenciales conflictos. Por otra parte, el Modelo de Relación deberá garantizar la flexibilidad y la adaptación del servicio a la evolución de la organización, pudiendo cambiar durante la vigencia del contrato, en particular ante eventuales reorganizaciones.

El Modelo de Relación constará principalmente de:

- Una estructura de comités que sirva como principal elemento de decisión y seguimiento del contrato y de los servicios prestados por los contratistas adjudicatarios.
- La definición de unos interlocutores de ámbito de actividad que actuarán de interlocutores en la relación por ambas partes, tanto a nivel de comité, como en la línea operativa de coordinación diaria.
- Un modelo de trabajo general, con las fronteras e interacciones claramente delimitadas a nivel de actividad y esquematizada hacia cada una de las áreas de la DGSD que interviene en cualquier lugar del ciclo de vida de las aplicaciones.

Será necesario, una vez adjudicados los contratos, que cada una de las contratistas adjudicatarios redacte un Modelo de Relación que cubra todo el ámbito de este contrato, así como la relación con el resto de las unidades de la DGSD. Este Modelo estará supervisado y validado por la Dirección de la organización y será elaborado por los contratistas adjudicatarios en la etapa de arranque y transición. En el caso de conflictos en la definición del Modelo, el Lote 1 junto a la DGSD establecerá el modelo definitivo a seguir por todos los lotes.

El Comité Director, será el órgano de consulta, supervisión y control que ponga en valor la misión y visión de los servicios y actuará en todas las fases del ciclo de vida. Estará compuesto por responsables del servicio, tanto de la DGSD, o quienes la DGSD delegue/invite, así como los/as directores/as del servicio de la empresa adjudicataria del Lote 1. Además, podrán hacer partícipes al resto de lotes si fuese de interés. Este comité mantendrá una periodicidad mensual. Entre sus funciones se contemplará:

- Alineamiento de la estrategia del servicio de seguridad con las necesidades planteadas, estableciendo la relación e interlocución con los correspondientes responsables.

- Supervisión de la capacidad del servicio para absorber la demanda requerida, gestionando los riesgos de capacidad.
- Supervisión y reporte de la ejecución del gasto y la optimización de los recursos destinados.
- Promoción de la mejora continua, estimulando acciones asociadas a la mitigación de riesgos.
- Supervisión de la gestión del porfolio de iniciativas y proyectos, y la validez de la viabilidad de las iniciativas aliándolas a los resultados esperados de la estrategia de la OSSI.

Los Comités Operativos, se estructuran en base al conjunto de comités necesarios para el adecuado desarrollo del servicio. Estarán compuestos por un grupo de personas mixtas tanto del DGSD, o quienes DGSD delegue/invite, como de las empresas adjudicatarias de los servicios, según proceda. La periodicidad de estos comités se establecerá de acuerdo con las necesidades del servicio. Aunque se establece al menos, un comité de seguimiento, con carácter bimensual donde la adjudicataria será la responsable de su organización, estructura y contenido en base a los requerimientos del DGSD. Estos equipos se sustentarán en el refuerzo de sinergias entre las partes, donde la toma de decisiones se acordará y tratará de manera colegiada, en la medida de lo posible, para ofrecer un servicio de calidad.

7.1. Áreas de la DGSD implicadas en el servicio del contrato

Centro de Soporte a Usuarios

El Centro de Soporte a usuarios (CESUS), es el interlocutor con el que contactarán los usuarios de la CSCM ante problemas o incidencias o peticiones que puedan surgir en relación con dichos servicios.

Se encarga de:

- Registrar en primera instancia la apertura y cierre de incidencias y solicitudes en el ámbito de los portales y servicios para los profesionales y ciudadanos.
- Registrar la solicitud de sitios, páginas y otras estructuras.
- Registrar la solicitud de permisos para espacios colaborativos.

Centro de Datos, Administración y Soporte

El Centro de Datos, Administración y Soporte (CEDAS) es el encargado de la gestión, operación y explotación de los Centros de Procesos de datos (CPD's), en los que están

instaladas las plataformas de gestión de contenidos y servicios actualmente operativas y se instalarán las nuevas implementaciones.

Por la criticidad de los sistemas en producción y su buen funcionamiento, será necesaria una labor de colaboración entre el servicio objeto del presente contrato y CEDAS en los aspectos relativos a la producción y explotación de los sistemas.

Además, todos los nuevos servicios deberán tener una validación expresa de este grupo en cuanto a la definición técnica propuesta para su implementación.

También será precisa una coordinación para establecer los pasos a producción en función de capacidades, disponibilidad y prioridades.

Servicio de Arquitectura y Normalización

Se encarga de fijar los criterios tecnológicos y proporcionar la información y asesoría necesarias para que los proveedores de servicios de implementación, mantenimiento e implantación de sistemas de información se ajusten a los estándares y políticas definidos por la DGSD en materia de arquitectura e integración.

En caso de que se requiera, las propuestas de diseño de arquitectura y de estándares que se realicen en el marco de este contrato deberán ser supervisadas y aprobadas por este servicio.

Otras áreas implicadas no dependientes de la DGSD directamente son:

Centro de Atención Personalizada

Como canal de comunicación con el ciudadano para servicios de cita previa e información de algunos servicios electrónicos.

Agencia para la Administración Digital de la Comunidad de Madrid

La Agencia para la Administración Digital de la CM, en adelante Madrid Digital, es un actor relevante y parte TIC y de ciberseguridad de la Consejería de Digitalización, de la Consejería de Sanidad y del propio SERMAS. Las funciones y competencias de Madrid Digital, en el ámbito sanitario, incluyen comunicaciones de voz y datos y el puesto de trabajo, y por añadido la ciberseguridad en esos ámbitos. Sobre las comunicaciones transita la información de los sistemas de información médica y gestión sanitaria, y en el puesto de trabajo se consulta, opera y procesa parte de esa información. Además, es Madrid Digital la que provee de acceso a Internet al SERMAS.

Tanto la OSSI (Lote 1), como la Oficina de Auditoría Interna (Lote 2) tendrán que relacionarse de forma continua con Madrid Digital, en el cumplimiento de las funciones referidas en el presente pliego.

Departamentos TI de los Centros Hospitalarios, de Atención Primaria y del SUMMA112

El SUMMA 112 y los distintos centros de atención sanitaria, disponen de servicios propios de TI, que dan soporte a las necesidades funcionales. Será necesario establecer un modelo de Relación de Servicio para la gestión de los portales y herramientas colaborativas y la integración de los servicios electrónicos para el ciudadano.

