



DIRECCIÓN GENERAL DE SISTEMAS
DE INFORMACIÓN SANITARIA
CONSEJERÍA DE SANIDAD

**PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL SERVICIO DE
OFICINA DE SEGURIDAD Y CENTRO DE SOPORTE
ESPECIALIZADO EN EL ÁREA DE SEGURIDAD DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN DEL SERVICIO
MADRILEÑO DE SALUD (OSSI-CERT)**



La autenticidad de este documento se puede comprobar en www.madrid.org/csy
mediante el siguiente código seguro de verificación: **1222547772914059724340**

Marzo 2018

ÍNDICE

1. ANTECEDENTES Y OBJETO DEL CONTRATO	4
1.1. Antecedentes.....	4
1.2. Objeto del contrato.....	4
2. MARCO FUNCIONAL Y TECNOLÓGICO	5
2.1. Marco Tecnológico.....	5
2.2. Esquema Nacional de Seguridad.....	7
3. ALCANCE.....	8
4. ESPECIFICACIÓN DETALLADA DE LOS SERVICIOS REQUERIDOS.....	9
4.1. Servicios de pago periódico mensual - cuota fija	9
4.2. Servicios de cuota variable, servicios específicos.....	14
5. EJECUCIÓN Y GESTIÓN DEL CONTRATO.....	14
5.1. Modelo de relación.....	14
6. ORGANIZACIÓN Y EQUIPO DE PRESTACIÓN DEL SERVICIO.....	15
6.1. Configuración y dimensión mínima para los perfiles profesionales	17
6.2. Equipo de monitorización	21
7. HORARIO DE PRESTACIÓN DEL SERVICIO, UBICACIÓN Y DOTACIÓN DEL PERSONAL PRESTADOR DEL SERVICIO.....	21
8. RECURSOS TÉCNICOS	22
8.1. Sistemas existentes.....	22
8.2. Medios técnicos a suministrar por el adjudicatario para la prestación del servicio	24
9. SEGUIMIENTO DE LOS TRABAJOS	24
9.1. Evaluación del servicio prestado.....	24
9.2. Medición de los niveles de servicio.....	25
9.3. Acuerdos de nivel de servicio (ANS).....	26
10. FASES DEL CONTRATO	27
11. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS	28
11.1. Gobierno del contrato.....	29
11.2. Gestión de riesgos de seguridad.....	31
12. CONDICIONES GENERALES	34
12.1. Propiedad de los trabajos	34
12.2. Calidad de los trabajos	34
12.3. Normativa de seguridad y protección de datos.....	34
13. CONTENIDO DE LAS OFERTAS.....	39
14. ANEXO I-FICHAS DE ANS	43
14.1. Indicador 1. TMAXRES.....	43
14.2. Indicador 2. TMAXSOL.....	43
14.3. Indicador 3. TMAXINF	44
14.4. Indicador 4. TMAXSER.....	44
14.5. Indicador 5. TMAXSOC.....	45
14.6. Indicador 6. NMAXQUE.....	46
14.7. Indicador 8. PERIPOR.....	46



14.8.	Indicador 9. PERINEW.....	47
14.9.	Indicador 10. NFORMAC	47
14.10.	Indicador 11. PORINCI.....	48
14.11.	Indicador 12. NDIACOB.....	48
14.12.	Indicador 12. IFR01.....	49
14.13.	Indicador 13. IFR02.....	50
14.14.	Indicador 14. INADE01	50



1. ANTECEDENTES Y OBJETO DEL CONTRATO

1.1. Antecedentes

La Dirección General de Sistemas de Información Sanitaria (DGSIS), del Servicio Madrileño de Salud (SERMAS), dentro de su estructura organizativa cuenta con un Área de Seguridad cuyo cometido es la gestión de la seguridad de los sistemas de información en el ejercicio de sus competencias, siendo el objeto de este pliego la contratación de la Oficina Técnica denominada Oficina de Seguridad de Sistemas de Información (OSSI), la cual actúa como grupo de apoyo.

La Oficina de Seguridad en la actualidad cuenta con un Centro de Operaciones de Seguridad (SOC), que se encuentra operativo a plena satisfacción y en un proceso de mejora continua. Se desea evolucionar este SOC para obtener capacidades adicionales de alerta temprana y respuesta a incidentes de seguridad (CERT).

1.2. Objeto del contrato

El objeto del presente contrato es el de proporcionar el servicio de gestión y de soporte especializado de Oficina de Seguridad de Sistemas de Información (OSSI), en temas relacionados con la seguridad y la protección de datos personales al Área de Seguridad de la DGSIS.

La OSSI se constituye como un instrumento de prevención, detección, respuesta a amenazas y riesgos de seguridad, así como órgano responsable de la coordinación e implantación de políticas y medidas de seguridad de la organización, prestando a la Consejería de Sanidad una serie de servicios tanto reactivos, como preventivos, con el objeto de impulsar y dar soporte a la implantación de las medidas de seguridad en sus distintos Centros, siendo sus premisas fundamentales las siguientes:

- Apoyo al desarrollo de políticas, guías y normativas en materia de seguridad.
- Asesoramiento multidisciplinar en materia de seguridad y protección de datos.
- Apoyo a los centros en materia de seguridad, ofrecido como un servicio, manteniendo siempre éstos un grado de autonomía suficiente para implantación de las medidas de seguridad
- Integración en el ciclo de vida de los proyectos de la DGSIS
- Auditorias y supervisión de implantación de medidas técnicas (SOC)
- Realización de diagnósticos de seguridad
- Monitorización de eventos de seguridad desde el Centro de Operaciones de Seguridad (SOC)
- Alerta temprana y prevención de riesgos y vulnerabilidades con su respuesta protocolizada (CERT)
- Respuesta a incidentes de seguridad

El contratista se encargará adicionalmente de asumir, dentro de sus funciones, el mantenimiento de las plataformas y componentes tecnológicos existentes y de la dotación de equipamiento (infraestructura de nuevos dispositivos de detección), que incluirá los servicios de soporte y mantenimiento.



2. MARCO FUNCIONAL Y TECNOLÓGICO

La DGSIS, dentro de su estructura organizativa, cuenta con un Área específica de seguridad, cuyo cometido es la gestión de la seguridad de los sistemas de información en el ejercicio de sus competencias.

La amplia red asistencial del SERMAS conlleva la existencia de sistemas de información con una alta diversificación y heterogeneidad distribuidos en diferentes centros, por lo que se hace imprescindible disponer de los mecanismos adecuados para garantizar la seguridad en todos los ámbitos de actuación y con el máximo alcance

Es en este marco de actuación y responsabilidad, donde se plantea la contratación de los servicios de apoyo y soporte especializado en materia de seguridad y protección de datos que abarquen los sistemas de información actuales y que se describen a continuación, así como también el soporte y apoyo en materia de seguridad en aquellos nuevos servicios que se pongan en ejecución durante el contrato, así como a las nuevas necesidades que puedan surgir en materia de seguridad.

2.1. Marco Tecnológico

El Área de Seguridad, que cuenta actualmente con certificación ISO/IEC 27001, para dar servicio a las necesidades en esta materia a todo el SERMAS, maneja o administra los siguientes aplicativos que deberán ser operados por el adjudicatario.

La prestación del servicio de operación y mantenimiento de los elementos descritos en este apartado, incluyendo las correspondientes licencias de funcionamiento si fuera necesario, estará dentro del alcance de lo estipulado en el presente contrato.

- DIAN@

Aplicación informática que permite gestionar de forma centralizada el cumplimiento de la Ley Orgánica de Protección de Datos personales (LOPD), permitiendo a los responsables de seguridad de cada centro

- Mantener actualizada la estructura de los ficheros de datos personales, y de la organización administrativa del propio SERMAS.
- Elaborar y mantener actualizado el Documento de Seguridad
- Dar respuesta al ejercicio de los derechos A.R.C.O (acceso, rectificación, cancelación y oposición), incluyéndolas, tramitándolas y resolviéndolas, con avisos y alertas automáticos.
- Gestionar y resolver las incidencias de seguridad.

- SGOSSI

Sistema de gestión de la OSSI, desarrollado en Apex (Oracle) que permite entre otras funcionalidades:

- Gestión de hospitales: gestión del contrato-programa y de CPDs
- Cuadro de mando
- Resultado de auditorías bienales de LOPD
- Gestión de la oficina



- Repositorio de evidencias

- HORUSTRACK

Herramienta de gestión de auditorías de acceso a información de pacientes, en cumplimiento de la legalidad vigente en materia de protección de datos, mediante mecanismos de control y registro de accesos:

- Justificación
- Análisis
- Motivación
- Detección de comportamientos anormales

- BUGSCOUT

Analizador de vulnerabilidades de código estático multilenguaje (SAST), integra un Analizador de Calidad de Código (Jenkins, sonar qube) y un Proceso de Integración Continua.

- ACUNETIX

Herramienta de análisis de software, de análisis de aplicativos web, analiza vulnerabilidades de código de lado cliente y vulnerabilidades de servicios web.

- NITRO

Lector y conversor de pdf a Word, Excel, etc.

- SIEM (Sistema de gestión de Eventos de seguridad)

Se trata de una plataforma de monitorización junto con los dispositivos y equipos necesarios para su funcionamiento, licencias y servicios para su administración y mantenimiento. Cuenta con una consola única que permite definir políticas y métricas de riesgo, y dispone de un interfaz de alto nivel con posibilidad de obtener informes de seguridad y gestionar incidencias. Incluye módulos y los elementos de hardware y software necesarios para su funcionamiento (correlación de logs, etc.), con al menos las siguientes funcionalidades:

- IDS, o sistema de detección de intrusos
- Detección de anomalías
- HIDS – Host IDS
- Escáner de vulnerabilidades
- Monitor de uso de la red
- Monitor de disponibilidad de servicios
- Sistema de inventariado automático
- Detector de ataques de nivel 2



- Analizador forense

La plataforma puede recibir eventos de dispositivos comerciales y de aplicativos desarrollados a medida, adaptándose a sus características. Dispone de una arquitectura en alta disponibilidad y tolerante a fallos, e incluye los siguientes elementos: sensores recolectores, servidor de gestión, base de datos y consola web.

La plataforma desplegada para la recolección de eventos de seguridad realiza la correlación con otras fuentes de información y genera alertas de seguridad en base a los requisitos establecidos por el SERMAS, que serán al menos los siguientes:

- Capacidad de monitorización de dispositivos de seguridad, elementos de electrónica de red y servidores del SERMAS, mostrando la información de manera integrada.
- Capacidad de generar alertas sobre comportamientos anómalos de cualquier dispositivo
- Permitir correlación de diferentes fuentes de información, como por ejemplo escaneo de vulnerabilidades, eventos de servidores de datos o dispositivos de seguridad e inventario de activos.
- Capacidad para implementar distintos enfoques de correlación.
- Facilidad de integración con distintas tecnologías de fuente de eventos.
- Reglas de búsqueda de anomalías y de respuesta ante eventos, permitiendo respuestas automáticas ante determinados tipos de alarmas.
- Capacidad para ejecutar análisis de vulnerabilidades programados o bajo demanda, presentando informes sobre puntos débiles, recomendaciones, específicos para cada elemento analizado, y personalizados conforme a las especificaciones del SERMAS.

Actualmente consta de:

- Consola de gestión del correlador SIEM de AlienVault
- 52 Sondas AlienVault, en diversas instituciones del SERMAS

2.2. Esquema Nacional de Seguridad

Como parte de la Administración Pública, la Consejería de Sanidad está comprendida dentro del ámbito de aplicación que se establece en el Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad (ENS) para sus servicios de Administración Electrónica, por lo que todas las actividades y servicios comprendidos en el presente pliego deberán estar orientadas a su cumplimiento, siendo el contratista el responsable de garantizar la adecuación y cumplimiento de los sistemas de información al mismo.

Actuaciones en el ámbito del ENS

Dentro de las actividades desempeñadas por la OSSI en el entorno del SERMAS estará la capacidad para llevar a cabo, bajo el ámbito del ENS, las siguientes actuaciones mínimas, enumeradas de modo no exhaustivo:

- a) Determinar si el ámbito de acción de un proyecto se enmarca dentro del establecido para la aplicación del ENS, y que actuaciones proceden en este sentido.



