

Pliego de Prescripciones Técnicas que han de regir el contrato de servicios denominado **“DISEÑO, IMPLEMENTACIÓN Y SUPERVISIÓN DE SERVICIOS DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID (2 Lotes)”** a adjudicar mediante procedimiento abierto con pluralidad de criterios



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**



CONTENIDO

CLÁUSULA 1.- INTRODUCCIÓN	4
CLÁUSULA 2.- OBJETO Y ALCANCE	4
CLÁUSULA 3.- CONSIDERACIONES GENERALES	5
CLÁUSULA 4.- LOTE 1: CENTRO DE OPERACIONES DE SEGURIDAD	6
4.1 Servicios requeridos.....	6
4.1.1 Servicios de prevención	7
4.1.2 Servicios de detección	8
4.1.3 Servicios de análisis y respuesta	10
4.1.4 Servicio de diseño y operación de procesos y tecnologías del SOC	11
4.1.5 Servicio de capacitación y formación en ciberseguridad.....	11
4.1.6 Servicio de soporte a la gestión y operación del SOC-MD.....	11
4.1.7 Servicios de asesoría y asistencia legal.	12
4.1.8 Incorporación de otros servicios de seguridad.	12
4.2 Modelo operativo y organización del SOC-MD	13
4.2.1 Modelo operativo: gobierno, operaciones y tecnologías del SOC.....	13
4.2.2 Modelo organizativo del SOC-MD	14
4.2.3 Equipo de trabajo	15
4.2.4 Horario y ubicación para la prestación del servicio	20
4.2.5 Tecnologías y herramientas del SOC-MD	20
CLÁUSULA 5.- LOTE 2: SOPORTE ESPECIALIZADO EN DISEÑO SEGURO.....	22
5.1 Servicio requerido	22
5.2 Equipo de trabajo	22
5.3 Organización de los recursos.....	24
5.4 Horario y ubicación.....	24
5.5 Tecnologías y herramientas	24
CLÁUSULA 6.- MODELO DE GESTIÓN	25
6.1 Dirección y seguimiento de los trabajos.....	25
6.1.1 Comité de Seguimiento del Contrato.	25
6.1.2 Comité Técnico y Operativo.....	26
6.2 Condiciones generales de los recursos del adjudicatario.....	26
6.3 Seguimiento y mejora continua del servicio.....	27
6.4 Facturación de los servicios	28
CLÁUSULA 7.- CONTENIDO DE LAS OFERTAS	29
7.1 Contenido de las ofertas para el LOTE I.....	30

7.1.1	Resumen ejecutivo.....	30
7.1.2	Solución técnica propuesta para los servicios requeridos.....	30
7.1.3	Planes operativos.....	31
7.2	Contenido de las ofertas para el LOTE II.....	32
7.2.1	Resumen ejecutivo.....	32
7.2.2	Solución propuesta para los servicios requeridos	32
7.2.3	Equipo de trabajo	32
7.2.4	Plan de Calidad.....	32
CLÁUSULA 8.- GESTIÓN DE LA SEGURIDAD		33
8.1	Protección de datos personales y Privacidad	33
8.1.1	Normativa	33
8.1.2	Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento	33
8.1.3	Obligaciones de la Agencia Madrid Digital para la prestación del servicio	36
8.1.4	Sub-encargos de tratamiento asociados a Subcontrataciones	36
8.1.5	Tratamiento de datos personales	37
8.2	Deber de Información.....	37
8.3	Seguridad en la utilización de medios electrónicos	38
8.3.1	Normativa	38
8.3.2	Conformidad con el Esquema Nacional de Seguridad	38
8.4	Medidas de Seguridad	38
8.4.1	Documentación de seguridad	38
8.4.2	Confidencialidad y deber de secreto.....	39
CLÁUSULA 9.- PROPIEDAD DE LOS TRABAJOS		39
CLÁUSULA 10.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS		39
CLÁUSULA 11.- CALIDAD DEL SERVICIO		40
CLÁUSULA 12.- PLAZO, DURACIÓN Y ETAPAS DE PRESTACIÓN DE LOS SERVICIOS		40
CLÁUSULA 13.- GARANTÍA DE LOS TRABAJOS.....		41
CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS.....		41
ANEXO I. REQUISITOS MÍNIMOS DEL SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM		42
ANEXO II. ENTORNO TECNOLÓGICO		49
ANEXO III. MODELO DE CURRÍCULUM.....		50
ANEXO IV. PRESUPUESTO		51
ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES.....		55

La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

CLÁUSULA 1.- INTRODUCCIÓN

La **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante Madrid Digital), según se establece en la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas, modificada parcialmente por la Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015), tiene asignada, entre otras funciones, la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente la seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad (Artículo 10, Tres).

Para cumplir esa función de seguridad, Madrid Digital, en su plan estratégico 2016-2020, ha definido una medida de ciberseguridad que comprende tres líneas de actuación:

1. Estrategia corporativa de seguridad de los servicios digitales.
2. Garantizar la seguridad de los servicios, los datos y su disponibilidad.
3. Fortalecer las capacidades de prevención, detección y respuesta ante ciberataques.

Como desarrollo de la línea estratégica 2, Madrid Digital está rediseñando su estrategia de seguridad para potenciar la definición de arquitecturas más seguras para los sistemas, servicios e infraestructuras de tecnologías de la información y de las comunicaciones (en adelante TIC) prestados a la Comunidad de Madrid, mediante la puesta en marcha de un servicio de Soporte especializado en Diseño Seguro de infraestructuras y tecnologías TIC, (en adelante SDS-MD).

Respecto a la línea estratégica 3, Madrid Digital requiere centralizar y mejorar sus capacidades en materia de ciberseguridad mediante la creación de un Centro de Operaciones de Seguridad, (en adelante SOC—Security Operation Center, SOC-MD), que aglutine y desarrolle las funciones de monitorización de seguridad, detección de incidentes, vigilancia antes nuevas fuentes de amenazas y análisis de vulnerabilidades, optimizando la capacidad de reacción y respuesta ante cualquier ataque. Por su naturaleza centralizada, el SOC-MD facilitará tanto la implantación de las herramientas y/o tecnologías más adecuadas en cada momento, como la adopción de las medidas oportunas para una defensa eficiente.

La puesta en marcha de ambos servicios, SDS-MD y SOC-MD permitirá la prevención de incidentes, gracias a la mayor resiliencia de los sistemas, servicios e infraestructuras TIC, debido al aumento de su seguridad desde el diseño, y a la mejora de su capacidad de respuesta y recuperación en caso que se materialice algún incidente de seguridad.

CLÁUSULA 2.- OBJETO Y ALCANCE

El objeto de este pliego es la prestación de servicios de diseño, implementación y supervisión de servicios de ciberseguridad de la Comunidad de Madrid, orientados a la mejora de la seguridad desde el diseño, y a la potenciación de las capacidades de seguridad en materia de prevención, detección, análisis y respuesta a incidentes de seguridad.

El ámbito de aplicación de estos servicios de seguridad se circunscribe a los sistemas, servicios e infraestructuras TIC competencia de Madrid Digital.

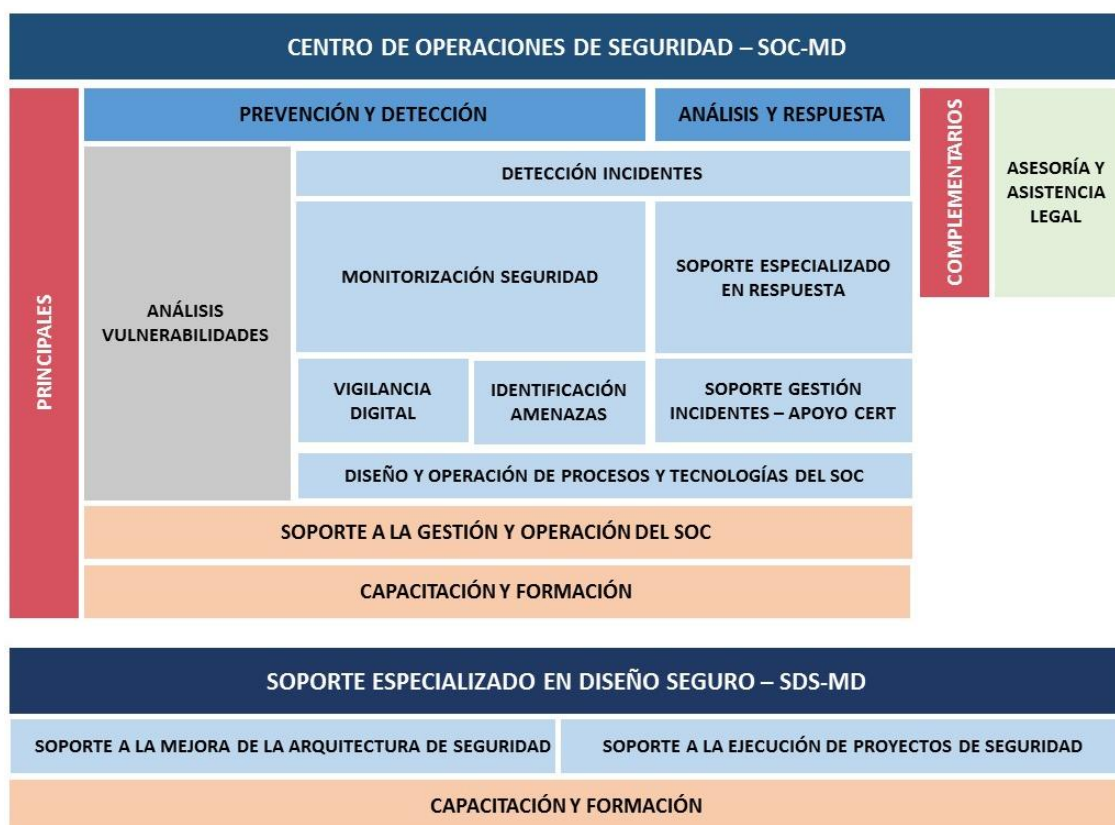
Debido a la diferente naturaleza de los servicios a contratar, el presente pliego establece una división en dos lotes atendiendo a la tipología de servicios requeridos, permitiendo así un correcto desarrollo de la estrategia de ciberseguridad definida por Madrid Digital:

- **Lote 1:** Centro de Operaciones de Seguridad, SOC-MD
- **Lote 2:** Soporte especializado en Diseño Seguro, SDS-MD

El Lote 1 tendrá por objeto la creación un **Centro de Operaciones de Seguridad, SOC-MD**, que centralice las capacidades actuales y futuras en materia de ciberseguridad de Madrid Digital. Para ello se suministrará e instalará un sistema de gestión de eventos e información de seguridad (SIEM –Security Information and Event Management), como herramienta principal de monitorización de la seguridad de las infraestructuras TIC, además de capacidades para la prevención y detección temprana de amenazas e incidentes, análisis de vulnerabilidades técnicas, y análisis y resolución de incidentes de seguridad, todo ello de forma centralizada y con procesos y procedimientos operativos de seguridad consistentes, que permitan reportes efectivos sobre el estado global de la seguridad y los riesgos TIC.

Como complemento del SOC-MD se crea e implanta el **Servicio Especializado en Diseño Seguro, SDS-MD**, objeto del Lote 2, que permitirá disponer de un soporte especializado para la definición y establecimiento de controles de seguridad, nativos y complementarios en las infraestructuras TIC soporte de los servicios prestados, y la definición e implantación de nuevos procesos y procedimientos, integrados con los ya existentes de gestión TIC y de respuesta a incidentes de seguridad.

En la siguiente figura se recogen las capacidades demandadas en cada uno de los lotes objeto de contrato, desarrolladas posteriormente en este pliego de prescripciones técnicas:



CLÁUSULA 3.- CONSIDERACIONES GENERALES

Con carácter obligatorio, los adjudicatarios se responsabilizarán durante el periodo de ejecución del contrato de la correcta operación, mantenimiento y actualización de los servicios requeridos, así como de los equipamientos, soluciones y herramientas que propongan para la prestación de los mismos.

Estarán obligados a conocer y observar la normativa interna aplicable en Madrid Digital, así como a incorporarla y tenerla en cuenta durante la ejecución del contrato. Ejemplos de este punto son: políticas de

control de acceso y gestión de recursos vigentes, normativas de seguridad aplicables, de instalación, de gestión patrimonial de equipamientos, procedimientos operativos relacionados con la gestión de TIC, etc.

La prestación de los servicios objeto de este pliego de prescripciones técnicas conllevará el cumplimiento de unos niveles de servicio acordados o comprometidos (ANS – Acuerdo de Nivel de Servicio), así como la definición de una política de penalizaciones ante incumplimientos, que los adjudicatarios estarán obligados a aceptar. Los niveles de servicio definidos se recogen en el **ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**.

CLÁUSULA 4.- LOTE 1: CENTRO DE OPERACIONES DE SEGURIDAD

4.1 Servicios requeridos

Será objeto de este lote la creación de un **Centro de Operaciones de Seguridad, SOC-MD**, que preste los siguientes servicios de ciberseguridad, organizados en 2 bloques, debido a su mayor o menor grado de integración requerido:

- **Servicios PRINCIPALES:**

- **Servicios de prevención:** consistentes en el análisis de vulnerabilidades de seguridad de los sistemas e infraestructuras TIC.
- **Servicios de detección:** orientados al desarrollo de monitorización de eventos de seguridad, capacidades de detección temprana de incidentes y amenazas, y vigilancia digital.
- **Servicios de análisis y respuesta:** orientados a mejorar el proceso de evaluación del impacto y la respuesta de incidentes, a través de un servicio de soporte especializado para la respuesta a incidentes y un servicio de soporte en la gestión de los incidentes.
- **Servicios de diseño y operación de procesos y tecnologías del SOC:** que facilitarán la definición de los procesos y procedimientos operativos del SOC, las integraciones entre los diferentes servicios y las tecnologías soporte.
- **Servicios de capacitación y formación en ciberseguridad,** orientados a mejorar la cualificación técnica del personal de seguridad de Madrid Digital.
- **Servicios de soporte a la gestión y operación del SOC,** de gobierno del SOC, orientados a la definición de cuadros de mando, métricas e indicadores, gestión centralizada de los servicios y gestión del conocimiento.

- **Servicios COMPLEMENTARIOS:**

- **Servicios de asesoría y asistencia legal,** como apoyo en la ejecución de medidas legales por parte de Madrid Digital en casos de incidentes graves de seguridad o acciones derivadas de obligaciones normativas y/o regulatorias.

El adjudicatario dotará, para la prestación de los mismos, el equipo humano, las capacidades técnicas, herramientas, metodologías y estructuras organizativas necesarias.

En el apartado de tecnologías y herramientas propuestas para la prestación de los servicios, los licitadores deberán tener en cuenta la adecuación de las mismas a las herramientas actuales de que disponga Madrid Digital, en caso necesario.

Con carácter general, se considerará dentro del coste de los servicios solicitados todos los gastos derivados de herramientas, desarrollos e integraciones con sistemas ya existentes o similar, propuestos por los licitadores como respuesta técnica a este pliego de prescripciones técnicas y que no estén específicamente presupuestados en la valoración económica de los servicios.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

En los siguientes apartados de este pliego se detalla el alcance de cada uno de los servicios demandados.

4.1.1 Servicios de prevención

Se prestarán los siguientes servicios de seguridad, orientados a la prevención de incidentes de seguridad:

4.1.1.1 Servicio automatizado de análisis de vulnerabilidades

El servicio de análisis de vulnerabilidades facilitará las capacidades técnicas necesarias para el descubrimiento y análisis de vulnerabilidades de seguridad en las infraestructuras TIC, aplicaciones y servicios de Madrid Digital.

Proporcionará una gestión completa del ciclo de vida de las vulnerabilidades, contemplando la planificación y ejecución de las actividades de identificación, el análisis de resultados, la notificación y reporte correspondiente, para su evaluación, priorización y definición de acciones de remediación por parte de Madrid Digital, y el seguimiento de las acciones correctivas definidas.

El servicio deberá cubrir los siguientes requisitos mínimos:

- Elaborar el inventario de activos y catalogar los mismos, permitiendo así un control de la planta instalada, las vulnerabilidades que afectan a cada activo y su configuración de seguridad.
- Identificar las principales fuentes de información y clasificación de vulnerabilidades en base a los activos instalados en Madrid Digital, siguiendo las referencias de vulnerabilidades publicadas por CVE (Common Vulnerabilities and Exposures) o por el NIST (National Institute of Standards and Technology).
- Planificar y ejecutar los análisis de vulnerabilidades, tanto de infraestructura como de sitios web, según las franjas horarias y restricciones trasladadas por Madrid Digital.
- Evaluar y validar los resultados obtenidos, en base a los activos y servicios descubiertos y vulnerabilidades detectadas.
- Explotar, de forma controlada, las vulnerabilidades detectadas, sin comprometer información sensible ni el servicio prestado, para verificar el impacto de la vulnerabilidad.
- Notificar los resultados para su seguimiento y gestión por parte de Madrid Digital.
- Facilitar un soporte técnico experto para la mejor comprensión del impacto de las vulnerabilidades detectadas, su priorización y la definición de plan de acción por parte de Madrid Digital.

