MINISTERIO
DE SANIDAD

DIRECCIÓN GENERAL DE SALUD DIGITAL Y SISTEMAS
DE INFORMACIÓN PARA EL SNS

SUBDIRECCIÓN GENERAL DE INFRAESTRUCTURA
TECNOLÓGICA SANITARIA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS DE ASISTENCIA TÉCNICA PARA LA ADMINISTRACIÓN Y OPERACIÓN DE LA INFRAESTRUCTURA DE SOPORTE TIC DEL MINISTERIO DE SANIDAD

PASEO DEL PRADO, 18-20
28071 MADRID
TEL.: 91 596 12 60
sgits@sanidad.gob.es

TABLA DE CONTENIDO

1. INTRODUCCIÓN Y ALCANCE DEL CONTRATO

El contrato tiene como objetivo **la contratación de servicios de Asistencia Técnica especializada para la Administración y Operación de diversas plataformas que sirven de soporte a la infraestructura TIC del Ministerio de Sanidad.** La administración de estas infraestructuras es responsabilidad de la Subdirección General de Infraestructura Tecnológica Sanitaria (SGITS) del Ministerio de Sanidad.

El contrato se estructurará en tres lotes:

- Lote 1: Administración y Operación de la plataforma de Seguridad.
- Lote 2: Administración y Operación de la plataforma de gestión de servicios TI.
- Lote 3: Administración y Operación de la plataforma de Monitorización.

Estas plataformas e infraestructuras dan soporte directa o indirectamente a aplicaciones y/o servicios críticos del Ministerio y del Sistema Nacional de Salud.

2. CONDICIONES GENERALES Y GESTIÓN DEL SERVICIO

La empresa adjudicataria establecerá todos los mecanismos necesarios para la planificación, puesta en marcha, ejecución, seguimiento y finalización del servicio, corriendo de su cuenta todos los gastos generados.

La organización y dirección de los trabajos se llevará a cabo por un Comité de seguimiento, con función ejecutiva, encargado de realizar el control de los mismos. Este comité estará integrado por el Gestor del Servicio de la empresa adjudicataria y representantes de la SGITS, uno de los cuales actuará como Director Técnico.

Corresponde al Director Técnico de cada lote la supervisión y dirección de los trabajos, proponer las modificaciones que convenga introducir o, en su caso, proponer la suspensión de los trabajos si existiese causa suficientemente motivada.

Las funciones del Director Técnico en relación con los trabajos a realizar serán las siguientes:

- Velar por el cumplimiento de los trabajos exigidos y ofertados.
- Emitir las certificaciones parciales de recepción de los mismos.

El Director Técnico podrá delegar sus funciones en una o varias personas de su equipo.

Asimismo, podrá incorporar al proyecto, durante su realización, a las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

La oferta de la empresa podrá incluir aportación de personal dedicado a la coordinación de los efectivos asignados al lote, y de apoyo a la dirección de los trabajos, como prestación complementaria a las exigidas en este pliego, sin coste alguno para la Administración.

Cada mes, el Gestor del Servicio de la empresa adjudicataria de cada lote remitirá al Director Técnico un informe de ejecución del lote en el que se detallará, para cada perfil, las jornadas dedicadas a la ejecución del servicio y los trabajos realizados con detalle diario. El plazo máximo de entrega de estos informes será de 10 días naturales desde la finalización del mes correspondiente.

Se entregará también, con periodicidad trimestral, un informe consolidado y resumido que combine los informes mensuales de todos los perfiles.

El seguimiento y control del servicio se realizará sobre las siguientes bases:

- Se realizará un seguimiento continuo de los trabajos realizados por parte del Director Técnico de la SGITS y del Gestor del Servicio de la empresa, así como sus equipos respectivos.
- Adicionalmente se llevarán a cabo reuniones de seguimiento cuando se considere oportuno por cualquiera de las partes, en las que se revisará el grado de cumplimiento del servicio a las condiciones estipuladas en el presente pliego.
- Durante estas revisiones técnicas, el Director Técnico podrá rechazar en todo o en parte los trabajos realizados, en la medida en que no respondan a lo estipulado en el presente pliego o no superasen los controles de calidad. En estos casos se levantará acta de la reunión.

3. DESCRIPCIÓN DE LOS SERVICIOS A PRESTAR

3.1. Lote 1: Administración y Operación de la plataforma de Seguridad.

Los principales servicios y tareas a llevar a cabo por el personal técnico de la empresa adjudicataria serán, entre otros, los siguientes:

- Gestión y resolución de Incidentes de seguridad en el Ministerio reportados por Sondas SAT-INET, SAT-SARA, LUCÍA, GLORIA y servicio del Centro de Operaciones de Ciberseguridad de la AGE utilizando las herramientas LUCÍA, GLORIA, GrayLog.

- Gestión y realización de auditorías de infraestructuras utilizando herramientas de auditoría como Nessus, Burp, etc. Integración con herramientas de auditoría continua del CCN (ANA, entre otras).

- Gestión y realización de auditorías de caja negra y caja gris sobre sistemas y aplicaciones del Ministerio basadas en la metodología OWASP.

- Gestión, seguimiento y resolución de vulnerabilidades detectadas en Sistemas del Ministerio.

- Gestión y mantenimiento de autorizaciones de software para instalar en puestos de trabajo. Análisis de software con herramientas sandboxing (MARTA CCN).

- Gestión y mantenimiento de autorizaciones de navegaciones web permitidos/prohibidos desde el Ministerio a través de su ProxyWeb.

- Elaboración de Instrucciones Técnicas de Seguridad y revisión de Instrucciones Técnicas de Seguridad del área de Infraestructuras del Ministerio.

- Elaboración de informes y análisis técnicos sobre cualquier tema relacionado con la ciberseguridad del Ministerio de Sanidad.

- Realización de integraciones de sistemas, dispositivos de comunicaciones y sistemas de seguridad del Ministerio con el SIEM (LogICA) del Ministerio y con el SIEM del COCs de la AGE (GLORIA).

- Resolución de consultas sobre seguridad técnica para el Ministerio.

- Realización de Análisis de Riesgos ENS/RGPD sobre la herramienta PILAR del CCN-CERT.

- Asistencia para la confección de Valoraciones ENS de Sistemas del Ministerio.

- Realización de Business Impact Analysis de servicios del Ministerio.

- Realización de Planes de Continuidad de servicios del Ministerio.

- Gestión, mantenimiento, realización y revisión de Política de seguridad, Normas y Procedimientos del Sistema de Gestión de la Seguridad de la Información del Ministerio.
- Realización de Autoevaluaciones básicas ENS de Sistemas del Ministerio.
- Asistencia técnica para las auditorías de cumplimiento y de certificación de Sistemas ENS del Ministerio.
- Asistencia técnica para las auditorías de cumplimiento y de certificación ISO 27000 del Ministerio.
- Gestión del plan de formación y concienciación en Seguridad de la información.
- Realización e impartición de cursos, trípticos, píldoras, etc., de seguridad de la información.
- Resolución de consultas sobre seguridad de la información y sistemas para el Ministerio.
- Gestión, mantenimiento de accesos a la herramienta ASSI-RGPD.
- Gestión de peticiones de accesos a datos personales sobre la herramienta ASSI-RGPD.
- Impartición de asistencias en la utilización y formación en la herramienta ASSI-RGPD.
- Realización de Evaluaciones de Impacto en Protección de Datos sobre tratamientos de datos personales que esté efectuando el Ministerio de Sanidad.
- Colaborar con el personal técnico asignado a otros contratos, tanto de administración y operación de infraestructuras TIC, como de desarrollo de aplicaciones, siempre que sea necesario o que así lo demande el Director Técnico del contrato.
- En general, cualquier otra tarea que demande el Director Técnico dentro del área de especialización del contrato y relacionada con la finalidad y los objetivos del mismo.