[redacted]

8. DIRECCION Y SEGUIMIENTO DE LOS TRABAJOS

La DGSD realizará de manera continuada la dirección, seguimiento y evaluación de los servicios contratados en los distintos lotes.

En cualquier caso, la organización de los recursos técnicos y funcionales corresponderá a los contratistas adjudicatarios que asumen la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante de sus equipos de trabajos encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular asumirá la negociación y pago de los salarios, la fijación de su jornada de trabajo, la concesión de permisos, licencias y vacaciones, las sustituciones de trabajadores en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y obligaciones se deriven de la relación contractual entre empleado y empleador, y ello sin perjuicio de la verificación por la Dirección del Proyecto por parte de la DGSD, del cumplimiento y calidad de los trabajos realizados y marcará las prioridades en base a las necesidades de la DGSD.

Los recursos humanos que el contratista asigne a la prestación de los servicios objeto de este contrato en ningún caso podrán alegar derecho alguno en relación con la Administración contratante, ni exigirse a ésta responsabilidades de cualquier clase, como consecuencia de las obligaciones existentes entre el prestador de los servicios y sus empleados, aún en el supuesto de que los despidos o medidas que pudiera adoptar el contratista, se basen en el incumplimiento, interpretación o resolución del contrato.

La DGSD nombrará un interlocutor que realice las funciones de Director del Proyecto y que configurará el Comité de Dirección por parte de la DGSD.

Este Director velará por el cumplimiento del contrato y se encargará de las relaciones con el contratista para todo lo referente a este contrato. Supervisará y evaluará el desempeño de servicio. Sus funciones principales, en relación con el objeto del presente pliego serán la gestión y supervisión continua del desarrollo de los trabajos y la toma de decisiones que en su caso corresponda. Este Director podrá realizar esta labor con el apoyo de las personas que a su vez establezca.

Cada uno de los contratistas adjudicatarios de cada Lote deberá nombrar a un **Responsable del Servicio**, para que coordine la prestación del servicio y sea el interlocutor con el Director del Proyecto.

Los Responsables del Servicio tendrán entre sus obligaciones las siguientes:

- Actuar como interlocutor de cada contratista adjudicatario frente a la DGSD, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo adscrito al contrato, de un lado, y la DGSD, de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.
- Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratado.
- Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.
- Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente el contratista adjudicatario con la DGSD, a efectos de no alterar el buen funcionamiento del servicio.
- Informar a la DGSD acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato, cumpliendo lo establecido en el apartado 5 del presente pliego.

Los Responsables del Servicio designados por los contratistas adjudicatarios deberán proporcionar informes periódicos, así como todos aquellos otros que, a petición de la DGSD, pudieran servir para la óptima consecución de los objetivos previstos. Como mínimo estos informes deberán especificar el grado de cumplimiento de los indicadores de nivel de servicio comprometidos, así como resaltar:

- Tareas realizadas en el período anterior.
- Desviación de objetivos y plazos, y las correspondientes medidas correctoras.
- Incidencias y riesgos a destacar y acciones tomadas.
- Planificación concreta para el siguiente período.

El personal adscrito al servicio no recibirá ninguna instrucción directa del personal de la DGSD, salvo a través del responsable del servicio y de la propia organización en niveles que el contratista proponga.

Los contratistas adjudicatarios responderán de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiere o que se pudieran derivar.

La DGSD podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a los especificados en los objetivos de la planificación o no superasen los niveles de calidad acordados.

Con periodicidad mensual, los contratistas adjudicatarios confeccionarán un informe de seguimiento que contenga toda la información relevante en cuanto a actividades realizadas, planificadas, incumplimientos, puntos críticos, etc.

Se establecerán reuniones periódicas entre el Director del Proyecto por parte de la DGSD y los Responsables del servicio por parte de los contratistas adjudicatarios, tantas veces como sea requerido para la consecución de los objetivos del contrato.

Los contratistas adjudicatarios no realizarán contacto telefónico con el usuario final a no ser que se lo solicite expresamente la DGSD o se acuerde lo contrario.

A continuación, se describen los procesos de gestión del servicio que deberán seguir los contratistas adjudicatarios. Estos procesos podrían evolucionar durante el periodo de prestación del servicio y se basarán en las normativas y procedimientos de la DGSD en cuanto a Modelos de Relación se establezcan con los proveedores y el resto de las unidades de la DGSD.

8.1. Modelo de Gestión de línea fija

Para la realización de los servicios objetos del presente pliego los contratistas adjudicatarios asignarán un equipo de recursos fijos y de dedicación exclusiva con el dimensionamiento y perfiles mínimos descritos anteriormente. Esto se corresponderá con la línea fija, y que se corresponderá a una serie de actuaciones de dimensión predecible.

La facturación de esta línea se realiza en función del cumplimiento de los Acuerdos de Nivel de Servicio (Apartado 13).

8.2. Modelo de Gestión de la línea variable del lote 1 (bajo demanda variable)

La solicitud de servicios de la línea variable se canaliza a través del **Director del Proyecto** o la persona que designe expresamente para ello, y que se establecerá como interlocutor con los contratistas adjudicatarios.

Línea variable del Lote 1

La DGSD podrá requerir los servicios de la línea variable cuando surja una necesidad fuera de horario habitual del servicio. Estos recursos estarán disponibles con la puesta en marcha del servicio de inmediato, en función de las necesidades de la DGSD. Esta parte variable se facturará

a las tarifas estipuladas, con su posterior certificación de conformidad de los servicios realizados por parte de la DGSD de su dedicación, sin que pueda rebasar el límite económico establecido.

9. SEGURIDAD Y CONFIDENCIALIDAD

La empresa adjudicataria cumplirá cada uno de los requisitos expuestos a continuación.

La empresa licitadora asegura ser consciente de las obligaciones legales en materia de Tecnologías de la Información que adquirirá, en caso de resultar adjudicataria, tales como el Esquema Nacional de Seguridad, conforme a lo indicado en el **Apartado 9.1 Seguridad de Información**.

La adjudicataria, informará a la DGSD de la ubicación geográfica desde donde se presta el servicio. Debido a la importancia del servicio deberá obligatoriamente prestarse desde España.

La empresa licitadora asegura que, en caso de resultar adjudicataria, 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 **Apartado 9.1 Seguridad de Información**, y entregará dicha estrategia y dicho plan durante los tres primeros meses de vigencia del contrato.