El servicio de análisis automatizado de vulnerabilidades descrito se prestará como un servicio continuo, en base a las solicitudes de revisión de infraestructuras o sitios web que solicite Madrid Digital.

El adjudicatario estará obligado a asegurar que las actividades derivadas de este servicio no comprometan la integridad y disponibilidad de las infraestructuras y servicios analizados.

Los licitadores propondrán en su respuesta al apartado **4.2.5 Tecnologías y herramientas del SOC-MD** las herramientas de descubrimiento de activos, base de datos, catalogación, análisis de vulnerabilidades, notificación y gestión del ciclo de vida, que utilizarán para la prestación de este servicio, considerándose dentro del coste del servicio todos los gastos derivados de las mismas (licencias, mantenimientos, actualizaciones, etc.).

Para la prestación de este servicio, el adjudicatario pondrá a disposición de Madrid Digital los recursos recogidos en el apartado **4.2.3 Equipo de trabajo**.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

4.1.1.2 Servicio manual de análisis de vulnerabilidades o pruebas de intrusión.

El servicio manual de análisis de vulnerabilidades o pruebas de intrusión, tendrá como objetivo identificar vulnerabilidades de las aplicaciones en ejecución, desde el punto de vista de un atacante externo, analizando la lógica de negocio de cada aplicación.

Se estudiarán, como mínimo, las siguientes áreas de seguridad:

- Vulnerabilidades del sistema soporte de la aplicación.
- Vulnerabilidades que permitan la ejecución de código remoto por incorrecta validación de datos.
- Vulnerabilidades relacionadas con la autenticación, autorización y gestión de sesiones.
- Vulnerabilidades derivadas de configuraciones erróneas de seguridad o inadecuada actualización de componentes.
- Vulnerabilidades derivadas de empleo de métodos criptográficos débiles.
- Vulnerabilidades derivadas de incorrecta gestión de errores y logs de eventos de la aplicación.

El adjudicatario elaborará un informe de resultados en cada revisión, donde se describa el alcance, las pruebas realizadas y los resultados obtenidos, categorizados en base a niveles de riesgo e impacto para el servicio.

Los licitadores deberán indicar, en su oferta técnica, el equipo técnico de seguridad que pondrán a disposición de este servicio, así como la metodología de análisis que aplicará, áreas de seguridad a analizar y técnicas y herramientas de explotación de vulnerabilidades utilizadas.

Los análisis manuales de seguridad se realizarán habitualmente en el entorno de producción estando obligado el adjudicatario a asegurar que las actividades no comprometan la integridad de los datos objeto de revisión, la disponibilidad del servicio analizado ni otros servicios ajenos a la aplicación en revisión. De igual forma, por tratarse de aplicaciones en producción, las ventanas horarias de trabajo deberán ser acordadas entre Madrid Digital y el adjudicatario, normalmente fuera del horario de producción, para asegurar el mínimo impacto en el servicio analizado.

Para la prestación de este servicio, el adjudicatario pondrá a disposición de Madrid Digital los recursos recogidos en el apartado **4.2.3 Equipo de trabajo**.

4.1.2 Servicios de detección

Se prestarán servicios de monitorización de eventos de seguridad, vigilancia digital e identificación de amenazas, con los siguientes requisitos:

4.1.2.1 Servicio de monitorización de eventos de seguridad.

El servicio de monitorización de eventos de seguridad permitirá obtener un conocimiento centralizado del estado de la seguridad, mediante la recolección, procesamiento, explotación y correlación de los eventos o registros de log de las fuentes de información que defina Madrid Digital.

A tal fin, el servicio deberá contemplar la ejecución de las siguientes actividades:

- Suministro, instalación y mantenimiento de un sistema de Gestión de Eventos e Información de Seguridad (SIEM –Security Information and Event Management), incluyendo todos los elementos software y hardware necesarios para la recogida, análisis y almacenamiento de eventos.

El sistema de gestión de eventos deberá cumplir los requisitos mínimos recogidos en el **ANEXO I. REQUISITOS MÍNIMOS DEL SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE**



SEGURIDAD - SIEM, de este pliego de prescripciones técnicas. Esta actividad, a efectos de presupuesto, se recoge como **"Inversiones"**.

- Operación del servicio de monitorización, contemplando todas las tareas de mantenimiento y operación de la plataforma como son actualizaciones del sistema, backups, informes de servicio, integraciones de nuevas fuentes de eventos, y monitorización de la plataforma. Esta actividad, a efectos de presupuesto, se recoge como **"Mantenimiento plataforma SIEM"**.

Durante la ejecución del contrato, prioritariamente en la fase de operación del servicio, Madrid Digital podrá solicitar al adjudicatario la integración como una nueva fuente de datos de monitorización los eventos recogidos y recolectados por la plataforma actual de SIEM AlienVault del Servicio Madrileño de Salud (SERMAS) de la Consejería de Sanidad de la Comunidad de Madrid, sin incremento de coste en lo relativo a la integración de esta fuente en el sistema de gestión de eventos ni en la operación del servicio de monitorización.

4.1.2.2 Servicio de vigilancia digital e identificación de amenazas.

El servicio de vigilancia digital e identificación de amenazas se prestará como una solución integral dirigida a la detección temprana de posibles amenazas de seguridad.

Permitirá una valoración del impacto potencial en los servicios TIC prestados por Madrid Digital en caso de materialización de una amenaza de seguridad, y el análisis de las alternativas posibles de mitigación y/o contramedidas de seguridad a implementar.

Se prestará con dos enfoques:

- Uno, orientado a la recopilación y evaluación de amenazas de seguridad publicadas por fuentes externas como SOC's del adjudicatario, fabricantes de tecnología TIC, proveedores de servicios, servicios de alertas tempranas de seguridad, CERTS, etc., que puedan afectar a la seguridad de los servicios, sistemas e infraestructuras TIC gestionados por Madrid Digital.
- Otro, de monitorización de fuentes diversas de información, como redes sociales, sitios web, redes P2P, blogs, foros especializados, etc., que permita detectar:
 - publicaciones accidentales o premeditadas de información de servicios TIC de la Comunidad de Madrid, que puedan suponer un riesgo o perjuicio a su imagen,
 - fugas de información sensible propiedad de Madrid Digital o de la Comunidad de Madrid,
 - información sobre ataques organizados, suplantación de identidad, o actividades en general fraudulentas, relacionadas con usuarios y/o servicios de la Comunidad de Madrid.

El servicio facilitará una gestión completa del ciclo de vida de las amenazas detectadas, contemplando desde la recopilación y almacenamiento centralizado de los datos privados y públicos obtenidos, el procesamiento inteligente de los mismos, su clasificación y evaluación, la generación de alertas e informes, hasta las propuestas para mitigación y/o eliminación de la amenaza.

4.1.2.3 Servicio de detección de incidentes - Nivel N1

El servicio de detección de incidentes de seguridad de Nivel 1 facilitará una monitorización continua de los eventos y alarmas generadas por el resto de servicios de detección, monitorización, vigilancia digital e identificación de amenazas.

Se realizarán las funciones de identificación, clasificación, categorización, nivel de peligrosidad, impacto potencial, y documentación de los eventos de seguridad, así como un primer nivel de investigación a fin de identificarlo como posible incidente de seguridad, para su análisis por el siguiente nivel de atención.



El servicio se prestará en modalidad mixta, con personal desplazado en dependencias de Madrid Digital, en las condiciones recogidas en el apartado **4.2.3 Equipo de trabajo**, y personal en dependencias del adjudicatario, tal y como se recoge en el apartado **4.2.4 Horario y ubicación para la prestación del servicio**.

4.1.3 Servicios de análisis y respuesta

En el apartado de análisis y respuesta frente a incidentes y amenazas de seguridad, se demandarán los siguientes servicios:

4.1.3.1 Servicio de detección de incidentes nivel N2

El servicio de detección de incidentes de seguridad de Nivel 2 realizará las siguientes funciones:

- Confirmar los incidentes de seguridad, analizando la información recibida del Nivel 1 de detección y la información de vulnerabilidades obtenida del servicio de prevención.
- Estudiar el impacto del incidente, los activos afectados y el nivel de compromiso de los servicios.
- Proponer el plan de mitigación y remediación del incidente, en base a los procedimientos establecidos al efecto.
- Coordinar la ejecución de los planes de mitigación y remediación iniciados, hasta su finalización.
- Escalar si procede a los servicios especializados de respuesta a incidentes el caso detectado, para su evaluación y tratamiento.
- Documentar todos los casos tratados.

Para la prestación de este servicio, el adjudicatario pondrá a disposición de Madrid Digital los recursos recogidos en el apartado **4.2.3 Equipo de trabajo**.

4.1.3.2 Servicio especializado de respuesta a incidentes

El servicio de soporte especializado de respuesta a incidentes de seguridad facilitará capacidades avanzadas de apoyo en la evaluación de incidentes de seguridad graves, la identificación de la causa raíz, su alcance, la relación de activos afectados y el impacto para el negocio, así como el análisis de contexto o análisis forense de los eventos de la red, que permita situar el incidente en el tiempo determinar los orígenes del ataque, los medios utilizados y los objetivos.

El servicio facilitará también capacidades expertas en la definición de las medidas de contención a aplicar, así como las medidas para su eliminación, recuperación del servicio y preservación de evidencias.

Este servicio se prestará con personal del adjudicatario que, bien de forma remota o *in situ*, colabore con el personal de Madrid Digital aportando los procedimientos, procesos y herramientas necesarias en cada escenario.

Los requisitos del personal puesto a disposición por el adjudicatario para este servicio se recogen en el apartado **4.2.3 Equipo de trabajo**.

4.1.3.3 Servicio de soporte a la gestión de incidentes de seguridad.

El servicio de soporte a la gestión de incidentes de seguridad facilitará capacidades avanzadas de apoyo para la coordinación de la gestión de incidentes críticos, el despliegue de las medidas de contención definidas, y la aplicación de planes de recuperación del servicio, si procede, como complemento y apoyo al equipo de respuesta a incidentes de seguridad de Madrid Digital (CSIRT Computer Security Information Response Team o CERT – Computer Emergency Response Team).



Este servicio se prestará a demanda, con personal del adjudicatario que colabore con el personal de Madrid Digital aportando los procedimientos, procesos y herramientas necesarias en cada escenario.

Los requisitos del personal puesto a disposición por el adjudicatario para este servicio se recogen en el apartado **4.2.3 Equipo de trabajo**.

4.1.4 Servicio de diseño y operación de procesos y tecnologías del SOC

Dentro de este servicio se definirán e implementarán todos los procesos y procedimientos de gobierno y operativos del SOC, se definirán las arquitecturas de las diferentes soluciones para los servicios demandados y se implantarán, adaptarán y evolucionarán los servicios y las herramientas soporte correspondientes.

Serán funciones del servicio, entre otras, la identificación e integración inicial de las fuentes de eventos a monitorizar, y de las sucesivas que Madrid Digital solicite a lo largo del contrato, el modelado de amenazas, la definición y desarrollo de los casos de uso de monitorización, y la prestación en general, de un soporte experto al resto de componentes del SOC de las tecnologías implantadas para el servicio.

Se definirá y coordinará también dentro de este servicio la implantación de todas las herramientas de gestión del SOC, teniendo en cuenta los requisitos mínimos recogidos en el apartado **4.2.5 Tecnologías y herramientas del SOC-MD**, así como el diseño del portal de ciberseguridad, descrito en el apartado **4.1.6 Servicio de soporte a la gestión y operación del SOC-MD**

Para la prestación de este servicio, el adjudicatario pondrá a disposición de Madrid Digital los recursos recogidos en el apartado **4.2.3 Equipo de trabajo**.

4.1.5 Servicio de capacitación y formación en ciberseguridad

Los licitadores deberán incluir en su propuesta un Plan de Formación continuo, sin coste adicional, orientado a la capacitación del personal técnico de Madrid Digital sobre los servicios de seguridad, equipamientos y herramientas de gestión puestas a disposición del contrato.

La propuesta formativa deberá contemplar, como mínimo, lo siguiente:

- Formación en análisis de vulnerabilidades TIC: orientadas a la obtención de conceptos básicos de seguridad en infraestructuras TIC, configuraciones de seguridad, seguridad en entornos web y manejo de las herramientas de análisis automatizados y manuales propuestas para el servicio.
- Formación en administración y operación del sistema de gestión de eventos: Arquitectura del sistema desplegado, funcionalidades de los componentes y administración básica de la plataforma, reglas de detección y correlación, y componentes de recolección de datos.
- Formación en análisis forense: conceptos de la informática forense, técnicas y metodologías de análisis y evidencia digital.

Además, como impulso a las acciones de divulgación y sensibilización en materia de seguridad TIC y orientado al personal técnico de Madrid Digital, se valorará la puesta a disposición del contrato de contenidos formativos de carácter general, en forma de píldoras formativas, cursos on-line, vídeos divulgativos, o ejecución de campañas de evaluación del grado de concienciación en seguridad.

4.1.6 Servicio de soporte a la gestión y operación del SOC-MD

Como soporte a la gestión y operación del SOC, el adjudicatario del contrato deberá desarrollar y mantener un **Portal de Ciberseguridad TIC** desde el que se facilite un reporte integrado de todos los servicios puestos a disposición del contrato.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

Desde el portal se facilitará un acceso integrado a las consolas de gestión de los distintos servicios, las herramientas de seguimiento de vulnerabilidades, las bases de datos de conocimiento y activos, así como a los sistemas de reporting y control del servicio propuestos, procedimientos, cuadros de mando, indicadores, sistemas de alerta, informes de trabajos y, en general, toda la información de seguimiento y control generada.

El portal facilitará una vista pública, orientada a todo el personal de Madrid Digital, de carácter informativo y de divulgación general sobre las actividades del Centro de Operaciones de Seguridad, seguridad, y una vista privada, mediante autenticación y autorización de usuarios, para el seguimiento y control de los servicios, orientada al equipo de seguridad de Madrid Digital.

El portal de gestión será accesible vía web desde Internet, debiendo cumplir la metodología de desarrollo de portales de Madrid Digital. La tecnología de desarrollo preferente será Drupal o Joomla.

4.1.7 Servicios de asesoría y asistencia legal.

Los servicios de asesoría y asistencia legal complementarán el resto de servicios solicitados, facilitando un soporte legal en todas aquellas iniciativas que Madrid Digital deba realizar relativas a lo siguiente:

- La recuperación de información o contenidos publicados, obtenidos de forma fraudulenta y publicados en sitios web, foros o similar, detectados por los servicios de vigilancia digital.
- Asesoría en los procesos legales de respuesta a incidentes de seguridad detectados que puedan iniciarse.
- En general, en el análisis y adecuación de los procesos y procedimientos internos del SOC-MD a las obligaciones derivadas del cumplimiento de la normativa vigente.

Los requisitos del personal puesto a disposición por el adjudicatario para este servicio se recogen en el apartado **4.2.3 Equipo de trabajo**.

4.1.8 Incorporación de otros servicios de seguridad.

La constante y rápida evolución de las amenazas de seguridad, obliga a adaptar al mismo ritmo las capacidades de prevención, detección y respuesta de las organizaciones y sus mecanismos de protección frente a ataques a la seguridad de los sistemas, servicios e infraestructuras TIC.

Por ello, hay que tener en cuenta que en el ámbito de la Ciberseguridad es prácticamente imposible, definir con absoluta precisión el alcance y límites de todos los servicios de seguridad que se puedan requerir durante el periodo de ejecución del contrato, considerando que la tecnología evoluciona y cambia día a día, los ataques se profesionalizan y las TIC están ya presentes en todos los ámbitos competencia de la Administración de la Comunidad de Madrid (sanidad, educación, transportes, gestión administrativa, etc.)

En consecuencia, se contempla la posibilidad de incorporación, durante la vigencia del contrato, de servicios adicionales de seguridad orientados a la prevención, detección, análisis y respuesta de incidentes y amenazas de seguridad, que en el caso de que resulten estrictamente necesarios, se incorporarán de acuerdo con lo establecido para las modificaciones no previstas en la cláusula 27 – Modificación del contrato, del Pliego de Cláusulas Administrativas Particulares.