- b) Concretar el alcance que los requerimientos del ENS aplican a un determinado sistema de información.
- c) Continuar con la adecuada categorización de los sistemas existentes, de acuerdo a unos criterios de proporcionalidad razonables y mensurables, generados a partir de las directrices marcadas en el Anexo I del RD 3/2010.
- d) Plasmar dicha categorización en la correspondiente declaración de aplicabilidad para el sistema o sistemas categorizados.
- e) Efectuar los análisis de riesgos pertinentes, utilizando las metodologías y herramientas previamente acordadas con la DGSIS.
- f) Proceder a realizar las evaluaciones y diagnósticos de la situación, siguiendo las directrices que fija el Anexo II del RD 3/2010, y apoyándose en estándares de seguridad y guías de buenas prácticas de reconocido prestigio a nivel mundial, tanto en el sector público como en el privado.
- g) Identificar dentro del sistema la existencia de tratamientos de datos personales a los que haya de aplicar la legislación de Protección de Datos.
- h) Establecer las recomendaciones que se consideren oportunas y convenientes, con el fin de cumplir los objetivos de adecuación al ENS, de cara a lograr un sistema de gestión de la seguridad de la información que se ajuste a las necesidades y exigencias requeridas.
- i) Formalizar esas recomendaciones en el plan o los planes de acción necesarios.
- j) Poder llevar a cabo tareas de gestión, o de apoyo y consultoría, durante la fase de implantación del plan o planes de acción.
- k) Efectuar auditorias periódicas de cumplimiento en aquellos sistemas que tengan ya implantado el ENS, elaborando los informes correspondientes, que serán elevados a la DGSIS.

3. ALCANCE

El contratista deberá proporcionar servicio de gestión y soporte especializado al Área de Seguridad, unidad organizativa de la DGSIS, realizando las actuaciones de asesoramiento, prevención y resolución que se requieran como consecuencia de la implantación y evolución de las políticas e iniciativas de seguridad formuladas por el SERMAS, prestando a este una serie de servicios tanto reactivos, como preventivos, con el objeto de impulsar y dar soporte a la implantación de las medidas de seguridad en sus distintos Centros.

Dentro de las mencionadas actuaciones, sin perjuicio de eventuales modificaciones derivadas de cambios normativos, estructurales o requerimientos del SERMAS, se consideran prioritarios los ámbitos de actuación que se citan en esta cláusula.

El contrato y sus sucesivas prórrogas, incluyen el mantenimiento y soporte de las plataformas, licencias y componentes tecnológicos existentes, descritos en el apartado 2.1 “Marco Tecnológico” y de los nuevos componentes que se incorporen durante la ejecución del contrato y sus prórrogas.



El contrato incluye adicionalmente la adquisición de dispositivos de detección (21 sondas), cuyos servicios de soporte y mantenimiento se encuentran también incluidos durante la vigencia del presente contrato y de sus posibles prórrogas.

Cualquier documento solicitado, alerta de vulnerabilidad o informe de cualquier tipo solicitado por el SERMAS, se deberá proporcionar en idioma castellano y en un formato de presentación conforme a las características de la identidad institucional (cabeceras, gráficos, logos) del SERMAS.

Cualquier elemento imprescindible software o hardware utilizado por el contratista para la prestación del servicio, pasará a ser propiedad del SERMAS a la finalización del contrato, o se asegurará la continuidad del uso del mismo (para soluciones abiertas).

El adjudicatario deberá presentar en cualquier momento que le sea solicitado:

- Información detallada de arquitectura desplegada.
- Configuraciones de servicios y dispositivos
- Recomendaciones para la continuidad del servicio
- Procesos y procedimientos operativos necesarios para poder continuar con los servicios desplegados
- Formación que le sea requerida para una adecuada transferencia de conocimiento
- Cualquier otra información que le sea solicitada.

4. ESPECIFICACIÓN DETALLADA DE LOS SERVICIOS REQUERIDOS

4.1. Servicios de pago periódico mensual - cuota fija

Los servicios requeridos, objeto del presente pliego y que se detallan seguidamente, deben caracterizarse por los atributos siguientes:

- Calidad en la atención.
- Rapidez y eficiencia en la resolución.
- Capacidad de anticipación.
- Aseguramiento de la calidad y mejora continua.
- Satisfacción del Cliente final (Centros del SERMAS).

Se relacionan a continuación los ámbitos de actuación y los servicios que, como mínimo, se prestarán desde la OSSI de la DGSIS y a los que debe dotarse de recursos técnicos y humanos presenciales.

Servicio de cumplimiento legal y normativo

Está orientado al desarrollo de actividades de asesoría y consultoría para el cumplimiento de la legislación vigente y normativa relacionada con las tecnologías de la información, incluyendo actividades relacionadas con administración electrónica.

Comprende actividades tales como:

- Asesoría y consultoría legal y normativa en protección de datos de carácter personal, nuevas tecnologías y seguridad informática.



- Asesoría ante incidencias legales y procedimientos sancionadores.
- Adecuación a la normativa vigente (ENS, otras).
- Soporte a la DGSIS en los aspectos relacionados con la Agencia Española de Protección de Datos (AEPD).
- Asesoría en la gestión de derechos de ciudadanos sobre datos personales.
- Auditorías de cumplimiento normativo.
- Mantenimiento y mejora del SGSI de la OSSI.
- Soporte a la DGSIS en el desarrollo de normativa, políticas, procedimientos, protocolos, guías, etc. de acuerdo a legislación, normativa, estándares y/o códigos de buenas prácticas.
- Consultoría en administración electrónica. Certificados digitales y firmas electrónicas. Servicios al ciudadano y manejo seguro de documentación digital.

Servicio de asesoría y auditoría de controles de seguridad de TI

Tiene como objetivo velar por un adecuado grado de madurez de la seguridad de los sistemas de información en los centros del SERMAS, que asegure la continuidad del servicio y prevenga otros riesgos como pérdida de datos o confidencialidad. Este proceso se basa en la asesoría y el seguimiento de la normativa aplicable, así como de estándares y códigos de buenas prácticas, relacionados con la seguridad de los sistemas de información.

Comprende actividades tales como:

- 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.
- Desarrollo de planes de continuidad de negocio.
- Implantación de dispositivos y soluciones de seguridad en la infraestructura de comunicaciones de la Consejería de Sanidad de la Comunidad de Madrid
- Configuración de elementos de seguridad en la red de comunicaciones
- Asesoramiento en arquitecturas de red
- Realización de Análisis de Riesgo, Evaluaciones de Impacto y otras actividades derivadas del cumplimiento del RGPD.

Servicio de análisis de software y hardware

La Oficina de seguridad es responsable del establecimiento del modelo de seguridad dentro del ciclo de vida de desarrollo de aplicaciones informáticas, dentro del cual desarrolla la función de verificación de los niveles de seguridad reales de los sistemas de información, aplicaciones y dispositivos hardware del SERMAS, así como de los nuevos que se quieran implantar o adquirir, procurando de esta forma que lleguen a tener un nivel de seguridad adecuado para la entidad y así evitar potenciales pérdidas de información confidencial o indisponibilidad de los sistemas, entre otros. De forma reactiva se desarrollan actividades de informática forense.

Comprende actividades tales como:

- Auditorías de seguridad de aplicaciones.
 - Análisis de código fuente.



- Análisis de vulnerabilidades.
- Test de intrusión.
- Asesoría en soluciones técnicas para mitigar los riesgos en las aplicaciones.
- Análisis de riesgos y pruebas de seguridad sobre dispositivos hardware.
- Consultoría en análisis forense.

Servicio de comunicación y formación en seguridad de la información

El servicio que se presta está orientado a la concienciación y formación en materia de seguridad de la información, y al entendimiento de la legislación y normativa que les aplica a todos los entes del SERMAS. Incluye además el uso de las nuevas tecnologías para hacer llegar la información a todo el personal de la Consejería de Sanidad de la Comunidad de Madrid, como por ejemplo redes sociales y alertas de contenido, que ayuden a dar a conocer los avances en la materia.

Comprende actividades tales como:

- Desarrollo de material de formación relacionado con la seguridad de la información, legislación y normativa relacionada.
- Impartir cursos sobre:
 - Seguridad de la información.
 - Normativa: LOPD, ENS, RGPD, etc.
 - Estándares y códigos de buenas prácticas: ISO 27000, ITIL, etc.
- Gestión del contenido del portal de intranet de la OSSI.
- Creación y comunicación del boletín de seguridad del SERMAS.
- Generación de canales de comunicación para la concienciación en materias de seguridad de la información.
- Gestión y asesoría en utilización de herramientas Web 2.0: redes sociales, plataformas educativas, aulas virtuales, encuestas en línea, agregadores de noticias, entre otras.
- Servicios de formación no presencial tales como los ofrecidos a través de herramientas e-learning y red social interna.
- Servicios de asesoramiento en procesos de Transformación Digital de la Administración Pública.

Servicio de seguridad TI en Infraestructura y comunicaciones:

Comprende actividades en infraestructura tales como:

- Análisis de seguridad perimetral para dar cobertura a posibles incidentes de seguridad física.
- Análisis de cumplimiento y regulación TIER en línea de las auditorías físicas realizadas en los CPDs de los centros.
- Dar apoyo en la realización de planes de contingencia y realizar actividades de gestión de riesgos (planificación, detección, mitigaciones).
- 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.
- Alinear las actividades programadas al marco de los estándares existentes (ISO 27001, COBIT, ISAE3402, SOX, otras).



Comprende actividades en comunicaciones tales como:

- Desarrollar e implementar las políticas y procedimientos de seguridad. Monitorear su cumplimiento.
- Gestionar incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.
- Asistir a los desarrolladores en la solución de vulnerabilidades, realizar recomendaciones de mejora y continuidad del servicio.
- Conocimiento y gestión de configuración de cortafuegos.
- Realizar análisis de riesgos en nuevas tecnologías. Aplicar metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas modelos formales, análisis forense, etc. así como en áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones.
- Realizar actividades de gestión de riesgos (planificación, detección, mitigaciones). Desarrollar tareas de Pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir vulnerabilidades para luego gestionar soluciones.

Centro de Operaciones de Seguridad (Servicio SOC). Servicio de monitorización y correlación de eventos de seguridad

En una atención 24x7 durante todos los días del año, está orientado a la ejecución de actividades relacionadas con servicios SOC (Centro de Operaciones de seguridad), permitiendo gestionar y administrar las vulnerabilidades y amenazas de una forma proactiva y reactiva, mediante la monitorización de las redes de comunicación y equipos que albergan los sistemas informáticos, así como el acceso a los datos del SERMAS. Pretende ofrecer asesoría y plantear las opciones más innovadoras para llevar un control de las comunicaciones y detección de vulnerabilidades, con el objetivo de que no se vea afectado el servicio en los sistemas de información del SERMAS, tanto desde el interior de la red de la entidad como desde el exterior.

Comprende actividades tales como:

- Monitorización del estado de la seguridad:
 - Monitorización de dispositivos
 - Cumplimiento políticas.
 - Detección y gestión de vulnerabilidades (dispositivos de red y equipos).
 - Aplicación de parches para corrección de vulnerabilidades.
 - Alerta temprana ofrecido a través de la red social interna o por otros medios.
- Instalación de dispositivos de seguridad y gestión de su configuración de dispositivos (aplicación de políticas y filtros de firewalls, elementos de red, etc.).
- Gestión y correlación de logs de dispositivos. Instalación de Sondas, correlación de eventos de seguridad y generación de alertas.
- Análisis de vulnerabilidades.
- Consultoría y asesoría en Ciberseguridad (servicios y amenazas externas: plataformas cloud, phishing, malware, reputación, otras).
- Respuesta a incidencias de seguridad.
- Alerta temprana a través de su conexión a un CERT homologado.



El Centro de operaciones SOC deberá cumplir las normas de la Certificación ISO 22301 (Sistemas de gestión de la continuidad del negocio), como garantía de disponibilidad y continuidad de servicios y de la norma ISO-27001 como sistema de gestión de la seguridad para la continuidad de negocio.

Se valorará de acuerdo al criterio de valoración establecido en el PCAP, que el Centro de Operaciones de Seguridad (SOC) este acreditado o en trámite de acreditarse como Equipo de Respuesta ante Emergencias Informáticas (**CERT**, del inglés **Computer Emergency Response Team**) autorizado por la UCM - Universidad Carnegie Mellon, o conectado con un CERT homologado por esta Universidad o bien ser miembro de la organización FIRST, para mejor garantía de los servicios de alerta temprana.