3.2. Lote 2: Administración y Operación de la plataforma de gestión de servicios TI.

Los principales servicios y tareas a llevar a cabo por el personal técnico de la empresa adjudicataria serán, entre otros, los siguientes:

- Realizar el primer nivel gestión entre los equipos peticionarios del servicio y los equipos

técnicos de infraestructuras, conformando así un servicio de CAU-Infraestructuras.

- Recibir, validar, registrar y gestionar las peticiones en la herramienta de ticketing ITSM del Ministerio de Sanidad.
- Detectar recurrencias en el servicio aportando nuevas peticiones y automatismos y mejoras al catálogo.
- Realizar análisis de los procedimientos internos de la SGITS y proponer mejoras y optimizaciones de los mismos, incluyendo su implementación en la herramienta de ticketing.
- Asegurar el mantenimiento y actualización de activos gestionados a través de la herramienta de ITSM del Ministerio de Sanidad.
- Gestionar el conocimiento de procesos, los niveles del servicio, la capacidad y la disponibilidad del CAU Infraestructuras.
- Administrar y operar la herramienta de ticketing y gestión de activos disponible en el Ministerio de Sanidad.
- Configurar y proponer mejoras para la optimización y evolución continua de la herramienta de ticketing.
- Gestionar el Catálogo de Cambios, peticiones, incidencias y activos.
- Colaborar con el personal técnico asignado a otros contratos, tanto de administración y operación de infraestructuras TIC, como de desarrollo de aplicaciones, siempre que sea necesario o que así lo demande el Director Técnico del contrato.
- Mantenimiento de los procedimientos operativos, manuales, instrucciones técnicas, esquemas y diagramas de arquitectura de las plataformas objeto del lote.
- En general, cualquier otra tarea que demande el Director Técnico dentro del área de especialización del contrato y relacionada con la finalidad y los objetivos del mismo.

3.3. Lote 3: Administración y Operación de la plataforma de Monitorización.

Los principales servicios y tareas a llevar a cabo por el personal técnico de la empresa

adjudicataria serán, entre otros, los siguientes:

- Administración y operación de la Infraestructura de monitorización
- Atención de incidencias graves de los entornos de producción de la Infraestructura de monitorización
- Supervisión del correcto funcionamiento de las alertas y su configuración con las peticiones de los diferentes equipos.
- Creación y mantenimiento de cuadros de mando en función de las necesidades que tengan el resto de equipos
- Gestión y configuración de agentes para monitorizar los elementos hardware necesarios.
- Creación y mantenimiento de scripts para monitorizar servicios, mediante programación en VuGen, creación de navegación guiada por navegador para simular un usuario.
- Generación de informes periódicos del estado de todos los elementos que se monitorizan, así como también informes específicos sobre sucesos anómalos y su análisis para determinar la causa, mediante los datos obtenidos con las herramientas de monitorización.
- Propuestas de mejora en la infraestructura, definiendo proyectos para optimizar y evolucionar los sistemas, así como también valorar nuevas herramientas que puedan sustituir las actuales o mejorarlas.

4. COMPOSICIÓN Y DEDICACIÓN DEL EQUIPO DE TRABAJO

4.1. Composición mínima

La composición mínima de los equipos técnicos asignados a cada uno de los lotes, así como el número estimado de jornadas a realizar por cada uno de los técnicos a lo largo de los dos años de duración prevista del contrato se detalla en la siguiente tabla:

Lote	Descripción	Perfil	Jornadas totales
1		Jefe de proyecto	450

	Administración y Operación de la plataforma de Seguridad.	Técnico Sénior 1	450
		Técnico Sénior 2	450
		Técnico Sénior 3	450
		Técnico Sénior 4	450
		Técnico Júnior 1	450
		Técnico Júnior 2	450
		Técnico Júnior 3	450
		Técnico Júnior 4	450
		Técnico Júnior 5	450
2	Administración y Operación de la plataforma de gestión de servicios TI.	Jefe de proyecto	450
		Técnico de peticiones 1	450
		Técnico de peticiones 2	450
		Técnico de peticiones 3	450
		Técnico de peticiones 4	450
		Técnico de peticiones 5	450
		Técnico de peticiones 6	450
		Técnico de peticiones 7	450
		Técnico administrador ITSM	450
3	Administración y Operación de la plataforma de Monitorización.	Jefe de proyecto	450
		Técnico de Monitorización	450

En los apartados siguientes se resumirá la tipología de las tareas a desempeñar por cada uno de los perfiles. En el Anexo I, Perfiles Profesionales, se detallarán los requisitos mínimos de cada uno de los perfiles. En el Anexo A de la Hoja Resumen del PCAP se detallan los requisitos valorables de dichos perfiles.

La dedicación en número de las jornadas definidas se indica a título estimativo, pudiendo variar en función de la naturaleza y cantidad de trabajos solicitados y en cualquier caso tienen la consideración de mínimos, pudiendo ser mejorados por el adjudicatario.

Durante la ejecución del contrato esta distribución de jornadas podrá variar en función de las necesidades puntuales del contrato contando, en todo caso, con la aceptación de la SGITS.

4.1. Roles y dedicación de cada uno de los perfiles

El jefe de proyecto de cada lote, será el responsable de coordinar técnicamente al resto de perfiles asignados a dicho lote. Además, colaborará con el Director Técnico del lote y su equipo en la realización de proyectos, definición de soluciones, diseño y certificación de arquitecturas, elaboración de procedimientos, resolución de incidencias y problemas críticos y mantenimiento de la documentación operativa y técnica.

Los perfiles de los Técnicos, tanto sénior como júnior, deberán encargarse de las tareas rutinarias de administración, configuración y operación de las plataformas objeto de cada lote, siguiendo los procedimientos operativos autorizados por el Director Técnico correspondiente, así como de la resolución de todo tipo de incidencias, elaboración de análisis e informes técnicos, así como aquellas tareas que le encomiende el jede de proyecto. Colaborarán con el jefe de proyecto en las tareas asignadas al mismo.

5. CONDICIONES RELATIVAS AL EQUIPO DE TRABAJO

5.1. Constitución inicial del equipo de trabajo

El equipo técnico que se incorporará para la ejecución de los trabajos, tras la formalización del contrato correspondiente, deberá estar formado por los componentes relacionados en la oferta adjudicataria y consecuentemente valorados.

No obstante, se autorizarán cambios puntuales en la composición del equipo de trabajo respecto al ofertado cuando se den las condiciones siguientes:

- Justificación escrita, detallada y suficiente, explicando los motivos del cambio.
- Presentación de posibles candidatos con un perfil, en cuanto a los conocimientos y la cualificación técnica requerida, igual o superior al de la persona que se pretende sustituir.
- Aceptación de alguno de los candidatos por el Director Técnico del correspondiente lote.

Una vez adjudicado el contrato, y con carácter previo al inicio del trabajo, el equipo propuesto podrá ser evaluado por el Director Técnico del lote al objeto de comprobar la adecuación real del mismo a las condiciones de la oferta.