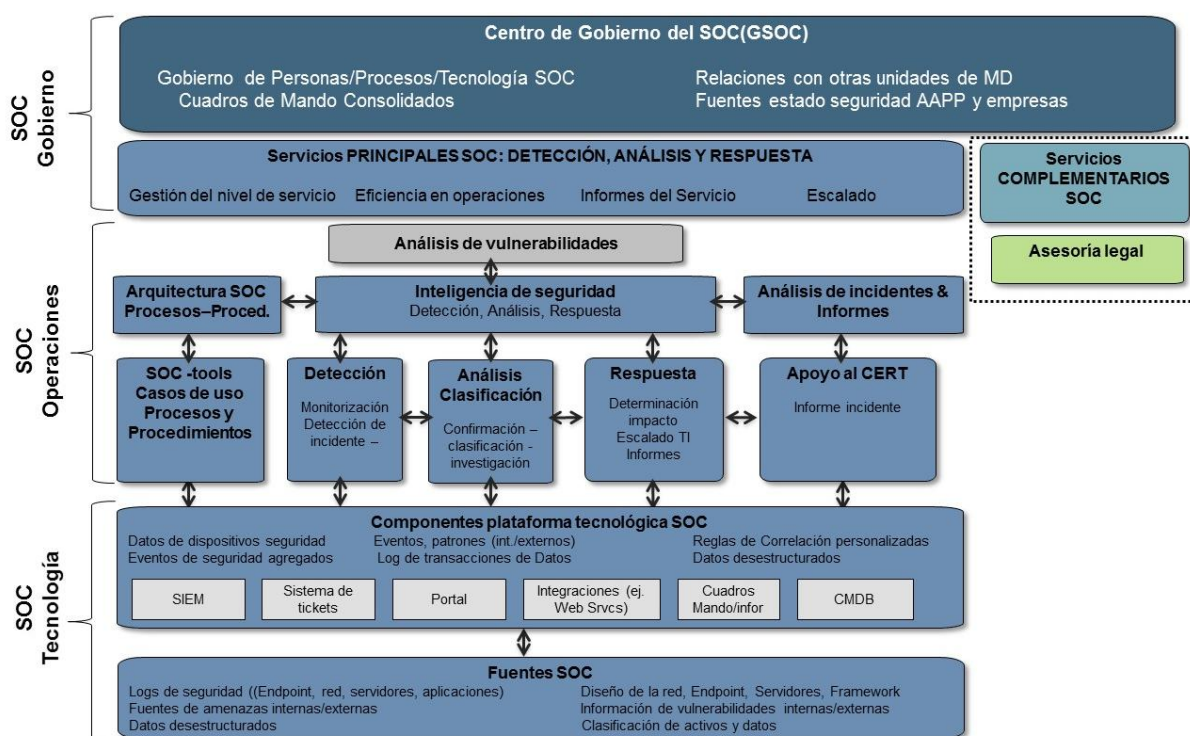
4.2 Modelo operativo y organización del SOC-MD

4.2.1 Modelo operativo: gobierno, operaciones y tecnologías del SOC

El modelo operativo relaciona los servicios que se prestan dentro del SOC, con las operaciones, procesos y procedimientos que las regulan, considerando las herramientas y tecnología que se requieren para su soporte. Es un modelo de Personas, Procesos y Tecnologías interrelacionadas, cuyo objetivo es prestar los servicios del SOC de forma eficaz y eficiente.

Todas estas operaciones deben de estar sujetas a la supervisión y control del centro de gobierno del SOC.

De forma gráfica el modelo operativo del SOC que se quiere implantar en Madrid Digital se resume de la siguiente forma:



Por tanto, el modelo operativo incluye su centro de gobierno, responsable de las actividades de gobierno y estrategia de las personas, procesos y tecnologías empleadas en el SOC, de las relaciones con otras unidades de Madrid Digital y con empresa, organismos de AAPP, etc. en materia de seguridad.

En lo que respecta al modelado de operaciones y tecnologías por cada servicio, el modelo operativo deber realizar las siguientes actividades para cada servicio:

- Descripción del servicio: detallando su objetivo, alcance y modelo de servicio.
- Definición de los procesos y procedimientos asociados: se deben documentar los procesos y procedimientos operativos, detallando los requisitos del proceso, responsables, actividades y resultados. Esto incluye:
 - Procedimientos de provisión.
 - Procedimientos de operación: gestión de peticiones, consultas e incidencias.
 - Procedimientos de soporte: gestión de cambios, gestión de la configuración, gestión de la capacidad, gestión de problemas, etc.

- Definición de los niveles de servicio: se deben especificar los diferentes indicadores de riesgo y de rendimiento asociados con cada uno de los servicios, que permita establecer niveles de acuerdo de servicio, ANS.
- Diseño de los interfaces, relaciones entre procesos, entradas salidas de información y flujos de información a integrar.
- Diseño de las herramientas y tecnologías que permitan prestar y gestionar los servicios de forma completa.

La relación de estas herramientas será desarrollada en su apartado correspondiente.

4.2.2 Modelo organizativo del SOC-MD

El modelo organizativo del SOC recoge como deben organizarse los recursos para prestar los servicios de forma eficiente.

Bajo la dirección del responsable del SOC de Madrid Digital y su equipo, el adjudicatario deberá nombrar un responsable único del servicio del SOC, Service Manager, que actuará a su vez como responsable único del proyecto.

Este responsable de servicio del SOC, organizará los recursos humanos del SOC en seis (6) funciones que se corresponden con los servicios principales y complementarios del SOC. Cada una de estas funciones contará con el equipo de trabajo que define en el apartado **4.2.3 Equipo de trabajo**, y al frente de cada una de ellas el adjudicatario pondrá un responsable de función, con el objetivo de facilitar la comunicación con el equipo de SOC de Madrid Digital.

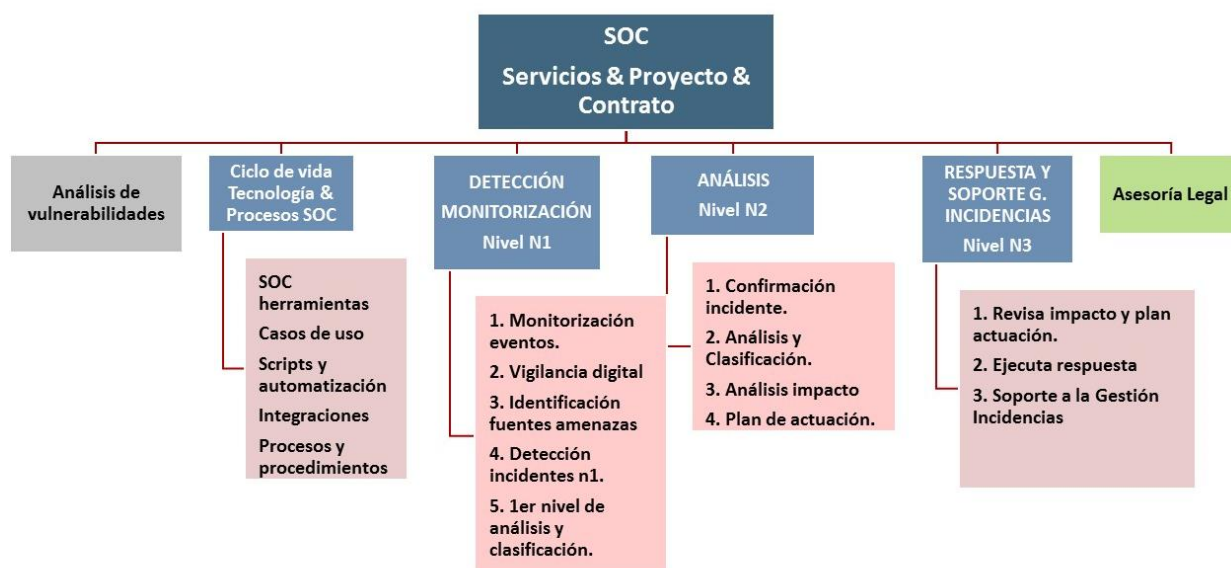
Estas 6 (seis) funciones son las siguientes:

- Detección, Monitorización – Nivel N1 de SOC.
- Análisis – Nivel N2 de SOC.
- Respuesta y Soporte a la Gestión de incidentes – Nivel N3 de SOC.
- Procesos & Tecnología de SOC.
- Análisis de vulnerabilidades.
- Asesoría Legal.

Dentro de este modelo organizativo el adjudicatario deberá considerar los requisitos de equipo mínimo que se indican en el apartado **4.2.3 Equipo de trabajo**, y los horarios, ubicación del equipo, indicados en el apartado **4.2.4 Horario y ubicación para la prestación del servicio**.

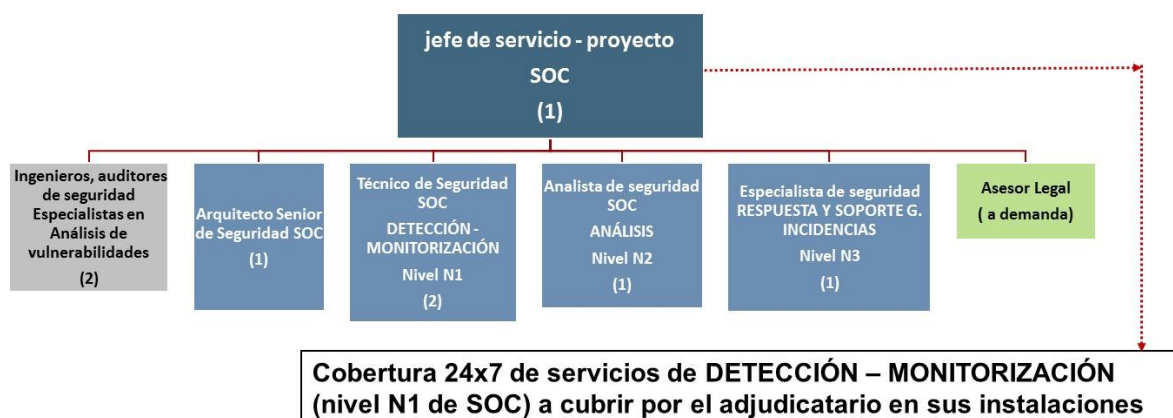
A continuación, se resume el modelo organizativo:





4.2.3 Equipo de trabajo

A continuación, se muestra el gráfico que resume la organización y funciones de las personas necesarias para constituir el SOC, indicando el mínimo de personas que deben constituir los equipos:



Los perfiles profesionales, sus funciones y sus requisitos de titulación, formación y experiencia son los siguientes:

- Jefe de servicio, jefe de proyecto del SOC (1 persona):
 - Responsable del diseño, implantación y operación diaria de los servicios y equipo de trabajo del SOC. Para ello deberá:

- Coordinar todo el proyecto y ser el responsable, en último término, de la buena marcha de los trabajos.
 - Interlocutor principal del responsable del SOC de Madrid Digital.
 - Ejercer el mando y la responsabilidad sobre el equipo completo del SOC.
 - Realizar la planificación general de los trabajos y de las tareas asociadas.
 - Asegurar la ejecución de las operaciones diarias del SOC según los ANS establecidos.
 - Asegurar que todo el personal del SOC sigue los procedimientos existentes y que todos ellos están documentados y a disposición de Madrid Digital.
 - Gestionar problemas e incidencias en las operaciones de seguridad que puedan comprometer el servicio y garantizar que se gestionen adecuadamente.
 - Asegurar el soporte técnico a los responsables de las unidades técnicas y de servicios de Madrid Digital, en relación a las integraciones de las fuentes de datos y eventos de seguridad con la plataforma de gestión de la seguridad (SIEM).
- Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager,) de la organización ISACA o CISSP (Certified Information Systems Security Professional) de la organización ISC², y formación en gestión de proyectos y/o gestión de servicios TI con certificaciones en ITIL, CoBIT, PRINCE2, PMP o equivalentes.
 - Requisitos en cuanto a EXPERIENCIA PROFESIONAL MÍNIMA: persona con diez (10) años de experiencia como responsable o gerente de SOC, o bien como jefe de proyecto y/o gerente de operaciones de seguridad TIC.
- Arquitecto senior de seguridad de SOC (1 persona):
 - Arquitectos especialistas funcionales y técnicos en la implantación de servicios de SOC, y por consiguiente en su diseño, despliegue de herramientas, procesos y tecnologías. Para ello deberá:
 - Diseñar e implantar la plataforma centralizada de gestión de eventos de seguridad (SIEM), asegurando la integración de las fuentes de datos de eventos necesarias.
 - Automatizar la carga de logs, eventos, modelado de amenazas, etc. en el SIEM
 - Crear y probar los casos de uso de modelado de comportamientos anómalos, probables incidentes, para su implantación en el SOC.
 - Definir y divulgar los procesos y procedimientos de operación del SOC.
 - Diseñar y mantener el portal del SOC, los cuadros de mando, la CMDB y el sistema de ticketing.
 - Detectar, mitigar y/o resolver problemas e incidencias en las operaciones de seguridad que puedan comprometer el servicio y garantizar que se gestionen adecuadamente.
 - Dar soporte técnico a los responsables de las unidades técnicas y de servicios de Madrid Digital, en relación a las integraciones de las fuentes de datos y eventos de seguridad con la plataforma de gestión de la seguridad (SIEM).
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA o OSCP (Offensive Security Certified Professional) de Offensive Security

- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con diez (10) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño y operación de sistemas SIEM, arquitectura de sistemas de detección y prevención de intrusión (IDS, IPS) de host y red, arquitectura de sistemas de seguridad perimetrales, cortafuegos de nivel 4 y nivel 7, proxys de control de acceso a Internet y sondas de análisis de seguridad de red.
- Técnicos de seguridad SOC DETECCIÓN nivel 1 (2 personas):
 - Técnicos de seguridad con experiencia en la monitorización de eventos de seguridad y detección de incidentes de seguridad. Realizará las siguientes actividades:
 - Identificar, categorizar, priorizar e investigar eventos de seguridad.
 - Controlar las colas de eventos entrantes para asegurar el procedimiento de detección
 - Realizar la investigación inicial y la clasificación inicial de posibles incidentes, y escalar o cerrar eventos según corresponda.
 - Supervisar la cola del ticket SOC (o correo electrónico) para posibles informes de eventos de entidades externas y usuarios individuales.
 - Mantener registros de cambios de SOC con actividad relevante.
 - Documentar los resultados de la investigación, asegurando que los detalles relevantes se pasen al nivel 2 para el análisis del posible incidente.
 - Actualizar las herramientas de actividad del SOC según sea necesario.
 - Realizar las actividades de vigilancia digital, recopilación información e inteligencia sobre amenazas y exploits emergentes.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: Técnico Superior en Administración de Sistemas Informáticos en red, o cualquier otra titulación de formación profesional de grado superior relacionada con las tecnologías de la información y de las comunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna certificación de fabricantes de soluciones de seguridad, Cisco, Palo Alto, HP Fortify, HP ArcSight, IBM, etc.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con tres (3) o más años de experiencia demostrable en operación y mantenimiento de plataformas de gestión de seguridad SIEM, análisis de logs de seguridad y tratamiento de eventos de redes, hosts, bases de datos, y de infraestructuras de seguridad perimetral, o bien, experiencia en labores de operación de cortafuegos, proxys de acceso a Internet, sistemas IPS, IDS y sistemas antimalware de puestos y servidores.
- Analistas de seguridad SOC ANÁLISIS – DETECCIÓN nivel 2 (1 persona):
 - Analistas de seguridad con experiencia en la confirmación, clasificación y análisis de incidentes de seguridad, determinando el impacto y proponiendo plan de actuación. Realizará las siguientes actividades:
 - Confirmación del incidente a través del análisis de la información pasada por el nivel 1 del SOC.
 - Análisis en profundidad del incidente, cotejando información de fuentes de amenazas, vulnerabilidades y eventos de seguridad, considerando toda la información recogida por el nivel 1.
 - Determinar el impacto del incidente, identificando activos afectados y nivel de compromiso.
 - Hacer el primer plan de mitigación, remediación del incidente.



- Ejecutar si procede y según los procedimientos establecidos la mitigación, remediación del incidente.
- Mantener registros de cambios de SOC con actividad relevante.
- Documentar los resultados de la investigación, haciendo el informe final en caso de resolución del incidente y cerrando el caso.
- Escalar a nivel 3 en caso de incidentes que no puedan resolverse en este nivel, asegurando que los detalles relevantes se pasen al nivel 3.
- Actualizar las herramientas de actividad del SOC según sea necesario.
- Requisitos en cuanto a TITULACIÓN MÍNIMA: Técnico Superior en Administración de Sistemas Informáticos en red, o cualquier otra titulación de formación profesional de grado superior relacionada con las tecnologías de la información y de las comunicaciones.
- Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA deberá disponer de alguna certificación de fabricantes de soluciones de seguridad, Cisco, Palo Alto, HP Fortify, HP ArcSight, IBM, etc.
- Requisitos en cuanto a EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) o más años de experiencia demostrable en administración de plataformas de gestión de seguridad SIEM, modelado de casos de uso, análisis en profundidad de logs de seguridad, detección de amenazas, detección y gestión de incidentes de seguridad, elaboración y ejecución de planes de mitigación de impacto, o bien, experiencia en labores de diseño y administración de cortafuegos, proxys de acceso a Internet, sistemas IPS, IDS y sistemas antimalware de puestos y servidores.
- Especialista de seguridad SOC RESPUESTA nivel 3 (1 persona):
 - Ingenieros expertos en seguridad TIC con experiencia en resolución o mitigación de incidentes. Realizará las siguientes actividades:
 - Resolución y/o mitigación de incidentes complejos que no puedan ser resueltos en el nivel 2.
 - Análisis en profundidad del incidente escalado, cotejando información de fuentes de amenazas, vulnerabilidades y eventos de seguridad, considerando toda la información recogida por el nivel 1 y nivel 2.
 - Realizar y/o completar el análisis de impacto del incidente, identificando activos afectados y nivel de compromiso.
 - Ejecutar si procede y según los procedimientos establecidos la mitigación, remediación del incidente.
 - Análisis de los resultados de los análisis de vulnerabilidades, de los tests de intrusión realizados a las infraestructuras tecnológicas y aplicaciones ejecutados en Madrid Digital, con el objetivo de prevenir la materialización de incidentes de seguridad, proponiendo los planes de mitigación.
 - Informar y dar soporte al CERT según los procedimientos establecidos.
 - Mantener registros de cambios de SOC con actividad relevante.
 - Documentar los resultados de la investigación, haciendo el informe final y cerrando el caso.
 - Actualizar las herramientas de actividad del SOC según sea necesario.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: : deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified



Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA o OSCP (Offensive Security Certified Professional) de Offensive Security.

- Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia en correlación avanzada de eventos y logs de seguridad, análisis de incidentes complejos de seguridad, mitigación de incidentes y realización de planes de análisis de impacto, respuesta y recuperación. Experiencia en gestión de incidentes y colaboración con equipos de CERT de comunicación de incidentes. Debe de disponer de experiencia en procesos y tecnologías de análisis de vulnerabilidades y detección de amenazas, con el objetivo de prevenir la materialización de incidentes de seguridad.
- Ingenieros, auditores, analistas de seguridad de vulnerabilidades (2 personas):
 - Especialistas con experiencia en la realización de escaneos de vulnerabilidades y test de intrusión a sistemas, BBDD, sistemas operativos, entornos virtuales, redes y aplicaciones.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA, OSCP (Offensive Security Certified Professional) de Offensive Security, o certificaciones de fabricantes de escáneres de vulnerabilidades de Nessus o Qualys.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en técnicas y herramientas de escaneos de vulnerabilidades en sistemas, aplicaciones, hosts y equipos de red, realización de análisis de resultados de escaneos, determinación de impacto y propuesta de mitigación.
- Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones (a demanda):
 - Expertos en ordenamiento jurídico en materias de derecho de las tecnologías de la información y de las comunicaciones, seguridad de la información y protección de datos.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado en Derecho, Licenciado en Derecho, o equivalente.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de algún postgrado relacionado con derecho de Internet, derecho de las TIC, etc.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia en asesoría legal en empresas y/o AAPP en relación a la legislación vigente en materia de seguridad de la información y protección de datos, aplicada a la protección de información, sistemas, redes e infraestructuras tecnológicas.

Al efecto, el licitador que presente la mejor oferta, deberá aportar el *currículum vitae* de las personas asignadas a la ejecución del contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).



4.2.4 Horario y ubicación para la prestación del servicio

El horario de prestación del servicio será con carácter general de 8 a 20:00 horas en días laborables, **en modo presencial en las dependencias de Madrid Digital**. Madrid Digital podrá requerir al adjudicatario la prestación de determinados servicios en sus dependencias, lo que se definirá en la fase de puesta en marcha del servicio. El personal del SOC-MD tendrá disponibilidad para desplazarse a los distintos centros dependientes de la Comunidad de Madrid dentro del ámbito de competencia de Madrid Digital.

Los servicios del SOC-MD especialmente para las tareas de monitorización de eventos de seguridad y vigilancia digital, serán prestados en horario de 24 horas, 7 días a la semana. En el caso de la necesidad de ejecutar tareas planificadas relacionadas con las herramientas del SOC y/o con sus integraciones con fuentes de datos de eventos, o bien, si se confirmara un incidencia de seguridad, y en ambos casos, 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, Madrid Digital no aceptará sobre-coste adicional por estas circunstancias, que deberán ser absorbidos siempre por el contratista.

4.2.5 Tecnologías y herramientas del SOC-MD

Todos los servicios del SOC requieren de tecnología y herramientas para cumplir su cometido. Se distinguirán entre herramientas para prestar los servicios de seguridad y herramientas de gestión y soporte a la operación del SOC.

El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas del SOC-MD. Preferentemente se optará por soluciones opensource, y en todo caso, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para Madrid Digital. A la finalización del contrato todas estas herramientas pasarán a ser propiedad de Madrid Digital.

Estas herramientas se instalarán en hardware facilitado por Madrid Digital, acorde a las tecnologías y soluciones establecidas por su departamento de sistemas. A tal fin, los licitadores detallarán en su propuesta el hardware necesario para cada herramienta y propuesta alternativa en caso de no disponer de este (soluciones en nube, equipamiento propio, etc.).

Queda fuera de las condiciones anteriores el sistema de gestión de eventos, SIEM y de todas sus tecnologías complementarias, como pueden ser sondas, analizadores de flujo de red o escáner de vulnerabilidades integrados, que deberá ser suministrado y valorado por el licitador tal y como se indica en este pliego.

La relación de herramientas MÍNIMAS necesarias (excluido el SIEM) son las siguientes:

- **Herramientas mínimas de prestación de servicios de seguridad del SOC:**
 - **Análisis de vulnerabilidades:** Analizadores de vulnerabilidades de hosts y red. Inspección del estado de seguridad de servicios, sistemas y tecnologías. Herramientas de descubrimiento de activos, base de datos, catalogación y gestión del ciclo de vida de las vulnerabilidades.
 - **Monitorización:** plataforma de monitorización de seguridad SIEM + sondas + integración con fuentes de amenazas externas, cuya funcionalidad es la centralización y correlación de eventos de seguridad.
 - **Vigilancia digital:** Rastreadores, analizadores, agregadores de información en Internet de amenazas y riesgos tecnológicos. Detección de amenazas, riesgos y ataques publicados en Internet contra los servicios TIC de la Comunidad de Madrid.
- **Herramientas de gestión y soporte a la operación del SOC:**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

- **Sistema integral de CMDB:** como referencia se podrá optar por una solución integral opensource, llamada GLPI, y que será mantenida por el personal del SOC. Entre sus características se encuentran:
 - Sistema de gestión de cambios.
 - Sistema de ticketing integral, para dar apoyo al sistema de ticketing principal.
 - Sistema de notificaciones.
 - Inventario, contactos.
 - Características Multi Tennant.
 - Gestión de SLA.
 - Calendarios de técnicos y entidades.
 - Perfiles de gestión.
 - Base de conocimiento.
- **Sistema de monitorización de salud:** el sistema de monitorización de salud de toda la plataforma asociada al SOC estará basado en plataforma opensource, por ejemplo Nagios.
- **Sistema de gestión documental:** se propone utilizar el propio sistema de gestión documental y BBDD de conocimiento disponible en GLPI.
- **Cuadros de mando e informes.**
- **Software de gestión de contenidos de portales:** tipo opensource Joomla, Drupal, etc.



CLÁUSULA 5.- LOTE 2: SOPORTE ESPECIALIZADO EN DISEÑO SEGURO

Será objeto de este lote la creación de un **Servicio de Soporte Especializado en Diseño Seguro, SDS-MD**, que facilite un soporte especializado para la mejora de la arquitectura de seguridad de las infraestructuras y servicios TIC prestados por Madrid Digital a la Comunidad de Madrid.

El objetivo del servicio será proponer, definir y diseñar controles técnicos de seguridad, nativos y complementarios, que mejoren las arquitecturas de los servicios e infraestructuras desde su diseño.

El entorno tecnológico de referencia sobre el que se desarrollarán las actividades de soporte se recoge en el **ANEXO II. ENTORNO TECNOLÓGICO**.

A continuación se detallan las actividades a realizar y el equipo de trabajo requerido para la prestación del servicio.

5.1 Servicio requerido

Las actividades a desempeñar con carácter general para este servicio de soporte especializado en diseño seguro, al amparo del servicio son las siguientes:

- Mejora de la seguridad de las arquitecturas técnicas desde el diseño, mediante la definición de las políticas y controles de seguridad en cada escenario, considerando la legislación, normativa de seguridad de Madrid Digital, buenas prácticas y referencias de arquitecturas seguras, como son las del NIST (National Institute of Standards and Technology del gobierno de EEUU), las del CCN (Centro Criptológico Nacional de España) teniendo en cuenta la arquitectura técnica implantada. Básicamente deberán trabajar en la realización de:
 - Procedimientos e instrucciones técnicas de bastionado seguro de componentes de arquitecturas técnicas.
 - Recomendaciones de soluciones y tecnologías adicionales que puedan complementar la seguridad del servicio, sistema y/o infraestructura tecnológica.
 - Guías de mejora de la seguridad de los procedimientos operativos de tecnologías de información.
 - Revisiones de estado de seguridad y propuesta de mejora.
- La creación de una base de datos de configuraciones de seguridad, que complemente los procesos de gestión de configuraciones existentes en Madrid Digital.
- La definición, creación de scripts y herramientas que sean capaces de detectar y comprobar si los controles de seguridad están aplicados.
- La asistencia técnica en materia de seguridad en las fases de definición y diseño de proyectos tecnológicos y de desarrollo en el ámbito de Madrid Digital.

En el apartado siguiente de equipo de trabajo se especifica los requisitos de titulación, formación y experiencia, para cada perfil requerido, que son los siguientes:

- Perfil de experto en seguridad perimetral y de las comunicaciones.
- Perfil de experto en seguridad de sistemas.
- Perfil de experto en seguridad de otras tecnologías.

5.2 Equipo de trabajo

Se requerirá el siguiente equipo mínimo de trabajo:



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: 0981582682548263284025

- Arquitecto, Ingeniero de seguridad perimetral y de las comunicaciones (2 personas): expertos en diseño seguro con experiencia en labores de diseño e implantación de tecnologías de seguridad perimetral y de las comunicaciones de voz y datos.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CCNA (Certified Network Associate Security) de la empresa Cisco, Certificaciones de seguridad de Palo Alto o Checkpoint, o bien CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad perimetral de red datos, con experiencia demostrable en diseño, administración y soporte de seguridad de redes, cortafuegos, gestión de soluciones VPN, y diseño seguro de elementos de comunicaciones de nivel 2, 3 (switches, routers).

Excepcionalmente, se admitirán perfiles con titulaciones mínimas de formación profesional de grado superior relacionadas con las tecnologías de la información y las comunicaciones, como Técnico Superior en Administración de Sistemas Informáticos, siempre que acrediten una experiencia profesional mínima de diez (10) años en los entornos requeridos para este perfil.

- Arquitecto, ingeniero de seguridad de sistemas (1 persona): expertos en diseño seguro de sistemas operativos de servidor UNIX y Windows, bases de datos Oracle, SQL Server y MySQL (1 persona)
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, OSCP (Offensive Security Certified Professional) de Offensive Security, certificaciones de seguridad en sistemas operativos de servidor y bases de datos.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: persona con cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño seguro de servidores y bases de datos.
- Arquitectos de seguridad, expertos en seguridad de otras infraestructuras TIC (a demanda) como pueden ser entornos web y de colaboración, puesto de trabajo ofimático, servicios en cloud, y cualquier otro que Madrid Digital tenga en producción o esté evaluando su implantación.
 - Requisitos en cuanto a TITULACIÓN MÍNIMA: titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
 - Requisitos en cuanto a FORMACIÓN MÍNIMA COMPLEMENTARIA: deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, CSX (Cybersecurity Fundamentals Certificate) de la organización ISACA, OSCP (Offensive Security Certified Professional) de Offensive Security, y certificaciones de seguridad de Microsoft.
 - Requisitos en cuanto EXPERIENCIA PROFESIONAL MÍNIMA: debido a que este perfil es a demanda se asume que pueden ser varias personas las que pueden prestar el servicio según su tipología, servicio específico: seguridad en entornos de trabajo, entornos de colaboración, puesto de trabajo ofimático o servicios en cloud. En todo caso la persona que preste el servicio, debe disponer



de cinco (5) años de experiencia como arquitecto de seguridad en cada servicio de seguridad requerido.

Este servicio se ofrecerá a demanda, en función de las necesidades de Madrid Digital. En todo caso, el licitador deberá acreditar la disponibilidad de personal técnico cualificado, experto en, como mínimo, las siguientes tecnologías:

- Entornos de colaboración: Sharepoint, Office 365.
- Gestores de contenidos: Joomla, Drupal.
- Puesto de trabajo ofimático: sistemas operativos Windows Android e IOS, para PC, portátil, Smartphone y tablets.
- Aplicaciones web, entornos web, y servicios CDN.

Al efecto, el licitador que presente la mejor oferta, deberá aportar el *currículum vitae* de las personas asignadas a la ejecución del contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).

5.3 Organización de los recursos

Bajo la dirección del responsable del servicio SDS-MD de Madrid Digital y su equipo, el adjudicatario deberá nombrar un responsable de servicio por su parte.

Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la Dirección de Madrid Digital designe a los efectos.

El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que Madrid Digital determine, informará sobre la planificación de trabajos, el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas. En particular, este responsable será el interlocutor único entre el adjudicatario y Madrid Digital. Coordinará toda la prestación del servicio y será el responsable, en último término, de la buena marcha de los trabajos. Entre sus tareas principales cabe destacar las siguientes:

- Coordinar la ejecución de los trabajos.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Supervisar y controlar la calidad de las actividades desarrolladas por su equipo.
- Hacer entrega a Madrid Digital de los documentos desarrollados por su equipo.

5.4 Horario y ubicación

El horario de prestación del servicio será con carácter general de 8 x 5, en la franja horaria de 8:00 a 18:00 horas en días laborables, en modo presencial en las dependencias de Madrid Digital. Madrid Digital podrá requerir al adjudicatario la prestación de determinados servicios en sus dependencias, lo que se definirá en la fase de puesta en marcha del servicio. El personal del SDS-MD tendrá disponibilidad para desplazarse a los distintos centros dependientes de la Comunidad de Madrid dentro del ámbito de competencia de Madrid Digital.

5.5 Tecnologías y herramientas

El adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas del servicio SDS-MD, tanto de gestión como de soporte a sus actividades. Preferentemente se optará por soluciones opensource, y en todo caso, estarán valoradas dentro del coste de los servicios, por lo que no incurrirá en costes adicionales para Madrid Digital. A la finalización del contrato todas estas herramientas



pasaran a ser propiedad de Madrid Digital. El licitador detallará en su propuesta el hardware necesario para cada herramienta que será provisionado por Madrid Digital.

CLÁUSULA 6.- MODELO DE GESTIÓN

6.1 Dirección y seguimiento de los trabajos

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de Madrid Digital, con objeto de garantizar la correcta ejecución de los mismos, y el cumplimiento por tanto de los objetivos del proyecto.

De cara a alcanzar estos objetivos estratégicos, se define una estructura de seguimiento para cada uno de los lotes del contrato en dos niveles:

- **Nivel estratégico:** orientado a asegurar la correcta evolución del contrato y la mejora de los servicios, que se encargará de velar porque la estrategia y objetivos de la contratación de servicios estén alineados con los objetivos de Madrid Digital, así como de controlar y garantizar que todas las decisiones y operaciones se ajusten a dicha estrategia.
- **Nivel operativo,** ligado a la ejecución concreta de los servicios, que se encargará de transformar las decisiones estratégicas en planes de acción y de dirigir y controlar los esfuerzos necesarios para su ejecución.

Atendiendo a la estructura señalada y para cada uno de los lotes, se establecerán Comités diferenciados a dos niveles para el control y la toma de decisiones:

- **Nivel Estratégico:** Comité de Seguimiento del Contrato (CSC).
- **Nivel Operativo:** Comité Técnico y Operativo (CTO).

Una vez iniciada la ejecución del contrato, se procederá al nombramiento de ambos Comités, de Seguimiento del Contrato y Técnico y Operativo, que incorporarán personal perteneciente a Madrid Digital y a la empresa adjudicataria de cada lote.

6.1.1 Comité de Seguimiento del Contrato.

El Comité de Seguimiento del Contrato estará compuesto por el Responsable del Contrato de Madrid Digital y las figuras que éste defina al respecto, y por parte de los adjudicatarios, el Responsable Comercial y el Responsable del Servicio.

Las funciones de este Comité serán, entre otras, las siguientes:

- Monitorizar el avance global de los servicios.
- Aprobar los cambios propuestos en el seno del Comité Técnico y Operativo que afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión o que, por su impacto o importancia estratégica, requieran la aprobación del Comité.
- Controlar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo.
- Acordar la adopción de propuestas de mejora y medidas correctoras o preventivas que deba desarrollar e implantar el adjudicatario, previa autorización de Madrid Digital, en caso de incumplimiento de los ANS o derivadas de planes de mejora.
- Revisar los niveles de servicio inicialmente requeridos, en base a la mejora continua del mismo.
- Determinar el grado de incumplimiento de ANS con el objeto de aplicar las correspondientes penalizaciones que se establecen en el presente pliego de prescripciones técnicas.
- Revisar y resolver cualquier incidencia o problema relacionado con la facturación de los servicios.



- Aprobar ajustes de los ANS definidos en el Pliego y su adaptación a la evolución de los servicios contratados.
- En el caso de que se observase la necesidad de incorporar nuevos servicios de seguridad o componentes que supongan nuevas unidades facturables, y resulten necesarios para la adaptación de la prestación del servicio a las nuevas demandas de seguridad, proponer la modificación de contrato necesaria.
- Cualquier otro asunto que el propio Comité considere de interés.

El Comité de Seguimiento del Contrato celebrará sus reuniones en las dependencias de Madrid Digital, con la periodicidad que él mismo determine o, en ausencia de otras indicaciones al respecto, a propuesta del Responsable del Contrato.

Los acuerdos adoptados en el seno del CSC deberán ser de mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario de cada lote será responsable de la elaboración de las actas, y su paso a revisión por los asistentes al Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y a la presentación del acta definitiva para la firma.