Otras prestaciones a realizar

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

- 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 la Ley de Administración electrónica y mejora continua de los procesos contemplados en ella. Soporte a la implantación tecnológica del uso del DNle y otros certificados digitales u otros sistemas de identificación y firma electrónica, por los ciudadanos y profesionales.
- Adecuación progresiva de ficheros manuales.
- Soporte a los centros en la realización de las Auditorías legales.
- 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 OSSl, pertenecientes al SERMAS.

Dada la naturaleza dinámica de la seguridad informática y su constante actualización, el contenido de los servicios y, en general, de las prestaciones requeridas, se podrá modificar, siguiendo el procedimiento previsto en el presente pliego, para su adecuación a los cambios normativos y estructurales, que se produzcan con posterioridad a la



adjudicación del contrato, siempre que la modificación guarde relación con el objeto del contrato y no suponga mayor coste para el contratista.

4.2. Servicios de cuota variable, servicios específicos

Se define una línea variable de servicios específicos, que se corresponderá a actuaciones a demanda, que no se conocen de antemano, y que dependerán de las necesidades del SERMAS durante la vigencia del contrato, por lo que su facturación dependerá de los servicios realmente ejecutados en ese periodo.

Los servicios serán prestados por personal con un perfil de consultor de alta especialización, dependiendo de la prestación a realizar en cada caso concreto y con experiencia en las materias demandadas.

5. EJECUCIÓN Y GESTIÓN DEL CONTRATO

5.1. Modelo de relación

El contratista se encargará de la realización de todas las actividades requeridas en el alcance de los servicios objeto del contrato. Para ello, deberá establecer un modelo de relación con las distintas unidades de los hospitales, la DGSIS y del SERMAS, con las cuales se requiere la adecuada coordinación:

- **Servicio de Informática de los hospitales:** responsable de la gestión, administración, operación y mantenimiento de los sistemas de información y la infraestructura existente en los centros. Así mismo, apoyan a las labores de coordinación de otras áreas de los hospitales implicadas en el proceso (grupos de usuarios) y proveedores de otras soluciones a integrar. Además, proporcionan un soporte de primer nivel a los usuarios de sus respectivos hospitales.
- **CEDAS (Centro de Datos de Administración y Soporte):** responsable de los servicios de gestión integral de los CPDs del SERMAS, y por tanto, de la gestión, administración, operación y mantenimiento de la infraestructura centralizada en los Centros de Procesos de Datos Corporativos del SERMAS.
- **MEDAS:** tiene a su cargo el Mantenimiento, Evolución y Desarrollo de las Aplicaciones Sanitarias del SERMAS. MEDAS proporciona los requisitos de integración con las aplicaciones corporativas en uso y explotación desde el Hospital o que requieren la integración de datos a partir de los Sistemas de Información del Hospital.
- **CESUS:** dentro del ámbito de la gestión de los servicios TIC del SERMAS, es el interlocutor con el que contactarán los usuarios del SERMAS ante problemas o incidencias que puedan surgir en relación a dichos servicios. Es, asimismo, el canal principal de entrada de solicitudes de modificación, adecuación y evolución de aplicaciones, y apoya y da soporte al personal de informática de los Centros en las labores de operación y administración de las infraestructuras tecnológicas.



- **Oficinas Técnicas:** Encargadas de la planificación, puesta en marcha, seguimiento y control de los proyectos en los distintos ámbitos de actividad del SERMAS.
- **OT de Proyectos:** encargada de la planificación, seguimiento y gestión de los proyectos de carácter corporativo (transversales) del SERMAS. Proporcionan las directrices y estándares a considerar para la integración del proyecto específico con otras iniciativas o proyectos que, desde Servicios Centrales, estén en progreso o en producción.
- **Agencia para la Administración Digital de la Comunidad de Madrid (AADCM),** con la cual se relacionará en el ámbito de sus competencias. Deberán contemplarse las labores de integración / coordinación con un SOC a nivel de la Comunidad de Madrid, operado por AADCM, así como también, la coordinación entre SERMAS y AADCM a efectos de intercambio de información de alertas sobre amenazas e incidentes.

6. ORGANIZACIÓN Y EQUIPO DE PRESTACIÓN DEL SERVICIO

La DGSIS realizara de manera continuada la dirección, seguimiento y evaluación de los servicios contratados, sin perjuicio de las labores de coordinación, control, y aseguramiento que sobre el proceso global corresponden al contratista.

En cualquier caso, la organización de los recursos técnicos corresponderá a la empresa contratista que asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo 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 del SERMAS, enfocando los recursos en función de las necesidades de los distintos proyectos y en los diferentes ámbitos y/o soluciones descritos, de forma que se proporcione cobertura completa a todo el alcance del pliego en cada momento.

El contratista responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiere o que se pudieran derivar.

La DGSIS 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.

El contratista garantizará la continuidad del servicio en cualquier circunstancia y en cualquier época del año.

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.

El contratista nombrará a un responsable del servicio por parte del contratista.

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

La DGSIS solicitará al responsable del servicio del contratista, en el caso del incumplimiento de los acuerdos de nivel de servicio, que realice los cambios adecuados para la correcta prestación del servicio. El contratista dispondrá de un plazo de quince días para subsanar las deficiencias. En el caso de que se produzca el cambio de recursos, estos deberán ser de igual categoría y cumplir con los requisitos establecidos para el perfil. Si bien la DGSIS entiende que la gestión de los recursos técnicos del contratista no forma parte de su responsabilidad, sí que lo es obtener una rentabilidad de la inversión.

Por rotación planificada de un recurso técnico asignado se entienden los cambios promovidos por el contratista, por causas ajenas a la DGSIS, que cumplen los siguientes requisitos:

- Deberá solicitarlo con al menos 20 días de antelación, con justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de posibles candidatos para un perfil cuya cualificación sea igual o superior al de la persona que se pretende sustituir.
- Verificación por la DGSIS del cumplimiento de los requisitos por los candidatos propuestos.
- En caso de llevarse a cabo la sustitución a solicitud del contratista, y de cara a subsanar los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto, se establecerán períodos de solapamiento sin coste adicional. Dicho plazo de solapamiento mínimo entre el perfil entrante y el saliente será de 2 semanas.
- El adjudicatario asumirá la impartición de la formación necesaria a las personas de nueva incorporación y hará los controles adecuados para asegurar el correcto traspaso de conocimientos

En todo caso, la incorporación o sustitución de recursos técnicos deberá mantener los requisitos establecidos como mínimos para cada perfil.

El incumplimiento de las condiciones anteriores, implicará la consideración de una rotación no planificada del recurso.

El contratista deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada del personal que compondrá el equipo prestador del servicio, para evitar la pérdida de capacidad de gestión del servicio, de conocimiento y el impacto en los niveles de servicio.

El contratista deberá presentar un modelo organizativo, que cubra la totalidad de las áreas de conocimiento de los entornos tecnológicos contemplados en el contrato.

El servicio prestado por el contratista deberá poseer la flexibilidad necesaria para adaptarse a la evolución funcional y tecnológica, siendo responsabilidad del contratista la formación del equipo para capacitarlo en las tecnologías del SERMAS.

Si como consecuencia de algún proyecto asociado a la evolución de la gestión de la Seguridad de los sistemas de Información del SERMAS el contratista tiene que incorporar perfiles nuevos, el contratista tendrá que incorporarlos o sustituir aquellos que dejan de tener un perfil acorde con la prestación del servicio. En estos casos, el contratista presentará un



plan de sustitución de recursos con el cambio de los perfiles con al menos 30 días de antelación. La DGSIS será quien en último término acepte o rechace la propuesta. En todo caso, el cambio de unos perfiles por otros tendrá que hacerse conservando el número de recursos así como el nivel de titulación, formación y años de experiencia, no pudiendo ser intercambiado un perfil por otro de menor titulación, formación y experiencia.

El contratista dimensionará de la manera adecuada el servicio, de manera que se cumplan los Acuerdos de Nivel de Servicio y los requisitos de trabajo presencial y en disponibilidad o guardia, que se explican en este pliego.

6.1. Configuración y dimensión mínima para los perfiles profesionales

El equipo mínimo para la prestación del servicio estará compuesto de 13 personas con dedicación exclusiva al servicio, que será prestado de forma presencial en las Oficinas del SERMAS.

Todos los recursos deberán estar a tiempo completo. El periodo vacacional se deberá cubrir de forma adecuada estableciendo los turnos necesarios entre las personas que conforman el equipo de trabajo.

A continuación se detallan los requisitos de titulación y experiencia de cada perfil:

El Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior (MECES), establece cuatro niveles de cualificación en función de los resultados de aprendizaje que proporcionan los estudios oficiales: el nivel de Técnico Superior (FP) se incluye en el Nivel 1, el de Grado universitario en el Nivel 2, el de Máster universitario en el Nivel 3, y el de Doctor en el Nivel 4

En todos los casos cuando se mencione titulación universitaria de nivel 3 se entenderá referida a la posesión de estudios de máster universitario o su equivalencia según MECES. De manera análoga para la titulación universitaria de nivel 2 referida a la posesión de grado universitario o su equivalencia según MECES.

A efectos de valoración la presentación de candidatos doctorados universitarios, se considerará equivalente a la titulación universitaria de nivel 3.

▪ 1 Jefe de Proyecto:

- Titulación universitaria Nivel 2 ó 3 preferiblemente en Derecho o en Ingeniería Informática.
- Estudios de postgrado en Derecho de las Tecnologías o similar.
- Experiencia acreditada mínima:
 - 2 años con categoría de Jefe de Proyecto.
 - 4 años como Consultor Sénior.
 - Acreditará además al menos dos años de experiencia en gestión de proyectos de seguridad de las tecnologías de la información y al menos dos en materias de protección de datos.



- **2 Consultores Sénior, Especialista en Derecho de las Tecnologías:**
 - Titulación mínima universitaria Nivel 2 ó 3 en Derecho.
 - Estudios de postgrado en Derecho de las Tecnologías o similar.
 - Experiencia acreditada mínima:
 - 3 años como especialista en el ámbito de asesoría legal en protección de datos.
 - Acreditará además al menos un año de experiencia en proyectos de seguridad de las tecnologías de la información.
- **2 Consultores, Especialista en Derecho de las Tecnologías:**
 - Titulación mínima universitaria Nivel 2 o 3 preferiblemente en Derecho.
 - Experiencia acreditada mínima:
 - 2 años como especialista en el ámbito de asesoría legal en protección de datos.
 - Acreditara al menos un periodo no inferior a 1 año de experiencia en proyectos de seguridad de las tecnologías de la información.
- **1 Consultor Sénior, Especialista en Normativa y Auditorías de TI:**
 - Titulación mínima universitaria Nivel 2 en materias TIC (Informática o Telecomunicaciones).
 - Estudios de postgrado en Seguridad TI o similares.
 - Experiencia acreditada mínima:
 - 3 años como especialista en auditorías y consultoría de Seguridad TI.
 - Acreditará además al menos un año de experiencia en proyectos de seguridad de las tecnologías de la información.
 - Experto en seguridad de los sistemas de información con conocimientos en legislación y normativas de las tecnologías, así como gestión de la seguridad de la información.
 - Conocimientos de metodologías y buenas prácticas (COBIT, ITIL, etc.).
- **2 Consultor Sénior, Especialista en Desarrollo de Proyectos y Sistemas de Seguridad de TI:**
 - Titulación mínima universitaria Nivel 2 en materias TIC (Informática o Telecomunicaciones).
 - Estudios de postgrado en Seguridad TI, o similares.
 - Experiencia acreditada mínima:
 - 1 año con categoría de Consultor Sénior o 3 años acumulando las categorías de Consultor Sénior y Consultor.
 - Acreditará además al menos un año de experiencia en proyectos de seguridad de las tecnologías de la información.
 - Expertos en ciclo de vida de sistemas de información, con conocimiento en programación en diversos lenguajes y bases de datos.