En caso de rechazo de algún integrante del equipo, será potestad del Director Técnico del Lote requerir del adjudicatario la presentación de posibles candidatos alternativos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.

La empresa adjudicataria de cada uno de los lotes, deberá asumir todas las tareas descritas en el apartado *DESCRIPCIÓN DE LOS SERVICIOS A PRESTAR* y en las condiciones descritas en este apartado, desde la fecha de inicio del contrato, para lo cual el Ministerio facilitará al adjudicatario toda la documentación técnica disponible.

5.2. Modificación del equipo de trabajo

La valoración final de la productividad y calidad de los trabajos del equipo técnico asignado al servicio corresponde al Director Técnico, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de diez días laborales, por otra persona de igual categoría y experiencia, si existen razones justificadas que lo aconsejen. La aceptación del sustituto, entre los candidatos propuestos por el adjudicatario, corresponderá al Director Técnico.

Asimismo, el Director Técnico podrá solicitar la incorporación o baja (sin sustitución) de efectivos, cuando así interese a efectos del cumplimiento de los objetivos, en este último caso también con un preaviso de diez días laborales. En el caso de incorporación de efectivos, deberán ser previamente aceptados por el Director Técnico, entre los candidatos propuestos por el adjudicatario.

Del mismo modo, cualquier cambio propuesto por el adjudicatario deberá ser comunicado con un plazo mínimo de preaviso de diez días laborales, que, en todo caso, deberá ser aprobado por el Director Técnico. Si no se respetara el plazo de preaviso, se penalizará como período no

facturable equivalente al doble de los días laborales de incumplimiento del preaviso.

En este caso de cambio propuesto por el adjudicatario (y aceptado por el Director Técnico), la incorporación de nuevo personal al equipo de trabajo se hará de forma que se produzca un solapamiento de diez días laborales entre el personal saliente y el entrante, no facturable respecto al personal entrante. Si no se respetara el plazo de solapamiento, se penalizará como período no facturable equivalente al doble de los días laborales de incumplimiento.

5.3. Horario del servicio y tiempo de respuesta

El equipo técnico asignado a cada lote prestará sus servicios **de forma rutinaria en horario laboral estándar de lunes a viernes no festivos, dentro de la franja de 7h a 20h**. El Director Técnico de cada lote establecerá el horario de cobertura exacto en función de las necesidades del servicio, así como el número de técnicos que se requerirán en cada franja horaria. **Como mínimo, el servicio se prestará de 9h a 18h**.

La duración de las jornadas, a efectos de facturación, se entenderá de 8h.

El calendario de días festivos aplicable será el correspondiente a la ciudad de Madrid.

En caso de incidencia durante este horario, el tiempo de respuesta por parte del personal técnico de la empresa será inferior a 30 minutos.

5.4. Actividad del equipo de trabajo

La dedicación para cada uno de los perfiles profesionales requeridos será el indicado en el apartado 4.

Por defecto, el personal técnico asignado por las empresas adjudicatarias a cada uno de los lotes estará dedicado exclusivamente a este proyecto. Salvo autorización expresa del Director Técnico no se admitirán técnicos que estén asignados a otros proyectos de la empresa.

Las tareas descritas en el apartado correspondiente para cada lote son estimativas y podrán ser sustituidas por otras prestaciones o proyectos equivalentes dentro del mismo ámbito funcional.

Cuando el desarrollo de las actividades previstas en el pliego exigiera una contribución neta de recursos humanos inferior a la considerada en el pliego, la SGITS optará entre que el

adjudicatario se comprometa a aportar los recursos restantes en aquel proyecto informático, dentro del mismo entorno tecnológico, que dicha Subdirección General establezca, o porque el remanente de horas no sea objeto de facturación, sin que pueda implicar coste o pen alización alguna para el órgano contratante.

Análogamente, si en momentos puntuales se requiriera disponer de un mayor número de técnicos para atender a cargas de trabajo temporales, el Director Técnico podrá solicitar a las empresas adjudicatarias la incorporación al proyecto de perfiles adicionales, con perfiles similares a alguno de los ya incorporados y con tarifas idénticas, siempre dentro de la disponibilidad presupuestaria asociada al contrato.

5.5. Uso de herramientas corporativas para la gestión de tareas

El equipo técnico asociado a cada uno de los lotes deberá usar las herramientas corporativas definidas por el Ministerio para interactuar con el resto de unidades y empresas responsables de prestar algún servicio al Ministerio. Como mínimo, el personal técnico asociado a cada uno de los lotes deberá de hacer uso de las siguientes herramientas:

- Correo electrónico corporativo.
- Plataforma corporativa de videoconferencia y chat.
- Herramienta de ticketing para la gestión de cambios y tareas.
- Herramienta de gestión de proyectos para la planificación de tareas o proyectos complejos.
- Repositorio corporativo de instrucciones técnicas, procedimientos operativos, etc.

El Ministerio definirá en cada caso las herramientas concretas a utilizar. El personal técnico de las empresas adjudicatarias deberá usar estas herramientas según los procedimientos operativos que se definan en cada caso.

5.6. Lugar de prestación de los servicios y equipamiento informático del equipo de trabajo

Dada la naturaleza de los trabajos a realizar, estos se llevarán a cabo preferentemente en las dependencias del Ministerio, pero podrán ser realizados total o parcialmente en modalidad de teletrabajo o en las dependencias de las empresas adjudicatarias en los casos en que así lo

decida el Director Técnico del lote.

En estos casos de trabajo en modo remoto, las empresas adjudicatarias deberán de proveer al personal técnico asignado al contrato de los medios técnicos (PC o portátil, teléfono móvil, conexión a Internet, etc.) que sean necesarios para la realización de las tareas objeto del contrato.

En este caso, el personal de la empresa contratista ocupará espacios de trabajo diferenciados en la SGITS y separados en todo caso del que ocupan los empleados públicos para los que se presta el servicio. Corresponde también a la empresa contratista velar por el cumplimiento de esta obligación. Se recomienda que dicho personal utilice tarjetas identificativas de su empresa.

Salvo los supuestos en los que sea necesario por las características del servicio a desarrollar, los empleados del contratista no podrán acceder a servicios reservados a los empleados públicos como correo electrónico corporativo, intranet corporativa u otros de análogo carácter.

El contratista se someterá a las normas de acceso y control existentes en las dependencias donde se preste el servicio.

En estos casos de trabajo en modo remoto, las empresas adjudicatarias deberán de proveer al personal técnico asignado al contrato de los medios técnicos (PC o portátil, teléfono móvil, conexión a Internet, etc.) que sean necesarios para la realización de las tareas objeto del contrato.

Además, y por razones de seguridad, la SGITS podrá exigir a las empresas cuyos técnicos trabajen remotamente, que el equipamiento informático asignado a dichos técnicos sea maquetado, configurado y administrado por el propio Ministerio, de forma que se garantice la seguridad de los accesos a la red interna del Ministerio desde dichos equipos. En estos casos, se podrá exigir a las empresas que todos los equipos asignados a los técnicos sean idénticos con el objeto de facilitar la maquetación de los mismos.

La SGITS podrá establecer las condiciones, tanto organizativas como tecnológicas, para asegurar el correcto desempeño del personal en cualquiera de las modalidades de trabajo. La empresa contratista deberá proporcionar a sus empleados todos los medios tecnológicos necesarios, que podrán ser definidos por la SGITS, para garantizar en todo momento la seguridad en los accesos remotos a la red del Ministerio. A tal fin, la SGITS podrá indicar, durante la ejecución del contrato, qué programas informáticos y configuraciones específicas son

aceptables para garantizar un acceso seguro a su red, siendo estas condiciones de obligado cumplimiento por parte del adjudicatario.