La empresa licitadora, asegura que, en caso de resultar adjudicataria, describirá su estrategia, metodologías y herramientas / soluciones / activos que se plantea utilizar para lograr el objetivo establecido en el **Apartado 9.1 Seguridad de Información**, y entregará dichas descripciones durante los tres primeros meses de vigencia del contrato.

La empresa licitadora garantiza que, en caso de resultar adjudicataria, pondrá a disposición de la DGSD 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 **Apartado 9.1 Seguridad de Información**.

La empresa licitadora se compromete, en caso de resultar adjudicataria, a estar **certificado en el ENS nivel medio**, condición indispensable al estar sujeto la propia DGSD al ámbito de aplicación. En caso de no estar certificado el licitador se compromete a solicitar dicha certificación durante los 6 primeros meses de prestación del servicio. Si se dispone de una certificación en el ámbito de la Seguridad de la Información, basado en la 27001 o similar, el licitador se compromete a solicitar dicha certificación durante los 8 primeros meses de prestación del servicio.

Adicionalmente, la empresa licitadora se compromete a que, si no se va a realizar un desarrollo exclusivo según las necesidades demandadas por la DGSD donde el código será único y no compartido y/o obtenido por otros medios, solicitará la certificación en el ENS nivel medio.

La empresa licitadora asegura que, de conformidad con la Ley 12/2018, de 7 de septiembre, se satisfacen las obligaciones en relación con los incidentes de seguridad, conforme a lo indicado en el **Apartado 9.1 Seguridad de Información**.

La empresa licitadora asegura que dispone de las siguientes figuras, estando debidamente recogidas y documentadas, y siendo personas distintas, conforme a lo indicado en el **Apartado 9.1 Seguridad de Información**:

- Responsable del Proyecto.
- Responsable de Seguridad.

La empresa licitadora asegura que dispondrá de los procesos, normas, procedimientos, recursos, actividades, informaciones, registros, facilidades, herramientas y disposición de colaboración que faciliten a la DGSD, 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 **Apartado 9.1 Seguridad de Información**.

9.1. Seguridad de la información

En el presente apartado del pliego se especifica la Normativa Legal Aplicable en materia de seguridad de la información, y se destacan actividades, entregables, procedimiento, responsabilidades, etc. que emanan de las mismas, sin que ello suponga una reducción en su ámbito de aplicación o en el objeto de dicha Normativa. Se incluye a efectos de facilitar la comprensión de la implicación del contratista como elemento esencial en la organización de seguridad.

En los lotes específicos se incluyen requisitos de seguridad que afectan a los equipos y productos de las arquitecturas y soluciones objeto del contrato. Dichos requisitos de seguridad están relacionados con medidas de seguridad normativas por lo que se deberá de tener en cuenta su especificidad y granularidad, garantizando siempre el nivel de seguridad requerido por encima de la especificidad y granularidad del requisito de seguridad expuesto en el lote correspondiente.

9.1.1. Normativa legal aplicable

El Esquema Nacional de Seguridad (en adelante ENS), publicado mediante Real Decreto 311/2022, así como sus modificaciones posteriores en vigor durante la vida del contrato, serán la referencia normativa para garantizar la confidencialidad, integridad, disponibilidad,

autenticidad y trazabilidad de la información de la Consejería de Sanidad de la Comunidad de Madrid sobre la que la adjudicataria realice cualquier tipo de tratamiento dentro del ámbito del presente contrato. En particular, serán de aplicación las guías CCN-STIC-807 relativa a la criptología de empleo en el ENS, y la guía CCN-STIC-817 relativa a la gestión de los ciberincidentes.

Será de aplicación igualmente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. También será aplicable cualquier otra legislación europea o española que desarrolle dicho Reglamento.

El contratista, como suministrador de las Administraciones Públicas, estará obligado a cumplir con las medidas de seguridad aplicables por normativa legal y acorde a los requisitos específicos determinados en el presente pliego, que siempre se entenderán como ampliatorios o reguladores. La Consejería de Sanidad de la Comunidad de Madrid se reserva el derecho a trasladar futuros requisitos de seguridad al proveedor dentro del marco de actividades objeto del presente contrato que así se requiera por cumplimiento legal o por adecuación al Estado del Riesgo del Servicio.

9.1.2. Plan de seguridad de la información

La adjudicataria elaborará un Plan de Seguridad donde se detallarán los controles orientados a garantizar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información de la Consejería de Sanidad de la Comunidad de Madrid que maneje la adjudicataria en virtud del presente contrato.

El Plan de Seguridad deberá describir las medidas de carácter organizativo, físico y lógico que implementará la adjudicataria para proteger la información asociada a los trabajos objeto del presente contrato.

Estas medidas deberán incluir, como mínimo:

- Medidas de tipo organizativo:
    - Política de seguridad, normas y procedimientos de seguridad de la información de la adjudicataria.
    - Estructura de responsabilidades de seguridad de la información de la adjudicataria.
    - Asignación del rol de Responsable de Seguridad de la Información del contrato.

- Procedimientos para la gestión de las autorizaciones de acceso y asignación de privilegios a los/as usuarios/as.
- Procedimiento de gestión de incidentes de seguridad de la información.
- Plan de formación del personal en seguridad de la información.
- Plan de continuidad, de acuerdo a los requisitos de disponibilidad y fiabilidad que establezca la Consejería de Sanidad de la Comunidad de Madrid para cada servicio.

- Medidas de seguridad física:
  - Medidas de control de acceso físico a los locales donde se ubicarán los equipos de tratamiento de la información.
  - Medidas para la protección frente a desastres naturales y/o pérdida de servicios esenciales.
  - Medidas para la protección de soportes físicos de información, tanto en las instalaciones de la adjudicataria como durante su transporte fuera de las instalaciones.
- Medidas de seguridad lógica:
  - Medidas de control de acceso lógico a los sistemas.
  - Medidas de protección frente a intentos de intrusión en los sistemas.
  - Mecanismos para garantizar la confidencialidad de las comunicaciones y de la información almacenada.
  - Medidas para garantizar la integridad de la información y la protección del equipamiento lógico frente a software dañino.
  - Medidas para garantizar la trazabilidad de las acciones del personal que opera la plataforma.
  - Medidas para la gestión de la configuración del equipamiento lógico y la aplicación de configuraciones seguras.

El **Plan de Seguridad** deberá ser validado y aceptado por la DGSD con objeto de verificar la inclusión de las medidas de seguridad, adicionales a las propuestas por la adjudicataria, derivadas de las Políticas de Seguridad específicas del SERMAS.