6.1.2 Comité Técnico y Operativo.

El Comité Técnico y Operativo estará formado por personal de las áreas técnicas de Madrid Digital y por los responsables del servicio que designen los adjudicatarios. Su principal objetivo será el seguimiento de la implantación y explotación de los servicios.

Las funciones de este Comité serán, entre otras, las siguientes:

- Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de riesgos.
- Garantizar que el personal asignado por el contratista para la ejecución de los servicios está disponible y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.
- Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los acuerdos de nivel de servicio (ANS) de cada periodo.
- Analizar y validar, si procede, las propuestas de mejora del servicio efectuadas por el adjudicatario. En caso de que las propuestas afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o tengan impacto o importancia estratégica, serán elevadas al Comité de Seguimiento del Contrato.
- Revisar el estado y evolución de los planes de mejora acordados y cumplimiento de los compromisos aprobados.
- Cualquier otro asunto que el propio Comité considere de interés.

Los acuerdos adoptados en el seno del Comité deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. Los adjudicatarios serán responsables de la elaboración de las actas y su traslado 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 de los asistentes.

6.2 Condiciones generales de los recursos del adjudicatario

Para la correcta prestación de los servicios requeridos se considera imprescindible dedicar a la ejecución del contrato, los recursos humanos mínimos detallados en los apartados **4.2.3 Equipo de trabajo**, para el Lote I, y **5.2 Equipo de trabajo**, para el Lote II, siendo responsabilidad de cada adjudicatario la aportación de los recursos adicionales necesarios para el cumplimiento de los acuerdos de nivel de servicio exigidos. Los



adjudicatarios deberán poder garantizar los recursos humanos que satisfagan la demanda de requerimientos durante la vigencia del contrato.

Los empleados de los adjudicatarios que ejecuten por cuenta de éste trabajos directamente relacionados con el objeto del presente contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por su propia organización, entendiendo como tal ordenador personal, teléfonos móviles, tablets, licencias software ofimático, etc., a excepción de los equipos PCs, puestos de trabajo en las dependencias de Madrid Digital, que serán provisionados por ésta siguiendo sus estándares de configuración.

Específicamente para el personal del Lote I, dado que los servicios del SOC de Madrid Digital a los que da cobertura dicho lote necesitan una disponibilidad o localización en horario de 24 x 7, el adjudicatario debe proveer a su personal de teléfonos móviles para su localización inmediata fuera del horario presencial.

Los licitadores deberán aportar, en el **Sobre Nº 1: Documentación Administrativa** documento de compromiso en el que señalen, que de resultar adjudicatarios del contrato, pondrán a disposición del servicio un equipo de trabajo, con un número de integrantes adecuado, que cumpla los requerimientos mínimos exigidos, y de estabilidad del equipo, recogidos en el presente pliego de prescripciones técnicas.

Los licitadores que presenten la mejor oferta y en el plazo que le sea requerido, aportarán Currículum Vitae de las personas propuestas para la ejecución del contrato, siguiendo el modelo definido en el **ANEXO III. MODELO DE CURRÍCULUM**, que detalle sus datos profesionales (Categoría profesional, titulación, formación y experiencia), así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

Una vez iniciada la ejecución del contrato y por motivos debidamente justificados, Madrid Digital podrá solicitar la sustitución, sin coste adicional, de los recursos asignados a la ejecución del contrato, debiendo realizarse en el plazo de un mes desde su solicitud.

La falsedad en el nivel de conocimientos y experiencia de los miembros del equipo asignado por el adjudicatario, así como la sustitución de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y requisitos exigidos en los apartados siguientes, facultará a Madrid Digital para instar la resolución del contrato.

Además, el adjudicatario deberá garantizar que dispone de los mecanismos adecuados para minimizar la rotación no planificada de los recursos puestos a disposición para el contrato, y así evitar la pérdida no controlada de conocimiento, el impacto en los niveles de servicio y la dedicación adicional de personal de Madrid Digital que estas situaciones suelen llevar asociadas.

6.3 Seguimiento y mejora continua del servicio.

Durante el periodo de ejecución del contrato, el adjudicatario de cada Lote propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada. Asimismo, las empresas adjudicatarias habilitarán un **Plan de Seguimiento y Control de Calidad** de los trabajos desempeñados por su personal efectuando, caso de no ser satisfactoria la calidad de los mismos, las medidas correctoras y las horas adicionales que sean necesarias para solventar cualquier incidencia, las cuales correrán por cuenta de cada adjudicatario, en caso de que las anomalías se debieran a falta de preparación de alguno de los técnicos o a otras causas imputables a la misma empresa.

A tal efecto, los licitadores deberán aportar, en el **Sobre Nº 2: Documentación Técnica**, un Plan de Calidad, indicando al menos lo siguiente:

- Cómo se pretende cumplir los niveles de calidad exigidos.
- Cómo se pretenden verificar los cumplimientos.

- Cómo se realimenta el proceso con correcciones en caso de desviaciones de los cumplimientos.

No obstante, durante el desarrollo de los trabajos objeto de contrato, Madrid Digital podrá establecer acciones de seguimiento sobre el control de la calidad y la actividad desarrollada. En todo caso, el seguimiento y control de la ejecución del contrato se efectuará sobre las siguientes bases:

- Seguimiento continuo de la evolución del servicio entre el Responsable del Servicio de cada adjudicatario y el Responsable de Contrato de Madrid Digital o quién éste designe.
- Madrid Digital podrá determinar los procedimientos y herramientas a utilizar para poder llevar cabo la planificación, seguimiento y control del servicio.
- Seguimiento, mejora y optimización de los servicios prestados.

Así, para el adecuado seguimiento del servicio, evaluación y mejora continua del grado de calidad del mismo se consideran necesarios al menos los siguientes documentos, a entregar con periodicidad mensual:

- Informe de seguimiento económico y ANS.
- Informe de seguimiento del servicio.

El incumplimiento de estas obligaciones dará lugar a la aplicación de la correspondiente penalización, según lo indicado en el **ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES** de este pliego y en el pliego de cláusulas administrativas.

6.4 Facturación de los servicios

Para el cálculo del presupuesto base de licitación que figura en el **ANEXO IV. PRESUPUESTO** se ha tenido en cuenta los conceptos que se detallan en los siguientes apartados de esta cláusula.

Según se detalla en el **ANEXO IV. PRESUPUESTO**, la facturación de cada lote se desglosará por tipo según se trate de cuota fija, cuota variable, y/o inversión. Dentro de cada tipo se han desarrollado ítems que representarán cada uno de los elementos facturables contemplados en el pliego.

Dentro del presupuesto, la estimación anual realizada de las unidades de cuota variable no implica un compromiso formal de adquisición, sino una estimación de la realidad prevista en la Comunidad de Madrid, a lo largo de la ejecución del contrato.

La facturación de estos servicios de cuota variable se realizará según el precio/hora establecido para el perfil técnico correspondientes, según se recoge en el pliego de cláusulas administrativas.

Por otra parte, aquellos conceptos relacionados con servicio, explotación o inversiones solicitadas a lo largo de este pliego de prescripciones técnicas, así como aquellos conceptos que los licitadores crean necesarios para la ejecución del contrato, pero que no aparecen explícitamente reflejados en el **ANEXO IV. PRESUPUESTO** deberán considerarse económicamente prorrateados en los conceptos contemplados en éste.

A continuación se describen los conceptos recogidos y su forma de facturación:



LOTE 1:

- **Cuota fija:** recoge todos los conceptos facturables mensualmente durante la vigencia del contrato, de los siguientes servicios:
 - Servicios de prevención:
 - Servicio automatizado de análisis de vulnerabilidades.
 - Servicio manual de análisis de vulnerabilidades.
 - Servicios de detección:
 - Servicio de monitorización de eventos de seguridad (mantenimiento de plataforma SIEM).
 - Servicio de vigilancia digital e identificación de amenazas.
 - Servicio de detección de incidentes – Nivel N1.
 - Servicios de análisis y respuesta:
 - Servicio de detección de incidentes – Nivel N2.
 - Servicio especializado de respuesta a incidentes.
 - Servicio de diseño y operación de procesos y tecnologías del SOC.
 - Servicio de soporte a la gestión y operación del SOC.
- **Cuota variable:** recoge todos los conceptos por los que se facturará a demanda, en base a hora de dedicación.
 - Servicios de análisis y respuesta:
 - Servicio de soporte a la gestión de incidentes de seguridad: perfil Especialista de Seguridad.
 - Servicios de asesoría y asistencia legal: perfil Consultor Legal.
- **Inversiones:** recoge todos los conceptos por los que se facturará una única vez cuando se produzca el hito de entrega o de puesta en servicio. Este apartado aglutina toda la infraestructura a suministrar asociada al sistema de gestión de eventos (SIEM).

LOTE 2:

- **Cuota fija:** recoge todos los conceptos facturables mensualmente durante la vigencia del contrato, de los servicios de:
 - Soporte especializado en seguridad perimetral y de las comunicaciones
 - Soporte especializado en seguridad de sistemas.
- **Cuota variable:** recoge todos los conceptos por los que se facturará a demanda, en base a hora de dedicación, asociados a los servicios de soporte especializado en seguridad de otras infraestructuras TIC.

CLÁUSULA 7.- CONTENIDO DE LAS OFERTAS

En este capítulo se describe la **estructura y el contenido de la documentación** que debe contener la propuesta técnica que las empresas licitadoras deben presentar y que se incluirá en el **Sobre Nº 2: “Documentación Técnica”** de cada lote.

Dentro de este sobre no se deberá incluir ninguna información sobre precios, la cual deberá entregarse exclusivamente en el **Sobre Nº 3: “Proposición Económica”** según se especifica en el Pliego de Cláusulas Administrativas.

Resulta obligatorio, para facilitar la valoración de las ofertas, que la documentación presentada en el **Sobre Nº 2: “Documentación Técnica”**, se ajuste al índice que se especifica en esta cláusula. Los licitadores podrán incluir documentación adicional en anexos si lo consideran necesario.

Adicionalmente, junto a la documentación anteriormente citada, los licitadores adjuntarán un resumen ejecutivo en el que, de forma esquemática y comprensible, recojan el contenido técnico de ese sobre.

En todo caso, cada licitador deberá ajustarse especialmente a lo indicado en este punto, y circunscribir su propuesta exclusivamente a lo demandado en el pliego, separando claramente en la documentación que entregue lo aplicable íntegramente como respuesta tecnológica, evaluable, de la información sobre servicios o productos comerciales que pueda tener en su catálogo comercial, no evaluable.

Las propuestas técnicas presentadas por cada licitador deberán justificar el cumplimiento de todos los requisitos solicitados en este Pliego de Prescripciones Técnicas, no teniéndose en cuenta aquellas ofertas que no cumplan dichos requisitos.

7.1 Contenido de las ofertas para el LOTE I

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 120 páginas**, incluidos los anexos, ni contener referencias a documentos externos o anexos no incluidos cuando éstos sean puntos clave en la valoración de la propuesta.

7.1.1 Resumen ejecutivo

Definirá los objetivos y el alcance, así como los aspectos relevantes de la oferta y del licitador.

El número máximo de páginas previsto para este apartado es de ocho (8) páginas.

7.1.2 Solución técnica propuesta para los servicios requeridos.

Los licitadores propondrán las diferentes soluciones para los servicios objeto del contrato:

- Servicio automatizado de análisis de vulnerabilidades.
- Servicio manual de análisis de vulnerabilidades.
- Servicio de monitorización de eventos de seguridad.
- Servicio de vigilancia digital e identificación de amenazas.
- Servicio de detección de incidentes, nivel 1 y nivel 2.
- Servicio especializado de respuesta a incidentes.
- Servicio de soporte a la gestión de incidentes.
- Servicio de diseño y operación de procesos y tecnologías del SOC.
- Servicio de capacitación y formación en ciberseguridad.
- Servicio de soporte a la gestión y operación del SOC.

La solución propuesta para cada servicio deberá contener la configuración de las infraestructuras y sistemas soporte, las especificaciones técnicas básicas de todos los elementos que lo componen, y las características de cada uno de ellos, de modo que cumplan los requerimientos descritos en el presente pliego.

Se valorará (criterio de valoración 3.5, Servicio de detección de incidentes, nivel 1 y nivel 2) la propuesta de soluciones integradoras y la incorporación de nuevas herramientas de análisis de comportamiento, de aprendizaje (machine learning) y procesamiento de datos (big data), orientados a automatizar los procesos de detección y análisis de eventos de seguridad, permitiendo una redistribución de los recursos técnicos mínimos solicitados para la ejecución de los servicios.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **0981582682548263284025**

7.1.3 Planes operativos

En este apartado, los licitadores presentarán los planes operativos propuestos para la prestación de los servicios requeridos, con detalle de todas las tareas y actividades implicadas, indicando los plazos previstos de cada una de ellas, los recursos materiales y humanos necesarios por parte del licitador, los hitos de interés, etc.

Deberán contemplarse como mínimo los siguientes planes operativos:

7.1.3.1 Plan de implantación de los servicios.

Los licitadores deberán presentar un Plan de Implantación de los servicios, en donde se recojan las distintas fases propuestas del proyecto en base a actividades, procesos y recursos, para la puesta en marcha de los servicios demandados.

El Plan de Implantación, que en todo caso deberá ser consensuado y aprobado por Madrid Digital al inicio del contrato, deberá recoger al menos los siguientes aspectos:

- Identificación de datos necesarios para el diseño del SOC, como datos críticos, capacidades de seguridad actuales en Madrid Digital o procedimientos operativos vigentes para la gestión de la seguridad.
- Definición de los procesos operativos del SOC para la monitorización de la seguridad y la respuesta a incidentes, y relaciones con otras áreas de Madrid Digital.
- Organización del SOC en niveles de atención, actividades y recursos técnicos.
- Organización de recursos operativos para prestación del servicio, organización del soporte 24x7 y distribución de recursos propuesta.
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación (SIEM, detección de vulnerabilidades, ticketing, etc.)
- Desarrollo del portal de gestión.

El Plan de Implantación, detallará claramente para cada fase propuesta el calendario de actividades asociado, plazos estimados y los medios técnicos y humanos dedicados. La puesta en marcha de los distintos servicios deberá ajustarse a los plazos recogidos en el **ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**.

7.1.3.2 Plan de operación y devolución de los servicios.

En este apartado se describirá el modelo de gestión propuesto para la operación de los servicios, contemplando como mínimo los siguientes aspectos:

- Metodología propuesta para la operación del servicio.
- Propuesta de mecanismos de control y seguimiento de los eventos de seguridad en sus distintas fases: triaje, clasificación, análisis y tratamiento.
- Mecanismos de control y seguimiento de eventos detectados.
- Procedimientos operativos de notificación de incidencias y peticiones al SOC.
- Procedimientos operativos de escalado de incidentes y relación entre los distintos niveles de soporte (1, 2, y 3), resto de equipos del SOC, y otras áreas de Madrid Digital.
- Propuesta de métricas (KPI's y KRI's) e indicadores del servicio y mecanismos de obtención y seguimiento.

- Plan de devolución de servicios que garantice la transferencia de conocimiento a la finalización del contrato, recogiendo la documentación mínima a entregar: documentación de procesos, de instalación de herramientas, de gestión del servicio, etc.

7.1.3.3 Plan de Calidad

Los licitadores deberán presentar un Plan de Calidad y especificar los parámetros de medición propuestos para asegurar el cumplimiento de los niveles de calidad del servicio prestado exigidos a lo largo del desarrollo de este pliego, en base a los requisitos especificados en el apartado **6.3 Seguimiento y mejora continua del servicio**.

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

7.2 Contenido de las ofertas para el LOTE II

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 50 páginas**.

7.2.1 Resumen ejecutivo

Definirá los objetivos y el alcance, así como los aspectos relevantes de la oferta y del licitador.

7.2.2 Solución propuesta para los servicios requeridos

En este apartado se dará respuesta ordenada a la propuesta de organización de cada licitador en lo referente a:

- Propuesta de controles técnicos de seguridad a definir e implementar por cada uno de los entornos tecnológicos recogidos en el **ANEXO II – ENTORNO TECNOLÓGICO**, considerando la legislación vigente y las buenas prácticas en seguridad.
- Contenido y estructura de la base de datos de configuración de seguridad, con indicación de campos, relaciones entre ellos y procesos de alta/baja y modificación.
- Plan de despliegue de herramientas y scripts para el descubrimiento y verificación de configuraciones y controles de seguridad.

7.2.3 Equipo de trabajo

En este apartado los licitadores facilitarán la relación de perfiles que conformarán el equipo de trabajo y principales actividades propuestas a desarrollar.

7.2.4 Plan de Calidad

Los licitadores deberán presentar un Plan de Calidad y especificar los parámetros de medición propuestos para asegurar el cumplimiento de los niveles de calidad del servicio prestado exigidos a lo largo del desarrollo de este pliego, en base a los requisitos especificados en el apartado **6.3 Seguimiento y mejora continua del servicio**.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

CLÁUSULA 8.- GESTIÓN DE LA SEGURIDAD

8.1 Protección de datos personales y Privacidad

8.1.1 Normativa

Los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad 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 (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

La Agencia Madrid Digital, en virtud de lo previsto en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de medidas fiscales y administrativas de la Comunidad de Madrid (BOE núm. 52, Jueves 2 marzo 2006) y lo establecido en la citada Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, actuará en calidad de Encargado del Tratamiento de la Comunidad de Madrid en el ámbito de su competencia. Y como Responsable del Tratamiento para aquellos tratamientos así previsto en el registro de actividades de tratamiento (www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos).