En cualquier caso, la SGITS podrá exigir la verificación y confirmación de los equipos de usuario utilizados para acceder a sus redes de forma remota por los empleados de la empresa contratista.

5.7. Formación del equipo de trabajo

El adjudicatario proveerá, sin coste adicional, la formación técnica necesaria para adaptar los conocimientos del equipo de trabajo a la evolución de la tecnología y de las funciones objeto del contrato. A tal fin, incluirá en su oferta el correspondiente Plan de formación continua.

6. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal.

Este contrato no implicará el tratamiento de datos personales.

El adjudicatario deberá cumplir todas las medidas aplicables al tratamiento de la información recogidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como las aplicables al tratamiento de datos personales recogidas en el Reglamento (UE) 2016/679 General de Protección de Datos y demás normas aplicables.

Asimismo, el adjudicatario deberá cumplir con la Política de Seguridad del Ministerio de Sanidad y toda la normativa de Seguridad e la Información vigente.

Los técnicos de la empresa adjudicataria deberán firmar un acuerdo de confidencialidad para garantizar el cumplimiento de este apartado.

7. TRANSFERENCIA TECNOLÓGICA Y DOCUMENTACIÓN DE LOS TRABAJOS

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el centro directivo a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y

de las tecnologías, métodos y herramientas utilizados para resolverlos.

La documentación generada durante la ejecución del contrato será de propiedad exclusiva del órgano directivo sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de este órgano directivo, que la daría en su caso previa petición formal del contratista con expresión del fin.

La propiedad intelectual del resultado de cualquier trabajo objeto de este contrato es en exclusiva del Ministerio de Sanidad.

Toda la documentación se entregará en español en formato electrónico, preferentemente en PDF, de forma que el contenido esté en formato texto. No se admitirán documentos escaneados o en modo imagen, aunque se hayan utilizado herramientas tipo OCR para extraer el texto de los mismos.

El adjudicatario deberá suministrar, en su caso, al órgano directivo las nuevas versiones de la documentación que se vayan requiriendo.

PROPONE

EL SUBDIRECTOR GENERAL

Enrique Quintanilla Cabañero

APRUEBA

EL SECRETARIO DE ESTADO

P.D. Orden SND/1298/2022, de 22 de diciembre, (BOE 28/12/2022)
EL SECRETARIO GENERAL DE SALUD DIGITAL, INFORMACIÓN
E INNOVACIÓN DEL SISTEMA NACIONAL DE SALUD,

JUAN FERNANDO MUÑOZ MONTALVO

ANEXO I: PERFILES PROFESIONALES

A continuación, se enumeran los **requisitos mínimos** que deberán cumplir los candidatos a formar parte del equipo técnico asignado al contrato. No se admitirán ofertas en donde alguno de los candidatos presentados no cumpla estos requisitos. En el caso de la experiencia mínima exigida, solo se computará como tal **la acumulada a lo largo de los últimos 12 años**.

Tal y como se detalla en el Anexo A de la Hoja Resumen que acompaña al PCAP, se valorará la experiencia adicional de los candidatos ofertados hasta un máximo de 36 meses adicionales con respecto al mínimo exigido.

I.1. LOTE 1: Administración y Operación de la plataforma de Seguridad

Perfil: Jefe de proyecto

a) Titulación mínima y formación

- **Titulación:** Titulación de Grado, Licenciatura, Ingeniería Superior o equivalente

- **Idiomas:** Nivel Medio de inglés

b) Tareas y responsabilidades

- Dirección de proyectos, coordinación, supervisión y asignación de tareas al resto de técnicos asignados al lote.
- Coordinación con el Director Técnico del Ministerio.
- Elaboración de propuestas de mejora tecnológica en el ámbito del contrato. Asesoramiento tecnológico.
- Planificación y seguimiento de proyectos de cambio complejos.
- Colaborar en la definición de los objetivos a largo plazo con la Dirección Técnica del Ministerio y seguimiento de los mismos.
- Definición de objetivos a corto plazo, planificación y asignación de responsabilidades.
- Dirección de proyectos de adecuación (ENS e ISO 27000) del marco normativo del Sistema de Gestión de la Seguridad del Ministerio.

- Definición y mantenimiento de procedimientos técnicos de acuerdo con las directrices del ENS.
- Realización de presentaciones de carácter técnico.
- Atender las peticiones de las diferentes unidades relacionadas con el Servicio.
- Seguimiento de tareas e incidencias en las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.
- Colaborar con otras unidades de la SGITS (Comunicaciones, Sistemas, Desarrollo, etc.) para la realización de las tareas asignadas al servicio.
- Colaborar en la definición de la metodología de análisis de riesgos, evaluaciones de impacto y planes de continuidad.
- Supervisar y planificar los procedimientos de adecuación de sistemas al marco normativo vigente (ENS, ISO 27000, RGPD/LOPDGDD, NIS2, LPIC etc).
- Coordinar la planificación y ejecución del calendario de auditorías de seguridad, tanto técnicas como de adecuación y certificación, del Ministerio de Sanidad.
- Gestionar el seguimiento y resolución de las vulnerabilidades detectadas que afecten a los sistemas del Ministerio de Sanidad.
- Colaborar en la definición, implantación y seguimiento de planes de formación y concienciación.
- Analizar y dar respuesta a aquellas peticiones y consultas sobre normativa de seguridad que se reciban en el servicio.
- Elaborar informes y análisis técnicos y normativos sobre las materias objeto del presente lote.
- Supervisar la gestión de las peticiones internas de acceso a datos personales y los riesgos de seguridad asociados.

c) Experiencia previa para la capacitación del puesto

- Experiencia de al menos **9 años** en dirección de unidades y equipos de Seguridad de la Información.

- Experiencia de al menos **9 años** en proyectos de revisión, adecuación y certificación de conformidad de estándares y normativas relativas a la ciberseguridad en el marco de la arquitectura de seguridad de la organización. En particular:
  - ISO 27000 sobre Sistemas de Gestión de Seguridad de la información.
  - Esquema Nacional de Seguridad (ENS).
  - Directiva NIS2, LPIC.
  - Utilización de la normativa del CCN-CERT sobre ciberseguridad, en particular la serie 800.
- Experiencia profesional de al menos **5 años** en proyectos de adecuación en materia de protección de datos (RGPD, LOPDGDD) así como formación o titulación específica en normativa legal y jurídica sobre protección de datos de carácter personal
- Experiencia de al menos **5 años** en proyectos de modernización tecnológica de la arquitectura de Seguridad.
- Experiencia de al menos **2 años** en gestión de equipos de respuesta ante incidentes.
- Experiencia de al menos **2 años** en gestión de equipos de análisis de vulnerabilidades, test de caja negra y blanca.
- Experiencia laboral de al menos **3 años** en el diseño, planificación y definición de metodologías de análisis de riesgo (PILAR) y evaluaciones de impacto.