En su caso, se podrá exigir a la adjudicataria del lote las responsabilidades a que haya lugar por los posibles incidentes que afecten a la disponibilidad, confidencialidad o integridad de las comunicaciones, según lo contemplado en los Acuerdos de Nivel de Servicio, y en la legislación vigente.

9.1.3. Equipo de seguridad

Para la realización de todas las tareas relativas al cumplimiento con el marco legal aplicable, la adjudicataria dispondrá de un equipo de seguridad, liderado por un Responsable de Seguridad, con la cualificación necesaria requerida por dicho marco legal. El equipo de seguridad deberá contar con la especialización, conocimiento y experiencia, demandadas por las actividades de seguridad en el ciclo de vida del servicio, como son, por ejemplo: análisis y gestión del riesgo, gestión del cumplimiento, gestión de incidentes de seguridad y análisis forense, gestión de amenazas y vulnerabilidades, gestión de pruebas y auditorías de seguridad, etc.

9.1.4. Análisis y gestión de riesgos

La adjudicataria del lote 1, en colaboración con el Responsable de Seguridad de la DGSD, elaborará **el análisis y gestión de riesgos**, acorde al nivel de seguridad de los activos de información tratados. Dicho análisis y gestión de riesgos deberá ser validado y aceptado por la DGSD con carácter de entregable del presente pliego. El análisis y gestión de riesgos deberá estar actualizado dinámicamente acorde a los cambios que afecten a la seguridad de los activos de información.

En función de los riesgos detectados, la adjudicataria elaborará un **Plan de Seguridad** que garantice el cumplimiento del marco legal aplicable en base al Plan de Tratamiento de los riesgos identificados en el análisis y gestión de riesgos y que deberá ser validado y aceptado por la DGSD.

El **Plan de Tratamiento de Riesgos del Plan de Seguridad** incluirá la realización de todas las actividades y el desarrollo e implantación de todos los productos indicados en la **declaración de aplicabilidad**. Una vez ejecutado conllevará una evaluación conjunta entre adjudicataria y la DGSD que permita determinar el cumplimiento de la declaración de aplicabilidad, para mediante los procedimientos de auditoría que establezca la DGSD obtener la Declaración de Conformidad y cualquier otro informe requerido para el cumplimiento de la legislación vigente durante el desarrollo del contrato.

De manera explícita se quiere señalar que se deben de analizar y gestionar los riesgos tanto de los activos relativos al tratamiento de la información de las Entidades, como aquellos activos de información derivados de la gestión del servicio por la adjudicataria.

9.1.5. Auditabilidad

La Consejería de Sanidad de la Comunidad de Madrid se reserva el derecho de verificar, mediante revisiones, inspecciones o auditorías, el cumplimiento de toda medida de seguridad indicada en los documentos asociados al contrato. Esto incluye la posibilidad de realización de revisiones o auditorías de cualquier equipamiento o sistemas tanto si están ubicados en las instalaciones de la Consejería de Sanidad de la Comunidad de Madrid, como si lo estuvieran en

las de la adjudicataria, o procedimiento de trabajo, implicado en el marco de la prestación de los servicios especificados en este contrato.

La adjudicataria deberá permitir el acceso a las instalaciones donde se ubica y la comprobación de la infraestructura que se utiliza por los representantes de la DGSD encargados de realizar la revisión. Éstos deberán acudir debidamente acreditados según el procedimiento acordado entre la DGSD y la adjudicataria.

Asimismo, se reserva el derecho de realizar un seguimiento de los servicios contratados mediante las correspondientes auditorías, con objeto de verificar el cumplimiento de los acuerdos firmados. La adjudicataria deberá otorgar acceso a la DGSD cualquier fichero de configuración o registro de actividad creado para la ejecución de los trabajos encuadrados en el presente pliego.

En relación con los proveedores (primarios o secundarios) que participen en la ejecución del contrato, la DGSD se reserva el derecho a solicitar la identificación e información sobre los proveedores, productos y procesos implicados en la provisión de cualesquiera materiales, suministros y servicios utilizados para el cumplimiento del contrato. Esta solicitud podrá realizarse en cualquier momento durante el ciclo de vida del contrato y deberá ser respondida en tiempo suficiente para no perjudicar a la prestación del servicio por parte de la adjudicataria. La DGSD se reserva el derecho a requerir un proceso de auditoría sobre dichos proveedores, así como sobre la cadena de suministro utilizada por el contratista, que será realizada sin coste adicional para la DGSD. Como consecuencia de esta auditoría, la DGSD se reserva el derecho a rechazar la participación en el contrato de estos proveedores secundarios, en cuyo caso la adjudicataria ofrecerá otro proveedor alternativo.

9.1.6. Uso de productos certificado

La adjudicataria, en cumplimiento con el ENS, deberá aportar productos, equipos o personal certificado cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes acreditadas según la legislación aplicable o de reconocida solvencia. Los productos criptográficos, de acuerdo a los resultados del análisis de riesgo cumplirán con la medida del ENS op.pl.5 relativa a componentes certificado.

Tendrán la consideración de normas europeas o internacionales, además de las específicas referidas por el ENS y por el RGPD y su cuerpo normativo que los desarrolla, la ISO/IEC 15408 (Modelo para la evaluación en seguridad informática a productos software) u otras de naturaleza y calidad análogas. Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de

los certificados de la seguridad de la tecnología de la información u otras de naturaleza análoga que haya firmado España.

En los casos en los que sea exigible la utilización de productos y equipos certificados, en todas aquellas tipologías de productos y equipos que se encuentren referenciadas en el documento CCN-STIC 105 (Catálogo 20 de Productos de Seguridad de las TIC), la adjudicataria proporcionará los productos y equipos referenciados en dicho catálogo u otros con un nivel de certificación equivalente, garantizando el despliegue y configuración de los mismos conforme a un Procedimiento de Empleo Seguro, aprobado para los mismos en dicho catálogo aportado por el fabricante.

9.1.7. Incidentes de seguridad de la información

Uno de los procesos singulares y críticos de seguridad es el que corresponde a la gestión de los incidentes de seguridad de la información. Por ello la adjudicataria deberá definir dicho proceso, que al igual que el resto de los que componen el Plan de Seguridad, será revisado y aprobado por la DGSD.

La adjudicataria del lote 1, en coordinación con la DGSD y Madrid Digital, sobre todo para aquellos incidentes de alto impacto y en función de los tipos de incidentes de seguridad habidos en el Real Decreto 43/2021, por el que se desarrolla el Real Decreto-ley 12/2018, deberá elaborar el **Plan de Respuesta** ante dichos incidentes de seguridad, siguiendo el marco de normativa legal aplicable, así como los estándares y buenas prácticas del mercado. Para ello deberá disponer en el ámbito del servicio del equipo de expertos con los perfiles necesarios para la elaboración y la ejecución de las tareas de los **Planes de Respuesta ante Incidentes de Seguridad**.