8.1.2 Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento

Para el cumplimiento del objeto de este pliego, el adjudicatario deberá tratar los datos personales de los cuales la Agencia Madrid Digital es Responsable o Encargado del Tratamiento de la manera que se especifica más adelante, en el apartado denominado "Tratamiento de datos personales".

Ello conlleva que el adjudicatario actúe en calidad de Encargado del Tratamiento y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Si el adjudicatario destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerada también como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en el apartado referido al "Tratamiento de Datos Personales", el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que la Agencia Madrid Digital estuviese de acuerdo con lo solicitado emitiría un apartado referido al "Tratamiento de Datos Personales" actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario garantiza el cumplimiento de las siguientes obligaciones, complementadas con lo detallado en el apartado referido al "Tratamiento de Datos Personales":

La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

- a) Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Pliego o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de la Agencia Madrid Digital por escrito en cada momento. El adjudicatario informará inmediatamente a la Agencia Madrid Digital cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.
- b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato.
- c) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso. En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detallados en el apartado referido al "Tratamiento de Datos Personales".
- d) Mantener absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.
- e) Llevar un listado de personas del equipo prestador del servicio que están autorizadas para tratar los Datos Personales objeto de este pliego, así como los roles asignados a cada una de ellas y la relación de permisos y perfiles autorizados que son estrictamente necesarias para el desempeño de las funciones encomendadas. Garantizar que cada una de las personas del equipo prestador del servicio se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición de la Agencia Madrid Digital dicha documentación acreditativa.
- f) Garantizar la formación e información necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.
- g) Salvo que cuente en cada caso con la autorización expresa de la Agencia Madrid Digital, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.
- h) Nombrar Delegado de Protección de Datos en caso de que sea necesario según el RGPD, o alternativamente, nombrar Responsable de Seguridad del Servicio del adjudicatario a efectos de protección de los Datos Personales en calidad de responsable del cumplimiento de la regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad. Así como comunicar la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por el adjudicatario.
- i) Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, a devolver (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario por causa del tratamiento; y destruir (iii) los soportes y documentos en que cualquiera de estos datos consten cuando no tengan la consideración de entregable del servicio contratado, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. El Encargado del Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con la Agencia Madrid Digital. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

- j) Según corresponda, llevar a cabo las instrucciones para el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que se especifiquen, equipamiento que podrá estar bajo el control de la Agencia Madrid Digital o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por la Agencia Madrid Digital, según se establezca en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.
- k) Salvo que se indique otra cosa en el apartado referido al “Tratamiento de Datos Personales” o se instruya así expresamente por la Agencia Madrid Digital, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Pliego o demás documentos contractuales, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito a la Agencia Madrid Digital de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a la Agencia Madrid Digital, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

- l) Con el objeto de dar cumplimiento al artículo 33 RGPD, comunicar a la Agencia para la Administración Digital de la Comunidad de Madrid, de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.
- m) Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable) ante el Encargado del Tratamiento, éste debe comunicarlo a la Agencia Madrid Digital con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derechos, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho. Asistirá a la Agencia Madrid Digital, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.
- n) Colaborar con la Agencia Madrid Digital en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de riesgos e impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

Asimismo, pondrá a disposición de la Agencia Madrid Digital, a requerimiento de esta, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Pliego y demás



- documentos contractuales y colaborará en la realización de auditoras e inspecciones llevadas a cabo, en su caso, por la Agencia Madrid Digital.
- o) En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la Agencia Madrid Digital, que contenga, al menos, las circunstancias a que se refiere dicho artículo.
 - p) Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de la Agencia Madrid Digital a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición de Agencia Madrid Digital toda información, certificaciones y auditorías realizadas en cada momento.
 - q) Derecho de informar: El encargado del tratamiento, en el caso de realizar la recogida de los datos personales, debe facilitar a los interesados la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe aprobar por la Agencia Madrid Digital antes del inicio de la recogida de los datos.

La presente cláusula y las obligaciones en ella establecidas constituyen el contrato de encargo de tratamiento entre la Agencia Madrid Digital y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este pliego y su contrato, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este pliego no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de la Agencia Madrid Digital y que no esté referido en el presente pliego, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el apartado referido al "Tratamiento de Datos Personales". Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales responsabilidad de la Agencia Madrid Digital no contemplados en el apartado referido al "Tratamiento de Datos Personales" el adjudicatario deberá ponerlo en conocimiento de Agencia Madrid Digital, en concreto de su Delegado de Protección de Datos (Dirección de Seguridad Corporativa), con la mayor diligencia y a más tardar en el plazo de 72 horas.

8.1.3 Obligaciones de la Agencia Madrid Digital para la prestación del servicio

- a) Facilitar el acceso del encargado a los datos a los que se refiere el apartado primero del apartado referido al "Tratamiento de Datos Personales".
- b) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

8.1.4 Sub-encargos de tratamiento asociados a Subcontrataciones

Cuando el pliego permita la subcontratación de actividades objeto del servicio contratado, y en caso de que el adjudicatario pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario lo pondrá en conocimiento previo de la Agencia Madrid Digital, identificando qué tratamiento de datos personales conlleva, para que la Agencia Madrid Digital decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a la Agencia Madrid Digital la decisión de si otorgar, o no, dicho consentimiento):



- a) Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones de la Agencia Madrid Digital.
- b) Que el adjudicatario y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente pliego, el cual será puesto a disposición de la Agencia Madrid Digital a su mera solicitud para verificar su existencia y contenido.

El adjudicatario informará a la Agencia Madrid Digital de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así a la Agencia Madrid Digital la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta de la Agencia Madrid Digital a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

8.1.5 Tratamiento de datos personales

Madrid Digital solo autorizará al adjudicatario a acceder a datos de carácter personal en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, en cuyo caso el adjudicatario asumirá la condición de encargado de tratamiento conforme al artículo 28 del Reglamento General de Protección de Datos, con las obligaciones que lleva aparejadas.

Salvo autorización expresa y por escrito de Madrid Digital, el adjudicatario tendrá prohibido el acceso a los datos personales que se conserven en cada una de las dependencias o sistemas a cuyo interior o contenido deba de acceder. En consecuencia, el adjudicatario habrá de impartir las instrucciones oportunas a su personal para que éste se abstenga de examinar el contenido de los documentos que, en soporte informático, en soporte papel o en cualquier otro tipo de soporte, se encuentre en el interior de las dependencias o sistemas en los que desarrollen sus actividades.

Las actividades de tratamiento a las que pudiera tener acceso el adjudicatario, en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, se encuentran enmarcadas por la norma de la Comunidad de Madrid relativa a las funciones y competencias del Responsable del Tratamiento, así como lo recogido en el Registro de Actividades de Tratamiento publicado en www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos.

En concreto, el Encargado de Tratamiento realizará los siguientes tratamientos en el marco de dicha prestación de servicios: Recogida, Registro, Consulta, Conservación, Destrucción, Transmisión por redes públicas/privadas.

8.2 Deber de Información

Los datos de carácter personal del adjudicatario serán tratados por la Agencia Madrid Digital para ser incorporados al sistema de tratamiento "Gestión de los expedientes de adquisición y contratación", cuya finalidad es la gestión administrativa de los expedientes de contratación de la Agencia y la gestión administrativa de los pedidos a los proveedores de adquisición de bienes y servicios.

Finalidad necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Los datos de carácter personal podrán ser comunicados a Unidades Administrativas encargadas de su tramitación, Boletines oficiales, Intervención General o la Cámara de Cuentas.

Se conservarán durante el tiempo que es necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran de dicha finalidad y del tratamiento de los datos.



Los derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, se pueden ejercitar ante la Agencia Madrid Digital, C/Embajadores, 181, 28049 - Madrid o en la dirección de correo electrónico protecciondatosmadriddigital@madrid.org.

Asimismo, los datos del personal del adjudicatario, así como de sus empresas contratistas, si las hubiere, serán tratados por Madrid Digital cuando sea necesario para dar cobertura a la realización de los trabajos objeto del contrato. Su tratamiento quedará incorporado al registro de actividades de tratamiento de la Agencia. Estos datos personales podrán ser comunicados a usuarios y clientes de Madrid Digital cuando así lo requiera la prestación del servicio y se conservarán durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron.

8.3 Seguridad en la utilización de medios electrónicos

8.3.1 Normativa

El adjudicatario está obligado al cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, ENS, (Real Decreto 3/2010 de 8 enero) en lo referido a la adopción de medidas de seguridad de las soluciones tecnológicas o la prestación de servicios ofertados.

El adjudicatario deberá concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

8.3.2 Conformidad con el Esquema Nacional de Seguridad

La Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, determina que cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad según corresponda.

Por ello, Madrid Digital podrá solicitar en todo momento al adjudicatario los correspondientes informes de Autoevaluación o Auditoría, al objeto de verificar la adecuación e idoneidad de lo manifestado en las Declaraciones o Certificados de Conformidad, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de contrato.

8.4 Medidas de Seguridad

8.4.1 Documentación de seguridad

El adjudicatario deberá poseer al inicio de la prestación de los servicios, los siguientes documentos, los cuales deberán estar permanentemente actualizados y a disposición de la Agencia a lo largo de la ejecución del contrato:

- a) Un documento denominado "Política de Seguridad", que estará basada en la Política de Seguridad Corporativa de la Agencia, que consistirá en un documento de alto nivel que defina lo que significa la 'Seguridad de la Información' en la organización y aplicable al servicio prestado. El documento deberá estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

- b) Un documento denominado “Documento de Seguridad” coherente con los hitos y medidas de seguridad que se exigen en la presente cláusula y que recoja la información estructurada y ordenada de forma que describa la relación de las medidas de seguridad propuestas por el adjudicatario para dar respuesta a lo contenido en el presente pliego y que acredite la forma en la que se procederá al cumplimiento de las mismas. Asimismo, deberá, identificar las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio y del Delegado de Protección de Datos del adjudicatario.

8.4.2 Confidencialidad y deber de secreto

El adjudicatario se compromete de forma específica a tratar como confidencial toda aquella información responsabilidad de Madrid Digital a la que pueda tener acceso, con motivo de la prestación de sus servicios y se compromete a que dichos datos permanezcan secretos incluso después de finalizado el presente Acuerdo.

Debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.

A estos efectos, el adjudicatario se compromete a tomar, respecto de sus empleados o colaboradores, las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como encargado de tratamiento y que, en consecuencia, deben respetar, así como a garantizar que los datos personales que conozcan en virtud de la prestación del servicio permanecen secretos incluso después de finalizado el presente Acuerdo por cualquier causa.

Dicha obligación de información a los empleados y colaboradores del adjudicatario se llevará a cabo de modo tal que permita la documentación y puesta a disposición de la Agencia Madrid Digital del cumplimiento de aquella obligación.

CLÁUSULA 9.- PROPIEDAD DE LOS TRABAJOS

Todos los informes, estudios y documentos, elaborados por los contratistas como consecuencia de la ejecución de los contratos serán propiedad de Madrid Digital, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

Los adjudicatarios renuncian expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución de los contratos pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de Madrid Digital.

CLÁUSULA 10.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS

Los contratistas no adquieren ningún derecho sobre el hardware (material), software e infraestructuras propiedad de Madrid Digital, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanadas del contrato.

Los contratistas no podrán utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato, y no podrán transmitirla sin el consentimiento expreso y escrito de Madrid Digital.

Finalizado el presente contrato, los desarrollos software, herramientas y licencias incluidas en el alcance de los servicios del presente pliego pasarán a ser propiedad de Madrid Digital.

CLÁUSULA 11.- CALIDAD DEL SERVICIO

Durante el periodo de ejecución del contrato, el adjudicatario propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada. No obstante, Madrid Digital podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, Madrid Digital podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

CLÁUSULA 12.- PLAZO, DURACIÓN Y ETAPAS DE PRESTACIÓN DE LOS SERVICIOS

El plazo de ejecución del contrato será de **36 MESES**, desde el 1 de abril de 2019 hasta el 31 de marzo de 2022.

Si en la fecha de inicio de la ejecución, los trabajos objeto del contrato no hubieran comenzado y no se pudiera contar en tal fecha con la disponibilidad del equipo necesario para la atención de los mismos, Madrid Digital quedará facultada para instar la resolución del contrato.

Durante el periodo final de vigencia del contrato o, en su caso, en cualquiera de sus prórrogas, Madrid Digital establecerá un periodo transitorio de ejecución en condiciones especiales, de modo que se garantice la prestación del servicio de forma ininterrumpida, comprometiéndose los adjudicatarios a colaborar con los nuevo adjudicatarios en aquellas actividades necesarias, encaminadas a la planificación y ejecución del cambio.

Por tanto, los adjudicatarios de los contratos se comprometen a garantizar la completa y correcta operatividad de todos los servicios durante el posible periodo de transición requerido a la finalización del contrato, que permita el cambio de contrato y de proveedor de servicios.

Se divide la prestación del servicio en tres fases o etapas:

- **Fase de Implantación de los servicios:**

- **LOTE I:** 6 meses desde el inicio de ejecución del contrato, con los hitos de puesta en marcha de cada servicio recogidos en el ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES.

El calendario de implantación de los servicios desde el inicio del contrato, será el siguiente:

- Servicio Automatizados de análisis de vulnerabilidades: Mes 2.
- Servicio manual de análisis de vulnerabilidades: Mes 2.
- Servicio de monitorización de eventos de seguridad (Mantenimiento de plataforma SIEM): Mes 7.
- Servicio de vigilancia digital e identificación de amenazas: Mes 3.
- Servicio de detección de incidentes de seguridad Nivel 1: Mes 7.
- Servicio de detección de incidentes de seguridad Nivel 2: Mes 7.
- Servicio especializado de respuesta a incidentes: Mes 7.
- Servicio de diseño y operación de procesos y tecnologías del SOC: Mes 1.
- Servicio de soporte a la gestión y operación del SOC: Mes 1.
- Servicio Soporte a la gestión de incidentes de seguridad: Mes 1.
- Servicio de Asesoría y asistencia legal: Mes 1.

La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

- **LOTE II:** 1 mes desde el inicio de ejecución del contrato.
- **Fase de Operación:**
 - **LOTE I:** 30 meses, desde la finalización de la fase de implantación.
 - **LOTE II:** 35 meses, desde la finalización de la fase de implantación.
- **Fase de Devolución del servicio:** (ejecutar en paralelo en los últimos meses de la fase de operación)
 - **LOTE I:** 3 meses antes de la finalización del contrato.
 - **LOTE II:** 1 mes antes de la finalización del contrato.

CLÁUSULA 13.- GARANTÍA DE LOS TRABAJOS

Se establece un plazo de garantía de **DOCE MESES**, cuyo cómputo se iniciará desde la fecha de recepción o conformidad de los trabajos.

Hasta que no tenga lugar la finalización del periodo de garantía, cada adjudicatario responderá de la correcta realización de los trabajos que se le hayan contratados, de los equipamientos instalados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de Madrid Digital los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales, e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente pliego de prescripciones técnicas, el licitador podrá dirigirse a:

Agencia para la Administración Digital de la Comunidad de Madrid
Subdirección General de Infraestructuras y Operaciones
Área de Ciberseguridad
E-mail: md_seguridad_sistemas@madrid.org

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con Madrid Digital, para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Por su parte la Agencia se compromete a responder en los términos indicados en la Cláusula 10 del Pliego de Cláusulas Administrativas Particulares.



ANEXO I. REQUISITOS MÍNIMOS DEL SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD - SIEM

Las características funcionales y técnicas mínimas que debe cumplir el suministro del sistema de gestión de eventos e información de seguridad, el SIEM, son las siguientes:

1. Arquitectura del sistema y dimensionamiento

Módulos principales

El sistema de gestión de eventos de seguridad debe contar con, al menos, los siguientes elementos conceptuales, no debiendo identificarse éstos con dispositivos físicos o módulos software:

- Recolector de logs: encargado de recoger la información de las diferentes fuentes de información, y consolidar y normalizar los eventos recogidos.
- Procesador de eventos con funciones de correlación, que se encargará de tareas como normalizar, priorizar, recolectar, evaluar el riesgo y ejecutar el motor de correlación.
- Base de datos, para el almacenamiento de los eventos recogidos, alertas generadas, informes, inventario de activos e información útil para la gestión del sistema.
- Consola de administración y operación centralizada, para la administración unificada de la plataforma.

Los elementos de la plataforma, en formato appliance, deben facilitarse con medidas de redundancia ante fallos hardware (discos en RAID, doble fuente de alimentación, etc.), alta disponibilidad configurable sin componente adicionales (balanceadores, etc.), gestión remota fuera de banda (mediante protocolo IPMI o similar), e interfaz SNMP para monitorización de los componentes. Debe ser capaz de almacenar los logs tanto en disco local como en almacenamiento externo (iSCSI, Fibre Channel).

Los diferentes componentes del sistema se desplegarán en los dos centros de proceso de datos (CPD) de Madrid Digital.