Perfil: Técnico Sénior 1 y 2

a) Titulación mínima y formación

- **Titulación:** Titulación de Grado, Licenciatura, Ingeniería Superior o equivalente

b) Idiomas: Nivel Medio de inglés

c) Tareas y responsabilidades

- Gestión y realización de auditorías de técnicas de seguridad
- Gestión y realización de auditorías de caja negra y caja gris sobre sistemas y aplicaciones del Ministerio basadas en la metodología OWASP.
- Seguimiento y resolución de incidentes y vulnerabilidades detectadas en los Sistemas del Ministerio.
- Apoyo en la elaboración de propuestas de mejora de la arquitectura de seguridad.
- Recogida y preparación de información para su utilización en el análisis de incidentes de seguridad o para servir de base a la toma de decisiones.
- Diseño y construcción de arquitecturas para la identificación, detección y mitigación de ataques contra la seguridad de la información.
- Colaborar en la definición, implantación y seguimiento de planes de formación y concienciación. Realización e impartición de cursos, trípticos, píldoras, etc., de seguridad de la información.
- Realización de presentaciones de carácter técnico y transmisión del conocimiento.
- Gestión y realización de integraciones de sistemas, dispositivos de comunicaciones y sistemas de seguridad del Ministerio con servicios del COCS de la AGE.
- Elaboración de procedimientos e instrucciones técnicas de Seguridad del área de Infraestructuras del Ministerio.
- Gestión y realización de pruebas de penetración
- Resolución de consultas sobre seguridad técnica para el Ministerio
- Colaborar con otras unidades de la SGITS (Comunicaciones, Sistemas, Desarrollo, etc.) para la realización de las tareas asignadas al servicio.

d) Experiencia previa para la capacitación del puesto

- Experiencia de al menos **7 años** en consultoría tecnológica relacionada con la ciberseguridad: análisis de vulnerabilidades, evaluación y selección de medidas de protección y soluciones tecnológicas, indicadores de compromiso (IOC), pentesting, hacking ético, etc., así como experiencia y conocimiento en bastionado sobre arquitecturas .NET, J2EE, Windows (Active Directory & SCCM/MECM), Unix, Linux.

- Experiencia laboral contrastada de al menos **5 años** en proyectos de adecuación y modernización de arquitecturas de seguridad. Se exigirá amplio conocimiento del estado del arte de tecnologías de ciberseguridad
- Experiencia de al menos **5 años** en el uso, implantación y administración de herramientas habitualmente empleadas en análisis de vulnerabilidades (OWASP Zap Proxy, Burp Suite, SOAP UI, Nessus, etc.); así como consulta de repositorios y gestión de alertas (MITRE CVE/CWE).
- Experiencia de al menos **2 años** en Centros de Operaciones de Seguridad y Equipos de Respuesta ante incidentes de Ciberseguridad.
- Experiencia de al menos **2 años** en el uso de herramientas y soluciones de ciberseguridad del Centro Criptológico Nacional (CCN): ANA, LUCÍA, MARTA y microCLAUDIA.
- Se valorará experiencia en el uso, implantación y administración de herramientas habitualmente empleadas en las arquitecturas de ciberseguridad como: IDS/IPS, SIEM, WAF, protección perimetral y del puesto de trabajo, etc.
- Se valorará experiencia en proyectos de adecuación e implantación de estándares y normativas relativas a la ciberseguridad en el marco de la arquitectura de seguridad de la organización. En particular ENS, ISO 27000.
- Se valorará disponer de alguna certificación o titulación de ciberseguridad emitida por organizaciones habilitadas al efecto:
    - SANS (GISF, GCED, GDSA, etc).
    - ISC2 (CISSP, ISSAP, ISSEP, ISSMP, etc).
    - EC-Council (ECSS, CEH, APT, CND).
    - ISMS (CCSP).
    - Microsoft (MTA:Security Fundamentals)
    - CompTIA (Security+, PenTest+, CySA+)

Perfil: Perfil: Técnico Sénior 3 y 4

a) Titulación mínima y formación

- **Titulación:** Titulación de Grado, Licenciatura, Ingeniería Superior o

equivalente

b) Idiomas: Nivel Medio de inglés

c) Tareas y responsabilidades

- Organización y coordinación de los procesos de auditoría de cumplimiento y certificación (ENS e ISO 27000) según el plan establecido. Supervisión de las entrevistas y de los entregables.
- Participar en proyectos de adecuación del marco normativo del Sistema de Gestión de la Seguridad del Ministerio.
- Mantenimiento del documento de arquitectura de seguridad de acuerdo con las directrices del ENS.
- Colaborar en la definición de la metodología de análisis de riesgos y en la elaboración de planes de continuidad.
- Gestión y realización de los procedimientos de autoevaluación, valoración ACIDT y análisis de impacto sobre los sistemas del Ministerio según establece el ENS.
- Mantenimiento, realización y revisión de Política de seguridad, Normas y Procedimientos del Sistema de Gestión de la Seguridad de la Información del Ministerio.
- Supervisar y planificar los procedimientos de adecuación de sistemas al marco normativo vigente (ENS, RGPD/LOPDGDD, etc).
- Colaborar en la definición, implantación y seguimiento de planes de formación y concienciación. Realización e impartición de cursos, trípticos, píldoras, etc., de seguridad de la información.
- Analizar y dar respuesta a aquellas peticiones y consultas sobre normativa de seguridad que se reciban en el servicio.
- Colaborar con otras unidades de la SGITS (Comunicaciones, Sistemas, Desarrollo, etc.) para la realización de las tareas asignadas al servicio.
- Gestión de las peticiones internas de acceso a datos personales y los riesgos de seguridad asociados.
- Realización de Evaluaciones de Impacto en Protección de Datos sobre tratamientos de datos personales que esté efectuando el Ministerio de

Sanidad.

- Seguimiento de tareas y peticiones a través de las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.

d) Experiencia previa para la capacitación del puesto

- Experiencia de al menos **7 años** en proyectos de revisión, adecuación y certificación de conformidad de estándares y normativas relativas a la ciberseguridad en el marco de la arquitectura de seguridad de la organización. En particular:
  - ISO 27000 sobre Sistemas de Gestión de Seguridad de la información.
  - Esquema Nacional de Seguridad (ENS).
  - Directiva NIS2, LPIC.
  - Utilización de la normativa del CCN-CERT sobre ciberseguridad, en particular la serie 800.
- Experiencia profesional de al menos **5 años** en proyectos de adecuación en materia de protección de datos (RGPD, LOPDGDD), uso de herramientas gestión de tratamientos de datos peronales, así como formación o titulación específica en normativa legal y jurídica sobre protección de datos de carácter personal.
- Experiencia de al menos **3 años** con herramientas de GRC.
- Experiencia laboral de al menos **5 años** en el diseño, planificación y definición de metodologías de análisis de riesgo (MAGERIT y PILAR) y evaluaciones de impacto.
- Se valorará disponer de experiencia en herramientas de ticketing y gestión de incidencias (BMC Remedy, Jira, Redmine)
- Se valorará disponer de certificaciones de auditoría de Seguridad emitida por organizaciones habilitadas al efecto (ej: CISA)