El proceso de gestión de incidentes de seguridad contemplará un procedimiento de registro de incidentes de seguridad de la información, mediante el cual se recogerá cualquier incidente que afecte a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información de las Entidades que la adjudicataria maneje en virtud del presente contrato.

La adjudicataria deberá poner a disposición de la DGSD el registro de incidentes en todo momento durante la duración del contrato cuando ésta lo requiera, así como comunicar sin dilación indebida cualquier incidente que pueda afectar gravemente a la confidencialidad de la información, especialmente cuando se trate de datos de carácter personal, o la disponibilidad del servicio. La adjudicataria colaborará en las tareas de notificación a la autoridad competente, así como las comunicaciones a los posibles afectados.

El Registro de Incidentes de Seguridad se deberá mantener separado del Registro de Incidencias y Peticiones para preservar su confidencialidad. La DGSD deberá de aprobar la herramienta a utilizar a tal efecto para garantizar la propia seguridad del Registro de Incidentes de Seguridad. Dicho registro será entregado a la DGSD a la finalización de contrato.

El registro de incidentes deberá recoger, para cada incidente que tenga lugar, toda la información requerida por el marco legal aplicable:

- Activos de información afectados.
- Descripción del incidente, detallando las circunstancias asociadas y las dimensiones de la seguridad (confidencialidad, integridad, disponibilidad), tipo de incidentes y criticidad del mismo.
- Clasificación y criticidad de Incidentes acorde a los requisitos establecidos por la normativa legal aplicable que garanticen la aplicación del Plan de Respuesta a Incidentes de Seguridad, así como la notificación a la Autoridad Competente.
- Equipo responsable de su resolución.
- Informe sobre la ejecución del Plan de Respuesta a incidentes de seguridad, que detallará cronológicamente las actividades, y productos generados durante su ejecución, así como toda la documentación o cualquier tipo de información manejada durante la Respuesta al incidente de seguridad.

9.1.8. Personal autorizado y política de gestión de accesos

La adjudicataria, dentro del marco legal normativo, elaborará una **Política de Autorización y Gestión de Acceso al Servicio** por la que se comprometa a controlar y limitar el acceso a las infraestructuras dedicadas a prestar servicio exclusivamente al personal, procesos, dispositivos y otros sistemas de información debidamente autorizados y únicamente a las funciones indispensables para la prestación del servicio.

La adjudicataria deberá garantizar que el personal, previo a la incorporación a los trabajos asociados a la ejecución del presente pliego, conoce y acepta la Política de Seguridad, tanto de la adjudicataria como de aquellas Entidades a los que prestará servicio. La adjudicataria será responsable de que el personal cumpla dichas políticas de seguridad.

Cualquier cambio en el listado de personal autorizado que tenga lugar durante la ejecución del contrato deberá ser comunicado a la DGSD, que deberá dar su aprobación de forma previa a la incorporación del nuevo personal a los trabajos asociados a este pliego, a los solos efectos de verificar el cumplimiento de la normativa de seguridad y del mantenimiento de las características del personal ofertado cuando hayan sido elementos considerados en el proceso de adjudicación. Por ello, esta aprobación no supone alteración alguna del vínculo jurídico establecido entre la

adjudicataria y el personal que efectivamente preste los servicios derivados del presente contrato.

Durante la total duración del contrato, la adjudicataria deberá mantener un listado de personal autorizado para la gestión de la plataforma de comunicaciones asociada al presente contrato, así como listado de usuarios/as administrativos/as y direcciones IPs utilizadas por el personal dedicado a este servicio.

Tanto los/as usuarios/as como las direcciones IPs utilizadas deben ser unipersonales, de manera que permitan trazabilidad. Dicho listado deberá incluir un organigrama de funciones y roles del personal con las respectivas responsabilidades de cada uno perfectamente detallado. Asimismo, se deberá concretar el perfil de acceso de cada uno de los miembros del personal, detallando las infraestructuras a las que pueda acceder, así como el horario.

La política de autorización y control de acceso a los elementos que intervengan en el servicio proporcionado deberá garantizar:

- Que los administradores y operadores estarán correctamente identificados, cada uno con un identificador único, estableciendo un proceso de gestión de los/as usuarios/as, que garantice la correcta asignación y revocación de permisos.
- Que los perfiles de acceso deberán asignarse a cada persona usuaria garantizando que los mismos sólo les permiten las funcionalidades y niveles de acceso mínimos e indispensables para la correcta prestación del servicio.
- La asignación de perfiles se estructurará de manera que se separen al menos las siguientes funciones:
    - Desarrollo de operación.
    - Configuración y mantenimiento del sistema de operación.
    - Auditoría o supervisión de cualquier otra función.

Para controlar el acceso a las infraestructuras que presten servicio, la adjudicataria deberá contar con un sistema de registro de actividades de su personal, particularmente de operadores y administradores, de forma que se garantice:

- El registro de quién realiza cada actividad, cuándo se realiza la misma y sobre qué información y sistemas.
- Qué tareas son exitosas y cuáles no y por qué.
- La determinación de qué actividades se deben registrar y con qué nivel de detalle se hará en base y de manera coherente con el análisis general de riesgos presentados, y de forma consensuada con la DGSD, contemplándose medidas técnicas y procedimentales

que puedan requerir la integración de dicho registro con herramientas de gestión de eventos aportadas por la DGSD.

Los mecanismos de autenticación, así como los sistemas de comunicación a utilizar por el personal, procesos, dispositivos y otros sistemas de información, de soporte para la gestión del servicio a las Organismos, deberán de considerarse como activos críticos en la realización del análisis de riesgos y, por lo tanto, garantizar la propia seguridad de los mismos como medida critica que a su vez garantice la propia seguridad de la información y del servicio.

9.1.9. Configuraciones seguras

La adjudicataria mantendrá un inventario actualizado de todos los elementos de infraestructura dedicados a prestar servicio, detallando su naturaleza, su titularidad y su personal responsable.