Módulos adicionales

Adicionalmente, el sistema dispondrá también de:

- Recolectores y analizadores de seguridad de tráfico de red, que podrá ser provisto en dos modalidades alternativas:
 - sondas de red, encargados de analizar y detectar el tráfico de red malicioso de forma pasiva, incluye las funciones propias de un sistema de detección de intrusión de red (NIDS). Deberán instalarse recolectores de tráfico de red en cada CPD para el análisis del tráfico de salida a Internet y el tráfico interno de entrada a los CPD's.
 - analizadores de flujos de red enriquecidos, que permita inspeccionar en profundidad los paquetes de red y extraer como mínimo datos de identificación de aplicación, login de usuario, email, URLs y DNS queries y responses. Estos analizadores de flujo deberán ser capaces de definir reglas para identificar y alertar sobre tráfico sospechoso y ser gestionados de forma centralizada desde la consola principal. Se prevé la necesidad de analizar un millón de flujos de red por minuto (FPM).
- Pantallas de monitorización de eventos de seguridad detectados, a instalar en la sede de Madrid Digital, donde residirán los servicios de SOC.

Dimensionamiento

El sistema de gestión de eventos deberá estar dimensionado y correctamente licenciado durante el periodo de ejecución del contrato, incluida su prórroga, para:



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: 0981582682548263284025

- Recolectar y analizar al menos 10 Gbit/s de tráfico de red por CPD y flujo, flujo de tráfico de salida a Internet y flujo de tráfico interno de entrada a cada CPD.
- Recolectar un volumen mínimo de 15.000 eventos por segundo (EPS) de media al día en cada CPD, de las distintas fuentes de eventos.
- Procesar y correlar un mínimo de 5.000 eventos por segundo (EPS) en tiempo real y sin descarte de eventos.
- Almacenar toda la información de eventos y correlación de forma on-line durante un periodo mínimo de seis meses, y un periodo mínimo de retención de eventos off-line de 24 meses.

2. Fuentes de eventos.

La plataforma de gestión de eventos recibirá y almacenará los eventos de fuentes diversas, por lo que deberá tener la funcionalidad para procesar de forma nativa eventos de las siguientes fuentes:

- Cortafuegos de red.
- Balanceadores de tráfico
- Routers.
- Switches.
- Pasarelas de navegación web y pasarelas inversas.
- Servicios de nombres de dominio (DNS).
- Servicios de acceso remoto RADIUS.
- Servicios de directorio LDAP y DA.
- Servicios de redes privadas VPN.
- Servidores web Apache, Oracle Web Cache y Nginx.
- Servidores de aplicaciones Weblogic, Tomcat...
- Bases de datos Oracle 11g, MySQL y Postgree.
- Sistemas operativos Linux, Windows.

En el **ANEXO II. ENTORNO TECNOLÓGICO** se facilita detalle de fabricantes principales.

Deberá disponer del mayor número de analizadores sintácticos (parsers) para otros sistemas de terceros, siendo imprescindible que todos ellos estén completamente documentados, incluyendo las tareas requeridas sobre los sistemas de terceros para su correcta integración en la plataforma.

Permitirá también el desarrollo de nuevos analizadores mediante expresiones regulares estándar o un interfaz de programación (API).

3. Protocolos de intercambio de eventos.

La plataforma debe permitir, al menos, los siguientes protocolos de intercambio de eventos entre las fuentes y el sistema de recolección:

- Protocolos SNMP (en todas sus versiones), SYSLOG y SYSLOG-NG (UDP/TCP/TLS).
- Flujos de red en formato NetFlow o IPFIX (en todas sus versiones tanto para IPv4 como IPv6).
- Push/Pull de ficheros en texto y descarga de información desde URL.
- Fuentes de información externas en formatos XML, TXT, y CSV.

4. Características generales a cumplir.

El sistema de gestión de eventos propuesto por el licitador deberá cumplir los siguientes requisitos funcionales mínimos:

- **Recolectores de logs:**



- Actualización de los interfaces/plugin para asegurar la integración de la plataforma con las evoluciones del software de los dispositivos y sistemas externos.
 - Posibilidad de modificación de firmas de detección existentes y creación de firmas nuevas, personalizadas.
 - Posibilidad de detección de eventos basada en reputación (de direccionamiento, URL's, geolocalización, etc.).
 - Correlación básica.
 - Envío cifrado de eventos desde el equipo recolector al correlador.
 - Reducción de falsos positivos mediante ajuste de umbrales de detección.
 - Mecanismos disponibles para evitar la pérdida de eventos en caso de superación puntual de límite de la capacidad máxima soportada o licenciada.
 - Posibilidad de configuración independiente de detección en cada sensor.
 - Capacidad de almacenamiento local temporal de los eventos procesados.
 - Capacidad de integración con fuentes externas de inteligencia.
- **Procesador de eventos con capacidad de correlación:**
 - Actualización de los formatos de eventos y bases de datos de eventos, para asegurar la integración de la plataforma con las evoluciones del software de los dispositivos y sistemas externos.
 - Disponibilidad de reglas de correlación actualizadas, durante la vigencia del contrato.
 - Posibilidad de agregación y normalización de las distintas fuentes de datos monitorizadas y detectadas.
 - Posibilidad de correlación empleando operaciones lógicas sobre los eventos detectados.
 - Posibilidad de correlación relacionando los eventos detectados y la información contenida en la base de datos de conocimiento, como inventario de activos o información sobre los mismos.
 - Posibilidad de correlación de fuentes de flujos de red.
 - Posibilidad de correlación basada en datos históricos.
 - Posibilidad de correlación basada en vulnerabilidades.
 - Posibilidad de detección por anomalías.
 - Posibilidad de detección por analítica de comportamiento.
 - Posibilidad de priorización de eventos según distintos criterios como valoración de activos, tipo de evento, etc.
 - Posibilidad de priorización de eventos basada en reputación de IP.
 - Posibilidad de priorización de eventos basada en taxonomías personalizables.
 - Posibilidad de asignación de políticas de filtrado de eventos a grupos de activos.
 - Posibilidad de filtrado y aplicación de políticas en la detección de eventos según las necesidades del entorno (modificación de la prioridad, eliminación del panel de eventos, notificación de eventos, activación/desactivación de la opción de correlación, etc.) que se den en ciertos activos.
 - Capacidad de que no se produzcan pérdidas de eventos en caso de superación puntual del límite de la capacidad máxima soportada o licenciada.
 - Posibilidad de visualización del contenido de los paquetes de red (payload) de los eventos de red para análisis forense.
 - Posibilidad de modificación y ajuste de las reglas de correlación existentes y creación de reglas de correlación nuevas a medida.
 - Posibilidad de reducción en la detección de falsos positivos mediante ajuste de los umbrales de detección.
 - Posibilidad de ofrecer información de contexto (información histórica de DNS, país, reputación IP,...) durante el análisis del evento.



- Capacidad de integración con fuentes de inteligencia basadas en estándares STIX/TAXII.
- **Base de datos:**
 - Posibilidad de registro de activos manual y masiva, e información sobre los mismos en la base de datos conocimiento, especialmente el valor del activo.
 - Posibilidad de registro, actualización y eliminación masiva de activos. Posibilidad de exportación/importación de base de datos de activos en diferentes formatos de salida/entrada que facilite su tratamiento.
 - Posibilidad de registro de otra información útil para la detección, correlación y gestión de los incidentes detectados (vulnerabilidades conocidas, amenazas actuales, geolocalización de orígenes, reputación, etc.).
 - Posibilidad de almacenar los datos por niveles, de tal manera que el primer nivel será el año, el segundo el mes, días,..., y que resulte posible hacer copias de estos en almacenamiento externo organizados por periodos de tiempo.
 - Funcionalidad de configurar múltiples periodos de retención de logs para eventos y flujos basados en filtros sobre los eventos y flujos.
 - Funcionalidad de archivado de aquellos logs/eventos que sobrepasen el periodo de retención determinado.
 - Capacidad de firma y sellado de tiempo de los logs y eventos almacenados en formato original.
 - Capacidad de integridad de los datos almacenados mediante algoritmos de HASH (SHA2-256 o superior).
 - Compresión de datos de al menos de 10 a 1.
- **Gestión de la plataforma:**
 - Acceso de usuarios a la plataforma mediante protocolo HTTPS.
 - Control de acceso basado en usuario y contraseña.
 - Control de acceso y autenticación de usuarios mediante base de datos externa LDAP.
 - Asignación de privilegios a usuarios basada en roles que permitan asignar diferentes niveles de permisos en la plataforma, así como la creación de grupos de usuarios.
 - Acceso a las distintas funcionalidades e información de la plataforma basado en roles. Posibilidad de restringir el acceso a ciertas secciones de la herramienta a roles, usuarios o grupos de usuarios.
 - Funcionalidades de registro de actividad de usuarios.
 - Configuración y gestión de realización de copias de seguridad de la información albergada en la solución.
 - Gestión centralizada de todos los elementos: sensores, fuentes de datos de monitorización, motores de correlación, interfaces de gestión o consulta, etc.
 - Gestión centralizada de políticas de detección y correlación, firmas, orígenes de firmas, inventario, base de datos de conocimiento, etc...
 - Actualización automática de la solución y/o los elementos que la componen (corrección de bugs, implementación de mejoras en las funcionalidades, etc...).
 - Posibilidad de integración con herramientas externas de análisis de vulnerabilidades y amenazas.
 - Integración con soluciones de ticketing externas mediante servicios web, especialmente con ARS Remedy y LUCIA (herramienta de ticketing definida por el CCN-CERT).
 - Generación de informes personalizados según distintos criterios (sensor, activo y/o grupo de activos, propietario de activos, geolocalización, etc.).
 - Funcionalidad para exportar datos en diferentes formatos de salida, al menos CSV, XML, PDF y HTML.



- Funcionalidad para configurar paneles informativos personalizados con datos estadísticos de los eventos y demás información relevante proporcionada por la plataforma.
- Generación de mapas de riesgo en tiempo real.
- Notificación automática de alertas de seguridad a través de diferentes medios, tales como correo electrónico, consola de operación, servicio web configurable, etc.
- Definición de políticas de notificación de alertas en base a criterios personalizables como grupo de activos, propietario de activos, sensores de detección, etc.
- **Recolectores de tráfico de red:**
 - Disponibilidad de firmas de detección de patrones actualizadas.
 - Monitorización de tráfico de red de interfaz de 10 Gbps (incluyendo capa 7).
 - Capacidad de generar flujos de red de interfaz de 10 Gbps (incluyendo capa 7).
 - Capacidad de modificación de firmas de detección existentes y creación de nuevas firmas personalizadas.
 - Envío cifrado de eventos desde el equipo sensor al correlador.
 - Reducción de falsos positivos mediante ajuste de los umbrales de detección.
 - Mecanismos disponibles para evitar la pérdida de eventos en caso de superación puntual de límite de la capacidad máxima soportada o licenciada.
 - Posibilidad de configuración independiente de detección en cada sensor.
 - Posibilidad de captura de paquetes de red (payload) que generan los eventos para análisis forense.
 - Capacidad de integración con fuentes de inteligencia externas.
- **Seguridad:**
 - La solución SIEM debe permitir cifrar todas las comunicaciones entre sus componentes.
 - La solución SIEM debe permitir la configuración en HA sin componentes adicionales (balanceadores, etc.).
 - La solución SIEM debe permitir autenticar mediante LDAP, Directorio Activo, RADIUS y TACACS.
 - La solución SIEM debe permitir autenticar utilizando Single Sign-On.
 - La solución SIEM deben disponer de una interfaz SNMP para monitorización de los componentes.
 - La solución SIEM debe permitir ofuscar campos o parte del log para evitar que los analistas vean ciertos datos en claro.
 - La solución SIEM debe auditar todas las acciones realizadas por el usuario tanto en la interfaz web como vía línea de comandos en los appliances.
 - La solución SIEM debe permitir definir accesos basados en roles para limitar el acceso a ciertos logs y flujos dependiendo del rol.
 - La solución SIEM debe permitir definir accesos basados en roles para limitar el acceso a las funcionalidades como la administración, informes, filtrados, correlación y/o cuadros de mando.
- **Correlación y Casos de Uso**
 - La solución SIEM debe permitir correlacionar información de Logs, Flujos y vulnerabilidades en tiempo real.
 - La solución SIEM debe permitir correlacionar entre sí la información de Logs, Flujos y vulnerabilidades.
 - La solución SIEM debe permitir la correlación histórica de Logs y Flujos (correlación de una selección de eventos pasados contra Indicadores de Compromiso (IoCs) y Reglas actuales).
 - La solución SIEM debe proporcionar casos de uso por defecto, documentados y mantenidos por el propio fabricante.



- La solución SIEM debe proporcionar Informes por defecto, documentados y mantenidos por el propio fabricante.
 - La solución SIEM debe permitir definir reglas de anomalía evaluados en tiempo real que detecten cambios repentinos de un valor o suceso (por ejemplo: incremento repentino del volumen de tráfico).
 - La solución SIEM debe permitir definir reglas de anomalía estacionales que detecten desviaciones en un valor o suceso (como el volumen de tráfico o número de logins fallidos) en comparación al mismo día de la semana anterior.
 - La solución SIEM debe incorporar algoritmos de Machine Learning para modelar el comportamiento habitual de usuarios y detectar desviaciones.
 - La solución SIEM debe agrupar y encadenar eventos relacionados (con el mismo host atacante, mismo usuario, misma víctima, etc.) en un único incidente, aunque los eventos sucedan de forma separada en el tiempo (a lo largo de varias horas o días) para detectar patrones “Low and Slow”.
 - La solución SIEM debe tener la capacidad de detectar en tiempo real el uso de una nueva IP o puerto en una subred.
 - La solución SIEM debe tener la capacidad de detectar en tiempo real el uso de un nuevo nombre de usuario en el entorno.
 - La solución SIEM debe tener la capacidad de integrarse con el directorio activo y utilizar esta información en las reglas de correlación (por ejemplo, para detectar que un usuario no está registrado en el DA).
- **Flexibilidad y Colaboración:**
 - La solución SIEM debe incorporar un feed de inteligencia con clasificación de IPs y URLs.
 - La solución SIEM debe soportar la integración de IoCs mediante STIX/TAXII tanto para importar IoCs como para exportarlos.
 - La solución SIEM debe permitir la colaboración mediante la creación de colecciones (públicas o privadas) para compartir IoCs.
 - **Pantallas de monitorización de eventos de seguridad**, de 55 pulgadas, con resolución full HD, certificadas para uso semi intensivo en régimen de 12x5 horas de explotación, luminosidad mínima de 350 nits, conectividad LAN, y soporte de pared VESA.

5. Instalación y aceptación del sistema.

El sistema de gestión de eventos se instalará en los dos CPD's de Madrid Digital, ubicados en Tres Cantos y Julián Camarillo.

Con carácter general, el adjudicatario deberá observar toda la normativa interna de aplicación para el suministro e instalación del equipamiento en Madrid Digital, como son procedimientos de acceso a los centros, etiquetado de componentes, normativa técnica de instalación, etc., que será facilitada al adjudicatario al inicio del contrato.

Para la instalación y aceptación del sistema, el adjudicatario deberá realizar las siguientes actividades mínimas:

- **Diseño detallado de la solución:** junto con Madrid Digital, el adjudicatario elaborará el Plan Detallado de Instalación, en donde se definirá la arquitectura final del sistema, en base a la situación de partida y las necesidades específicas de Madrid Digital. El plan de instalación incluirá el diseño final de la arquitectura a desplegar, el plan de puesta en marcha con detalle de tareas concretas y tiempos estimados de ejecución, requerimientos de la instalación (espacio en racks, conectividad de red, direccionamiento IP, etc.), la propuesta de integración con los sistemas externos identificados, las políticas generales de configuración y alarmas, y el plan de pruebas.



- **Instalación del todo el equipamiento:** el adjudicatario deberá observar toda la normativa interna de aplicación para el suministro e instalación del equipamiento en Madrid Digital, como son procedimientos de acceso a los centros, etiquetado patrimonial de componentes, normativa técnica de instalación, etc., que será facilitada al inicio del contrato.
- **Configuración básica del sistema,** necesaria para operar la plataforma y poder comenzar a recoger eventos, fuentes de logs y tráfico de red. El sistema deberá optimizarse para que sólo almacene los datos de interés.
- **Integración de fuentes y otros sistemas:**
 - Elementos de red: configuración y captura de los eventos generados por los sistemas de detección de intrusión ofertados (Recolectores de tráfico de red).
 - Elementos de seguridad: captura de logs generados por los sistemas de seguridad perimetral de los CPD's.
 - Integración de las fuentes de inteligencia de amenazas propuestas por el adjudicatario.Y en general la integración con todas las fuentes y sistemas descritos en este anexo.
- **Configuración de casos de uso de monitorización:** el sistema deberá quedar configurado al menos con los siguientes casos de uso:
 - Detección de tráfico de red de código malicioso.
 - Detección de ataques por denegación de servicio.
 - Detección de ataques por explotación de vulnerabilidades.
 - Detección de sistemas pertenecientes a botnets.
 - Detección de accesos sospechosos a dispositivos, sistemas y aplicaciones.
- **Optimización, pruebas y aceptación del sistema:** tras la integración de fuentes y configuración de casos de uso, el adjudicatario establecerá un periodo de optimización del sistema para reducir el porcentaje de falsos positivos y falsos negativos. Finalizado este periodo, se ejecutará el plan de pruebas aprobado y la aceptación del sistema.