Perfil: Técnico Júnior 1, 2 y 3

a) Titulación mínima y formación

- **Titulación:** Titulación universitaria de grado, diplomatura o Ingeniería técnica

b) Idiomas: Nivel Medio de inglés

c) Tareas y responsabilidades

- Gestión y resolución de Incidentes de seguridad en el Ministerio reportados por sondas SAT-INET, SAT-SARA, LUCÍA, GLORIA y servicio del Centro de Operaciones de Ciberseguridad de la AGE utilizando las herramientas LUCÍA, GLORIA, GrayLog.
- Gestión de Vulnerabilidades reportadas por avisos y alertas de fuentes externas: servicios del COCS de Prevención, CCN, CVE-MITRE...
- Realización de auditorías técnicas internas de seguridad sobre infraestructuras y puesto de trabajo del Ministerio
- Gestión de autorizaciones para la instalación de software en puestos de Trabajo y navegación a través de proxy WEB
- Elaboración de procedimientos e instrucciones técnicas de Seguridad del área de Infraestructuras del Ministerio
- Apoyo a las integraciones de sistemas, dispositivos de comunicaciones y sistemas de seguridad del Ministerio con servicios del COCS de la AGE
- Resolución de consultas sobre seguridad técnica para el Ministerio
- Realización de pruebas de penetración
- Realización de auditorías de caja negra y caja gris sobre sistemas y aplicaciones del Ministerio basadas en la metodología OWASP

d) Experiencia previa para la capacitación del puesto

- Experiencia de al menos **3 años** en consultoría tecnológica relacionada con la ciberseguridad: análisis de vulnerabilidades, evaluación y selección de medidas de protección y soluciones tecnológicas, indicadores de compromiso (IOC), pentesting, hacking ético, etc., así como experiencia y conocimiento en bastionado sobre arquitecturas .NET, J2EE, Windows (Active Directory & SCCM/MECM), Unix, Linux.
- Experiencia de al menos **3 años** en el uso, implantación y administración de

herramientas habitualmente empleadas en análisis de vulnerabilidades (OWASP Zap Proxy, Burp Suite, SOAP UI, Nessus, etc.); así como consulta de repositorios y gestión de alertas (MITRE CVE/CWE).

- Experiencia de al menos **2 años** en Centros de Operaciones de Seguridad y Equipos de Respuesta ante Incidentes de Ciberseguridad.
- Experiencia de al menos **2 años** en el uso de herramientas y soluciones de ciberseguridad del Centro Criptológico Nacional (CCN): ANA, LUCÍA, MARTA y microCLAUDIA.
- Se valorará experiencia en el uso, implantación y administración de herramientas habitualmente empleadas en las arquitecturas de ciberseguridad como: IDS/IPS, SIEM, WAF, protección perimetral y del puesto de trabajo, etc.
- Se valorará disponer de alguna certificación o titulación de ciberseguridad emitida por organizaciones habilitadas al efecto:
  - SANS (GISF, GCED, GDSA, etc).
  - ISC2 (CISSP, ISSAP, ISSEP, ISSMP, etc).
  - EC-Council (ECSS, CEH, APT, CND).
  - ISMS (CCSP).
  - Microsoft (MTA:Security Fundamentals)
  - CompTIA (Security+, PenTest+, CySA+)

Perfil: Perfil: Técnico Júnior 4 y 5

a) Titulación mínima y formación

- **Titulación:** Titulación universitaria de grado, diplomatura o Ingeniería técnica

b) Idiomas: Nivel Medio de inglés

c) Tareas y responsabilidades

- Apoyo a los procesos de auditoría de cumplimiento y certificación (ENS e ISO 27000) según el plan establecido. Participación en las entrevistas y

preparación de los entregables.

- Participar en proyectos de adecuación del marco normativo del Sistema de Gestión de la Seguridad del Ministerio.
- Apoyo al análisis de riesgos y la elaboración de planes de continuidad.
- Realización de autoevaluaciones, valoraciones ACIDT y análisis de impacto sobre los sistemas del Ministerio según establece el ENS.
- Apoyo al mantenimiento, realización y revisión de Política de seguridad, Normas y Procedimientos del Sistema de Gestión de la Seguridad de la Información del Ministerio.
- Colaborar en la definición, implantación y seguimiento de planes de formación y concienciación. Realización e impartición de cursos, trípticos, píldoras, etc., de seguridad de la información.
- Analizar y dar respuesta a aquellas peticiones y consultas sobre normativa de seguridad que se reciban en el servicio.
- Colaborar con otras unidades de la SGITS (Comunicaciones, Sistemas, Desarrollo, etc.) para la realización de las tareas asignadas al servicio.
- Gestión de las peticiones internas de acceso a datos personales y los riesgos de seguridad asociados.
- Apoyo a la realización de Evaluaciones de Impacto en Protección de Datos sobre tratamientos de datos personales que esté efectuando el Ministerio de Sanidad.
- Seguimiento de tareas y peticiones a través de las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.

d) Experiencia previa para la capacitación del puesto

- Experiencia de al menos **3 años** en proyectos de revisión, adecuación y certificación de conformidad de estándares y normativas relativas a la ciberseguridad en el marco de la arquitectura de seguridad de la organización. En particular:
  - ISO 27000 sobre Sistemas de Gestión de Seguridad de la información.
  - Esquema Nacional de Seguridad (ENS).

- Directiva NIS2, LPIC.
- Utilización de la normativa del CCN-CERT sobre ciberseguridad, en particular la serie 800.

- Experiencia profesional de al menos **2 años** en proyectos de adecuación en materia de protección de datos (RGPD, LOPDGDD), uso de la herramienta de gestión de tratamientos de datos de carácter personal, así como formación o titulación específica en normativa legal y jurídica sobre protección de datos de carácter personal.
- Experiencia de al menos **2 años** con herramientas de GRC.
- Experiencia laboral de al menos **2 años** en el diseño, planificación y definición de metodologías de análisis de riesgo (MAGERIT y PILAR) y evaluaciones de impacto.
- Se valorará disponer de experiencia en herramientas de ticketing y gestión de incidencias (BMC Remedy, Jira, Redmine)
- Se valorará disponer de certificaciones de auditoría de Seguridad emitida por organizaciones habilitadas al efecto (ej: CISA)

I.2. Lote 2: Administración y Operación de la plataforma de gestión de servicios TI.

Perfil: Jefe de proyecto

a) Titulación mínima y formación

- **Titulación: Titulación:** Titulación de Grado, Licenciatura, Ingeniería Superior o equivalente

- **Idiomas:** Nivel Medio de inglés

b) Tareas y responsabilidades

- Coordinar, supervisar y asignar tareas al resto de técnicos asignados al lote.
- Coordinar con el Director Técnico del Ministerio.

- Dirigir y coordinar un servicio de atención y gestionar las peticiones de carácter tecnológico para las diversas unidades de la SGITS.
- Elaborar propuestas de mejora tecnológica en el ámbito del contrato. Asesoramiento tecnológico.
- Planificar y supervisar proyectos de cambio complejos.
- Gestionar los cambios que afectan al servicio en tiempo y forma para facilitar la correcta operativa del servicio tanto a nivel operativo interno como las relaciones del mismo con los equipos y unidades operativas con las que tiene relación en los procesos de negocio que le afectan.
- Gestionar la correcta operativa del servicio tanto a nivel operativo interno como las relaciones del mismo con los equipos y unidades operativas con las que tiene relación en los procesos de negocio que le afectan.
- Gestionar y supervisar a los Técnico especialistas en procesos de gestión de peticiones pertenecientes al equipo.
- Asegurar la nomenclatura y relación entre todos los documentos y textos del servicio. (Herramientas, Wiki, Instrucciones técnicas y diagramas incluidos).
- Elaborar y mantener los documentos operativos del servicio NAS y Wiki interna (Bienvenida, manuales de uso de herramientas, Instrucciones técnicas).
- Elaborar informes operativos, cuadros de mando, análisis técnicos y operativos del ámbito tecnológico objeto del lote.
- Proponer mejoras en la gestión del conocimiento.
- Planificar a alto y bajo nivel las iniciativas aprobadas.
- Instanciar los proyectos en la herramienta corporativa.
- Realizar la dirección de proyectos, diseño arquitectura y administración a alto nivel de las plataformas, infraestructuras y servicios objeto del lote.
- Realizar la dirección de proyectos, diseño arquitectura, implementación y

administración a alto nivel de los mecanismos de contingencia y de continuidad de negocio, en el ámbito de las plataformas, infraestructuras y servicios objeto del lote.