- Conocimientos en redes sociales, contenidos web y seguridad de las tecnologías de la información.
- **1 Consultor Sénior, Especialista en Auditorías de Seguridad TI y Gestión de Proyectos de TI:**
 - Titulación mínima universitaria Nivel 2 en materias TIC (Informática o Telecomunicaciones).
 - Experiencia acreditada mínima:
 - 3 años con categoría de Consultor Sénior o 6 años acumulando las categorías de Consultor Sénior y Consultor.
 - Acreditará además al menos tres años de experiencia en la Gestión de Proyectos de TI, y al menos un año de experiencia en proyectos de seguridad de las tecnologías de la información.
 - Experto en ciclo de vida de sistemas de información, con conocimiento en planificación de proyectos de desarrollo, diseño y programación en diversos lenguajes y bases de datos, así como análisis y creación de informes con herramientas de Business Intelligence.
 - Debe tener conocimientos y experiencia en auditorías de seguridad de TI y Análisis de Riesgos.
 - Conocimientos en normativas de gestión de seguridad de la información.
- **2 Consultores Sénior, Especialista Técnico en Seguridad TI en Infraestructura y Redes :**
 - Titulación universitaria Nivel 2 en materias TIC (Informática o Telecomunicaciones) o Nivel 1 formación Profesional de Grado superior en Informatica o telecomunicaciones.
 - Debe aportar certificaciones reconocidas en el campo de las comunicaciones y sistemas de seguridad asociados.
 - Experiencia acreditada mínima:
 - 3 años con categoría de Consultor Sénior o 6 años acumulando las categorías de Consultor Sénior y Consultor.
 - Acreditará además al menos tres años de experiencia en administración y/o análisis de redes.
 - Expertos en administración de redes y análisis de redes.
 - Deben tener conocimientos y experiencia sobre tecnologías relacionadas con infraestructura de tecnologías de información (arquitectura, seguridad, sistemas, etc.), así como de Centros de Procesamiento de Datos (CPD' s).
 - Conocimientos y experiencia sobre auditorías de TI y análisis de riesgos, así como en normativas de gestión de seguridad de la información.
- **1 Consultor Sénior, Especialista Técnico de Seguridad TI en Comunicaciones:**
 - Titulación: Técnico Superior Nivel 2 o diplomatura en materias TIC (Informática o Telecomunicaciones).
 - Estudios de postgrado en Seguridad de TI o similar.
 - Debe aportar certificaciones reconocidas en el campo de las comunicaciones y sistemas de seguridad asociados.



- Experiencia acreditada mínima:
 - 3 años con categoría de Consultor Sénior o 6 años acumulando las categorías de Consultor Sénior y Consultor.
 - Acreditará además al menos dos años de experiencia en monitorización de redes, análisis de vulnerabilidades, administración de herramientas de seguridad perimetral y antimalware, y al menos un año de experiencia en proyectos de seguridad de las tecnologías de la información.
 - Expertos en seguridad de TI, específicamente como análisis de vulnerabilidades, monitorización de redes, gestión de incidencias y problemas.
 - Deben tener conocimientos sobre tecnologías relacionadas con infraestructura de tecnologías de información (arquitectura, seguridad, sistemas, etc.), así como de Centros de Procesamiento de Datos (CPDs).
- **1 Documentalista:**
- Titulación licenciatura o grado universitaria
 - Experiencia en Biblioteconomía y Documentación.
 - Gestión Documental.
 - Conocimiento de Gestores Documentales.
 - 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.
- 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.
- Tecnologías y soluciones de firma electrónica.
- Conocimientos generales en materia de Derecho aplicado a las TIC, y de la normativa relacionada a continuación:
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los datos de carácter personal (LOPD).
 - Ley 59/2003, de 19 de diciembre, de firma electrónica.
 - Ley 39/2015 de 1 de Octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.



- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
 - Real Decreto 1720/2007 de desarrollo de la LOPD
 - Real Decreto 4/2010 Esquema Nacional de Interoperabilidad
 - Ley 41/2002 Básica reguladora de la Autonomía del Paciente
 - Resoluciones e instrucciones de la Agencia Española de Protección de Datos (A.E.P.D).
 - Reglamento (UE) 2016/679 , de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales
- Hacking ético
 - Monitorización en sistemas de correlación de eventos
 - Análisis de código fuente

Al menos tres perfiles, entre los perfiles de jefe de proyecto y consultores, tienen que demostrar experiencia en Oficinas de Seguridad en el Sector Público, a través de certificados expedidos por la Administración correspondiente.

6.2. Equipo de monitorización

Además del equipo anterior, el contratista deberá asegurar la monitorización y el escalado de incidencias propias de nuestra red o debidas a agentes u ataques externos en horario de 24 horas los 365 días del año, por un grupo específico y especializado que prestará sus servicios desde el Centro de Operaciones de Seguridad del contratista (SOC) o de forma presencial si así fuera requerido por el SERMAS. Este equipo deberá ser dimensionado por el contratista en base a la información suministrada en el pliego así como a su experiencia por el tipo de actividades a realizar.

El personal a cargo del SOC tendrá más de 5 años de experiencia demostrable en servicios de seguridad gestionada, gestión de dispositivos, gestión de vulnerabilidades y monitorización de seguridad.

7. HORARIO DE PRESTACIÓN DEL SERVICIO, UBICACIÓN Y DOTACIÓN DEL PERSONAL PRESTADOR DEL SERVICIO

El horario de prestación del servicio del equipo mínimo será de 9 a 18 horas, en modo presencial, en las oficinas centrales SERMAS. Tendrán disponibilidad para desplazarse a realizar estancias en los distintos centros dependientes del SERMAS.

Los servicios del equipo de monitorización del Centro de Operaciones de Seguridad (SOC) serán prestados en modo no presencial, en **horario de 24 horas, los 7 días de la semana**, especialmente para las tareas de monitorización de servicios y para



consultas no presenciales, sin que estas consultas supongan un gasto adicional para el SERMAS.

Si por las razones que fuera, tales como una incidencia grave de seguridad, pudiera existir la necesidad de realizar trabajos por el personal prestador del servicio fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, el SERMAS no aceptará sobre-coste adicional por estas circunstancias, que deberán ser absorbidas siempre por el contratista. Para estos casos, el contratista debe proveer a su personal de teléfonos móviles para su localización inmediata fuera del horario de oficina presencial

Los medios de trabajo necesarios para el personal adscrito a la prestación del servicio, tales como, Ordenador personal, Teléfonos Móviles, Tablet, licencias software ofimático, etc., correrán a cargo de la empresa adjudicataria. Respecto al software ofimático, entre otras herramientas necesarias, el personal de la OSSI deberá manejar y tener licencias para su trabajo habitual de:

- Microsoft Publisher 2013.
- Project Standard 2013 y Visio.
- Adobe Acrobat XI Pro (versión completa).

Así mismo, proveerán a los miembros de cada uno de los equipos del material de oficina y fungibles correspondientes.

8. RECURSOS TÉCNICOS

El contratista será el encargado del mantenimiento y soporte de los sistemas o licencias ya existentes, y de los que se pongan en funcionamiento durante la vida del contrato, incluyendo sus prorrogas.

El contratista será responsable de la puesta en marcha de los medios técnicos recogidos en este capítulo. No podrán ser computadas como horas de trabajo del equipo técnico, sino que correrán por cuenta del contratista como un concepto adicional.

8.1. Sistemas existentes

En el apartado 2.1 Marco Tecnológico, donde se describe el marco tecnológico, se detallan los sistemas existentes en la OSSI. En éste epígrafe se harán algunas precisiones sobre la actividad prevista en ellos y en otros sistemas actualmente comenzados o proyectados.

El contratista deberá asumir dentro del presente contrato, el servicio de soporte y mantenimiento de licencias oficial de cada fabricante de los sistemas existentes, citados en el apartado 2.1

El mantenimiento de las licencias y soporte de la infraestructura existente, así como el software necesario para el correcto funcionamiento de cualquier dispositivo en general, se considera incluido en el presente contrato durante toda su duración. (incluidas sus prorrogas)



La infraestructura existente desplegada en el SERMAS se mantendrá en la misma ubicación actual dentro de las instalaciones del SERMAS y no se contempla una migración de la misma a las instalaciones del contratista.

Software de análisis de vulnerabilidades:

El presente contrato incluye el servicio del mantenimiento de las licencias de uso de la herramienta Accunetix y Bugscout u otra de funcionalidades equivalentes, que se instalará en las dependencias del SERMAS y será utilizada por el equipo de prestación del servicio, es decir, no será operada desde el SOC del adjudicatario. Dicha herramienta se utilizará para realizar el análisis de aplicaciones web en busca de posibles fallos de seguridad, que puedan poner en peligro la integridad de la página publicada en Internet. Esta aplicación ejecuta una serie de pruebas, totalmente configurables por el usuario, para identificar las vulnerabilidades tanto de programación de la página como de configuración del servidor y emite informes de las auditorías de seguridad realizadas.

Consolas de control:

Servicio de mantenimiento de las licencias de uso y mantenimiento de la consola de control, del sistema de correlación de todas las sondas. Incluye el servicio de mantenimiento de las 52 sondas existentes y de las que se suministran con el contrato y en la prórroga del mismo

La consola de control (SIEM) existente deberá evolucionarse para dar servicio en **alta disponibilidad**, manteniendo la capacidad de retención de log actual (120 días como mínimo) incluso cuando se incorporen nuevas sondas, suministradas al amparo del presente contrato o en la prórroga del mismo.

Otras herramientas o dispositivos

Dada la diversidad y grado de avance tecnológico al que están sometidos las herramientas y dispositivos objeto del presente contrato, durante la prestación del servicio, podrán ser actualizadas o sustituidas por el contratista, por otras cuyas funcionalidades se ajusten mejor a las necesidades del SERMAS, dentro del alcance económico del contrato.

Su mantenimiento y soporte estará incluido como un servicio durante la duración del contrato y sus prorrogas.

Certificación ISO:

El presente contrato incluye todos los costes de renovación y mantenimiento de la certificación ISO 27000 de la Oficina de Seguridad existente.

Formación:

El presente contrato incluye formación y la certificación CISM “Certified Information Security Manager” CISM para 4 personas del personal adscrito a la Consejería de Sanidad.



8.2. Medios técnicos a suministrar por el adjudicatario para la prestación del servicio

Sondas:

El contrato incluye el suministro de 21 sondas, adicionales a las existentes, compatibles con la plataforma de correlación existente, con funcionalidades de gestión de malware, detección de firmas de ataques, vulnerabilidades de software y navegación, de tipo snort para complementar gestión del malware en el resto de hospitales y red de Atención Primaria. Las características técnicas de las sondas deberán ser las adecuadas para dar servicio a los distintos tipos de centros y cubrir sus distintas necesidades de rendimiento.

Las sondas podrán ser sustituidas por otros dispositivos de monitorización de importe equivalente, si a criterio del SERMAS esto resultara más conveniente para la mejor prestación del servicio. Para realizar un cálculo adecuado, se contrastarían los precios de lista publicados por los fabricantes de las sondas con los de los dispositivos sustitutorios. El suministro de las sondas incluirá su soporte y mantenimiento durante el contrato y sus prórrogas.

La prórroga del contrato supondrá el suministro de 21 sondas adicionales con el soporte y mantenimiento incluido

9. SEGUIMIENTO DE LOS TRABAJOS

9.1. Evaluación del servicio prestado

La DGSIS realizará de manera continuada la dirección, seguimiento y evaluación de los servicios contratados, sin perjuicio de las labores de coordinación, control, y aseguramiento que sobre el proceso global corresponden al contratista, el cual responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiere o que se pudieran derivar.

La DGSIS 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.

Independientemente de las actas de reuniones o informes de seguimiento que se soliciten por la DGSIS en cualquier momento, el seguimiento del servicio se realizará mediante un conjunto de indicadores estructurados en un cuadro de mando que será provisionado por el adjudicatario (a menos que la DGSIS indique lo contrario), consolidando la información de seguridad proporcionada desde los distintos proyectos y ámbitos de actuación.

Como resultado de la realización de estas actividades, los sistemas de información de la DGSIS deberán mantener el nivel de seguridad acorde a los requisitos establecidos en el marco jurídico y en la normativa que le aplica.



9.2. Medición de los niveles de servicio

La DGSIS establece el conjunto de **Acuerdos de Nivel de Servicio (ANS)** que serán objeto de seguimiento mensual y el nivel de cumplimiento de los mismos como umbral de calidad del servicio.

Se entiende como ANS el acuerdo entre el contratista del servicio y la DGSIS con objeto de garantizar unos niveles de calidad mínimos sobre el servicio prestado. En él se indica el servicio o actividad concretos, se documenta el objetivo de Nivel de Servicio y se especifican los compromisos que debe cumplir el adjudicatario.