La adjudicataria deberá comprometerse a que todos los equipos utilizados en la infraestructura al servicio de la Consejería de Sanidad de la Comunidad de Madrid deberán quedar configurados de manera que:

- Se den de baja las cuentas y contraseñas estándar.
- Se aplicará la regla de "mínima funcionalidad":
    - Los sistemas deberán proporcionar la funcionalidad requerida para alcanzar los objetivos fijados por la Consejería de Sanidad de la Comunidad de Madrid en cada momento y ninguna otra funcionalidad.
    - No se activarán funcionalidades no requeridas para la prestación contratada del servicio, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma el área de exposición a proteger al mínimo imprescindible.
    - Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.
- Se aplicará la regla de "seguridad por defecto":
    - La configuración por defecto de los sistemas no debe exponer a los/as usuarios/as a riesgos inadvertidos.
    - Para que dicha configuración pueda suponer riesgos de seguridad, los/as usuarios/as tendrán que realizar acciones conscientes de ello.
- Las configuraciones de todos los activos se mantendrán correctamente actualizadas de manera que:
    - Se adapten a las nuevas necesidades de la evolución tecnológica determinada por la DGSD.
    - Los sistemas reaccionen a las vulnerabilidades e incidencias reportadas.

- Las configuraciones se realizarán teniendo en cuenta Guías Técnicas de aplicación de la normativa legal y los procedimientos de empleo publicados por el Centro Criptológico Nacional (CCN) siempre que el producto proporcionado disponga del mismo y en su defecto siguiendo las buenas prácticas del mercado acorde al estado del arte.

La adjudicataria proveerá y provisionará todos los medios necesarios para hacer backups de todos los activos, tanto de configuración como snapshots de las máquinas virtuales en sistemas virtualizados. La adjudicataria realizará backup obligatoriamente con la periodicidad que la DGSD considere oportuna, siendo el responsable de su gestión, y en caso de necesidad, también de su implantación, asegurando la privacidad de los datos guardados; dichas copias podrán ser solicitadas si se requieren por la DGSD y serán almacenadas en servidores externos a la Consejería de Sanidad de la Comunidad de Madrid bajo la custodia de la adjudicataria y cumpliendo, tanto en el sistema original que da servicio, como en la realización del backup y su posterior custodia, con las directrices dictaminadas por el RGPD. Los backups tendrán un periodo de retención mínimo de dos años. La DGSD podrá solicitar backups de forma discrecional cuándo y dónde lo considere necesario.

9.1.10. Plan de mantenimiento y gestión de vulnerabilidades

La adjudicataria deberá garantizar que cuenta con un plan de mantenimiento de activos que garantice su seguridad. Para ello deberá:

- Contar con acuerdos de mantenimiento con todos los fabricantes de la infraestructura implicada, de manera que se disponga en todo momento de actualizaciones oficiales.
- Atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas.
- Efectuar un seguimiento continuo de las noticias sobre vulnerabilidades o defectos de los sistemas, para identificar mediante el correspondiente análisis del riesgo, la aplicación de las medidas de seguridad requeridas para solventarlas.
- Disponer de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la actualización.
- El estudio del nivel de actualización de las infraestructuras deberá realizarse, como mínimo, cada 6 meses.

La adjudicataria se coordinará con la DGSD para llevar a cabo todas las tareas de mantenimiento que puedan afectar al servicio prestado. Para ello presentará un análisis de impacto de cada una de las tareas de mantenimiento a realizar de manera que la DGSD pueda aceptar, rechazar o modificar el plan de intervención propuesto en base a la valoración efectuada del análisis de impacto ofrecido.

La adjudicataria, antes del paso a producción, a lo largo de todo el ciclo de vida del contrato realizará análisis de vulnerabilidades y pruebas de intrusión para garantizar el nivel de seguridad de los activos. La DGSD revisará y aprobará el **Plan de Pruebas de Seguridad** y supervisará su ejecución. Las vulnerabilidades detectadas deberán ser solventadas para garantizar la seguridad de los activos en su paso a producción.

Adicionalmente la DGSD realizará un Plan de Pruebas de Seguridad independiente del contratista, a los efectos de verificación requerida por el marco normativo legal.

9.2. Deberes y obligaciones del contratista

Adicionalmente a los requisitos expuestos en apartados anteriores relativos a la elaboración del Plan de Seguridad mediante análisis y gestión de riesgos, así como la exposición de las medidas de seguridad más significativas relativas a los diferentes tipos de activos (físicos, lógicos y personal), la propia adjudicataria adquiere, en lo relativo a seguridad, deberes y obligaciones en cuanto a confidencialidad, protección de datos de carácter personal como encargado de tratamiento, así como todas aquellas derivadas de los procedimientos de seguridad establecidos para la Gestión del Servicio acorde a ENS.

9.3. Confidencialidad de la información

La adjudicataria de cada lote queda expresamente obligada a mantener absoluta confidencialidad sobre la información manejada con ocasión del cumplimiento del contrato, que no podrá copiar o utilizar con fin distinto al que figura en este PPT, ni tampoco ceder a otros, ni siquiera a efectos de conservación.

La adjudicataria se compromete asimismo a no divulgar ni publicar dicha información, bien directamente, bien a través de terceras personas o empresas, ni a ponerla a disposición de terceros sin el previo consentimiento por escrito de la DGSD.

En el caso de que leyes u otras normas impongan criterios de confidencialidad sectoriales (Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, etc.), se deberá dar cumplimiento por la adjudicataria a la misma, así como implantar las medidas adicionales derivadas de la misma que les soliciten las Entidades.

La adjudicataria informará a su personal, colaboradores y subcontratistas de las obligaciones de confidencialidad establecidas en el presente contrato. Todo el personal, previo a la incorporación a los trabajos asociados a la ejecución del presente pliego, deberá firmar los correspondientes acuerdos de confidencialidad. La adjudicataria pondrá todos los medios a su alcance para que su personal cumpla tales obligaciones.

La duración de las obligaciones de confidencialidad establecidas en el presente contrato será indefinida mientras la misma ostente tal carácter, manteniéndose en vigor con posterioridad a la finalización por cualquier causa, de la relación entre el contratista y la adjudicataria, y de la relación entre el personal, colaboradores y subcontratistas destinados a la efectiva prestación del contrato.

Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas y previamente a retirarlos, deberá realizar un borrado seguro de toda la información utilizada o que se derive de la ejecución del contrato, mediante el procedimiento técnico adecuado. La destrucción de la documentación de apoyo, si no se considerara indispensable, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos. Esto mismo será aplicable a cualquier otro soporte de información.

Asimismo, a la finalización del contrato la adjudicataria quedará obligada a la entrega a la DGSD, o destrucción en caso de ser solicitada, de cualquier información obtenida o generada como consecuencia de la prestación del servicio objeto del presente contrato. La adjudicataria queda obligada a emitir, a petición de la DGSD, certificación acreditativa de la destrucción de la información.