- Realizar la dirección de proyectos, diseño arquitectura, implementación y administración a alto nivel de nuevas plataformas que puedan sustituir a las existentes a lo largo del periodo de ejecución del contrato.
- Resolver las incidencias que surjan en estas plataformas y escalado de las mismas a proveedores.
- Elaborar planes de pruebas en estas plataformas.
- Atender a las peticiones de las unidades de Desarrollo y de Atención al Usuario (CAUs) a las que la SGITS preste servicio.
- Establecer procedimientos operativos para la optimización de estas tareas minimizando tanto los tiempos necesarios para la resolución de las mismas como el uso de recursos.
- Colaborar con otras unidades de la SGITS (Comunicaciones, Seguridad, Explotación, etc.) para la realización de las tareas mencionadas anteriormente.
- Realizar el seguimiento de las tareas e incidencias en las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.
- Mantener y elaborar documentación técnica.
- Participar en el mantenimiento de los inventarios relacionados con las plataformas objeto del contrato.

c) Experiencia previa para la capacitación del puesto

- Experiencia laboral contrastada de al menos **7 años** gestionando proyectos de dirección de equipos de atención de peticiones.

- Experiencia laboral contrastada de al menos **5 años** involucrado en proyectos de análisis, diseño e implantación de servicios de atención a usuarios TI basados en ITIL y/o Planes Directores en Calidad de servicios de la Información, conforme a la Norma ISO 20000 y su certificación.

- Experiencia laboral contrastada de al menos **5 años** involucrado en proyectos de análisis, diseño e implantación de mejoras en herramientas ITSM y CMDB.

- Experiencia laboral contrastada de al menos **3 años** en el Área de calidad involucrado en proyectos de Transformación de servicios, gestión del cambio y Experiencia de usuario TI.

- Experiencia de al menos **3 años** en proyectos de mejora e implantación de metodologías en Servicios de Atención al usuario TI.

- Se valorará experiencia de al menos **3 años** con el ecosistema de herramientas de ticketing JIRA (JIRA Service Management, JIRA Data Center, JIRA Assets, Insight, etc).

Perfil: Gestores de peticiones

a) Titulación mínima y formación

- **Titulación:** No se requiere

b) Tareas y responsabilidades

- Gestionar peticiones, cambios e incidencias a través de las herramientas que usa el servicio, incluidas en el catálogo del servicio. Gestionar un volumen promedio diario según número, complejidad, abiertas, cerradas y en curso. Cumplimiento de SLAs/SLOs asociados a KPIs del servicio y del gestor.

- Atender solicitudes, según instrucciones técnicas, de la gestión del buzón de solicitudes.

- Atender solicitudes no catalogadas, bloqueadas o nuevas.

- Gestionar de manera integral el inventario de activos y la CMDB, incluyendo

cargas masivas y del ciclo completo de vida de los activos.

- Asegurar la ejecución efectiva por parte de todos los GPs, según instrucciones técnicas, de la gestión del buzón de solicitudes.
- Documentar instrucciones técnicas y manuales.
- Participar en posibles mejoras del servicio.
- Formar a nuevas incorporaciones tanto en la operativa del CAU con en la gestión del buzón de solicitudes.
- Asistir al Director Técnico en la elaboración de informes operativos.
- Proponer mejoras en la gestión del buzón de solicitudes y las instrucciones técnicas del mismo.

c) Experiencia previa para la capacitación del puesto

- Experiencia profesional de al menos **2 años** como gestor de peticiones en servicios de atención a usuarios en departamentos TI.
- Experiencia de al menos **2 años** con herramientas de ITSM de gestión de peticiones e inventario de activos.
- Se valorará experiencia de al menos **1 año** como gestor de conocimiento, elaborando documentación de procesos, procedimientos, instrucciones técnicas, manuales, actas y/o informes.
- Se valorará experiencia de al menos **1 año** como gestor de configuración y activos en un sistema (CMDB) de un departamento TI.
- Se valorará experiencia de al menos **1 año** en el ecosistema de aplicaciones JIRA.

Perfil: Técnico Administrador de herramientas ITSM

a) Titulación mínima y formación

- **Titulación:** Grado, Diplomatura, Arquitectura Técnica o Ingeniería Técnica o experiencia equivalente.

- **Idiomas:** Nivel Medio de inglés

b) Tareas y responsabilidades

- Instalar, administrar, gestionar, operar y configurar la arquitectura de gestión de peticiones e inventario.
- Mantener y actualizar la herramienta ITSM instalando parches y plugins.
- Realizar el análisis, diseño e implantación del catálogo de servicios.
- Implementar y configurar formularios y automatismos del catálogo de peticiones.
- Parametrizar Jira y programar automatizaciones.
- Configurar y usar los add-ons del Marketplace de Atlassian.
- Realizar el seguimiento de la evolución y soporte de sistemas TIC.
- Realizar el análisis, diseño e implantación de mejoras en herramientas de ITSM y CMDB.
- Definir metodologías e implantación de Servicios de Atención al usuario.
- Configurar los procesos en la herramienta JIRA Data Center y JIRA Service Manager, así como de los plugins y demás módulos de JIRA.
- Gestionar los usuarios y grupos de trabajo dentro de la herramienta.
- Gestionar la configuración y explotación de la gestión de activos en herramienta JIRA Data Center y JIRA Service Manager.
- Realizar las tareas de definición, configuración y parametrización de los activos de la CMDB en Jira y el Discovery.
- Mantener y elaborar documentación técnica.
- Participar en el mantenimiento de los inventarios relacionados con las plataformas objeto del contrato.

c) Experiencia previa para la capacitación del puesto

- Experiencia laboral contrastada de al menos **6 años** como responsable de

administración de herramientas ITSM de Servicio de Atención a Usuarios TI.

- Experiencia laboral de al menos **4 años** en proyectos de análisis, diseño e implantación de mejoras en herramientas ITSM y CMDB.
- Experiencia laboral de al menos **3 años** en proyectos de implementación de peticiones TI en JIRA Date Center. Gestión de incidencias y problemas, gestión del cambio, etc.
- Experiencia laboral de al menos **3 años** en proyectos de implementación, configuración, mantenimiento y automatización de la gestión de activos.
- Experiencia laboral de al menos **3 años** en configuración y soporte de JIRA plugins: Automation, EazyBI, Tempo… Dashboards, informes y reportes.
- Experiencia de al menos **2 años** en proyectos de implantación de metodologías en Servicios de Atención al usuario.
- Experiencia profesional de al menos **2 años** en la elaboración de documentación de procesos e informes.
- Experiencia laboral de al menos **2 años** involucrado en proyectos de implantación de Servicios de Atención a Usuarios TI.
- Se valorarán las siguientes certificaciones:
    - Certificado ACP-JA Jira Administrator for Data Center.
    - ITIL Foundation o equivalente.
    - ITIL Specialist: “Direccionar valor a interesados” o equivalente.