- **FIN DEL ANEXO I –**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

ANEXO II. ENTORNO TECNOLÓGICO

El entorno tecnológico sobre el que se prestarán los servicios recogidos en el lote II será el siguiente:

SISTEMAS OPERATIVOS	
Servidor:	Red Hat, SUSE, CentOS Solaris, AIX, Tru64 Windows
Puesto ofimático:	Windows Android, iOS
SERVIDORES	
Web:	Apache, Oracle Web Cache, nGINX
Aplicaciones:	IAS, WebLogic, Tomcat, Jboss
BASES DE DATOS	
	Microsoft SQL Server MySQL Oracle
SEGURIDAD PERIMETRAL	
Cortafuegos:	Checkpoint, Juniper, Netscreen, Palo Alto
Proxy:	Blue Coat
COMUNICACIONES	
Routers:	Cisco
Switches:	Cisco, Extreme Networks, HP
WIFI:	Extreme, Cisco, Aruba
DNS, DHCP:	Infoblox
Balanceadores:	Radware, F5, Big-IP, Citrix
VPN:	Checkpoint
SOFTWARE NEGOCIO	
Gestión documental:	Documentum, Alfresco
Colaboración:	Sharepoint
ERP's:	SAP
Gestores de contenido:	Fatwire, Joomla, Drupal
Correo electrónico:	MS Exchange 2013
Servicios de autenticación:	Active directory, SunOne, SAP

- FIN DEL ANEXO II -



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: 0981582682548263284025

ANEXO III. MODELO DE CURRÍCULUM

MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO

(A aportar para cada miembro del equipo propuesto)

APELLIDOS:	
NOMBRE:	
CATEGORÍA PROFESIONAL:	
TTITULACIÓN / UNIVERSIDAD o CENTRO / HOMOLOGACIÓN (en caso de haberse obtenido la titulación fuera de España):	
FORMACIÓN:	
EXPERIENCIA – ACTIVIDAD PROFESIONAL (Especificando como mínimo: Empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta):	

Los licitadores que presenten la mejor oferta deberán aportar este documento, debidamente cumplimentado y firmado por la persona que ostente la representación de la empresa, para cada uno de los miembros del Equipo propuesto, indicando el perfil al que se adscribe, así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

- FIN DEL ANEXO III -



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

ANEXO IV. PRESUPUESTO

LOTE I: CENTRO DE OPERACIONES DE SEGURIDAD, SOC-MD

CUOTA FIJA								
EQUIPO DE TRABAJO	PERFIL	Nº Recursos	Nº Horas/Mes Recurso	Precio/Hora Recurso	Año 2019 1 abr - 31 dic	Año 2020 1 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
					9	12	12	3
Análisis de vulnerabilidades automatizado (1)	Analista Seguridad VULNERABILIDADES	1	160	35,10 €	44.928,00 €	67.392,00 €	67.392,00 €	16.848,00 €
Análisis de vulnerabilidades manual (1)	Analista Seguridad VULNERABILIDADES	1	160	35,10 €	44.928,00 €	67.392,00 €	67.392,00 €	16.848,00 €
Detección de incidentes de seguridad N1 (2)	Técnico Seguridad SOC DETECCIÓN	2	160	23,87 €	22.915,20 €	91.660,80 €	91.660,80 €	22.915,20 €
	Técnico Seguridad SOC DETECCIÓN - 24x7	1	512	23,87 €	36.664,32 €	146.657,28 €	146.657,28 €	36.664,32 €
Detección de incidentes de seguridad N2 (3)	Analista Seguridad SOC ANÁLISIS	1	160	35,10 €	16.848,00 €	67.392,00 €	67.392,00 €	16.848,00 €
Respuesta a incidentes (3)	Especialista Seguridad SOC RESPUESTA	1	160	48,00 €	23.040,00 €	92.160,00 €	92.160,00 €	23.040,00 €
Diseño y operación de procesos y tecnologías (4)	Arquitecto Seguridad SOC	1	160	45,00 €	64.800,00 €	86.400,00 €	86.400,00 €	21.600,00 €
	Jefe de Servicio SOC	1	160	45,00 €	64.800,00 €	86.400,00 €	86.400,00 €	21.600,00 €
TOTAL EQUIPO DE TRABAJO					318.923,52 €	705.454,08 €	705.454,08 €	176.363,52 €

SERVICIOS CONTÍNUOS	Precio/Mes Servicio	Año 2019 1 abr - 31 dic	Año 2020 1 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
Vigilancia digital e identificación de amenazas (5)	12.803,06 €	89.621,39 €	153.636,66 €	153.636,66 €	38.409,17 €
Soporte a la gestión y operación (4)	10.125,48 €	91.129,28 €	121.505,70 €	121.505,70 €	30.376,43 €
Mantenimiento Plataforma SIEM (6)	17.744,66 €	0,00 €	53.233,97 €	212.935,86 €	53.233,97 €
TOTAL SERVICIOS CONTÍNUOS		180.750,66 €	328.376,33 €	488.078,22 €	122.019,56 €

TOTAL CUOTA FIJA		499.674,18 €	1.033.830,41 €	1.193.532,30 €	298.383,08 €
------------------	--	--------------	----------------	----------------	--------------



Este documento puede ser verificado a través del siguiente código de verificación: 9891382682548263284025

CUOTA VARIABLE								
SERVICIOS DE APOYO	PERFIL	Nº Recursos	Nº Horas/Mes Recurso	Precio/Hora Recurso	Año 2019 1 abr - 31	Año 2020 1 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
Soporte a la gestión de incidentes	Especialista Seguridad SOC RESPUESTA	1	50	48,00 €	21.600,00 €	28.800,00 €	28.800,00 €	7.200,00 €
Asesoría y asistencia legal	Consultor legal	1	20	39,19 €	7.054,20 €	9.405,60 €	9.405,60 €	2.351,40 €
TOTAL SERVICIOS DE APOYO					28.654,20 €	38.205,60 €	38.205,60 €	9.551,40 €

TOTAL CUOTA VARIABLE	28.654,20 €	38.205,60 €	38.205,60 €	9.551,40 €
----------------------	-------------	-------------	-------------	------------

INVERSIONES							
EQUIPAMIENTO COMPLETO SISTEMA SIEM	Nº Unidades		Precio Unitario	Año 2019 1 abr - 31 dic	Año 2020 1 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
Sondas NIDS 10 GBIT/S o tecnología análisis de flujos de red (7)	4		91.816,10 €	367.264,40 €	0,00 €	0,00 €	0,00 €
SIEM (8)	1		612.885,52 €	612.885,52 €	0,00 €	0,00 €	0,00 €
Pantallas de monitorización	2		4.512,26 €	9.024,52 €	0,00 €	0,00 €	0,00 €
TOTAL EQUIPAMIENTO			989.174,44 €	0,00 €	0,00 €	0,00 €	

TOTAL INVERSIONES	989.174,44 €	0,00 €	0,00 €	0,00 €
-------------------	--------------	--------	--------	--------

DISTRIBUCIÓN DE IMPORTES LOTE I	2018	2019	2020	2021
TOTAL CUOTA FIJA	499.674,18 €	1.033.830,41 €	1.193.532,30 €	298.383,08 €
TOTAL CUOTA VARIABLE	28.654,20 €	38.205,60 €	38.205,60 €	9.551,40 €
TOTAL INVERSIONES	989.174,44 €	0,00 €	0,00 €	0,00 €
TOTAL LOTE I (sin IVA)	1.517.502,82 €	1.072.036,01 €	1.231.737,90 €	307.934,48 €
21% IVA	318.675,59 €	225.127,56 €	258.664,96 €	64.666,24 €
TOTAL LOTE I (IVA incluido)	1.836.178,41 €	1.297.163,57 €	1.490.402,86 €	372.600,72 €



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: 09815821825482694025

LOTE II: SOPORTE ESPECIALIZADO EN DISEÑO SEGURO, SD-2-MD

CUOTA FIJA								
EQUIPO DE TRABAJO	PERFIL	Nº Recursos	Nº Horas/Mes Recurso	Precio/Hora Recurso	Año 2019 1 abr - 31 dic	Año 2020 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
Seguridad perimetral y comunicaciones	Arquitecto Seguridad Sist y Com	2	160	45,00 €	129.600,00 €	172.800,00 €	172.800,00 €	43.200,00 €
Seguridad sistemas	Arquitecto Seguridad Sist y Com	1	160	45,00 €	64.800,00 €	86.400,00 €	86.400,00 €	21.600,00 €
TOTAL EQUIPO DE TRABAJO					194.400,00 €	259.200,00 €	259.200,00 €	64.800,00 €
TOTAL CUOTA FIJA					194.400,00 €	259.200,00 €	259.200,00 €	64.800,00 €
CUOTA VARIABLE								
EQUIPO DE TRABAJO	PERFIL	Nº Recursos	Nº Horas/Mes Recurso	Precio/Hora Recurso	Año 2019 1 abr - 31 dic	Año 2020 ene - 31 dic	Año 2021 1 ene - 31 dic	Año 2022 1 ene - 31 mar
Seguridad otras tecnologías	Arquitecto Seguridad Sist y Com	1	40	45,00 €	16.200,00 €	21.600,00 €	21.600,00 €	5.400,00 €
TOTAL EQUIPO DE TRABAJO					16.200,00 €	21.600,00 €	21.600,00 €	5.400,00 €
TOTAL CUOTA VARIABLE					16.200,00 €	21.600,00 €	21.600,00 €	5.400,00 €
DISTRIBUCIÓN DE IMPORTES LOTE II					2019	2020	2021	2022
TOTAL CUOTA FIJA					194.400,00 €	259.200,00 €	259.200,00 €	64.800,00 €
TOTAL CUOTA VARIABLE					16.200,00 €	21.600,00 €	21.600,00 €	5.400,00 €
TOTAL LOTE II (sin IVA)					210.600,00 €	280.800,00 €	280.800,00 €	70.200,00 €
21% IVA					44.226,00 €	58.968,00 €	58.968,00 €	14.742,00 €
TOTAL LOTE II (IVA incluido)					254.826,00 €	339.768,00 €	339.768,00 €	84.942,00 €

36



0981582682548763284025

RESUMEN CONTRATO POR SERVICIOS	2019	2020	2021	2022
TOTAL CUOTA FIJA	694.074,18 €	1.293.030,41 €	1.452.732,30 €	363.183,08 €
TOTAL CUOTA VARIABLE	44.854,20 €	59.805,60 €	59.805,60 €	14.951,40 €
TOTAL INVERSIONES	989.174,44 €	0,00 €	0,00 €	0,00 €
TOTAL CONTRATO (sin IVA)	1.728.102,82 €	1.352.836,01 €	1.512.537,90 €	378.134,48 €
21% IVA	362.901,59 €	284.095,56 €	317.632,96 €	79.408,24 €
TOTAL CONTRATO (IVA incluido)	2.091.004,41 €	1.636.931,57 €	1.830.170,86 €	457.542,72 €

RESUMEN CONTRATO POR LOTES	2019	2020	2021	2022
LOTE I	1.517.502,82 €	1.072.036,01 €	1.231.737,90 €	307.934,48 €
LOTE II	210.600,00 €	280.800,00 €	280.800,00 €	70.200,00 €
TOTAL CONTRATO (sin IVA)	1.728.102,82 €	1.352.836,01 €	1.512.537,90 €	378.134,48 €
21% IVA	362.901,59 €	284.095,56 €	317.632,96 €	79.408,24 €
TOTAL CONTRATO (IVA incluido)	2.091.004,41 €	1.636.931,57 €	1.830.170,86 €	457.542,72 €

NOTAS:

- (1) - Facturable a partir del segundo mes.
- (2) - No se presupuesta ningún recurso hasta el mes 7 que está montado el SIEM, aunque ya se reciba información del servicio de detección de amenazas.
En el caso de 24x7 solo se contabilizan las horas reales fuera de Madrid Digital, o sea, se descuentan las horas cuando los técnicos están trabajando en la Agencia.
- (3) - No se presupuesta ningún recurso hasta el mes 7 que está montado el SIEM.
- (4) - Facturable desde el inicio del contrato.
- (5) - Facturable a partir del tercer mes.
- (6) - Se estima 6 meses para implantación del SIEM y 12 meses de garantía por adquisición de producto, por lo que este concepto es facturable a partir del mes 19 del contrato
- (7) - Se presupuesta la adquisición de 4 sondas de red con capacidades IDS/IPS para las salidas centralizadas a Internet y la entrada de la red de usuarios (MLAN).
- (8) - La estimación del SIEM incluye: solución en alta disponibilidad para todos los elementos principales, y almacenamiento externo en retención para 24 meses.

FIN DEL ANEXO IV –

ANEXO V. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES

LOTE I:

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Servicio automatizado de análisis de vulnerabilidades	Implantación del servicio	T. Máximo = 30 días naturales	1.000 € por cada día natural de retraso
Servicio manual de análisis de vulnerabilidades	Implantación del servicio	T. Máximo = 30 días naturales	1.000 € por cada día natural de retraso
	Tiempo de entrega de informes de resultados de análisis.	T. Máximo = 21 días naturales	1.000 € por cada día natural de retraso
Servicio de monitorización de eventos	Implantación del servicio	T. Máximo = 180 días naturales	1.000 € por cada día natural de retraso
	Disponibilidad de la plataforma de monitorización y sus elementos	Disponibilidad $\geq 95\%$	10.000 € por indisponibilidad
	Tiempo de respuesta ante una incidencia del sistema	T. Máximo = 1 hora	100 € por cada hora de retraso
	Tiempo de resolución ante una incidencia en el sistema	T. Máximo = 48 horas	1.000 € por cada día natural de retraso
	Incorporación de nuevas fuentes de eventos de seguridad	T. Máximo = 30 días naturales	1.000 € por cada día natural de retraso
Servicio de detección de amenazas y vigilancia digital	Implantación del servicio	T. Máximo = 60 días naturales	1.000 € por cada día natural de retraso
Servicio de detección de incidentes Nivel 1 y Nivel 2	Implantación del servicio	T. Máximo = 60 días naturales	1.000 € por cada día natural de retraso
	Tiempo de notificación de actividades sospechosas desde su detección	T. Máximo ≤ 30 minutos	100 € por cada hora de retraso
	Tiempo de emisión de dictamen sobre actividad sospechosa detectada y acciones a realizar	T. Máximo ≤ 90 minutos	100 € por cada hora de retraso
	Eficacia de la detección	Nº Eventos sospechosos no descubiertos ≤ 0	1.000 € por cada evento sospechoso no descubierto
Servicio especializado de respuesta a incidentes	Implantación del servicio	T. Máximo = 15 días naturales	1.000 € por cada día natural de retraso
	Tiempo de entrega de informes de impacto	T. Máximo = 24 horas	1.000 € por cada hora de retraso
Servicio de soporte a la gestión de incidentes de seguridad	Implantación del servicio	T. Máximo = 15 días naturales	1.000 € por cada día natural de retraso
	Tiempo de asignación de recursos desde solicitud	T. Máximo = 4 horas	1.000 € por cada hora de retraso
Servicio de diseño y operación de procesos y tecnologías del SOC	Implantación del servicio	T. Máximo = 15 días naturales	1.000 € por cada día natural de retraso
Servicio de soporte a la gestión y operación del SOC	Implantación del servicio	T. Máximo = 6 meses	1.000 € por cada día natural de retraso
	Disponibilidad del portal	Disponibilidad $\geq 95\%$	1.000 € por indisponibilidad



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981582682548263284025**

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Servicio de asesoría y asistencia legal	Implantación del servicio	T. Máximo = 15 días naturales	1.000 € por cada día natural de retraso
	Tiempo de entrega de informes jurídicos	T. Máximo = 7 días naturales	1.000 € por cada día natural de retraso
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	1.000 € por cada día natural de retraso
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	10.000 € por cada cambio adicional
Entrega de informes	Tiempo de entrega de informes mensuales de servicios	Décimo día hábil del mes siguiente	1.000 € por cada día natural de retraso

Para todos aquellos ANS asociados al cálculo de disponibilidad, ésta se calculará, por periodos de 1 mes desde la última indisponibilidad no penalizada, aplicando la siguiente fórmula:

$$D = \frac{T_{tot} - T_{nodisp}}{T_{tot}} * 100 (\%)$$

Dónde:

D = disponibilidad

T_{tot} = tiempo total del periodo considerado (en minutos).

T_{nodisp} = tiempo de no disponibilidad del servicio dentro del intervalo T_{tot} considerado (en minutos).

No se computarán los tiempos de mantenimiento programado debidamente comunicados y autorizados por Madrid Digital dentro del plazo fijado.

LOTE II:

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales	1.000 € por cada día natural de retraso
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual	10.000 € por cada cambio adicional
Entrega de informes	Tiempo de entrega de informes mensuales de servicios	Décimo día hábil del mes siguiente	1.000 € por cada día natural de retraso

- **FIN DEL ANEXO V** -

La Subdirectora General de Infraestructuras y Operaciones

Fdo.: Zaida Sampedro Préstamo.