El principal objetivo de los ANS es establecer parámetros medibles que permitan a la DGSIS y al adjudicatario controlar la calidad de los servicios prestados, tanto de manera puntual como en su evolución en el tiempo. Por tanto, los servicios prestados por el adjudicatario serán supervisados por la DGSIS en base al seguimiento de los ANS, a la supervisión y análisis de los procesos seguidos por el contratista en la prestación de los servicios contratados y al continuo muestreo de la correcta ejecución de las actividades encomendadas.

El adjudicatario proporcionará la información necesaria para el seguimiento de los ANS establecidos mediante los correspondientes informes de seguimiento y garantizará el mantenimiento de históricos de actividad durante todo el período de vigencia del contrato. La información será objetiva y obtenida preferentemente a través de los registros elaborados con las herramientas de gestión. Tanto las herramientas de gestión como la forma de extracción de la información serán definidas por la DGSIS.

La medición y el seguimiento de ANS se realizarán con la periodicidad que garantice su correcto seguimiento y reporte dentro del Comité de Seguimiento del Contrato, sin perjuicio de que su seguimiento sea posible con periodicidad menor, mediante otras herramientas que permitan su vigilancia constante.

En la primera semana de cada mes se presentará a la DGSIS la consolidación de los indicadores correspondientes al mes previo y las recomendaciones para el siguiente período derivadas de los niveles alcanzados.

El adjudicatario presentará un informe formal de resultados de la medición de los ANS a la finalización del periodo mensual evaluado y antes del quinto día hábil del mes siguiente al período evaluado.

Dicha información deberá ser obtenida mediante los procedimientos y mecanismos establecidos, y la DGSIS se reserva el derecho de contrastar la información facilitada en cualquier momento durante la ejecución del contrato y sin previo aviso. La DGSIS podrá auditar tanto la información facilitada por el proveedor como su forma de extracción y las herramientas utilizadas. Si como resultado de la auditoría realizada, la DGSIS detectara que no se cumple el ANS, prevalecerá su decisión, y se podrá proceder a la aplicación de la correspondiente penalización.

El ANS inicialmente definidos serán de aplicación desde el momento en que el adjudicatario comience a prestar el servicio.

El incumplimiento de los valores comprometidos en los ANS podrá suponer la aplicación de las penalizaciones contempladas en el PCAP.

La aplicación de estas penalizaciones se concretará en el Comité de Seguimiento del Contrato.



9.3. Acuerdos de nivel de servicio (ANS)

Los Acuerdos de Niveles de Servicio comprenden un conjunto de indicadores orientados a disponer de mecanismos objetivos de medición de la calidad y agilidad en la prestación del servicio, especialmente en aquellos procesos en que se interactúa con el ciudadano y de intercambio de información con la Administración. Esos indicadores tienen como objeto la medición del rendimiento de los sistemas, la disponibilidad de los mismos y su adecuación a la normativa o directrices estratégicas de la Administración.

Los niveles de servicio establecidos como requisitos tienen carácter de mínimos y deberán ser aceptados o mejorados por el licitador. Su medición comenzará en el momento del inicio de la prestación de los servicios del Centro.

Los Niveles de Servicio Mínimos en los sistemas suministrados por el contratista serán los siguientes (la explicación detallada de cada indicador se encuentra en el ANEXO I del presente pliego):

NIVELES DE SERVICIO		
INDICADOR	DESCRIPCIÓN ANS	VALOR PERMITIDO
TMAXRES	Tiempo máximo de respuesta a una consulta, petición, llamada o incidencia	< o = 1 día
TMAXSOL	Tiempo máximo de solución, definitiva o parcial, a una consulta, petición, llamada o incidencia	< o = 3 días
TMAXINF	Tiempo máximo de elaboración de un informe solicitado	< o = 3 días
TMAXSER	Tiempo máximo de respuesta por el staff del adjudicatario a demandas de nuevos servicios, productos o aplicaciones o asesoramiento sobre cualquier materia	< o = 4 días
TMAXSOC	Tiempo máximo de respuesta por el servicio prestado en remoto a través del SOC a demandas de nuevos servicios, productos o aplicaciones o asesoramiento sobre cualquier materia	< o = 4 días
NMAXQUE	Número máximo de quejas mensuales recibidas por los usuarios sobre el servicio o el SOC	1 como máximo
PERIPOR	Período de actualización del Portal de Seguridad o Intranet	2 actualizaciones al mes
PERINEW	Período de actualización de Newsletter	2 meses de plazo medio de actualización



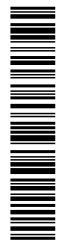
NIVELES DE SERVICIO		
INDICADOR	DESCRIPCIÓN ANS	VALOR PERMITIDO
NFORMAC	Número de peticiones mensuales de formación o concienciación solicitadas sin atender o impartir o con quejas de los usuarios	1 sin agendar o impartir o con quejas
PORINCI	Porcentaje de incidencias de seguridad que no han tenido participación del equipo o del SOC en su resolución	< o = 3% de las ocurridas en el mes
NDIACOB	Días sin cobertura de personal y/o transferencia de conocimiento	< o = 1 día sin cobertura de perfil válido a criterio de la DGSIS
IFR01	Cambio no planificado Jefe proyecto	1 desde inicio prestación servicio
IFR02	Cambio no planificado de Consultor	2 desde inicio prestación servicio
INADE01	Inadecuación al puesto sobrevenida en los 2 primeros meses desde la incorporación	0

El nivel mensual de cumplimiento establecido es el que permite alcanzar el objetivo global para todo el período de contrato. La DGSIS podrá autorizar una planificación de los trabajos en periodos diferentes al mensual, lo que podrá afectar al cumplimiento mensual del servicio, pero siempre manteniendo el cumplimiento global.

10. FASES DEL CONTRATO

Los trabajos se desarrollarán en las fases siguientes:

- **FASE I, periodo de transición:** 30 días naturales a partir de la entrada en vigor del contrato.
 - Transferencia de conocimiento.
 - Constitución del equipo de trabajo, identificación de las tareas inmediatas a realizar y suministro por parte del Director de Proyecto de la DGSIS de toda la información relativa para establecer el marco de trabajo.
 - En este periodo el contratista deberá tomar el total control de todos los servicios prestados por la OSSI, previa realización de un Programa de Trabajo.



- Servicio de monitorización y correlación de eventos de seguridad (Servicio SOC) operativo.
- **FASE II, periodo de ejecución estable:** Desde el final de la Fase I, anterior y hasta dos meses antes de la finalización del contrato.
 - Funcionamiento a pleno rendimiento del equipo de prestación del servicio y desempeño de los servicios citados en el pliego.
 - Se revisará la estructura de la gestión documental de la OSSI, conforme al ENS y a ISO 27001.
 - Adecuación de procedimientos y normativas a los cambios en legislación de la UE, en materia de protección de datos.
 - Se gestionará la renovación de la certificación ISO 27001.
- **FASE III, período de fin:** durante los dos últimos meses se preparará la **transferencia de conocimiento** y actividades para la renovación de los servicios, relación de actividades cerradas y en curso.

11. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde a la DGSIS dirigir y supervisar los trabajos y velar por el cumplimiento de los niveles de servicio acordados. La DGSIS nombrará un Director del servicio de servicio de oficina de seguridad y centro de soporte especializado en el área de seguridad de sistemas y tecnologías de la información (Director OSSI) que será el encargado del seguimiento de la ejecución del contrato. 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 las siguientes:

- Velar por el cumplimiento y el nivel de calidad de los trabajos.
- Planificar y priorizar las actividades del equipo prestador del servicio.
- Supervisar y validar la ejecución de las actividades a realizar.
- Dar conformidad a los resultados finales del servicio.

Es potestad del Director del Proyecto exigir en cualquier momento la adopción de cuantas medidas concretas y eficaces sean necesarias en relación con la prestación del servicio, si a su juicio, la calidad o efectividad del mismo se pone en peligro ante cualquier circunstancia.

Asimismo, es potestad del Director del Proyecto la evaluación de la gravedad de los riesgos e incidencias y la evaluación de los ANS y la aplicación de las correspondientes penalizaciones.

El Director OSSI podrá delegar sus funciones en una persona de su equipo. Así mismo, podrá incorporar al proyecto durante su realización, las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

El contratista designará un Responsable de Proyecto ante la DGSIS, al margen del equipo estable, y perteneciente al equipo directivo de su organización. Este



Responsable se encontrará en permanente contacto con el personal de la DGSIS designado por ésta y realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y supervisar el servicio a prestar e informar al Director del Proyecto de la DGSIS de las posibles incidencias y seguimiento o desviaciones de plazos.
- Mensualmente remitir a la DGSIS un **informe detallado** que permita constatar el cumplimiento de la calidad del servicio prestado, sin menoscabo de que la misma pueda realizar aquellas actuaciones que considere oportuno para contrastar la veracidad de los datos aportados.
- Mensualmente, como mínimo, mantener con la DGSIS una reunión de seguimiento del servicio prestado en el mes previo y validación de la propuesta para el mes siguiente a la misma.

El contratista acatará las políticas de la Consejería de Sanidad y de la Comunidad de Madrid en materia de seguridad.

11.1. Gobierno del contrato

Los servicios solicitados en el presente pliego precisan de un estrecho seguimiento en su ejecución por parte de la DGSIS con objeto de garantizar la correcta ejecución de los mismos.

Para alcanzar el objetivo, se define una estructura de seguimiento del contrato de 2 niveles, que da lugar al establecimiento de Comités diferenciados a 2 ámbitos para el control y la toma de decisiones:

- Nivel estratégico, orientado a la evolución del contrato y mejora de los servicios, que se encarga de velar porque la estrategia y objetivos del contrato estén alineados con los del SERMAS, y garantiza que las decisiones y operaciones se ajustan a dicha estrategia. En este nivel se certifica la recepción de los servicios prestados. Se controla en el Comité de Seguimiento del Contrato (CSC).
- Nivel operativo, ligado a la ejecución concreta de los servicios, y controla los esfuerzos necesarios para su ejecución. Se rige por el Comité Operativo (COP).

Estos comités se establecen al inicio del contrato.

CSC: El Comité de Seguimiento del Contrato se reunirá mensualmente y tendrán lugar en las dependencias de la DGSIS. Se iniciará a partir de la firma del contrato y finalizará con la conclusión del mismo. No obstante, tanto la DGSIS como el adjudicatario podrán convocar reuniones extraordinarias por la existencia de circunstancias que así lo requieran. Obligatoriamente han de asistir figuras directivas por ambas partes con capacidad de decisión suficiente como para adoptar acuerdos y tomar decisiones formales en relación con los servicios prestados por el contratista. Estará formado como mínimo por:

- Contratista: el Responsable del Proyecto y el jefe de Proyecto y otros miembros opcionales.



- DGSIS: la Dirección General de la DGSIS y la Subdirección responsable del Área de Seguridad, así como el Director del proyecto por parte de la DGSIS y otros miembros opcionales.

El CSC deberá realizar al menos las funciones definidas a continuación:

- Monitorizar el avance global de los Servicios y acordar la adopción de propuestas de mejora y medidas correctoras o preventivas que deba desarrollar e implantar el adjudicatario previa autorización de la DGSIS.
- Aprobar las propuestas de adecuación de los servicios a los cambios normativos o estructurales posteriores a la adjudicación de contrato
- Controlar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo y determinar el grado de incumplimiento de los ANS con el objeto de aplicar las correspondientes penalizaciones previstas en los Pliegos.
- Realizar el seguimiento de las acciones que quedaron pendientes del Comité anterior.
- Resolución de situaciones de especial significación surgidas en el servicio y no resueltas a nivel operativo.
- Formalizar la Recepción del Servicio
- Cualquier otro asunto en el ámbito de sus competencias que el propio Comité considere de interés.

Actas: Los acuerdos adoptados en el seno del CSC deberán ser de mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones, las cuales deberán ser expresamente aprobadas por el Director del Proyecto de la DGSIS. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma. Las actas no tendrán validez formal hasta su firma por parte del Director del Proyecto por parte de la DGSIS y del Responsable del Proyecto por parte del adjudicatario.

El Director del Proyecto de DGSIS certificará mensualmente, a partir de los informes aportados, los resultados alcanzados respecto a los ANS.

COP: En cada Comité Operativo la DGSIS toma conocimiento del estado y evolución del servicio a través de la información aportada sobre la actividad desarrollada en el periodo analizado y el seguimiento de los niveles de servicio estipulados. Los COP se celebrarán periódicamente (semanal o quincenalmente) y sus reuniones tendrán lugar en las dependencias de la DGSIS. Se iniciarán en el momento de la formalización del contrato y finalizarán con la conclusión del mismo. No obstante, la DGSIS podrá convocar cuantas reuniones extraordinarias sean necesarias para el seguimiento del servicio.