I.3. Lote 3: Administración y Operación de la plataforma de Monitorización.

Perfil: Jefe de Proyecto

a) Titulación mínima y formación

- **Titulación:** Formación Universitaria
- **Idiomas:** Nivel Medio de inglés

b) Tareas y responsabilidades

- Coordinación, supervisión y asignación de tareas al resto de técnicos asignados al lote.
- Coordinación con el Director Técnico del Ministerio.
- Elaboración de propuestas de mejora tecnológica en el ámbito del contrato. Asesoramiento tecnológico.
- Planificación y seguimiento de proyectos de cambio complejos.
- Creación de informes sobre situaciones anómalas detectadas en base a la información recogida por las herramientas de monitorización.
- Mantenimiento de la Infraestructura: Comprobación del correcto funcionamiento de las diferentes herramientas de monitorización, así como de planificar las mejoras necesarias en su mantenimiento.
- Creación y mantenimiento de pruebas sintéticas:
    - Altas, bajas y modificación de las diferentes aplicaciones desarrolladas que se van a monitorizar.
    - Creación de scripts para comprobar peticiones de correo, realizar navegaciones web, enviar peticiones web services (tipo SOAP, REST)
    - Configuración y gestión del sistema de escalado de alertas.
- Creación y mantenimiento de agentes:
    - Altas, bajas y modificación de los diferentes elementos hardware que se van a monitorizar.
    - Altas de monitorizaciones tipo Ping.
    - Gestión de umbrales de aquellos parámetros que se estén monitorizando
- Supervisión de Alertas:
    - Crear y revisar tanto la ejecución como el destinatario de las alertas en función de la evolución de los diferentes servicios.
- Creación y mantenimiento de cuadros de mando en función de las necesidades que tengan el resto de equipos.
- Agrupar las diferentes métricas obtenidas para dar una información de utilidad a los diferentes equipos.
- Dirección de proyectos, diseño arquitectura, administración y operación de las plataformas, infraestructuras y servicios objeto del lote.
- Dirección de proyectos, diseño arquitectura, implementación y administración

de los mecanismos de contingencia y de continuidad de negocio, en el ámbito de las plataformas, infraestructuras y servicios objeto del lote.

- Dirección de proyectos, diseño arquitectura, implementación, administración y operación de nuevas plataformas que puedan sustituir a las existentes a lo largo del periodo de ejecución del contrato.
- Resolución de incidencias que surjan en estas plataformas y escalado de las mismas a proveedores.
- Atender a las peticiones de las unidades de Desarrollo, Infraestructuras y de Atención al Usuario (CAUs) a las que la SGITS preste servicio.
- Atender a las peticiones de otras unidades del Área de Infraestructuras de la SGITS.
- Seguimiento de tareas e incidencias en las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.
- Mantenimiento y elaboración de documentación técnica.
- Participación en el mantenimiento de los inventarios relacionados con las plataformas objeto del contrato.

c) Experiencia previa para la capacitación del puesto

- Experiencia laboral de al menos **6 años** en proyectos de consultoría tecnológica de monitorización hardware y de servicios
- Experiencia laboral de al menos **6 años** en proyectos vinculados a la administración de herramientas de monitorización y gestión de eventos y alertas en entornos de producción
- Experiencia laboral de al menos **3 años** en proyectos de implantación, migración y gestión de herramientas de monitorización
- Experiencia de al menos **3 años** en gestión de servicios de monitorización con las siguientes herramientas de: Microfocus Business Process Monitor y/o BMC Truesight Operations Management (se requiere que uno de los dos perfiles del lote tenga la experiencia mínima en cada tecnología)
- Se valorará disponer de certificaciones de herramientas de monitorización, como: BMC Truesight Operations Management, Elastic Certified Observability, Opentext Application Performance Management (APM)

Certified Professional, etc.

- Se valorará conocimiento de al menos 1 año de otras herramientas de monitorización y observabilidad: Zabbix, ELK, Dynatrace, Nagios, etc.
- Se valorará conocimientos en Arquitecturas Orientadas a servicios y herramientas vinculadas a su monitorización y prueba, como SOAPUI

Perfil: Técnico de monitorización

a) Titulación mínima y formación

- **Titulación:** Formación Profesional o superior en materias TIC

b) Tareas y responsabilidades

- Mantenimiento de la Infraestructura de monitorización: Comprobación del correcto funcionamiento de las diferentes herramientas de monitorización, así como de planificar las mejoras necesarias en su mantenimiento.
- Creación y mantenimiento de pruebas sintéticas:
  - Altas, bajas y modificación de las diferentes aplicaciones desarrolladas que se van a monitorizar.
  - Creación de scripts para comprobar peticiones de correo, realizar navegaciones web, enviar peticiones web services (tipo SOAP, REST)
- Creación y mantenimiento de agentes:
  - Altas, bajas y modificación de los diferentes elementos hardware que se van a monitorizar.
  - Altas de monitorizaciones tipo Ping.
  - Gestión de umbrales de aquellos parámetros que se estén monitorizando
- Supervisión de Alertas: Crear y revisar tanto la ejecución como el destinatario de las alertas en función de la evolución de los diferentes servicios.
- Creación y mantenimiento de cuadros de mando en función de las necesidades que tengan el resto de equipos.

- Análisis de eventos: Analizar situaciones anómalas que se detecten y nuevos desarrollos que necesiten supervisión.
- Agrupar las diferentes métricas obtenidas para dar una información de utilidad a los diferentes equipos.
- Resolución de incidencias que surjan en estas plataformas y escalado de las mismas a proveedores.
- Atender a las peticiones de las unidades de Desarrollo, Infraestructuras y de Atención al Usuario (CAUs) a las que la SGITS preste servicio.
- Atender a las peticiones de otras unidades del Área de Infraestructuras de la SGITS.
- Seguimiento de tareas e incidencias en las herramientas existentes en el Ministerio: BMC Remedy, Jira, Redmine u otras diferentes que se implanten a lo largo del periodo de ejecución del contrato.
- Mantenimiento y elaboración de documentación técnica.
- Participación en el mantenimiento de los inventarios relacionados con las plataformas objeto del contrato.

c) Experiencia previa para la capacitación del puesto

- Experiencia laboral de al menos **3 años** en proyectos de consultoría tecnológica de monitorización hardware y de servicios
- Experiencia laboral de al menos **3 años** en proyectos vinculados a la administración de herramientas de monitorización y gestión de eventos y alertas en entornos de producción
- Experiencia laboral de al menos **3 años** en proyectos de implantación, migración y gestión de herramientas de monitorización
- Experiencia de al menos **3 años** en gestión de servicios de monitorización con las siguientes herramientas de: Microfocus Business Process Monitor y/o BMC Truesight Operations Management (se requiere que uno de los dos perfiles del lote tenga la experiencia mínima en cada tecnología)
- Se valorará disponer de certificaciones de herramientas de monitorización, como: BMC Truesight Operations Management, Elastic Certified Observability, Opentext Application Performance Management (APM) Certified Professional, etc.

- Se valorará conocimiento de al menos 1 año de otras herramientas de monitorización y observabilidad: Zabbix, ELK, Dynatrace, Nagios, etc.
- Se valorará conocimientos en Arquitecturas Orientadas a servicios y herramientas vinculadas a su monitorización y prueba, como SOAPUI