9.4. Protección de datos de carácter personal

La adjudicataria de cada lote está obligada a cumplir con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. También será aplicable cualquier otra legislación europea o española que desarrolle dicho Reglamento, durante la total duración del contrato.

La adjudicataria se compromete igualmente a utilizar los datos personales exclusivamente para la realización de los servicios contractualmente pactados y a que la información de datos de carácter personal sea manejada únicamente por el personal cuya intervención sea precisa para la finalidad contractual. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que se hubiera incurrido personalmente.

La adjudicataria se comprometerá a comunicar a la DGSD, de forma inmediata, cualquier falla en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la puesta en conocimiento de terceros de información confidencial relativa a datos

de carácter personal obtenida durante la ejecución del contrato. La adjudicataria colaborará con la DGSD a los efectos de realizar las necesarias Notificaciones a la Autoridad competente, así como las comunicaciones necesarias a los afectados, todo ello acorde a lo requerido en el RGPD.

La adjudicataria vendrá obligada a exonerar a la DGSD de cualquier tipo de responsabilidad frente a terceros, por reclamaciones de cualquier índole que tengan origen en el incumplimiento de las obligaciones de protección de datos de carácter personal que le incumben en su condición de encargado del tratamiento y responderá frente a estas entidades del resultado de dichas acciones.

9.5. Cesión o comunicación de datos a terceros.

El Adjudicatario no comunicará los datos accedidos o tratados a terceros, ni siquiera para su conservación. Así, el Encargado del Tratamiento de cada empresa adjudicataria no podrá subcontratar ninguna de las prestaciones que formen parte del objeto del pliego y que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios.

En caso de que el Encargado del Tratamiento de cada empresa adjudicataria necesitara subcontratar todo o parte de los servicios contratados por el Responsable del Tratamiento en los que intervenga el tratamiento de datos personales, deberá comunicarlo previamente y por escrito al Responsable del Tratamiento, con una antelación de 1 mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa sub-encargada, así como sus datos de contacto. La subcontratación podrá llevarse a cabo si el Responsable del Tratamiento no manifiesta su oposición en el plazo establecido.

El sub-encargado, también está obligado a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento de cada empresa adjudicataria y las instrucciones que dicte el Responsable del Tratamiento.

Corresponde al Encargado del Tratamiento de cada empresa adjudicataria exigir por contrato al sub-encargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.

El Encargado del Tratamiento de cada empresa adjudicataria seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.

9.6. Responsabilidad en caso de incumplimiento.

El Encargado del Tratamiento de cada empresa adjudicataria será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del encargo, respondiendo de las infracciones en que hubiera incurrido personalmente.

9.7. Cesión del contrato.

Los contratistas adjudicatarios no podrán ceder total o parcialmente los derechos y obligaciones que se deriven del contrato sin autorización expresa escrita de la DGSD, que fijará las condiciones de la misma, no autorizándose la cesión de los contratos a favor de empresas incursas en causa de inhabilitación para contratar.

10. PROPIEDAD INTELECTUAL

El contratista acepta expresamente que todos los derechos de propiedad intelectual sobre las configuraciones, parametrizaciones, adaptaciones, implementaciones complementarias, estudios, documentos, productos, subproductos, etc., generados al amparo del presente contrato, corresponden únicamente a la DGSD, con exclusividad y a todos los efectos, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el contratista autor material de los trabajos.

Así, podrán ser reutilizados sin coste en cualquier otra implantación en el ámbito del SERMAS.

No se incluye en el anterior apartado los derechos de uso sobre los productos protegidos con propiedad intelectual y que se adquieran para la puesta en marcha de los sistemas citados como complemento a esta contratación.

A decisión de la DGSD se incorporarán al SERMAS, mediante la correspondiente transferencia de conocimiento y producto, de aquellas herramientas que haya ofertado el adjudicatario que las considere adecuadas.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la DGSD.

11. PLAN DE CALIDAD

La adjudicataria deberá definir un Plan de calidad completo en el que se describa de forma detallada las medidas a adoptar para garantizar el correcto funcionamiento de los servicios y

equipamiento contratados. Dentro de este plan se definirán procesos de aseguramiento de la calidad orientados a:

- Garantizar el cumplimiento de los requisitos enunciados en este pliego.
- Garantizar el cumplimiento de los objetivos y plazos que, en línea con este pliego, de común acuerdo se establezcan.
- Supervisar el correcto desarrollo de las distintas fases del contrato y la toma de las decisiones necesarias.
- En la fase de operación, controlar la calidad del servicio, mediante la realización de auditorías y pruebas técnicas específicas, la revisión del plan de actuación de la adjudicataria, y la propuesta de actuaciones tendentes a absorber las nuevas demandas de servicio.
- Garantizar el cumplimiento de los requisitos de seguridad, aportando una coordinación adecuada con el Plan de Seguridad.

El plan deberá incluir la descripción de la metodología de seguimiento y control del servicio a aplicar en las diferentes fases del proyecto, que deberá ser aprobada por la Consejería de Sanidad de la Comunidad de Madrid.

Adicionalmente a los procesos establecidos en el Plan de Calidad de la adjudicataria, la DGSD podrá realizar controles de calidad adicionales sobre una muestra aleatoria de elementos, al objeto de verificar la adecuación de los mismos a las condiciones estipuladas en la oferta, para lo cual podrá solicitarse de la adjudicataria el soporte preciso.

La consecución de los objetivos de aseguramiento de la calidad se medirá a partir de los datos obtenidos de fuentes tales como estadísticas periódicas, medias de tráfico generadas por los elementos de red, registros de incidencias en el sistema, registro de reclamaciones y actuaciones no conformes, medición de la satisfacción de la Consejería de Sanidad de la Comunidad de Madrid con los servicios, etc.

Si los controles de calidad realizados arrojasen resultados que se desviasen desfavorablemente respecto a los definidos en los Acuerdos de Nivel de Servicio, la adjudicataria estará obligada a resolver las posibles deficiencias o, en su caso, a sustituir el elemento en cuestión en el menor plazo posible.

Las adjudicatarias de todos los lotes deberán acordar y asumir conjuntamente la responsabilidad de garantizar una calidad del servicio global acorde a los requisitos establecidos por la DGSD en aquellos casos en los que haya interdependencia entre las funcionalidades definidas en los lotes.