Obligatoriamente han de asistir figuras por ambas partes con capacidad de decisión suficiente como para adoptar acuerdos y tomar decisiones en relación con los servicios prestados por el adjudicatario, incluyendo siempre al Director del Proyecto por parte de la DGSIS y el Responsable y al Jefe de Proyecto por parte del contratista. En general, se seguirá el trabajo semanal o quincenal de los componentes del equipo de trabajo estable y los obstáculos encontrados.



En el seno de los distintos COP se deberá realizar al menos las funciones definidas a continuación:

- Monitorizar el servicio en el periodo bajo análisis con el fin de asegurar que se alcanzan los niveles de calidad y eficiencia acordados. Seguir y evaluar el progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de riesgos.
- Garantizar que el personal asignado para la ejecución de los servicios por el adjudicatario está disponible y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.
- Analizar y validar si procede las propuestas de mejora del servicio prestado. Proponer al CSC, para su aprobación, las adecuaciones de los servicios contratados a los cambios normativos y estructurales producidos con posterioridad a la adjudicación del contrato, siempre que guarden relación con el objeto del contrato y no supongan un mayor coste para el contratista.
- Cualquier otro asunto en el ámbito de su competencia que el propio Comité considere de interés.

Actas: Los acuerdos alcanzados en los Comités Operativos podrán quedar opcionalmente (según su importancia y lo que se acuerde en el COP) recogidos en un acta o documento de seguimiento y será responsabilidad del proveedor su elaboración y su paso a revisión por los asistentes en las 48 horas siguientes a la finalización de la reunión así como la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión. Estos documentos tendrán validez una vez que DGSIS ratifique su contenido mediante aprobación expresa del Director de Proyecto de la DGSIS.

Informes: para el adecuado seguimiento del servicio, evaluación y mejora continua del grado de calidad del mismo se consideran necesarios los siguientes documentos:

- Informe de ANS.
- Informe de seguimiento del servicio

La entrega mensual de estos informes debe ser a la finalización del periodo mensual evaluado y antes del quinto día hábil del mes siguiente. En caso de ser necesario realizar alguna corrección posterior a la fecha de entrega, se dispondrá de un margen de 2 días hábiles. Cualquier cambio realizado en el informe deberá ser comunicado previamente a DGSIS por correo electrónico. Los informes de seguimiento del servicio son un medio para entender cómo se ha comportado el servicio en el período analizado, contrastar si las previsiones y mejoras se cumplen y verificar la efectividad de las acciones preventivas o correctoras.

En lo relativo a los servicios incluidos en el pliego, los informes deben mostrar información, al menos, sobre los siguientes aspectos: ANS y grado de cumplimiento, riesgos, obstáculos encontrados, avances de cada servicio en el período considerado, retrasos, etc.

11.2. Gestión de riesgos de seguridad

El adjudicatario deberá contar con un proceso de gestión de riesgos de seguridad que deberá seguir todo el personal al que le aplique cualquier tipo de acceso a los datos o a



los sistemas de información del SERMAS independientemente del lugar en el que se presten.

El proceso deberá cumplir las siguientes medidas:

(a) Deberá existir un medio de comunicación de incidencias y un equipo gestor de las mismas, incluyendo un Coordinador de Seguridad (CSG).

(b) Todo el personal asignado al servicio deberá comunicar por el canal establecido cualquier incidencia que se detecte y que tenga relación con la información, los recursos del SERMAS o el servicio que se le presta. La falta de comunicación será considerada como una falta grave en la prestación del servicio y motivará la adopción de todas las medidas necesarias para evitar que ello se vuelva a producir.

(c) Cualquier usuario podrá trasladar al CSG sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que pueda tener relación con la seguridad de la información y las directrices contempladas en las políticas.

(d) Se deberá notificar al CSG cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de información, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.

(e) Todas las actividades relacionadas con la gestión de incidencias, desde su notificación hasta su solución o archivo deberá quedar registrado en un Registro de Incidencias, que estará disponible permanentemente y a disposición de la DGSIS.

El proceso incluirá los siguientes procedimientos:

- ☐ Análisis de la causa de la incidencia.
- ☐ Contención.
- ☐ Implementación de la acción correctiva.
- ☐ Comunicaciones a los afectados.
- ☐ Reporte de la acción a los interlocutores apropiados.

Un posible catálogo de incidencias de seguridad es, al menos, el que se relaciona a continuación:

- **ACCESOS NO AUTORIZADOS:** Esta categoría comprende las siguientes actividades:
 1. Uso compartido, o sospecha, de credenciales de acceso.
 2. Uso, o sospecha, de credenciales de un tercero.
 3. Accesos no autorizados, o sospecha, con o sin daños visibles a los componentes tecnológicos.
 4. Robo de información.
 5. Borrado de información.
 6. Alteración de la información.
 7. Intentos de acceso no autorizado.
 8. Abuso o mal uso de los servicios informáticos internos o externos que requieren autenticación.



- **CÓDIGO MALICIOSO:** Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica. Son parte de esta categoría:
 1. Virus informáticos.
 2. Troyanos.
 3. Gusanos informáticos.
- **DENEGACIÓN DEL SERVICIO:** Esta categoría incluye los eventos que ocasionan la pérdida de un servicio en particular. Los síntomas para determinar una incidencia de esta categoría son:
 1. Tiempos de respuesta muy bajos sin razones aparentes.
 2. Servicios internos inaccesibles, sin razón aparente.
 3. Servicios externos inaccesibles, sin razón aparente.
- **INTENTO DE OBTENCIÓN DE INFORMACIÓN:** Esta categoría agrupa los eventos que buscan obtener información sobre la infraestructura tecnológica. Son parte de esta categoría:
 1. Sniffers.
 2. Detección de Vulnerabilidades.
- **MAL USO DE LOS RECURSOS TECNOLÓGICOS:** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por su mal uso. Son parte de esta categoría:
 1. Mal uso o abuso de servicios informáticos internos o externos.
 2. Uso de la Red de la CSCM para acceso o descarga de datos, ficheros, archivos, etc. no relacionados con el objeto del presente contrato.
 3. Violación de las normas de acceso a internet de la CSCM. Acceso a información englobada o relacionada con cualquiera de estas categorías: pornografía infantil, violencia, incitación al odio, discriminación y violencia racial o de otro tipo, materiales que pueden afectar al desarrollo físico y mental de los menores, así como otras categorías tales como sexo, intolerancia, drogas, pornografía, incitación a la comisión de delitos y cualesquiera otros que pudieran no ser necesarios para la prestación de los servicios que son objeto del presente contrato.
 4. Mal uso del correo electrónico de la empresa que pudiera tener un impacto en los usuarios y sistemas de información de la CSCM.
 5. Violación de las normas, políticas y procedimientos de seguridad.

El adjudicatario deberá poner a disposición de la DGSIS, con periodicidad mensual, un informe de incidencias de seguridad relacionados con el servicio prestado, detallando la información asociada a cada uno de las incidencias que se recoja en el registro habilitado en el ámbito de la prestación del servicio.



12. CONDICIONES GENERALES

12.1. Propiedad de los trabajos

Todos los documentos, productos y demás entregables resultantes de la ejecución del presente contrato serán propiedad de la DGSIS, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera 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 DGSIS.

12.2. Calidad de los trabajos

Los estándares de calidad de servicio a prestar serán evaluados mensualmente, al menos a través de los indicadores reflejados en el apartado **9.3 Acuerdos de nivel de servicio**. No obstante lo anterior, durante el desarrollo de los trabajos, la DGSIS podrá establecer controles de calidad y acciones de aseguramiento de la calidad de la actividad desarrollada.

En cualquier caso, el adjudicatario deberá proponer las mejoras de calidad que estime oportunas para optimizar la actividad desarrollada durante el tiempo de ejecución del presente contrato.

12.3. Normativa de seguridad y protección de datos

En el caso de que el Adjudicatario, en el ejercicio de la prestación del servicio, tuviera que tratar con datos de carácter personal de la CSCM por razón de la prestación del servicio, cumplirá con la legislación vigente en materia de protección de datos de carácter personal que resulte de aplicación, en concreto 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos RGPD); la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal; así como las disposiciones de desarrollo de las normas anteriores o cualesquiera otras aplicables en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

Así, y a los efectos de este contrato, las Direcciones, organismos, entidades o entes de derecho público de la CSCM tendrán la consideración de Responsable del tratamiento y el



Adjudicatario tendrá la consideración de Encargado del Tratamiento conforme a lo establecido en los artículos 28 y 29 en el RGPD.

Encargado del Tratamiento.

El Adjudicatario o Encargado del Tratamiento se compromete a cumplir las medidas y requisitos de seguridad exigidos por la CSCM. El coste de las actuaciones de cualquier tipo, derivadas del cumplimiento de RGPD y normativa relacionada, serán por cuenta del Adjudicatario.

El tratamiento de datos de carácter personal por el Adjudicatario, se regirá por un contrato o acto jurídico análogo, donde se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, así como el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Las obligaciones derivadas de ésta responsabilidad asumida por el Encargado del Tratamiento, serán recogidas en un documento específico que será firmado por la CSCM y el contratista de forma previa al inicio de los trabajos, y que figura como Anexo al Pliego de Cláusulas Administrativas Particulares.

Limitación del acceso o tratamiento.

El Adjudicatario limitará el acceso o tratamiento de datos de carácter personal pertenecientes a los ficheros bajo titularidad de cualquiera de las Direcciones, organismos, entidades o entes de derecho público de la CSCM, limitándose a realizar el citado acceso o tratamiento cuando se requiera imprescindiblemente para la prestación del servicio y/o de las obligaciones contraídas, y en todo caso limitándose a los datos que resulten estrictamente necesarios.

Medidas de Seguridad.

A los efectos de la prestación del servicio por parte del Adjudicatario, en su calidad de Encargado del Tratamiento quedará obligado, con carácter general, por el deber de confidencialidad y seguridad de los datos de carácter personal (y de otros datos de carácter confidencial la CSCM que puedan tratarse). Y con carácter específico, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, en especial:

- El Adjudicatario y el personal encargado de la realización de las tareas guardarán y asegurarán la confidencialidad, disponibilidad e integridad sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, no revelando, transfiriendo o cediendo, ya sea verbalmente o por escrito, a cuantos datos conozcan como consecuencia de la prestación del servicio sanitario, sin límite temporal alguno.
- El Adjudicatario, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, atendiendo en especial, a los artículos 28, 29, 30 y 32 del RGPD.
- El Adjudicatario utilizará los datos de carácter personal única y exclusivamente, en el marco y para las finalidades determinadas en el objeto del servicio adjudicado y del presente documento, y bajo las instrucciones del Responsable del Tratamiento, y de la Dirección General de Sistemas de Información Sanitaria



del Servicio Madrileño de Salud, perteneciente al SERMAS, para aquellos aspectos relacionados con sus competencias.

- Accederá a los datos de carácter personal responsabilidad del Responsable del Tratamiento únicamente cuando sea imprescindible para el buen desarrollo de los servicios para los que ha sido contratado.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, el Encargado del Tratamiento deberá seguir los procedimientos e instrucciones que reciba del Responsable del Tratamiento, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.
- Si el Encargado del Tratamiento considera que alguna de las instrucciones del Responsable del Tratamiento infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al Responsable del Tratamiento.
- En caso de estar obligado a ello por el artículo 30 del RGPD, el Encargado del Tratamiento mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del Responsable del Tratamiento, que contenga la información exigida por el artículo 30.2 del RGPD.
- Garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- Dará apoyo al Responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dará apoyo al Responsable del Tratamiento en la realización de las consultas previas a la Autoridad de Control, cuando proceda.
- Pondrá a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen al Responsable del Tratamiento u otro auditor autorizado por este.
- En caso de estar obligado a ello por el artículo 37.1 del RGPD, designará un delegado de protección de datos y comunicará su identidad y datos de contacto al Responsable del Tratamiento, cumpliendo con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD.
- En caso de que el Encargado del Tratamiento deba transferir o permitir acceso a datos personales responsabilidad del Responsable del Tratamiento a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable del Tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.
- Se prohíbe el tratamiento de datos por terceras entidades que se encuentren en terceros países sin un nivel de protección equiparable al otorgado por la normativa de protección de datos de carácter personal vigente en España, salvo



que se obtenga la preceptiva autorización de la Agencia Española de Protección de Datos para transferencias internacionales de datos, de conformidad con los artículos 44, 45, 46, 47, 48, y 49 del RGPD.