12. DOCUMENTACIÓN

Durante la duración del contrato la adjudicataria deberá entregar diferente documentación en el formato y periodicidad acordado con la DGSD cumpliendo siempre los requisitos definidos en el apartado de acuerdos de nivel de servicio.

13. ACUERDOS DE NIVEL DE SERVICIO

Se establecen un conjunto de Acuerdos de Nivel de Servicio (ANS), que serán objeto de seguimiento en cuanto al nivel de cumplimiento con el objetivo de no traspasar unos umbrales mínimos de calidad de servicio.

El principal objetivo de los ANS es establecer parámetros medibles que permitan a la DGSD y al adjudicatario controlar la calidad de los servicios prestados, tanto de manera puntual como de su evolución en el tiempo.

Los contratistas adjudicatarios, deberán preparar y documentar un Plan de Calidad para los servicios contratados como medida de aseguramiento de la calidad del servicio proporcionado. El plan de calidad deberá incluir, al menos, los mecanismos que se van a implantar para poder hacer seguimiento de los indicadores de nivel de servicio y establecer las actividades de análisis y seguimiento.

Los contratistas adjudicatarios proporcionarán la información necesaria para el seguimiento de los niveles de servicio ofrecidos mediante los correspondientes informes de seguimiento y garantizará el mantenimiento de históricos de actividad durante todo el período de vigencia del contrato. Esta información se enviará al Comité de Dirección mostrando el cumplimiento de los indicadores definidos en el presente pliego. Dicha información deberá ser obtenida mediante los procedimientos y mecanismos establecidos por la DGSD, que se reserva el derecho de contrastar la información facilitada.

Los indicadores que se considerarán para la medición de los niveles de servicio se detallan a continuación. Se revisarán con periodicidad trimestral.

La imposición de descuentos en la facturación por el incumplimiento de los ANS no impide a la DGSD exigir al adjudicatario el cumplimiento de sus obligaciones contractuales ni la indemnización de daños y perjuicios a que esta pueda tener derecho.

13.1. Indicadores generales

CÓDIGO	LOTES AFECTADOS	NOMBRE	DESCRIPCIÓN	UNIDAD DE MEDICIÓN	NIVEL PERMITIDO
F01	1 y 2	Exceso de rotación	Abandono voluntario o forzoso del servicio por parte de un recurso humano incluido al inicio del periodo de medición del indicador	Número de personas desvinculadas del equipo	<=1
F02	1 y 2	Tiempo de reposición	Tiempo de sustitución de un recurso por otro en caso de rotación del personal	Días de desviación respecto del término de reposición de recursos definido	<=5
F03	Todos	Plazos de los entregables	Grado de satisfacción de la DGSD con respecto a los plazos en los que se remiten los entregables	Días de retraso	<=2
F04	Todos	Contenido, estructura y formato de los entregables	Grado de satisfacción de la DGSD, respecto a la estructura, formato y contenidos de los entregables	Un punto por cada informe con contenidos insuficientes. Medio punto por cada informe con estructura o formatos incorrectos.	<=2
F05	1	Tiempo de Resolución de peticiones de	Tiempo de entrega de informes ante consultas o asesoramiento técnico y/o	Días de retraso	<=1

		consultas e informes	legal de prioridad Alta superior a 3 días hábiles		
F06	1	Tiempo de Resolución de peticiones de consultas e informes	Tiempo de entrega de informes ante consultas o asesoramiento técnico y/o legal de prioridad Media superior a 6 días hábiles	Días de retraso	<=2
F07	1	Tiempo de Resolución de peticiones de consultas e informes	Tiempo de entrega de informes ante consultas o asesoramiento técnico y/o legal de prioridad Baja superior a 12 días hábiles	Días de retraso	<=3

13.2. Incidencias en las medidas de indicadores

En caso de incidencias en la medida del valor de un Indicador asociado a un ANS debidas a errores materiales, o cuando exista falta de colaboración por parte del adjudicatario en la determinación del valor correcto, se considerará que el indicador no ha llegado al Nivel Mínimo de Servicio, aplicándose el descuento en la facturación correspondiente.

Se considerará que hay incidencia en la medida de un Indicador cuando el valor de éste, facilitado por el adjudicatario, difiera en más de un 15% respecto del valor real auditado que resulte del proceso de auditoría que se lleve a cabo desde el servicio.

Se considerará falta de colaboración cuando confluyan todos los siguientes factores:

- Que el auditor que se designe en el mencionado proceso de auditoría aporte evidencia de una solicitud de información en un plazo concreto dirigida al adjudicatario.
- Que la solicitud de información pedida y el plazo sean razonables a juicio de la DGSD.

- Que el adjudicatario no pueda aportar ninguna evidencia que pruebe que se haya facilitado la información solicitada dentro del plazo especificado o en su defecto no haya dado una explicación razonable del motivo del retraso.

Madrid,

LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: NURIA RUIZ HOMBREBUENO [redacted]
Fecha: 2023.12.23 13:06

[redacted]

ANEXO I – DEFINICIONES GENERALES

ANS	Acuerdos de Nivel de Servicio
Backlog	Listado completo del trabajo a realizar, ordenado por prioridad
CMDB	Herramienta de catalogación de servicios y componentes automatizados
Dashboard	Panel de control con la información de datos e indicadores.
DevSecOps	Filosofía que integra la seguridad en la metodología de desarrollo
DGSD	Dirección General de Salud Digital
ENS	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
CCN	Centro Criptológico Nacional
ITIL	Metodología de Gestión de Servicios de Tecnologías de la Información
ITSM	Plataforma de gestión de procesos.
MAGERIT	Herramienta para la implantación y aplicación del ENS.
MD	Madrid Digital
OSSI	Oficina de Seguridad de Sistemas de la Información
PCAP	Pliego de Cláusulas Administrativas Particulares
PMI	Project Management Institute, metodología de gestión de procesos
Porfolio Management	Metodología de control de demanda que permite identificar y priorizar en todo el ciclo de vida las inversiones que se cursan en línea con objetivos estratégicos

PPM	Project and porfolio Management System, es la plataforma de gestión de proyectos y demandas
PPT	Pliego de Prescripciones Técnicas
Product Owner	Responsable de asegurar que el equipo aporte valor al negocio.
QA	Aseguramiento de la Calidad
Roadmap	Hoja de ruta de las actuaciones a realizar
SCRUM	Metodología de gestión de proyectos para el desarrollo ágil de los mismos.
SERMAS	Servicio Madrileño de Salud
SIEM	Funciones de gestión de eventos de seguridad y gestión de información de seguridad
TI	Tecnologías de la Información