- El Adjudicatario comunicará y hará cumplir a sus empleados, y a cualquier persona con acceso a los datos de carácter personal, las obligaciones establecidas en los apartados anteriores, especialmente las relativas al deber de secreto y medidas de seguridad.
- El Adjudicatario no podrá realizar copias, volcados o cualesquiera otras operaciones de conservación de datos, con finalidades distintas de las establecidas en el servicio adjudicado, sobre los datos de carácter personal a los que pueda tener acceso en su condición de Encargado del Tratamiento, salvo autorización expresa del Responsable del Tratamiento o de la Dirección General de Sistemas de Información Sanitaria del SERMAS.
- Adoptar y aplicar las medidas de seguridad estipuladas en el presente contrato, conforme lo previsto en el artículo 32 del RGPD, que garanticen la seguridad de los datos de carácter personal responsabilidad del Responsable del Tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
- El Adjudicatario se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanen, para lo cual programará las acciones formativas necesarias. Así mismo, el Adjudicatario tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El Adjudicatario comunicará al Responsable del Tratamiento y a la Dirección General de Sistemas de Información Sanitaria del SERMAS, para aquellos aspectos relacionados con sus competencias, de forma inmediata, cualquier incidencia en los sistemas de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la alteración, la pérdida o el acceso a datos de carácter personal, o la puesta en conocimiento por parte de terceros no autorizados de información confidencial obtenida durante la prestación del servicio.
- El Adjudicatario estará sujeto a las mismas condiciones y obligaciones descritas previamente en el presente documento, con respecto al acceso y tratamiento de cualesquiera documentos, datos, normas y procedimientos pertenecientes a la CSCM a los que pueda tener acceso en el transcurso de la prestación del servicio.
- Los diseños y desarrollos de software deberán, observar con carácter general, la normativa de seguridad de la información y de protección de datos de la Comunidad de Madrid y:



- En todo caso observarán los requerimientos relativos a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
- En ningún caso el equipo prestador del servicio objeto del contrato tendrá acceso ni realizará tratamiento de datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.

Destino de los datos al finalizar la prestación del servicio.

Una vez cumplida o resuelta la relación contractual acordada entre el Responsable del Tratamiento y el Encargado del Tratamiento, el Encargado del Tratamiento deberá solicitar al Responsable del Tratamiento instrucciones precisas sobre el destino de los datos de carácter personal de su responsabilidad, pudiendo elegir éste último entre su devolución, remisión a otro prestador de servicios o destrucción íntegra, siempre que no exista previsión legal que exija la conservación de los datos, en cuyo caso no podrá procederse a su destrucción.

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 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 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 subencargada, 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 subencargado, también está obligado a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el Responsable del Tratamiento.
- Corresponde al Encargado del Tratamiento exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.
- El Encargado del Tratamiento seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.

Responsabilidad en caso de incumplimiento.



El Encargado del Tratamiento 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.

Cesión del contrato.

El Adjudicatario no podrá ceder total o parcialmente, los derechos y obligaciones que se deriven del contrato sin autorización expresa escrita de la DGSIS, 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.

13. CONTENIDO DE LAS OFERTAS

Los licitadores deberán aceptar explícitamente en su propuesta, la totalidad de las cláusulas recogidas en los pliegos. Además deberán describir las peculiaridades de cada propuesta para que pueda ser valorada.

Las ofertas serán presentadas tanto en formato tradicional en papel, como en formato electrónico (DVD, USB...). La oferta técnica deberá recoger en su globalidad, los apartados del siguiente modelo propuesto, con independencia de que el licitador pueda hacer llegar adicionalmente cuanta información complementaria considere de interés. En base al contenido requerido, no se estima necesaria una extensión superior a 80 páginas.

Las mejoras para la valoración de los criterios de valoración, deberán incluirse en el sobre que se especifica para cada una más adelante, el resto de la documentación de la oferta se incluirá en el sobre 2-A.

0. ÍNDICE

1. RESUMEN EJECUTIVO

Resumen del contenido de la propuesta, resaltando lo que el licitador considere más importante.

2. MODELO DE SERVICIO

EL contratista deberá presentar una oferta que contemple las interacciones entre las distintas unidades que se mencionan, con las particularizaciones precisas para atender las características del SERMAS, y que contenga un plan para el despliegue de los servicios ofertados.

En la oferta se incluirá una descripción de las tareas a desarrollar, en términos ajustados al presente pliego, los recursos materiales disponibles para la ejecución del contrato así como la composición de los equipos de trabajo ofertados y cualquier otra circunstancia que incida en la ejecución de los trabajos, en los siguientes apartados:

2.1 Planteamiento general

Planteamiento general para la prestación del servicio solicitado, describiendo la visión del adjudicatario sobre el servicio a realizar en base a su conocimiento y/o experiencia en trabajos similares y el retorno y beneficios que recibirá la SERMAS. Modelo de ejecución y gestión del contrato.



Organización del servicio, describiendo en detalle el modelo de trabajo propuesto y el grado de involucración/participación del personal del SERMAS.

2.2 Modelo global

Descripción de la organización del equipo de prestación del servicio, distribución de responsabilidades y tareas, coordinación, dedicación al proyecto, flujos de comunicación, mecanismos de control, servicio de monitorización y correlación de eventos de seguridad (Servicio SOC) en relación con su adecuación a las necesidades y objetivos del proyecto. En su caso, propuestas que especifiquen mecanismos que permitan absorber nuevos requisitos.

2.3 Planteamiento específico por fases

Planteamiento para cada una de las fases de los servicios a prestar: descripción funcional, operativa y de relación, de acuerdo con los requisitos de la cláusula 10 Fases del Contrato, del presente pliego. Se podrán incluir propuestas concretas de mejoras en las fases de planificación y transferencia inicial, para una mejor consecución de los objetivos del servicio. Las empresas licitadoras independientemente de los acuerdos de nivel de servicio del presente pliego, presentarán un compromiso de hitos y plazos de despliegue comprometidos.

La información aportada deberá incluir:

- Ejecución de actividades al inicio del proyecto
- Procedimiento y metodología propuestos para el servicio de Gestión y Soporte Especializado en seguridad a proyectos tecnológicos de nueva creación y para sistemas en producción.
- Propuesta de cuadro de mando para el seguimiento del servicio de Gestión y Soporte Especializado en Seguridad. Niveles de servicio.
- Plan de devolución del servicio a la finalización del contrato para garantizar la transferencia del servicio a un eventual nuevo proveedor, sin impactar en los niveles del servicio prestado.

3. ASEGURAMIENTO DE LA CALIDAD

El licitador deberá describir en su oferta su propuesta de modelo de Aseguramiento de la Calidad y la Seguridad y la forma en que lo aplicará al servicio.

4. ASPECTOS RELATIVOS A SOPORTE DE SEGURIDAD

Se incluirán las propuestas relativas al soporte a usuarios incluidos en el modelo de relación. En particular, lo relativo a propuestas que detallen la integración y coordinación funcional y técnica con las unidades del SERMAS afectadas por el servicio, en especial con el servicio de gestión y administración de Centros de Proceso de Datos.

Planificación detallada de los trabajos a realizar desglosando tareas e hitos a cumplir.



5. SEGURIDAD DE LA INFORMACIÓN. MEDIDAS DE PROTECCIÓN DE DATOS PERSONALES Y DOCUMENTACIÓN

Los licitador/es aportarán en su oferta una memoria descriptiva de las medidas que adoptarán para asegurar la confidencialidad, disponibilidad e integridad de los datos manejados y de la documentación facilitada. Como se requiere el acceso a datos clínicos, se puntualizarán todas aquellas medidas, tanto técnicas como organizativas que aseguren la confidencialidad y las de registro que permita un completo seguimiento de la integridad de la información. Se podrá incluir un Plan de Seguridad general aplicable al servicio, herramientas informáticas para controlar la posibilidad de acceso a la información por parte de los técnicos de la empresa, herramientas que faciliten la obtención de información relativa a los accesos y actuaciones realizadas sobre los datos, así como medidas técnicas para preservar la seguridad de la información en actuaciones y accesos remotos.

6. CRITERIOS DE VALORACIÓN

Los licitadores podrán aportar una serie de mejoras a través de los criterios de valoración especificados en el del Pliego de Cláusulas Administrativas:

- Propuesta y enfoque metodológico para la gestión de la Oficina de Seguridad **(se incluirá en el sobre 2-A de la documentación)**: documentación detallada de dicha metodología y el enfoque y adaptación de dicha metodología a las particularidades del SERMAS. Se valorará la metodología global, las diferentes fases y para cada una de las líneas de trabajo y servicios, así como el plan general de aseguramiento de la calidad y de continuidad del servicio y posible mejora los tiempos de despliegue de los servicios requeridos
- Servicios anuales adicionales encuadrados dentro del Centro de Operaciones de Seguridad (SOC). Servicios adicionales que supongan mejoras que sean consideradas de interés por el SERMAS, para la mejor prestación del servicio **(se incluirá en el sobre 2-A de la documentación)**: servicio de análisis dinámico de aplicaciones, servicio de análisis forense de aplicaciones e incidentes de seguridad, servicio de vigilancia (footprinting) en redes sociales, servicio de análisis de malware y otros servicios de interés.
- Acreditación del Centro de Operaciones de Seguridad (Servicio SOC), de monitorización y correlación de eventos de seguridad **(se incluirá en el sobre 2-B de la documentación)**, Aportación de certificado expedido por la Universidad Carnegie Mellon, o/y aportación de certificado de adscripción a un CERT certificado por la Universidad Carnegie Mellon y/o aportación de certificado perteneciente a red FIRST.
- Oferta anual de jornadas de consultores especialistas en materia de análisis de riesgos y cumplimiento del RGPD, efectuadas por personal distinto al incluido en la oferta de forma presencial durante todo el contrato, **(se incluirá**



en el sobre 2-B de la documentación). Dicho personal tendrá la capacitación siguiente: Titulación universitaria de nivel 2, con al menos 2 años de experiencia en proyectos de cumplimiento normativo y conocimientos demostrables de la nueva legislación europea (RGPD y directiva NIST)

- Dotación de infraestructura de SW y HW adicional a la establecida como obligatoria en el pliego (**se incluirá en el sobre 2-B de la documentación**). Herramientas adicionales para análisis de software, sondas o dispositivos similares adicionales, con soporte y mantenimiento incluidos

Madrid,
DIRECTOR GENERAL DE SISTEMAS
DE INFORMACIÓN SANITARIA

Fdo: Jose Antonio Alonso Arranz



14. ANEXO I-FICHAS DE ANS

Para cada uno de los indicadores, se define y describe por prioridades, se proporciona su objetivo, se nombra al responsable de su medición y la fuente de información que usará, la métrica que se utiliza y la periodicidad de análisis.

14.1. Indicador 1. TMAXRES

Indicador: TMAXRES.

Título: tiempo máximo de respuesta a peticiones o incidencias.

Objetivo: reducir el tiempo de respuesta de la OSSI ante consultas, peticiones o incidencias gestionadas por el proveedor de forma que se minimicen los tiempos de espera de los usuarios.

Descripción: Indicador de la eficacia en la respuesta a las llamadas y peticiones remitidas por los usuarios, utilizando el tiempo máximo transcurrido desde que el usuario ha reportado su incidencia o petición hasta que ha sido respondido por la OSSI en función de la prioridad, al menos acusando recibo de la petición aunque no se proporcione aún la solución. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como definición y seguimiento.

Niveles de servicio: Se distinguirá según prioridades:

Todas las prioridades: TMAXRES debe ser como máximo de 1 día.

Periodicidad mínima de análisis: mensual.

Métricas: Para cada petición, consulta, incidencia o llamada:

Tiempo respuesta= [Fecha-hora petición]-[Fecha-hora respuesta OSSI].

Tiempo respuesta = < o = Tiempo reflejado en ANS.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en correos, llamadas, etc.

14.2. Indicador 2. TMAXSOL

Indicador: TMAXSOL.

Título: tiempo máximo de solución, definitiva o parcial, a peticiones o incidencias.

Objetivo: reducir el tiempo de solución, al menos parcial, de la OSSI ante consultas, peticiones o incidencias gestionadas por el proveedor de forma que se minimicen los tiempos de espera de los usuarios.

Descripción: Indicador de la eficacia en la respuesta a las llamadas y peticiones remitidas por los usuarios, utilizando el tiempo máximo transcurrido desde que el usuario ha reportado su incidencia o petición hasta que ha sido respondido por la OSSI en



función de la prioridad, al menos proporcionando una solución parcial. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como definición y seguimiento.

Niveles de servicio: Se distinguirá según prioridades:

Todas las prioridades: TMAXSOL debe ser como máximo de 3 días.

Periodicidad mínima de análisis: mensual.

Métricas: Para cada petición, consulta, incidencia o llamada:

Tiempo solución=[Fecha-hora petición]-[Fecha-hora solución parcial o definitiva OSSI].

Tiempo solución = < o = Tiempo reflejado en ANS.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en correos, llamadas, etc.

14.3. Indicador 3. TMAXINF

Indicador: TMAXINF.

Título: tiempo máximo de elaboración de informes.

Objetivo: reducir el tiempo de respuesta de la OSSI ante peticiones de informes o estudios de forma que se minimicen los tiempos de espera de los usuarios.

Descripción: Indicador de la eficacia en la elaboración de informes o estudios solicitados por el director de Proyecto DGSIS o por los usuarios, siempre bajo la dirección de aquél, utilizando el tiempo máximo transcurrido desde que el director ha solicitado el informe hasta que ha sido elaborada una primera versión aceptable del mismo por la OSSI en función de la prioridad. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como definición y seguimiento, y en ocasiones, como medición.

Niveles de servicio: Se distinguirá según prioridades:

Todas las prioridades: TMAXINF debe ser como máximo de 3 días.

Periodicidad mínima de análisis: mensual.

Métricas: Para cada petición de informe:

Tiempo informe=[Fecha-hora petición]-[Fecha-hora elaboración informe OSSI].

Tiempo informe = < o = Tiempo reflejado en ANS.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en correos, llamadas, actas de reuniones internas, etc.

14.4. Indicador 4. TMAXSER

Indicador: TMAXSER.

Título: tiempo máximo de respuesta del *staff*.



Objetivo: reducir el tiempo de espera en la DGSIS ante peticiones de nuevos servicios, productos o asesoramiento sobre materia de seguridad de forma que se minimicen los tiempos de espera y se mejore el servicio y el asesoramiento a los usuarios.

Descripción: tiempo máximo de respuesta por el *staff* del adjudicatario a demandas de nuevos servicios, productos o aplicaciones o asesoramiento comercial o técnico sobre cualquier materia relacionada con la seguridad. Será el director del Proyecto DGSIS quien solicitará dicho asesoramiento, utilizando el tiempo máximo transcurrido desde que el director lo ha solicitado hasta que ha sido elaborada una respuesta aceptable por el *staff* del adjudicatario. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como definición y seguimiento, y en ocasiones, como medición.

Niveles de servicio: Se distinguirá según prioridades:

Todas las prioridades: TMAXSER debe ser como máximo de 4 días.

Periodicidad mínima de análisis: mensual.

Métricas: Para cada petición de asesoramiento o servicio:

Tiempo espera=[Fecha-hora petición]-[Fecha-hora respuesta del *staff*].

Tiempo espera = < o = Tiempo reflejado en ANS.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en correos, llamadas, actas de reuniones internas, etc.

14.5. Indicador 5. TMAXSOC

Indicador: TMAXSOC.

Título: tiempo máximo de respuesta del servicio remoto del SOC a demandas de nuevos servicios o asesoramiento.

Objetivo: reducir el tiempo de espera en la DGSIS ante peticiones de nuevos servicios, productos, aplicaciones o asesoramiento sobre cualquier materia, que tenga que ver con el servicio remoto que presta el SOC, de forma que se minimicen los tiempos de espera y se mejore el servicio y el asesoramiento a los usuarios.

Descripción: tiempo máximo de respuesta en el servicio remoto del SOC del adjudicatario a demandas de nuevos servicios, productos o aplicaciones o asesoramiento comercial o técnico sobre cualquier materia. Será el director del Proyecto DGSIS quien pedirá dicho asesoramiento, servicio o aplicación, utilizando el tiempo máximo transcurrido desde que el director lo ha solicitado hasta que ha sido elaborada una respuesta aceptable a través del SOC del adjudicatario. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como definición y seguimiento, y en ocasiones, como medición.

Niveles de servicio: Se distinguirá según prioridades:

Todas las prioridades: TMAXSOC debe ser como máximo de 4 días.

Periodicidad mínima de análisis: mensual.



Métricas: Para cada petición de asesoramiento o servicio:

Tiempo espera SOC=[Fecha-hora petición]-[Fecha-hora respuesta del SOC].

Tiempo espera SOC= < o =Tiempo reflejado en ANS.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en correos, llamadas, actas de reuniones internas, etc.

14.6. Indicador 6. NMAXQUE

Indicador: NMAXQUE.

Título: número máximo de quejas recibidas por el servicio.

Objetivo: medir la calidad del servicio prestado, aumentando el grado de satisfacción de los usuarios del mismo.

Descripción: número máximo de quejas admisibles de los usuarios motivadas por el servicio, debidamente comunicadas. Se considera incluido el equipo presencial del adjudicatario, así como el equipo del SOC. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable del cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

Todas las criticidades: TMAXQUE debe ser igual o inferior a 1

Periodicidad mínima de análisis: mensual.

Métricas: Para cada período considerado:

Nº de quejas=[Nº quejas en el período].

Nº de quejas =< o = Nº máximo de quejas.

Fuente de información: Comunicaciones de usuarios en correos, llamadas, etc.

Fuente de información: Comunicaciones de rotaciones efectuadas por el proveedor.

14.7. Indicador 8. PERIPOR

Indicador: PERIPOR.

Título: período de actualización del Portal de Seguridad.

Objetivo: aumentar el grado de servicio útil a los usuarios, manteniendo un nivel adecuado de actualización de las informaciones sensibles para ellos.

Descripción: número de semanas que pasan sin efectuar actualizaciones de la información del Portal de Seguridad y de la Intranet que el equipo de la OSSI realiza en el período considerado. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

PERIPOR debe ser igual o inferior a 2 semanas.



Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Período de actualización=[Nº de semanas sin actualizaciones del Portal en el período].

Período sin actualización= < o = Período mínimo exigido.

Fuente de información: Sistema interno SGSSI y muestreo de tomas de datos manuales en la Intranet y Portal de Seguridad.

14.8. Indicador 9. PERINEW

Indicador: PERINEW.

Título: período de actualización de la Newsletter.

Objetivo: aumentar el grado de servicio útil a los usuarios, proporcionando con fluidez un nivel adecuado de información provechosa para ellos.

Descripción: período entre publicaciones de dos ediciones sucesivas de la Newsletter que el equipo de la OSSI realiza. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

PERINEW debe ser igual o inferior a 2 meses.

Periodicidad mínima de análisis: bimensual.

Métricas: En el período considerado:

Período de newsletter=[Tiempo entre ediciones sucesivas de Newsletter].

Período de newsletter= < o = Período máximo exigido.

Fuente de información: Sistema interno SGSSI.

14.9. Indicador 10. NFORMAC

Indicador: NFORMAC.

Título: número de peticiones de formación sin impartir en el período considerado.

Objetivo: medir la calidad percibida de la actividad del equipo del proveedor que logra subir el nivel de formación y concienciación de los usuarios respecto a los aspectos de seguridad.

Descripción: número de peticiones de formación o concienciación solicitadas por los usuarios que se han quedado sin atender o impartir, o ni siquiera planificadas con el usuario, o cuyo desarrollo ha sido deficiente, ocasionando alguna queja del usuario. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:



NFORMAC debe ser igual o inferior a 1.

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Nº peticiones =[Nº de peticiones no atendidas].

Nº peticiones = Nº máximo exigido.

Fuente de información: Sistema interno SGSSI y muestreos manuales en comunicaciones de usuarios.

14.10. Indicador 11. PORINCI

Indicador: PORINCI.

Título: porcentaje de incidencias de seguridad que no han tenido participación del equipo de la OSSI o del SOC en su resolución

Objetivo: aumentar la calidad del servicio dado, midiendo la influencia e importancia de la OSSI en la seguridad percibida en el SERMAS. Cumplir con la responsabilidad del seguimiento de las incidencias con el objetivo de mejorar la satisfacción del usuario de forma que se reduzca el tiempo de resolución, al hacer más eficiente la gestión.

Descripción: porcentaje de incidencias de seguridad ocurridos y comunicados a la OSSI, en los que para cuya solución o cierre no ha contribuido el equipo del proveedor, sea presencial o a través del SOC. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

PORINCI debe ser menor o igual al 3%

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Porcentaje de incidencias =[Nº incidencias sin participación OSSI]x100/[Nº incidencias seg].

Porcentaje de incidencias sin participación =< o = Porcentaje mínimo exigido.

Fuente de información: Sistema interno SGSSI y muestreos manuales en comunicaciones de usuarios.

14.11. Indicador 12. NDIACOB

Indicador: NDIACOB.

Título: Días sin cobertura de personal y transferencia de conocimiento.

Objetivo: consolidar el equipo de trabajo y garantizar la transferencia de conocimiento del servicio, minimizando el tiempo sin el equipo del proveedor completo, planificando las salidas y entradas de personal y asegurando los solapamientos entre el personal.



Descripción: número de días laborables sin cobertura de los perfiles exigidos a criterio de la DGSIS, debido a rotaciones no planificadas e incumplimiento de los solapes exigidos. La DGSIS podrá efectuar auditorías periódicas sin previo aviso.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable del cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: No se distinguirá según criticidad del caso de incumplimiento, siendo siempre grave:

NDIACOB es igual máximo un día

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Días sin cobertura=[Nº de rotaciones no planificadas en el período].

Días sin cobertura = Días máximos sin cobertura.

Fuente de información: Comunicaciones de rotaciones efectuadas por el proveedor y ausencias detectadas por la DGSIS.

14.12. Indicador 12. IFR01

Indicador: IFR01.

Título: Numero de rotaciones no planificadas del jefe de proyecto

Objetivo: aumentar la calidad del servicio dado, midiendo la influencia e importancia de la OSSI en la seguridad percibida en la CSCM.

Descripción: Numero de cambios no planificados desde el inicio de la prestación del servicio del jefe de proyecto.

Responsable del indicador: Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

IFR01 debe ser menor o igual a 1

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Penalización = **A*Σ PI**

Dónde:

A es el importe correspondiente a la cantidad económica mensual que resulta de repartir el importe total de la adjudicación del presente pliego entre todos los meses del mismo, es decir:

A = Importe económico de adjudicación del presente pliego / 48 meses (sin IVA)

PI es el % de penalización aplicable a cada incumplimiento de este apartado.



14.13. Indicador 13. IFR02

Indicador: IFR02.

Título: Numero de rotaciones no planificadas de consultor

Objetivo: aumentar la calidad del servicio dado, midiendo la influencia e importancia de la OSSI en la seguridad percibida en la CSCM.

Descripción: Numero de cambios no planificados desde el inicio de la prestación del servicio del jefe de proyecto.

Responsable del indicador: Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

IFR02 debe ser menor o igual a 2

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

Penalización = $A \cdot \Sigma PI$

Dónde:

A es el importe correspondiente a la cantidad económica mensual que resulta de repartir el importe total de la adjudicación del presente pliego entre todos los meses del mismo, es decir:

$A = \text{Importe económico de adjudicación del presente pliego} / 48 \text{ meses (sin IVA)}$

PI es el % de penalización aplicable a cada incumplimiento de este apartado.

14.14. Indicador 14. INADE01

Indicador: INADE01

Título: inadecuación al puesto sobrevenida en los 2 primeros meses desde la incorporación

Objetivo: aumentar la calidad del servicio dado, midiendo la influencia e importancia de la OSSI en la seguridad percibida en la CSCM. Cumplir con la responsabilidad del seguimiento de las incidencias, al hacer más eficiente la gestión.

Descripción: inadecuación al puesto asignado, sobrevenida durante los dos primeros meses desde la incorporación.

Responsable del indicador: Responsable del equipo del proveedor en la OSSI, como responsable de la medición y cumplimiento. Responsable de la DGSIS, como responsable de la definición, medición y seguimiento.

Niveles de servicio: En caso de incumplimiento:

INADE01 no hay valor permitido

Periodicidad mínima de análisis: mensual.

Métricas: En el período considerado:

