Ref: [redacted]

madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

Comunidad de Madrid | CONSEJERÍA DE DIGITALIZACIÓN

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SERVICIOS DENOMINADO "***SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL – 4 LOTES***" A ADJUDICAR POR PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS

[redacted]

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SERVICIOS DENOMINADO "*SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL – 4 LOTES*", A ADJUDICAR POR PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS.

Contenido

1. INTRODUCCIÓN

De acuerdo con lo establecido en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 30 de diciembre de 2005), 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), y por de la Ley 11/2022, de 21 de diciembre, de Medidas Urgentes para el Impulso de la Actividad Económica y la Modernización de la Administración de la Comunidad de Madrid –artículo 26– (B.O.C.M. núm. 304, de 22 de diciembre de 2022), la **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante, la **Agencia o Madrid Digital**), en el ejercicio de sus competencias, obra con plena autonomía financiera y de gestión, y opera bajo los objetivos de horizontalidad y centralización en la gestión de los servicios de informática y comunicaciones de la Administración de la Comunidad de Madrid, de modo que se garantice el mejor equilibrio técnico-económico entre las soluciones aplicadas y los servicios prestados, todo ello sin perjuicio de la necesaria atención a las peculiaridades propias de los servicios públicos que se prestan a los ciudadanos.

Entre las competencias que, conforme al apartado tercero del referido precepto, se atribuyen a la Agencia para el cumplimiento de sus objetivos se recoge/n, en concreto, la/s siguiente/s:

> *a) La dirección, planificación, impulso, desarrollo y ejecución de planes y proyectos de tecnología, de comunicación electrónica y de seguridad de la información de la Administración General e Institucional de la Comunidad de Madrid, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información.*
>
> *d) La adquisición, el diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica, sistemas de información y de comunicaciones electrónicas y seguridad de la información de titularidad de la Agencia, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento, los centros de procesos de datos, incluido el uso de nubes públicas y privadas de la Comunidad de Madrid y el archivo electrónico único de los expedientes y documentos electrónicos.*
>
> *j) Elaboración y aprobación de las políticas de seguridad de los sistemas de información y comunicación electrónicas de titularidad de la Agencia y la gestión de los recursos comunes para la prevención, detección y respuesta a los incidentes y amenazas de ciberseguridad en el ámbito de sus funciones.*

El desarrollo de estas competencias de seguridad de la información y ciberseguridad es uno de los cinco objetivos del Plan Estratégico 2022-26 de Madrid Digital, cuyo propósito es: *Hacer de la Comunidad de Madrid una Administración más segura, confiable y resiliente*. Este objetivo se desarrolla en dicho plan a través de cuatro líneas de actuación, dos de ellas dedicadas a la prevención, cibervigilancia y detección de amenazas y vulnerabilidades de forma proactiva y temprana, con el fin de eliminarlas, neutralizarlas, minimizando las consecuencias de materialización de incidente de seguridad, y otra de respuesta y recuperación ante incidentes de seguridad que permitan gestionar el riesgo, minimizando el impacto del incidente e identificando sus causas.

Hay que tener en cuenta que, según va avanzando y aumentando la digitalización de la Comunidad de Madrid y, por tanto, el número y diversidad de servicios digitales y sistemas de información que utilizan los ciudadanos y los empleados públicos, mayor es la necesidad de ciberseguridad que garantice de forma trasversal e integradora que la información y los datos personales están protegidos. Y más aún si consideramos que cualquier Administración se relaciona de forma continua con el ciudadano, con otras Administraciones y con las empresas por Internet, red abierta a todo el mundo, en la que se detecta una tendencia al alta sobre todo tipo de ciberdelitos (sobre todo el ransomware, el phishing y las estafas por Internet) como la propia INTERPOL informó en su último informe global de tendencias de criminalidad de octubre de 2022.

Es evidente, por tanto, el importante reto en materia de seguridad de la información y ciberseguridad que tiene la Comunidad de Madrid y Madrid Digital, lo que obliga a reforzar y aumentar de forma constante y proactiva las capacidades de personal especializado, procesos y tecnologías de ciberseguridad, necesarias para asegurar la disponibilidad, confidencialidad e integridad de la información y de los servicios digitales, todo ello bajo un enfoque de identificación y gestión de riesgos.

En consecuencia, con esta contratación se pretende:

- Aumentar y mejorar las capacidades humanas, organizativas y tecnológicas en materia de prevención, detección, análisis y respuesta.
- Disponer de más flexibilidad y capacidad ante los riesgos y amenazas actuales y futuras.
- Reforzar las capacidades avanzadas de respuesta y resiliencia en caso de incidentes o ataques premeditados, que permitan reducir los tiempos de detección, identificar la causa raíz y minimizar el impacto de los incidentes de seguridad.
- Poder realizar simulacros, ejercicios de ataque y defensa que permitan evidenciar riesgos y debilidades para mejorar las defensas.
- Impulsar la mejora de la seguridad desde el diseño y el refuerzo de las medidas y controles de ciberseguridad aplicados en las protecciones para evitar los daños que puedan producir las distintas amenazas y vectores de ataque.
- Mejorar la conciencia, comprensión y compromiso con la ciberseguridad en toda la organización.

2. OBJETO DEL CONTRATO

El objeto del presente contrato es la prestación de los servicios de ciberseguridad necesarios para dotar a Madrid Digital de: capacidades en materia prevención, detección y análisis de amenazas, ciberataques y vulnerabilidades; de capacidades de respuesta y recuperación ante incidentes de seguridad; de capacidades de simulacros y ejercicios de ataque y defensa; de prescripción y asesoramiento de medidas y controles de ciberseguridad que fortalezcan las arquitecturas tecnológicas existentes o las que nuevas que se requieren implantar; y de apoyo a Madrid Digital para el seguimiento y control de la prestación de los servicios.

Se divide en los siguientes lotes:

- LOTE 1: Centro de Operaciones de Ciberseguridad (SOC-MD).
- LOTE 2: Servicios de Supervisión y Control de las Protecciones (SSCP-MD).
- LOTE 3: Servicio de Ciberseguridad Ofensiva (SCO-MD).
- LOTE 4: Oficina Técnica de Seguimiento y Control de los Servicios Gestionados de Ciberseguridad (OTSC-Ciber).

Todo ello, dentro del ámbito de competencia de la Agencia, de conformidad con lo establecido en el pliego prescripciones técnicas.

3. ÁMBITO DE ACTUACIÓN

El ámbito de actuación de los servicios descritos en este documento se circunscribe a los sistemas, servicios e infraestructuras TIC que sustentan los servicios digitales de la Comunidad de Madrid, competencia de Madrid Digital, los sistemas de información del Servicio Madrileño de Salud (SERMAS) de la Consejería de Sanidad, y los sistemas facilitados a través de la plataforma educativa EducaMadrid.

De manera aproximada, los sistemas, servicios e infraestructuras TIC sobre los que se aplicarán las capacidades demandadas son los siguientes:

- Sistemas de información, disponiendo actualmente de unos 1.500 sistemas de información con 5.700 módulos técnicos asociados, de los cuáles 320 sistemas están clasificados como oro, competencia de Madrid Digital.
- Sistemas de información del SERMAS.
- Plataforma educativa EducaMadrid.
- Infraestructuras transversales necesarias para garantizar la conectividad y funcionamiento de los sistemas de información.
- Usuarios que explotan de forma efectiva los sistemas de información asociados a los servicios públicos.

4. LOTE 1: CENTRO DE OPERACIONES DE CIBERSEGURIDAD

El objeto de este lote será dotar a Madrid Digital de los servicios gestionados de seguridad del Centro de Operaciones de Ciberseguridad, en adelante SOC-MD, que aseguren su adaptación al contexto actual de riesgos y amenazas, estableciéndose como objetivos:

- Reducir el tiempo de detección de incidentes, limitando así la capacidad de los atacantes para comprometer activos y exfiltrar información sensible.
- Minimizar el impacto de los incidentes de seguridad, mediante el despliegue de medidas de contención inmediatas.
- Facilitar una visibilidad completa de la seguridad de todos los activos soporte de los sistemas de información, categorizados por criticidad, integrando los nuevos servicios en nube.
- Aplicar una defensa activa frente a una defensa reactiva, potenciando las actividades relacionadas con la búsqueda proactiva de amenazas.
- Apoyar en la elaboración de las hojas de ruta de seguridad de Madrid Digital, identificando puntos de mejora, y mejorar la comprensión por parte de la organización del riesgo que las amenazas de ciberseguridad suponen para el negocio.

Se exigirá al licitador propuesto como adjudicatario pertenecer la Red Nacional de SOC creada por el Centro Criptológico Nacional, en adelante CCN-CERT, y ser miembro de FIRST (Forum of Incident Response and Security Teams).

4.1 SERVICIOS REQUERIDOS

El número y complejidad de los sistemas de información y activos a proteger crece de forma continua, y las ciberamenazas a las que están expuestos son cada vez más complejas. Esto implica una mayor demanda de los servicios y procesos de ciberseguridad asociados que obliga a la adopción de estrategias de industrialización de aquellos servicios más maduros, permitiendo así enfocar los esfuerzos en el diseño de nuevos servicios.

Alineado con este planteamiento, todos los servicios demandados a lo largo de este pliego de prescripciones técnicas deberán diseñarse teniendo en cuenta criterios de eficiencia en recursos y herramientas, eficacia en resultados y mejora continua.

En la siguiente figura se recogen los servicios gestionados demandados:

Prevención	Monitorización y Detección	Análisis y Respuesta	Soporte a la Gestión, operación y procesos
Identificación de amenazas y vigilancia digital	Monitorización de eventos SIEM	Análisis y respuesta a incidentes	CMDB
Análisis de vulnerabilidades de sistemas y redes	Monitorización de tráfico Sondas IDS - NDR	Orquestación y automatización	Plataforma MISP
Análisis de vulnerabilidades de aplicaciones	Detección de ciberincidentes	Análisis forense	Portal y cuadros de mando
Ciberejercicios	Búsqueda proactiva de amenazas (Threat Hunting)	Gestión de cibercrisis	Herramientas auxiliares
Capacitación y formación			
Asesoría y asistencia legal			

Con carácter general, los licitadores deberán facilitar en la descripción de cada uno de los servicios, la siguiente información mínima:

- Relación detallada de herramientas principales y de apoyo que utilizará para ofrecer cada servicio, indicando versiones utilizadas, licenciamiento/subscripción si procede, y modalidad de uso.
- Relación detallada de fuentes de inteligencia públicas y comerciales, utilizadas en cada uno de los componentes que así lo requieren. Madrid Digital se reserva el derecho de continuar, a la finalización del contrato, con las fuentes comerciales propuestas.
- Los licitadores deberán contemplar como proyectos “llave en mano” la puesta en marcha de las plataformas o herramientas que proponga para los diferentes servicios. En caso de no existir partida económica específica al respecto deberá considerarse prorrateado en el importe de cada servicio, o bien en el importe global del contrato.
- La instalación de cualquier componente de los servicios en Madrid Digital deberá observar toda la normativa interna de aplicación, como son procedimientos de acceso a las CPD’s, etiquetado de componentes, normativa técnica de instalación, etc. Madrid Digital facilitará esta información al inicio del contrato.
- Propuesta de procedimiento para la prestación del servicio que será validada en todo caso por Madrid Digital al inicio de la ejecución del contrato.
- Interrelaciones con el resto de servicios demandados, y con los sistemas de información de Madrid Digital.

- Controles de seguridad internos establecidos orientados al cumplimiento normativo del Esquema Nacional de Seguridad (en adelante ENS) que podrán ser auditados por Madrid Digital.

Con carácter general, **las infraestructuras en nube que presten servicios deberán estar alojadas en datacenters de la Unión Europea.**

4.1.1 Servicios de prevención

El objetivo fundamental de los servicios de prevención requeridos será obtener un diagnóstico global del estado técnico de la ciberseguridad de los sistemas TIC responsabilidad de Madrid Digital que permita una detección temprana de las vulnerabilidades y una actuación proactiva en el despliegue de medidas de seguridad preventivas.

4.1.1.1 Identificación de amenazas externas y vigilancia digital

Este servicio facilitará una visión externa de las diferentes amenazas de seguridad que puedan afectar a la organización fuera de su perímetro, permitiendo el desarrollo de una defensa proactiva de ciberseguridad, una mejor gestión de los riesgos, la orquestación y automatización de acciones en base a una priorización de amenazas, y un mejor conocimiento de los atacantes y de sus intenciones.

El servicio se prestará sobre los diferentes activos públicos de Madrid Digital, como pueden ser entre otros: nombres de consejerías y organismos, marcas asociadas a la Comunidad de Madrid, direccionamiento IP público de servicios, aplicaciones, webs y dominios publicados, cuentas de correo electrónico corporativas, aplicaciones móviles desarrolladas por Madrid Digital y disponibles en los diferentes *stores* públicos, etc.

Al inicio de la ejecución del contrato, Madrid Digital definirá en colaboración con el adjudicatario, la relación completa de activos a vigilar. Esta relación podrá ser modificada a instancias de Madrid Digital en cualquier momento de vigencia del contrato.

Las actividades a desarrollar serán las siguientes:

- Alerta temprana de amenazas de seguridad, que puedan afectar a la seguridad de los servicios, sistemas e infraestructuras TIC gestionadas por Madrid Digital.
- Información de vulnerabilidades de seguridad, en base a los CPE (Common Platform Enumeration) de los activos expuestos.
- Monitorización de la superficie de exposición de Madrid Digital para la identificación de los recursos activos, cambios en resoluciones IP-dominio, creación de nuevos subdominios, apertura de puertos/servicios en IP's monitorizadas, etc.
- Monitorización de fuentes diversas de información para la detección temprana de, entre otros:
    - Suplantaciones de identidad.
    - Actividades relacionadas con el fraude.
    - Campañas de malware.
    - Fugas de información, accidentales o premeditadas.

- Exposición de credenciales.
- Venta de accesos/credenciales en mercados de la DeepWeb.
- Hacktivismo y ataques organizados.
- Abuso de marca.
- Dominios ilegítimos de reciente creación.

Los licitadores deberán indicar específicamente en su propuesta de servicios la relación de fuentes de información y actores relevantes en el contexto de ciberseguridad consultados, que serán monitorizados en tiempo real, debiendo cubrir al menos las siguientes:

- Fabricantes de tecnología TIC.
- Proveedores de servicio.
- CERTS públicos.
- Fuentes abiertas OSINT (Open Source INTelligence) y de acceso restringido.
- Canales de mensajería como Telegram.
- Webs de la DarkWeb.
- Redes sociales, foros, blogs y comunidades.
- Repositorios públicos de código tipo Github.
- Sitios relativos a fugas de información.

- Recopilación y análisis de indicadores de compromiso (IOC's) de interés e incorporación de los mismos a la MISP de Madrid Digital, para su notificación y consumo interno.
- Ejecución de las tareas necesarias de cierre técnico de dominios maliciosos detectados que suplanten dominios legítimos de la Comunidad de Madrid, y apoyo en las acciones legales que puedan derivarse de esta detección.

El servicio realizará una gestión completa del ciclo de vida de las amenazas detectadas, contemplando desde la identificación, recopilación y almacenamiento de los datos obtenidos, su procesamiento inteligente, clasificación y evaluación, la generación de alertas en base a peligrosidad de la amenaza y probabilidad de materialización, elaboración de informes, registro en los sistemas de seguimiento de Madrid Digital y propuestas para mitigación y/o eliminación de la amenaza.

Se valorará en la propuesta la puesta a disposición de Madrid Digital de una cuenta de acceso a las plataformas utilizadas para la prestación del servicio, propias o de terceros (plataforma de Threat Intelligence del adjudicatario, Shodan, Censys.io, servicios de protección frente a robo de cuentas, etc.) para análisis directo de la información obtenida.

4.1.1.2 Análisis de vulnerabilidades de seguridad de sistemas y redes

Este servicio tendrá como objetivo identificar las vulnerabilidades existentes en los activos soporte de los servicios y sistemas de información responsabilidad de Madrid Digital, con el objetivo de adoptar medidas orientadas a disminuir los riesgos de explotación de una vulnerabilidad, el número de incidentes de seguridad asociados y su afectación.

El servicio gestionará de forma completa el ciclo de vida de las vulnerabilidades de seguridad de todos los activos, ya estén desplegados en infraestructura on-premise o en infraestructura en nube (pública o privada), facilitando una priorización de cada vulnerabilidad e información suficiente que permita conocer el grado real de riesgo asociado, así como planificar las acciones para minimizar los riesgos asociados.

Las principales actividades a desarrollar en este servicio serán las siguientes:

- Descubrimiento de activos, ya sea on-premise o en nube, detallando nombre, IP, sistema operativo, puertos abiertos, aplicaciones en ejecución.
- Generación de una base de datos de los activos encontrados, clasificados por criticidad para el negocio y nivel de seguridad. Esta base de datos será la fuente de información posterior para el reporte de la postura de seguridad y priorización de las actividades de mitigación.
- Identificación y análisis de la superficie de exposición de Madrid Digital y construcción de la estrategia de protección correspondiente.
- Análisis de las distintas redes/activos descubiertos para búsqueda de vulnerabilidades, en las franjas y horarios aprobados por Madrid Digital.
- Auditorías técnicas específicas de sistemas críticos (correo, directorio activo, etc.).
- Clasificación de las vulnerabilidades por CVE (Common Vulnerabilities and Exposures).
- Registro de cada vulnerabilidad encontrada, criticidad y recomendaciones de mitigación.
- Explotación de cada vulnerabilidad, de forma controlada, sin comprometer información sensible ni la disponibilidad del servicio prestado, para verificar el impacto de la vulnerabilidad.
- Priorización del tratamiento de cada vulnerabilidad en base a factores como criticidad del activo para el negocio, nivel de exposición, facilidad de explotación, interés del atacante, facilidad de descubrimiento de la vulnerabilidad o contexto del negocio.
- Evaluación del impacto de nuevas vulnerabilidades, ya sean notificadas por el servicio de vigilancia digital o por terceros, en los activos de Madrid Digital, determinando a qué activos afecta, en qué grado, qué medidas de remediación hay que aplicar, etc.
- Notificación y gestión del ciclo de vida de las vulnerabilidades identificadas a las áreas internas de Madrid Digital responsables de su tratamiento. Para ello, hará uso de las plataformas de notificación y seguimiento de Madrid Digital (ITSM-FARO).

Este servicio se prestará en modalidad de servicio continuo, en base a las solicitudes de análisis de infraestructuras o sitios web que solicite Madrid Digital, o planificaciones acordadas.

Los licitadores deberán indicar en su oferta el conjunto de herramientas utilizadas para el servicio, considerándose dentro del coste del servicio todos los gastos derivados de las mismas (licencias, mantenimientos, actualizaciones, etc.). El personal técnico de Madrid Digital dispondrá de permisos de acceso a todas las herramientas.

La herramienta para escaneo de vulnerabilidades propuesta deberá cumplir los requisitos técnicos mínimos siguientes, debiendo integrarse los resultados obtenidos con la plataforma de gestión de

eventos e información de seguridad SIEM, para enriquecimiento de la información tratada por ésta, y con el sistema de seguridad, orquestación, automatización y respuesta (SOAR) propuesto.

Las principales características que debe cumplir esta herramienta son:

- Capacidad mínima de análisis simultáneos de 8.000 activos.
- Capacidad de escaneo de redes en función de un rango de IP, protocolo, puerto, etc.
- Visualización de la información/identificación de cada dispositivo mapeado.
- Identificador único para cada detección.
- Identificación de vulnerabilidades de software base y de los parches o comandos que deben aplicarse.
- Agrupación de vulnerabilidades según su posible solución.
- Cuadro de mando que permita acceder en una vista única, a todas las vulnerabilidades descubiertas y priorizar su corrección por estado, severidad o categoría.
- Detección continua y/o programada de activos.
- Posibilidad de iniciar/parar el escaneo en cualquier punto del proceso.
- Posibilidad de programar escaneos a una hora determinada, dependiendo del ámbito, o de los objetivos a escanear.
- Posibilidad de realizar auditorías basadas en políticas configurables.
- Posibilidad de realizar escaneos autenticados y no autenticados.
- Generación de informes con posibilidad de personalización.
- Descarga de informes en múltiples formatos, como PDF y Excel.
- Generación de informes en español.
- Capacidad de envío de correos con información de alarmas o incidencias.
- Posibilidad de envío programado de correos.
- Solución escalable, permitiendo el crecimiento natural de la infraestructura.
- Posibilidad de definición de perfiles de acceso y permisos asociados por grupos.
- Integración con directorio activo para identificación de usuarios.
- Registro de accesos de usuario a la herramienta.

Madrid Digital dispone de una plataforma de análisis de vulnerabilidades basada en Insight Rapid7, desplegada en infraestructura interna propia para la ejecución de análisis de activos on-premise. Los licitadores deberán indicar en su oferta si proponen una continuidad de la misma o su sustitución, debiendo tener en cuenta la obligación de renovación por parte del adjudicatario del contrato, de las licencias de producto correspondientes. En caso de sustitución, Madrid Digital no asumirá ningún coste adicional de despliegue de la nueva solución.

Adicionalmente**, se valorará la puesta a disposición del servicio de soluciones específicas de seguridad** para**:**

- **Analizar y auditar la postura de seguridad de los servicios en nube**, mediante la supervisión de los sistemas e infraestructuras en nube para identificar errores de configuración, infracciones en la política de seguridad, o vulnerabilidades potenciales en los servicios, las aplicaciones y los recursos en nube (soluciones CSPM – Cloud Security Posture Management).
- **Revisar de forma automatizada la explotabilidad de las vulnerabilidades identificadas en los sistemas internos**, emulando la perspectiva de un atacante, que permita el descarte de falsos positivos y la priorización de la remediación. La solución propuesta no requerirá la instalación de ningún agente.
- **Revisar de forma automatizada y continua las vulnerabilidades asociadas a la superficie de exposición**, explotación automática controlada de cada vulnerabilidad para descarte de falsos positivos y visualización del camino más fácil o probable de un atacante para descubrir la vulnerabilidad. La solución propuesta no requerirá la instalación de ningún agente. A efectos de dimensionamiento de esta solución, Madrid Digital dispone de una reserva de 1.275 IP's públicas (5 clases C) y 187 IP's activas.

Los licitadores indicarán en su oferta técnica el nivel de integración de la información obtenida con estas herramientas y la plataforma de gestión de eventos e información de seguridad SIEM propuesta.

4.1.1.3 Análisis de vulnerabilidades de seguridad de aplicaciones

Este servicio tendrá por objeto la realización de auditorías manuales de seguridad sobre las aplicaciones y sistemas de información gestionados por Madrid Digital en el entorno de producción, ya sean desarrollos propios o productos comerciales, mediante la ejecución de pruebas de penetración por parte de personal técnico experto.

Las auditorías de seguridad se realizarán indistintamente en modalidad de caja negra, gris o blanca, en los horarios acordados con Madrid Digital, debiendo estudiarse como mínimo las siguientes áreas:

- Lógica de negocio de cada aplicación.
- 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.

Podrán solicitarse auditorías específicas de sistemas concretos como servicios de directorio activo.

Con carácter general, las actividades de análisis no comprometerán la integridad de los datos objeto de revisión, ni la disponibilidad de los servicios analizados, si bien Madrid Digital se reserva la posibilidad de solicitar pruebas específicas de denegación de servicio para sistemas concretos, con el objetivo de valorar adecuadamente las protecciones antiDDoS instaladas.

Al igual que en el caso de las vulnerabilidades de sistemas y redes del punto anterior, la notificación y gestión de las vulnerabilidades identificadas a las áreas internas de Madrid Digital responsables de su tratamiento, se realizará a través de la plataforma de notificación y seguimiento de Madrid Digital (ITSM-FARO).

Los licitadores indicarán en su oferta técnica la metodología de análisis, tácticas, técnicas y procedimientos aplicados para la prestación del servicio, los criterios de valoración de las vulnerabilidades encontradas y las herramientas de análisis y explotación utilizadas por el equipo técnico de hacking ético.

4.1.1.4 Ciberejercicios

Este servicio consistirá en la realización de ejercicios de ciberseguridad destinados a entrenar las capacidades, procedimientos técnicos, operativos, de gestión y coordinación de Madrid Digital, con el objetivo de evaluar su grado de madurez en materia de ciberseguridad y medir su capacidad de respuesta ante ataques reales, identificando desviaciones, debilidades, fortalezas y puntos de mejor en los procesos y planes de respuesta existentes.

Los principales objetivos de estos ejercicios serán los siguientes:

- Entrenar a la organización para mejorar la respuesta ante ciberataques reales.
- Identificar puntos de mejora en los procesos de seguridad de la información afectados.
- Mejorar las relaciones y modelos de comunicación entre las áreas afectadas.
- Mejorar los planes de respuesta ante incidentes.

Se pondrá a disposición los siguientes tipos de ejercicios:

- Table-top: para valorar el funcionamiento del comité de crisis y los procedimientos internos de actuación.
- Simulaciones de phishing controlados, orientados a evaluar el nivel de concienciación en ciberseguridad del personal de Madrid Digital.

Los licitadores facilitarán en su respuesta técnica las metodologías y procedimientos aplicados para la realización de estos ejercicios, así como el calendario de ejecución propuesto, duración de cada ciberejercicio, recursos dedicados para su ejecución y tipología de ejercicios a realizar con periodicidad mínima anual.

Cada ciberejercicio irá acompañado de un informe de resultados en donde se recogerán los resultados obtenidos, las fortalezas, debilidades y puntos de mejora correspondientes.

4.1.2 Servicios de monitorización y detección

4.1.2.1 Monitorización de eventos de seguridad.

La monitorización de eventos de seguridad tendrá como objetivo fundamental la recolección de los eventos de seguridad de los diferentes componentes tecnológicos que sustentan las aplicaciones y sistemas de información, para que, analizados de forma conjunta, correlados y enriquecidos con el contexto tecnológico y la información de amenazas disponible, puedan convertirse en alertas de

seguridad. La confirmación tras su análisis de estas alertas de seguridad derivará en la apertura de un incidente de ciberseguridad a gestionar.

Las principales actividades a desarrollar en este servicio serán las siguientes:

- Implementar, administrar y operar el servicio de gestión de eventos e información de seguridad, SIEM (Security Information and Event Management) de Madrid Digital. Los requisitos técnicos a cumplir por el servicio están especificados en el apartado ***4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad - SIEM*.**

  Las tareas de gestión, mantenimiento y actualización de la plataforma asociada al servicio deberán realizarse de forma transparente, sin ningún tipo de indisponibilidad o inactividad total o parcial.

- Implementación, mantenimiento y configuración de las sondas de detección de intrusión IDS descritas en el apartado ***4.1.2.2.1 Análisis de tráfico para detección de intrusiones – sondas IDS***

- Suministrar, administrar y operar el servicio de análisis avanzado de tráfico – NDR, descrito en el apartado ***4.1.2.2.2 Análisis avanzado de tráfico – NDR*** Las alertas generadas por este servicio serán una fuente más de eventos de seguridad a gestionar desde la plataforma SIEM.

- Integrar las fuentes de eventos de seguridad que determine Madrid Digital. El proyecto técnico inicial de implantación deberá contemplar la integración de las fuentes operadas actualmente, recogidas en el apartado ***10.3 Plataforma SIEM actual de Madrid Digital-,*** así como las alertas generadas por el sistema EDR corporativo (Watchguard), y las generadas por el ecosistema Office 365, ambas no gestionadas de forma centralizada por el SIEM en la actualidad. Madrid Digital acordará con el adjudicatario del contrato la relación de fuentes de eventos susceptibles de integración a lo largo del contrato.

- Analizar y correlacionar todos los eventos y alertas de seguridad para detectar posibles anomalías o amenazas de seguridad.

- Creación y administración de los casos de uso de monitorización/reglas de detección para la detección de incidentes de seguridad. Los licitadores aportarán en su repuesta al pliego, su propuesta de casos de uso a generar, mapeados con las técnicas, tácticas y procedimientos recogidos en el framework MITRE ATT&CK.

  En todo caso, al inicio de la ejecución del contrato Madrid Digital facilitará la relación de casos de monitorización actualmente configurados (más de 195 casos), para su traslado si procede a la nueva plataforma.

- Generar indicadores de compromiso (IOC's) en base a alertas del servicio y consolidar estos indicadores en la plataforma MISP de Madrid Digital.

4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad - SIEM

Al amparo de este contrato, y como pieza fundamental del servicio de monitorización de eventos de seguridad, el adjudicatario pondrá a disposición de Madrid Digital una plataforma de gestión de eventos e información de seguridad, SIEM, como mejora y sustitución de la actual, que permita integrar

elementos ubicados en dependencias de la Comunidad de Madrid, físicos y virtuales, y servicios prestados en la nube (cloud) en cualquier modalidad (SaaS, PaaS, IaaS).

A continuación, se recogen los requisitos técnicos mínimos de la plataforma SIEM a suministrar.

Requisitos generales de la plataforma:

- **La solución propuesta deberá estar incluida en el Catálogo de Productos de Seguridad de las TIC (Catálogo CPSTIC) recogido en la Guía de Seguridad de las TIC CC-STIC-105 "Catálogo de productos y servicios de seguridad de las tecnologías de la información y la comunicación", con categoría ENS ALTA**.
- **Se valorará la posición de la plataforma SIEM propuesta en el último cuadrante de Gartner (Cuadrante SIEM) y Forrester (Cuadrante de plataformas de analíticas de seguridad).**
- La solución propuesta será en nube, preferiblemente pública tipo SaaS, y no debe requerir la instalación de ningún elemento físico o virtual en los Centros de Proceso de Datos (CPD's) de Madrid Digital, salvo los elementos imprescindibles para la recolección de eventos. En todo caso, si durante la fase de implantación del SIEM, antes de la finalización del tiempo previsto de esta fase (tres meses) el adjudicatario declarase la imposibilidad técnica de prestar el servicio requerido en nube ya sea de forma total o parcial, estará obligado a prestar el servicio con solución on-premise en los CPD's de Madrid Digital de forma completa, o bien, mediante solución hibridada en nube y on-premise en los CPD's de Madrid Digital. Todo ello no incurrirá en ningún caso en coste adicional para Madrid Digital ya sea de inversión en hardware o software o bien en servicios de diseño y puesta en marcha.
- Los servicios de infraestructura propuestos por los licitadores para prestar el servicio deberán estar alojados en centros de proceso de datos de la Unión Europea, y disponer de la certificación de ENS nivel ALTO.
- La plataforma deberá facilitar capacidades de orquestación, automatización y respuesta (SOAR). En caso de optar por una solución independiente de la solución SIEM propuesta, todos los costes derivados de la solución SOAR y de las integraciones con el resto de componentes solicitados, deberán considerarse incluidos dentro del licenciamiento de la solución SIEM. Las funcionalidades de este sistema se describen específicamente en el apartado ***4.1.3.2 Sistema de orquestación, automatización y respuesta***
- La línea de comunicaciones necesaria para la transmisión de los datos a la solución en nube tanto de las fuentes de eventos/alertas on-premise (por ejemplo: EDR, firewall, etc.) como de los logs de las fuentes que ya están en nube (por ejemplo: Office 365), deberá ser dedicada y cumplir con los protocolos de seguridad establecidos (cifrado TLS). Será responsabilidad del adjudicatario el dimensionamiento y mantenimiento operativo de esta conexión.
- Todos los elementos de la plataforma, incluidos los elementos a desplegar on-premise, contarán con medidas de redundancia ante fallos.
- La plataforma dispondrá de control de acceso con doble factor de autenticación, soportar SSO (SAML 2.0) para su integración con los sistemas de gestión de identidades de Madrid Digital, múltiples usuarios y diferentes roles.

- Facilitará capacidades de registro de auditoría de la actividad de los usuarios, incluyendo tareas administrativas (creación de usuarios, asignación de roles, etc.) y de operación. Esta información de auditoría debe ser accesible desde la propia interfaz o a través de API.
- Todas las comunicaciones entre componentes de la plataforma se realizarán de forma cifrada.
- La plataforma se integrará con el resto de las soluciones propuestas para los servicios y con soluciones de terceros y propias de Madrid Digital. Específicamente deberá integrarse con la solución corporativa de ticketing (ITSM-FARO) y con LUCIA, herramienta de ticketing del CCN-CERT.

Elementos conceptuales de la plataforma:

La plataforma constará de los siguientes elementos conceptuales, no siendo obligatorio su asociación unívoca a la propuesta:

- **Agente**: elemento software opcional para recoger información sobre eventos en un sistema y enviarlos a un recolector de ámbito superior o al procesador de eventos.
- **Recolector de eventos**: elemento encargado de recoger información de los diferentes dispositivos de la red, sistemas y aplicaciones; filtrar, consolidar y normalizar los eventos y flujos de red recogidos, y reenviarlos, total o parcialmente, al procesador de eventos. El sistema facilitará la posibilidad de almacenarlos localmente para consulta posterior.
- **Procesador de eventos**: elemento encargado de normalizar, priorizar y recolectar la información procedente de los elementos de captura de información y eventos, así como de realizar evaluaciones del riesgo, enriquecimiento, contextualización y correlación de eventos. El servidor de gestión podrá recibir información y eventos de seguridad desde elementos situados en su mismo nivel o bien en capas inferiores. Además, soportará la ejecución de tareas de mantenimiento del sistema y de tareas externas, como las copias de respaldo.
- **Repositorio de logs:** elemento en el que se realizará el almacenamiento de todos los eventos recogidos.
- **Base de datos de gestión:** elemento en el que se almacenarán los eventos representativos de seguridad, las alertas generadas, informes, inventario de activos e información útil para la gestión.
- **Consola de administración y operación centralizada:** interfaz para la operación centralizada de toda la plataforma.
- **Fuentes de inteligencia integradas:** ya sean externas o propias de cada licitador.

Dimensionamiento de la plataforma:

La plataforma deberá estar dimensionada y correctamente licenciada para cumplir los siguientes requisitos mínimos a lo largo de la ejecución del contrato:

- Capacidad mínima de ingesta diaria total de 3 TeraBytes, ampliable bajo demanda (y reducible) de eventos, flujos y alertas de seguridad.

  Cada 6 meses se procederá a la revisión del número medio de TeraBytes diarios ingestados para decidir si procede su regularización al alza o a la baja. A tal efecto, los licitadores indicarán

en su repuesta económica el coste unitario del servicio para una ingesta diaria de 500 GigaBytes, de forma que las ampliaciones/reducciones posteriores se realizarán en base a este valor. Este precio deberá tener prorrateado todos los costes asociados correspondientes, no admitiéndose ningún coste adicional por ampliación, mantenimiento, operación o gestión.

- La plataforma deberá ser capaz de asumir picos de EPS o de ingesta diaria, sin pérdida de eventos.
- **Se valorará la puesta a disposición, sin coste adicional, de soluciones software propias de la plataforma o independientes, orientadas a la reducción y optimización de los datos de cada una de las fuentes de eventos que finalmente se ingestarán en el procesador de eventos (en nube).** Estas soluciones buscarán minimizar el volumen de datos a ingestar en la nube. Los licitadores deberán indicar claramente en su propuesta cómo se realizará la gestión y retención de los eventos originales, las políticas de filtrado en origen aplicadas y/o la comprensión de los mismos, tanto para fuentes de eventos on-premise como en nube.
- La recolección de eventos de fuentes on-premise deberá realizarse tanto en los dos CPD's de Madrid Digital como en los dos CPD's de la Consejería de Sanidad.
- La recolección de eventos en nube de Office 365 deberá realizarse en el *tenant* de Microsoft.
- Para la recolección de eventos de otros servicios desplegados en nubes públicas (Amazon Web Service, Google Cloud, etc.), el licitador acordará con Madrid Digital la mejor estrategia a seguir.
- Almacenar toda la información de eventos y alertas para su correlación de forma on-line durante un periodo mínimo de tres meses, y un periodo mínimo de retención de eventos off-line de doce meses.
- Inclusión de nuevas fuentes de eventos y alertas en un plazo inferior a 10 días hábiles.
- Posibilidad de almacenar una copia de los eventos en sistemas on-premise.

Fuentes de eventos

La plataforma de gestión de eventos e información de seguridad recibirá y almacenará los eventos de fuentes diversas, por lo que deberá tener la funcionalidad para procesar de forma nativa tanto los eventos como las alertas de las fuentes indicadas a continuación o, en su defecto, de desarrollar el parseo necesario para su tratamiento.

La plataforma deberá poder integrarse con:

- Cortafuegos de red.
- Balanceadores de tráfico.
- Routers.
- Switches.
- Proxies de navegación.
- Servicios de nombres de dominio (DNS).
- Servicios de acceso remoto RADIUS.

- Servicios de directorio LDAP y DA.
- Sistemas de VPN y acceso remoto.
- Sistemas de correo corporativo.
- Sistemas antispam y antimalware de correo.
- Servidores web Apache, y Nginx.
- Servidores de aplicaciones Weblogic, Tomcat…
- Bases de datos Oracle, MySQL y Postgree.
- Sistemas operativos Linux, Windows.
- Sistemas EDR corporativos, de puesto de trabajo y de servidor.
- Servicios de ofimática en nube, Office 365.
- Sistema NDR.

Los protocolos mínimos de intercambio de fuentes de eventos soportados serán:

- Protocolo SNMP: SYSLOG.
- Fuentes de eventos en formatos XML, TXR, CSV, CEF o JSON.
- Flujos de red en formato NetFlow o IPFIX.

Correlación y casos de uso

La plataforma SIEM debe permitir:

- Correlacionar información de logs, flujos de red y vulnerabilidades en tiempo real.
- Correlación histórica de logs y flujos (correlación de una selección de eventos pasados contra indicadores de compromiso y reglas nuevas).
- Debe proporcionar casos de uso por defecto, documentados y mantenidos por el propio fabricante.
- Debe permitir la correlación automática de casos para ataques no conocidos por medio de técnicas de inteligencia artificial, **IA**, y capacidades de detección de anomalías.
- Debe incorporar algoritmos de aprendizaje automático, **Machine Learning,** para modelar y analizar el comportamiento habitual de entidades y usuarios y detectar desviaciones (capacidades de **UEBA** – User and Entity Behavior Analytics).
- Debe proporcionar informes por defecto, documentados y mantenidos por el propio fabricante.
- Debe permitir definir reglas de anomalías evaluadas en tiempo real que detecten cambios repentinos de un valor o suceso (por ejemplo: incremento repentino del volumen de tráfico).
- Debe permitir definir reglas de anomalías estacionales que detecten desviaciones en un valor o suceso (como el volumen de tráfico o número de logons fallidos) en comparación al mismo día de la semana anterior.

- 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”.
- Debe tener la capacidad de detectar en tiempo real el uso de una nueva IP o puerto en una subred.
- La capacidad de detectar en tiempo real el uso de un nuevo nombre de usuario en el entorno.
- Como se ha recogido anteriormente, debe ser capaz 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).
- Debe poder mapearse los casos de uso por defecto con la matriz MITRE ATT&CK.
- Se valorará la propuesta de los licitadores de la relación de casos de uso base de monitorización a implementar en la plataforma.

Inteligencia

La plataforma SIEM incluirá:

- Fuentes de inteligencia que faciliten la definición de reglas de correlación y detección.
- Capacidad de integración con fuentes de inteligencia externas basadas en estándares MISP y STIX/TAXII.
- Capacidad de ofrecer información de contexto durante el análisis del evento (geolocalización, reputación de IP, etc.).
- Librería de casos de uso alineados con el esquema Mitre ATT&CK.
- Clasificación de los eventos y alarmas según el esquema MITRE ATT&CK.

Instalación y aceptación de la plataforma

Con carácter general, el adjudicatario deberá observar toda la normativa interna de aplicación para el suministro e instalación de equipamiento en las instalaciones de Madrid Digital o de la Comunidad de Madrid, 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.

Madrid Digital considerará que la plataforma de monitorización objeto del contrato está plenamente operativa cuando se certifiquen las siguientes actividades:

- Entrega de documentación técnica de la plataforma instalada, detallando:
  - Arquitectura física y lógica de la plataforma, detallando todos los componentes de la solución.
  - Fuentes de eventos integradas. Como mínimo deberán estar instaladas la relación de fuentes de eventos integradas en la plataforma SIEM actual del Madrid Digital, recogida en el apartado ***10.3 Plataforma SIEM actual de Madrid Digital***.
  - Configuración inicial aplicada a la plataforma SIEM.

- **Casos de uso implementados.** El adjudicatario deberá haber analizado todos los casos de uso de monitorización definidos en la plataforma SIEM actual de Madrid Digital, e implementados al menos el 80% de los mismos o, en su defecto, justificación por escrito de su no implementación o sustitución por otros. Madrid Digital se reserva el derecho de exigir la implementación completa de todos los casos de uso actuales en la nueva plataforma.
- Relación detallada de licencias de servicios y productos contratados.

- **Plan de pruebas de aceptación: incluirá al menos el cumplimiento de todos los requisitos técnicos y funcionales del pliego y un informe de seguridad de la plataforma.**
- Plan de explotación y mantenimiento de la plataforma.
- Documentación técnica: casos de uso y manuales de uso, configuración y administración de la plataforma.

Funcionamiento de la plataforma

El servicio contemplará la ejecución, de forma transparente para Madrid Digital, de todas las acciones que garanticen la plena operatividad de la plataforma durante la vigencia del contrato de soporte y mantenimiento de la misma. Entre estas actividades se encuentran:

- Soporte hardware y software de la plataforma.
- Actualizaciones y parches de producto.
- Acceso a base de datos de conocimiento de la solución.
- Gestión de incidencias, cambios, parches y actualizaciones, control de acceso, usuarios y permisos.
- Monitorización de la disponibilidad de la plataforma.
- Mantenimiento preventivo y correctivo.
- Atención de consultas en horario 8x5 e incidencias en horario 24x7.
- Las tareas de gestión, mantenimiento y actualizaciones de la plataforma deben realizarse de forma transparente para el servicio.

En el apartado ***10.3 Plataforma SIEM actual de Madrid Digital*** se facilita una descripción somera de la plataforma SIEM actualmente instalada en Madrid Digital. **El adjudicatario estará obligado a su mantenimiento operativo hasta su sustitución por la nueva propuesta**. Este mantenimiento operativo incluirá el mantenimiento hardware de toda la plataforma actual y mantenimiento de licencias asociadas a *Elastic – SIEM-DATALAKE.* No se exigirá el mantenimiento de las licencias asociadas a Exabeam, SIEM-UEBA. Madrid Digital no asumirá ningún coste adicional por esta actividad.

Queda a criterio de los licitadores la reutilización total o parcial de la infraestructura actual. En este escenario, todos los costes derivados del mantenimiento operativo de los componentes (hw, sw) irán por cuenta del adjudicatario.

4.1.2.2 Servicio de monitorización de tráfico de red

4.1.2.2.1 Análisis de tráfico para detección de intrusiones – sondas IDS

Este servicio facilitará el mantenimiento, configuración y administración de las sondas de análisis de tráfico para detección de intrusiones IDS, en base a firmas de amenazas, desplegadas en las infraestructuras de Madrid Digital. El detalle de infraestructura asociada a esta capacidad se facilita en el apartado ***10.3 Plataforma SIEM actual de Madrid Digital.***

Madrid Digital considera que este servicio debe ser sustituido por el servicio de análisis avanzado de tráfico, toda vez que la detección de anomalías a través de firmas se ha visto ampliamente superado por los sistemas NDR, mucho más avanzado.

Únicamente se mantendrá en producción, y, por tanto, deberán ser operadas y mantenidas a lo largo del contrato por el adjudicatario, las sondas de análisis de tráfico SAT-INET y SAT-ICS desplegadas por el Centro Criptológico Nacional - CCN-CERT y administradas por estos. Madrid Digital no asumirá ningún coste adicional derivado del mantenimiento de los servidores sobre los que se despliegan estas sondas.

En todo caso, el adjudicatario estará obligado a la gestión y mantenimiento operativo de **toda** la infraestructura de sondas IDS hasta la puesta en marcha de la nueva solución NDR. Madrid Digital no asumirá ningún coste adicional por esta actividad.

En el caso específico de sondas IDS ubicadas en los centros hospitalarios, los licitadores deberán indicar en su propuesta técnica de sustitución, si consideran necesario instalar algún equipamiento adicional, en modo local como complemento a los equipamientos centrales a instalar en los CPD's, detallando ventajas e inconvenientes. Madrid Digital se reserva el derecho de aceptar o no la propuesta de equipos locales a instalar que realicen los licitadores.

4.1.2.2.2 Análisis avanzado de tráfico – NDR

El panorama actual de ciberamenazas y ataques provoca que las defensas tradicionales basadas en reglas y detecciones de firmas predefinidas, hayan perdido gran parte de su eficacia debido a la capacidad de los atacantes de modificar constantemente estos patrones. Esto provoca que las defensas de ciberseguridad ya no son capaces de detectar y neutralizar nuevas amenazas, APTs o insiders.

Ante esta situación, las tecnologías de análisis avanzado de tráfico NDR – Network Detection and Response, permiten atacar el problema desde otra perspectiva, utilizando tecnologías de inteligencia artificial y aprendizaje automático para detectar, neutralizar e investigar amenazas y ciberataques, priorizando los ataques reales frente a los falsos positivos.

Los licitadores suministrarán a través de este servicio una plataforma de detección y respuesta de red, NDR, que mediante aprendizaje automático y analítica de comportamiento sea capaz de identificar amenazas de red desconocidas.

Esta solución mejorará la eficacia de las técnicas de detección basadas en firmas al mirar más allá de las amenazas actuales y detectar atributos sospechosos en las nuevas, así como en versiones alteradas de amenazas conocidas.

La aplicación de técnicas de análisis estadístico permitirá analizar el comportamiento útil, desde un análisis sencillo de valores atípicos hasta análisis bayesianos básicos de patrones de tráfico de red.

Este análisis estadístico incluirá un componente de muestreo para establecer una línea base sobre la que se identifiquen actividades anómalas o sospechosas.

Las principales características que debe cumplir el servicio de análisis avanzado de tráfico son la siguientes:

- La solución analizará el tráfico este-oeste cursado tanto en los dos CPD's de Madrid Digital como en los dos CPD's de la Consejería de Sanidad.
- El dimensionamiento del equipamiento a instalar en los CPD's (sensores) será responsabilidad del adjudicatario, estimándose que el tráfico generado en cada CPD a analizar será como mínimo de 20 Gbit/seg.
- La solución estará dimensionada para proteger como mínimo los siguientes activos:
    - 126.0000 endpoints (PC's de usuario de sobremesa y portátiles).
    - 4.000 servidores, alojados en los dos CPD's de Madrid Digital.
    - 3.000 servidores alojados en los dos CPD's de la Consejería de Sanidad – SERMAS y en el CPD principal de EducaMadrid.

  Constituirían los 133.000 activos a proteger.
- La solución, mediante técnicas de análisis de comportamiento de tráfico con inteligencia artificial, permitirá analizar el tráfico cifrado cursado para encontrar actividades maliciosas de atacantes sin necesidad de descifrarlo, utilizando redes neuronales y aprendizaje profundo.
- La solución permitirá ver la progresión del ataque en base a las acciones realizadas por los atacantes.
- Permitirá el uso de firmas las cuáles servirán para reconocer una amenaza conocida en el futuro mediante el uso de indicadores de compromiso (IOC) específicos. Para ello, deberá ser capaz de realizar inspección profunda de paquetes, disponer de firmas de detección de patrones actualizadas y capacidad de modificación de firmas de detección existentes y creación de nuevas firmas personalizadas.
- La solución deberá poder alimentarse de flujos de datos (feeds de inteligencia de amenazas) que brinden información sobre amenazas en línea previamente identificadas. La inteligencia de amenazas ayudará a identificar amenazas conocidas y ofrecer información contextual adicional para clasificar una anomalía de red detectada.
- El envío de eventos desde el equipo sensor al correlador se realizará de forma cifrada.
- Reducción de falsos positivos mediante ajuste de los umbrales de detección.
- Triaje y priorización de detecciones basada en IA, analizando en tiempo real la gravedad y el impacto de las amenazas.
- Dispondrá de mecanismos para evitar la pérdida de eventos en caso de superación puntual 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.
- Integración con las soluciones SIEM/SOAR propuestas para otros servicios objeto de este contrato.
- Trabajar con reglas de detección de tráfico de red de formato SNORT/Yara.
- Deberá contar con una consola de gestión unificada, con independencia de la gestión que se pueda realizar en la solución SOAR.

Se valorará la posición de la plataforma de detección y respuesta NDR propuesta en el último cuadrante de Forrester (Cuadrante de visibilidad y análisis de red).

El servicio contemplará la ejecución de todas las acciones de soporte y mantenimiento de la plataforma NDR. Entre estas actividades se encuentran:

- Soporte hardware y software de la plataforma.
- Actualizaciones y parches de producto.
- Acceso a base de datos de conocimiento de la solución.
- Gestión de incidencias, cambios, parches y actualizaciones, control de acceso, usuarios y permisos.
- Monitorización de la disponibilidad de la plataforma.
- Mantenimiento preventivo y correctivo.
- Atención de consultas en horario 8x5 e incidencias en horario 24x7.
- Las tareas de gestión, mantenimiento y actualizaciones de la plataforma deben realizarse de forma transparente tanto para el servicio como para Madrid Digital.

4.1.2.3 Detección de ciberincidentes

El servicio de detección de ciberincidentes tendrá como objetivo principal la monitorización continua de los eventos o alertas generados por los servicios de prevención, monitorización, y vigilancia digital.

Las actividades fundamentales a realizar serán las siguientes:

- Triaje inicial de todas las alertas de seguridad recibidas para su identificación, clasificación y categorización en base a su nivel de peligrosidad. A tal fin, se seguirá lo recogido en la "***Guía nacional de notificación y gestión de ciberincidentes***" del Consejo Nacional de Ciberseguridad.
- Primer nivel de investigación y gestión del incidente, en base a procedimientos establecidos de tratamiento de cada alerta, identificación de impacto, activos afectados, nivel de compromiso de los servicios y acciones de mitigación y remediación a realizar. Escalado a grupos técnicos de Madrid Digital responsables de su ejecución.
- Escalado para su análisis al servicio de análisis y respuesta a incidentes para su tratamiento, en caso de no existencia de procedimiento, o peligrosidad inicial estimada.

- Documentar todos los casos tratados.
- Elaborar informes de actividad del servicio.
- Medición de ANS acordados.
- Operar los servicios de análisis de tráfico, sondas IDS y plataforma NDR.

El servicio se prestará en modalidad 24x7x365, con dedicación completa y combinación de prestación presencial en dependencias de Madrid Digital y remota en dependencias del adjudicatario.

El adjudicatario garantizará la asignación inicial al servicio del equipo mínimo recogido a continuación, con el horario indicado:

- 2 personas en horario de mañana, correspondientes a la prestación localizada en horario de 8 a 16 h.
- 1 persona en horario de tarde, correspondiente a la prestación localizada en horario de 12 a 20 h.
- 1 persona en prestación deslocalizada, en calendario y horario complementario al de la prestación localizada, para completar el servicio 24x7x365. Este recurso no requerirá adscripción exclusiva a este contrato.

El perfil profesional exigido a este servicio se recoge en el apartado ***4.2.3 Equipo de trabajo.***

4.1.2.4 Búsqueda proactiva de amenazas - Threat Hunting

El servicio de búsqueda proactiva de amenazas tiene por objetivo anticiparse a los incidentes de seguridad, mediante una búsqueda iterativa de amenazas persistentes, ocultas, que han pasado inadvertidas a los controles preventivos y de detección de la organización, que puedan encontrarse en las infraestructuras, servicios, y sistemas TIC de forma activa o latente.

Esta capacidad permitirá reducir los tiempos medios de detección, respuesta y contención de incidentes, y la superficie de exposición y ataque a amenazas internas/externas.

Los licitadores deberán indicar en su propuesta la metodología y enfoque de análisis que realizarán y los casos de búsqueda propuestos para el servicio, clasificados en base a la tipología de la búsqueda implementada, ya sea basada en inteligencia a través de IOC's y tácticas, técnicas y procedimientos de MITRE (TTP's), ya sea basada en hipótesis definidas por los analistas, o basada en análisis de valores atípicos o irregulares.

El servicio se prestará en modalidad 8x5, de forma remota, en dependencias del adjudicatario, y deslocalizada. No se requiere adscripción exclusiva de este recurso.

El adjudicatario garantizará la asignación inicial al servicio de un analista de seguridad con el perfil profesional recogido en el apartado ***4.2.3 Equipo de trabajo.***

4.1.3 Servicios de análisis y respuesta

Los servicios de análisis y respuesta ante incidentes de seguridad del SOC-MD serán el primer punto de notificación de incidentes relacionados con las infraestructuras y servicios responsabilidad de Madrid Digital, por parte de los administradores de seguridad correspondientes.

Será responsabilidad de este servicio la coordinación de todos los incidentes de ciberseguridad que requieran la actuación de varios equipos operativos de Madrid Digital, o bien que su nivel de peligrosidad estimada inicial sea ALTO, MUY ALTO o CRÍTICO, y que demanden además una notificación al CERT de referencia (CCN-CERT, CNPIC).

Además, recibirá toda la información de amenazas, alertas e incidentes de seguridad identificados por los diferentes servicios del SOC-MD, para su análisis y tratamiento correspondiente.

Los servicios demandados serán los detallados a continuación.

4.1.3.1 Análisis y respuesta a incidentes de seguridad

El servicio de análisis y respuesta recibirá los incidentes de seguridad identificados por el servicio de detección de ciberincidentes, el servicio de Threat Hunting, o cualquier otro canal establecido, para su análisis profundo, confirmación del ciberincidente, y respuesta para su contención, mitigación y eliminación.

Para ello, realizará las siguientes actividades:

- Recoger todas las alertas y/o incidentes de ciberseguridad escalados por el servicio de detección, para su análisis y respuesta, en base a los procedimientos y herramientas habilitados al efecto.
- Atender todos los canales de recepción de notificaciones de incidentes establecidos, como son: correo electrónico, llamada telefónica, sistema de gestión de ticketing corporativo ITSM, sistema de notificación de incidentes del CCN-CERT, LUCIA, etc.
- Gestionar y coordinar todos los incidentes de ciberseguridad en las plataformas de notificación y seguimiento de incidentes, ya sean propias del SOC-MD (plataforma SOAR) o de Madrid Digital (ITSM-FARO).
- Notificar en tiempo y forma a terceros cuando sea requerido por normativa vigente, a quien corresponda en cada caso.
- En los casos que proceda, activar el procedimiento corporativo de gestión de incidentes críticos (gestión de crisis).
- Elaborar los planes de respuesta a incidentes específicos.
- Proponer automatizaciones en el sistema de respuesta para mejorar la eficacia del proceso general de respuesta a incidentes.
- Proponer estrategias de contención de ciberataques.
- Investigación de incidentes y solicitud de análisis forense, si procede.
- Elaboración de informes de cada ciberincidente, incluyendo apartado específico de lecciones aprendidas.

El servicio se prestará en modalidad 24x7x365, con dedicación completa y combinación de prestación presencial en dependencias de Madrid Digital y remota en dependencias del adjudicatario.

El adjudicatario garantizará la asignación inicial al servicio del equipo mínimo recogido a continuación:

- 1 persona en horario de mañana, correspondiente a la prestación localizada en horario de 8 a 16 h.
- 1 persona en horario de tarde, correspondiente a la prestación localizada en horario de 12 a 20 h.
- Ante incidentes que puedan considerarse críticos, el adjudicatario deberá poner a disposición recursos para su gestión fuera del horario normal del servicio, para completar el servicio 24x7x365. Estos recursos no requerirán adscripción exclusiva a este contrato. Para este servicio se facilitará un teléfono de guardia, que garantizará la disponibilidad de este personal. Este servicio, en caso de requerirse, se facturará en base a la bolsa de horas definida para el servicio de ***4.1.3.4 Servicios de apoyo a la gestión de cibercrisis*.**

Los perfiles profesionales exigidos para este servicio se recogen en el apartado ***4.2.3 Equipo de trabajo.***

4.1.3.2 Sistema de orquestación, automatización y respuesta

Los licitadores deberán proponer un sistema de seguridad, orquestación, automatización y respuesta (SOAR) que, de forma centralizada, permita la administración y operación de todas las actividades de análisis y respuesta a incidentes.

Este sistema recibirá toda la información de amenazas, vulnerabilidades e incidentes de seguridad generados por las distintas plataformas/servicios del SOC-MD (escáner de vulnerabilidades, análisis manuales, SIEM, NDR, sondas IDS, incidentes recibidos a través de LUCIA, incidentes notificados a través del sistema de ticketing interno ITSM-FARO, etc.) y otras plataformas que Madrid Digital pueda solicitar a lo largo de la ejecución del contrato (EDR, sistemas CASB, etc.).

Se optará por soluciones que sean escalables y diseñadas para la gestión global de incidentes de seguridad desde su apertura hasta su cierre.

Además, dado el carácter confidencial de la información de esta herramienta y su interacción con el equipamiento de seguridad de Madrid Digital, **se valorará la instalación y configuración de la solución on-premise. En caso de optar por una solución en nube, se valorará la independencia de la misma con respecto a otros clientes del proveedor** de forma que, a la finalización del contrato, Madrid Digital pueda continuar con este servicio de forma sencilla.

La implantación progresiva de políticas de automatización y orquestación facilitará el trabajo de los analistas del servicio de detección de ciberincidentes, que dispondrán de un punto único de análisis, categorización y priorización de todas las alertas de ciberseguridad.

El sistema debe permitir la automatización de procesos mediante la elaboración y puesta en marcha de *playbooks* de actuación, debiendo facilitar:

- Número de usuarios analistas concurrentes: 4.
- Capacidades de orquestación de logs, eventos, alertas, flujos y vulnerabilidades provenientes de diferentes herramientas.
- Debe contar con *playbooks* por defecto, documentados y mantenidos por el propio fabricante, y con la capacidad de desarrollar nuevos *playbooks* personalizados mediante programación o uso de herramientas gráficas más visuales.

- Los *playbooks* se deben ejecutar a una velocidad razonable y no consumir excesivos recursos.
- La solución debe proporcionar documentación o proporcionar un registro de las acciones llevadas a cabo.
- Debe permitir la integración con herramientas o *feeds* de inteligencia de amenazas. A tal fin, los licitadores indicarán en su propuesta los *feeds* de inteligencia que pondrán a disposición del servicio, debiendo incluir como mínimo los siguientes:
    - *Feed* de inteligencia con clasificación sobre la reputación de IPs y URLs/dominios.
    - Debe soportar la integración de IOC's mediante distintos protocolos de intercambio de fuentes de eventos y de inteligencia soportados: API REST, SNMP, SYSLOG, XML, JSON, MISP, STIX/TAXII, …
    - La propuesta deberá indicar si la integración de estas herramientas de Threat Intelligence con la herramienta son nativas o hace falta algún tipo de desarrollo vía API.
- Debe contar, preferiblemente, con capacidades de inteligencia artificial, IA, que faciliten la labor de los analistas.
- Se debe indicar si proporciona un espacio seguro para la investigación de incidentes de ciberseguridad.
- Los *playbooks* se deben ejecutar de forma separada y no compartir recursos computacionales.
- Debe integrarse con el SIEM y el resto de las soluciones propuestas en este pliego, además de las herramientas y componentes de seguridad que no están definidos aquí, pero que son susceptibles de automatización con el fin de llevar a cabo tanto acciones preventivas como correctivas en los equipos de seguridad de Madrid Digital (cortafuegos, soluciones AntiDDoS, sistemas antimalware corporativo EDR para endpoint, sistemas antispam/antimalware de correo, sistemas de directorio, etc.).
- Debe permitir la integración con las soluciones ya existentes de *ticketing* de Madrid Digital (ITSM- FARO) y del Centro Criptológico Nacional CCN-CERT (herramienta LUCIA) vía API, así como el envío de correos electrónicos.
- Debe garantizar un modelo de datos robusto, permitiendo almacenar o cachear información en vuelo para una recuperación más rápida.

Los licitadores deberán recoger en su repuesta técnica cómo se realizará la interacción con elementos *on premise* y en nube (tanto en la misma nube en la que está desplegada la plataforma como con otras).

Tal y como se recoge en el apartado ***4.1.2.1.1 Plataforma de gestión de eventos e información de seguridad - SIEM***, en caso de optar por una solución independiente de la solución SIEM propuesta, todos los costes derivados de la solución SOAR y de las integraciones con el resto de componentes solicitados, deberán considerarse incluidos dentro del licenciamiento de la solución SIEM. Madrid Digital no asumirá ningún coste adicional derivado de este servicio.

4.1.3.3 Análisis forense

Enmarcado en las actividades de análisis y respuesta a incidentes, se requiere disponer de un servicio de análisis forense que permita investigar y analizar el contexto de un incidente, la causa raíz u origen del ataque, los medios utilizados y los objetivos, así como descartar comportamientos sospechosos en sistemas de información.

Este servicio desarrollará las siguientes tareas:

- Realizar análisis forense proporcional al riesgo detectado en los dispositivos de la organización afectados en un incidente o sospecha de un incidente, con el objeto de determinar el origen y causa del incidente, y ampliar los detalles del ataque, generando el correspondiente "Informe Forense".
- Se definirán dos tipos de análisis:
    - Peritaje informático: análisis en profundidad, orientado a la adquisición, conservación documentación, análisis y presentación, mediante metodologías estandarizadas de evidencias digitales con validez legal, relacionadas con un incidente o delito. El informe correspondiente deberá tener validez ante una autoridad judicial.
    - Análisis DFIR (Digital Forensic & Incident Response), más ligero, orientado a la respuesta rápida ante incidentes.
- Almacenamiento de la información forense durante la duración del contrato para poder realizar relaciones con posibles incidentes posteriores.
- Remisión de los IOC's encontrados por los canales establecidos.
- Elaboración de los procedimientos a seguir en los diferentes casos, para asegurar la preservación de evidencias, recolección correcta de datos y cadena de custodia, por tipo de análisis y dispositivo.

El servicio está compuesto por una bolsa de 960 horas y se prestará a demanda de Madrid Digital, estando el adjudicatario obligado a desplazar los recursos técnicos necesarios en cualquier centro de la Comunidad de Madrid donde se haya producido el incidente.

4.1.3.4 Servicios de apoyo a la gestión de cibercrisis

Este servicio facilitará, a demanda, capacidades avanzadas de apoyo para la gestión de *cibercrisis*, entendiendo como tal la gestión unificada de una situación de crisis o emergencia, cuyo cometido sea acelerar el proceso de toma de decisiones para la resolución de cualquier incidencia o vulnerabilidad de seguridad que deba ser tratada con máxima prioridad, en base a su peligrosidad potencial, impacto para el negocio, o compromiso grave de las operaciones de Madrid Digital y de la seguridad de sus activos.

Este servicio, por su naturaleza, deberá ser atendido por el adjudicatario de forma prioritaria hasta la resolución de la crisis.

Las tareas mínimas que podrán solicitarse al amparo de este servicio son las siguientes:

- Apoyo en la evaluación de incidentes de seguridad graves, identificación de la causa raíz y análisis de contexto, alcance, activos afectados e impacto para el negocio.

- Apoyo en la definición de medidas de contención y eliminación a aplicar.
- Apoyo en la definición y desarrollo de las medidas de recuperación del servicio a aplicar, si procede.
- Soporte a la designación de interlocutores, canales de comunicación y sistemas de compartición de conocimiento e información durante la crisis.
- Soporte a las actividades de comunicación corporativa de información del incidente, interna y externa.
- Elaboración del informe final de *cibercrisis*.

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

El servicio está compuesto por una bolsa de 960 horas que se prestará a demanda de Madrid Digital, estando el adjudicatario obligado a desplazar los recursos técnicos necesarios en cualquier centro de la Comunidad de Madrid donde se haya producido el incidente.

Los perfiles profesionales del equipo asignado para la realización de estas actividades se encontrarán dentro de los recogidos para el servicio en el apartado ***4.2.3 Equipo de trabajo.***

4.1.4 Servicios de soporte a la gestión, operación y procesos

Los servicios de ciberseguridad demandados requieren la definición de procesos y procedimientos operativos y de gobierno de dichos servicios. Madrid Digital dispone a tal fin de un cuerpo normativo de seguridad, que el adjudicatario deberá conocer, aplicar y colaborar en su mejora durante toda la ejecución del contrato.

Los servicios de ciberseguridad definidos requieren también disponer de plataformas tecnológicas y herramientas de soporte que se integren con las herramientas corporativas y de seguridad ya instaladas en Madrid Digital. Será función de este servicio la definición de la mejor arquitectura de la solución, a recoger en su oferta técnica, y evaluar y ejecutar las integraciones necesarias con los sistemas de información de Madrid Digital y de las plataformas que se desplieguen para el servicio.

El adjudicatario deberá suministrar, instalar y operar todas las plataformas descritas en apartados previos (escáner de vulnerabilidades, SIEM, SOAR, NDR, etc.) y las descritas en los siguientes apartados de este epígrafe. Serán funciones de este servicio coordinar su puesta en marcha, así como su mantenimiento, operación y gestión posterior durante todo el contrato, realizando la necesaria coordinación interna con los fabricantes y desarrolladores correspondientes.

Los licitadores deberán contemplar como proyectos “llave en mano” la puesta en marcha de estas plataformas o herramientas, debiendo considerar prorrateados en el coste de cada uno de los servicios todos los costes de adquisición de hardware, software, suscripciones, soporte, instalación o administración.

Madrid Digital se reserva el derecho, a la finalización del contrato, de asumir la titularidad de esos servicios. Para ello, los licitadores deberán indicar, claramente, la estructura de costes de mantenimiento de cada plataforma y herramienta.

Además, el adjudicatario realizará a través de este servicio las siguientes actividades:

- la identificación e integración de nuevas fuentes de eventos de seguridad en el SIEM.
- el modelado de amenazas.
- el desarrollo y evolución de nuevos casos de uso de monitorización y *hunting*, mapeados con las técnicas y tácticas de la matriz de MITRE AT&CK.
- la centralización, automatización y orquestado de respuesta a las alertas generadas por los distintos sistemas.
- Soporte experto al resto de componentes del SOC-MD de las tecnologías implantadas para el servicio.
- Soporte experto para el análisis e incorporación de nuevas capacidades de ciberseguridad.

A continuación, se describen las plataformas y herramientas consideradas de soporte a la operación que el adjudicatario deberá crear, o mantener, si Madrid Digital ya dispusiera de ellas.

Todos los costes derivados de este servicio, a excepción de los relativos al personal descrito en el apartado ***4.2.3 Equipo de trabajo***, deberán considerarse prorrateados en el resto de servicios. Madrid Digital no asumirá ningún coste adicional por su ejecución.

4.1.4.1 CMDB

Madrid Digital considera imprescindible disponer de información precisa del estado de seguridad de cada uno de los activos gestionados, necesaria para el análisis de riesgos y de impacto que la materialización de incidentes de seguridad o la explotación de amenazas puedan provocar en los servicios.

A tal fin, los licitadores deberán construir una base de datos de activos, en donde recogerán:

- Datos identificativos del activo: IP pública o privada, nombre DNS, tipo de activo (servidor web, servidor de aplicaciones, servidor de BBDD, cortafuegos, etc.), sistema operativo (Windows, Linux, etc.), nivel de exposición (Intranet, Internet), etc.
- Aplicaciones y sistemas de información a los que pertenece el activo.
- Nivel de seguridad de la aplicación/sistema de información: servicio esencial, criticidad para el negocio (oro, plata, bronce).
- Relación de vulnerabilidades identificadas para cada activo y grado de explotabilidad.

Esta base de datos será la fuente de información posterior para el reporte de la postura de seguridad y priorización de las actividades de mitigación. Será responsabilidad de los servicios de vulnerabilidades el mantenimiento actualizado de la información de activos y vulnerabilidades asociadas, tras cada análisis realizado.

4.1.4.2 Plataforma MISP

Madrid Digital dispone de una plataforma MISP (Malware Information Sharing Platform), de código abierto para el intercambio de información de inteligencia contra amenazas.

Esta plataforma es el punto central de consolidación de indicadores de compromiso, ya sean notificados por terceros (por ejemplo, CCN-CERT o proveedores de servicios de ciberseguridad) o generados por Madrid Digital en los procesos de análisis de incidentes, con dos objetivos:

- Compartición de información con terceros. Madrid Digital es miembro de la Red Nacional de SOC.
- Compartición de la información con áreas operativas internas de Madrid Digital, para mejora de las actividades preventivas y de detección correspondientes.

Será responsabilidad del adjudicatario garantizar la plena operatividad de esta plataforma, el mantenimiento operativo de esta plataforma, así como de su evolución, durante la vigencia del contrato. Se exigirá la consolidación de toda la información de inteligencia de amenazas puesta a disposición del contrato en esta plataforma.

4.1.4.3 Portal de ciberseguridad y cuadros de mando

Los licitadores facilitarán un Portal Web de acceso a todas las plataformas y herramientas requeridas, información de interés sobre los servicios contratados, informes de actividad, cuadros de mando, sistemas de gestión de peticiones, etc. Este portal facilitará un reporte integrado de todos los servicios puestos a disposición del contrato.

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 Ciberseguridad, 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.

Igualmente, los licitadores facilitaran una propuesta de cuadros de mando para seguimiento de:

- KPI’s de actividad de cada uno de los servicios e indicadores más significativos.
- ANS’s contractuales.

La propuesta deberá realizarse en PowerBI, herramienta corporativa de Madrid Digital para la elaboración de cuadros de mando.

4.1.4.4 Herramientas auxiliares de soporte a la gestión

Los licitadores deberán operar y mantener las herramientas enumeradas a continuación que redunden en una mejora del servicio soporte a la gestión, operación y procesos.

- La infraestructura técnica soporte de las herramientas open source facilitadas por el CCN-CERT a las administraciones públicas, desplegadas actualmente en Madrid Digital. Estas herramientas son las siguientes:
  - LUCIA: Plataforma para la gestión y notificación de ciberincidentes.
  - REYES: Plataforma para intercambio de información de amenazas.

Madrid Digital se reserva el derecho de incorporar a lo largo de la ejecución del contrato nuevas capacidades y herramientas facilitadas por el CCN-CERT. El adjudicatario del contrato asistirá a Madrid Digital en la evaluación de la herramienta e instalación si procede.

- Un entorno controlado y seguro de pruebas, denominado *sandbox*, que permita a los investigadores y analistas de ciberseguridad el análisis y ejecución de posible código malicioso. La solución de *sandbox*, entre otros, permitirá:
    - **Plataformado de equipos:** el *sandbox* permitirá la creación de maquetas de equipos de Madrid Digital de idénticas características técnicas que los de producción con el fin de poder realizar análisis mejor orientados a la situación real en la que se encuentran dichos equipos.
    - **Análisis forense:** Después de una ciberincidencia, los expertos en ciberseguridad podrán utilizar el *sandbox* para comprender la profundidad y el impacto del ataque con el fin de informar sobre la respuesta a las incidencias y la recuperación.
    - **Compatibilidad de aplicaciones:** Podrá utilizarse este entorno como plataforma de pruebas de rendimiento de aplicaciones, garantizando que no haya problemas de compatibilidad.
    - **Cumplimiento de normativas y políticas:** Con el fin de cumplir con las normativas sobre la seguridad, la integridad y el acceso a los datos, el entorno de pruebas ayudará a validar y garantizar que el software y los procesos cumplen dichas normativas sin arriesgarse a que se produzcan filtraciones de datos.
    - **Aprendizaje y experimentación:** El entorno podrá ser utilizado como parte del proceso de formación en ciberseguridad recogido en el apartado ***4.1.5 Servicios de capacitación y formación en ciberseguridad***.

4.1.4.5 Sala del SOC-MD

Los licitadores deberán habilitar un espacio en las dependencias de su centro de operaciones de ciberseguridad, dedicado a las actividades de monitorización, detección análisis y respuesta de este contrato.

Este espacio será visitable por personal de la Comunidad de Madrid, autoridades y responsables de ciberseguridad, como punto emblemático y representativo del servicio.

Este espacio estará dotado como mínimo de:

- Pantallas de visualización de los principales indicadores del servicio, como pueden ser alertas e incidentes activos, fuentes de eventos monitorizados, plataformas gestionadas, etc.
- Elementos tipográficos corporativos del servicio (SOC-MD), de Madrid Digital y de la Comunidad de Madrid (logos, banderas, etc.).
- Los elementos de comunicaciones y equipamientos informáticos necesarios para desarrollar las actividades indicadas de forma presencial por el equipo del trabajo adscrito al contrato (total o parcialmente).

Madrid Digital informará puntualmente y con la antelación acordada con el adjudicatario al inicio del contrato, de las visitas programadas a este espacio.

4.1.5 Servicios de capacitación y formación en ciberseguridad

Los licitadores deberán incluir en su respuesta técnica una propuesta de Plan de Formación continua, sin coste orientado a la capacitación del personal técnico de Madrid Digital. Este plan de formación deberá contemplar, como mínimo, las siguientes áreas:

- Formación en todos los servicios y herramientas propuestos para este pliego: sistema SIEM, NDR, escáner de vulnerabilidades, plataforma de orquestación SOAR, etc.
- Generación y puesta a disposición del personal de Madrid Digital de contenidos formativos de carácter general, en forma de píldoras, cursos on-line o videos divulgativos que, como consecuencia de la ejecución de los ciberejercicios previstos, se considere necesario como refuerzo a conceptos y conocimientos.

Los licitadores deberán facilitar, para cada propuesta formativa, los siguientes datos mínimos:

- Contenido de la propuesta formativa.
- Número de asistentes.
- Número de sesiones formativas.
- Duración de cada sesión formativa.
- Coste (a título informativo) de cada sesión.

4.1.6 Servicios de asesoría y asistencia legal

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

- La recuperación de información o contenidos, 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 perfiles profesionales exigidos para este servicio se recogen en el apartado ***4.2.3 Equipo de trabajo.***

El servicio está compuesto por una bolsa de 960 horas que se prestará a demanda de Madrid Digital.

4.2 MODELO OPERATIVO Y DE ORGANIZACIÓN

4.2.1 Procesos para la gestión del servicio

El Centro de Operaciones de Ciberseguridad deberá relacionarse con otras unidades de Madrid Digital, empresas externas, organismos públicos, reguladores, etc., por lo que es imprescindible que la definición de cada servicio/capacidad se realice teniendo en cuenta las personas, los procesos y las tecnologías que lo van a sustentar.

Así, la definición de cada uno de los servicios objeto de contratación, deberá contemplar los procesos y procedimientos asociados, los responsables, las actividades y los resultados esperados. Como mínimo, se revisarán y establecerán procesos específicos para la provisión de servicios, la operación (incidencias, peticiones y consultas), el soporte (gestión de configuraciones, gestión de cambios, gestión de capacidad), y la medición de los principales KPI y ANS asociados.

Madrid Digital facilitará al inicio del contrato la relación de procesos y procedimientos definidos hasta el momento, para su revisión, adaptación y completitud por parte del adjudicatario durante la ejecución del contrato.

4.2.2 Modelo organizativo del SOC-MD

El modelo organizativo del SOC-MD recoge como deben organizarse los recursos para prestar los servicios objeto del contrato 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-MD en cuatro áreas de actividad, que se corresponden con los servicios definidos. Cada una de estas áreas contará con el equipo de trabajo que se 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 del SOC de Madrid Digital.

Estas cuatro áreas de actividad son las siguientes:

- Área de soporte a la gestión, operación y procesos del SOC-MD.
- Área de prevención.
- Área de monitorización y detección.
- Área de análisis y respuesta.

Cada una de las áreas de actividad contará con los perfiles y equipos técnicos, desarrollados en detalle en el próximo apartado.

4.2.3 Equipo de trabajo

El adjudicatario estará obligado a observar las condiciones generales del equipo de trabajo que pondrá a disposición del contrato, recogidas en el apartado ***8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO.***

En la siguiente tabla se recoge la dimensión del equipo de trabajo mínimo requerido por Madrid Digital para el desarrollo de los servicios.

	Perfil - Función	Nº de personas	% Dedicación	Horas estimadas
Cuota fija	**Jefe de Proyecto**	1	100	3.840 horas
	Arquitecto senior seguridad	2	100	7.680 horas
	Analista seguridad vulnerabilidades de sistemas y redes	1	100	3.680 horas
	Analista seguridad vulnerabilidades de aplicaciones	1	100	3.680 horas
	Analista seguridad búsqueda proactiva de amenazas	1	100	3.360 horas
	Analista seguridad análisis y respuesta a incidentes	2	100	7.680 horas
	Técnico seguridad detección de ciberincidentes	3	100	11.520 horas
	Técnico seguridad detección de ciberincidentes	1	100	10.368 horas **(*)**
Cuota variable	**Analista seguridad ciberejercicios**	1	-	1.920 horas
	Analista seguridad forense	1	-	960 horas
	Analista seguridad cibercrisis	1	-	960 horas
	Consultor legal	1	-	960 horas

(*) Estimación de horas para completar el horario de atención en 24x7.

Para el cálculo de horas estimadas se considera como 100% de dedicación al proyecto un esfuerzo de 160 horas mensuales, 24 meses de duración del contrato.

Todos los perfiles identificados con un 100% de dedicación están asociados a servicios continuos facturables en modalidad de cuota fija, es decir, a los servicios de análisis de vulnerabilidades de seguridad de sistemas y redes, análisis de vulnerabilidades de seguridad de aplicaciones, monitorización y detección, análisis y respuesta, y soporte a la gestión, operación y procesos.

Los perfiles en los que no se detalla un porcentaje de dedicación están asociados a servicios a demanda, facturables en concepto cuota variable. Estos servicios son los relativos a Ciberejercicios, análisis forense, gestión de cibercrisis y asesoría y asistencia legal.

A continuación, se recogen los perfiles profesionales, funciones y requisitos de titulación, formación y experiencia, de cada uno de los recursos que conformarán el equipo de trabajo.

JEFE DE SERVICIO – PROYECTO	**1 Persona**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Responsable del diseño, implantación y operación diaria de los servicios y equipo de trabajo del SOC-MD.
- Coordinación del todo el proyecto y responsable, en último término, de la buena marcha de los trabajos.
- Interlocutor principal para el responsable del SOC de Madrid Digital.
- Ejercer el mando y la responsabilidad sobre el equipo completo del SOC-MD.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Asegurar la ejecución de las operaciones diarias del SOC-MD según los ANS establecidos.
- Asegurar que todo el personal del SOC-MD 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.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), y formación en gestión de proyectos y/o gestión de servicios TI con certificaciones en ITIL, CoBIT, PRINCE2, PMP o equivalentes.

EXPERIENCIA PROFESIONAL:

- Más de cinco (5) años de experiencia como responsable o gerente de servicios de SOC, o bien como jefe de proyecto de operaciones de seguridad TIC.

ARQUITECTO SENIOR DE SEGURIDAD – ÁREA DE SOPORTE A LA OPERACIÓN	**2 Personas**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Arquitectos especialistas funcionales y técnicos en la implantación de servicios de SOC, y por consiguiente en su diseño, despliegue de herramientas, procesos y tecnologías.
- Diseñar y coordinar la implantación de la plataforma centralizada de gestión de eventos e información de seguridad (SIEM), asegurando la integración de las fuentes de datos de eventos actuales y futuras necesarias.

- Diseñar y coordinar la implantación de la plataforma SOAR ofertada.
- Automatizar la carga de logs, eventos y el modelado de amenazas, en el SIEM.
- Coordinar y/o definir y probar los casos de uso de monitorización, el modelado de comportamientos anómalos, probables incidentes, para su implantación en el SOC.
- Diseñar y coordinar la implantación de la solución NDR ofertada.
- Definir y divulgar los procesos y procedimientos de operación del SOC.
- Diseñar y mantener las herramientas de gestión y operación del SOC: CMDB, MISP, portal, cuadros de mando, herramientas CCN-CERT, etc.
- Coordinar las actividades de operación y mantenimiento de todas las herramientas con las áreas internas implicadas del adjudicatario y con los fabricantes de hardware/software implicados.
- 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.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CCSP – Certified Cloud Security Professional, CEH (Certified Ethical Hacker), CISM (Certified Information Security Manage), OSCP (Offensive Security Certified Professional) , CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate).
- Formación específica en diseño y operación de las soluciones de SIEM y NDR propuestas para el servicio.

EXPERIENCIA PROFESIONAL:

- Más de cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño y operación de sistemas SIEM, sistemas de detección y respuesta de red (NDR), sondas de análisis IDS/IPS, arquitectura de sistemas de seguridad perimetrales, cortafuegos de nivel 4 y nivel 7, proxys de control de acceso a Internet, etc.

ANALISTA DE SEGURIDAD - ÁREA DE PREVENCIÓN	**2 Personas**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Especialistas en la realización de análisis de vulnerabilidades de redes, sistemas y aplicaciones, en sus distintas modalidades: descubrimiento y escaneo de redes y activos internos, auditorías técnicas, test de intrusión, postura de seguridad en nube, etc.
- Análisis de la superficie de exposición y explotación de las vulnerabilidades encontradas.

TITULACIÓN Y FORMACIÓN:

- T Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OSCP (Offensive

Security Certified Professional), ECSA – EC Council Certified Security Analyst), LPT (Licensed Penetration Tester), CompTIA Pentest+, eJPT (eLearning Junio Penetration Tester), eCPPT (eLearnSecurity Certified Professional Penetration Tester), o certificaciones de fabricantes de escáneres de vulnerabilidades como Rapid7, Nessus o Qualys y específicamente sobre la solución de escáner propuesta para el servicio.

- 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 siete (7) años.

EXPERIENCIA PROFESIONAL:

- Más de cinco (5) años de experiencia como analista de seguridad, con experiencia demostrable en técnicas y herramientas de escaneos de vulnerabilidades en sistemas, aplicaciones, hosts y equipos de red, ejecución de test de intrusión sobre aplicaciones y sistemas, y auditorías técnicas de infraestructuras.

TÉCNICO DE SEGURIDAD - ÁREA DE MONITORIZACIÓN Y DETECCIÓN	4 Personas
Dedicación al proyecto:	100 %

FUNCIONES:

- Especialistas en la monitorización de eventos de seguridad y detección de incidentes de seguridad.
- Identificar, registrar, categorizar, priorizar e investigar eventos de seguridad generados de los distintos elementos: SIEM, NDR, sondas IDS, etc.
- Operar el sistema NDR.
- Controlar las colas de eventos entrantes del sistema SOAR/SIEM para asegurar el procedimiento de detección.
- Realizar la investigación inicial y la pre-clasificación de posibles incidentes, y escalar o cerrar eventos según corresponda (falsos positivos).
- Documentar los resultados de la investigación, para su análisis por parte del equipo de respuesta a incidentes.
- Consolidar la información de inteligencia de amenazas facilitada por el servicio de vigilancia digital, para información de contexto de la actividad.
- Gestionar los incidentes de seguridad de peligrosidad estimada BAJA y MEDIA, de los que se disponga de procedimiento de respuesta establecido al efecto.
- Escalar incidentes de peligrosidad estimada ALTA, MUY ALTA o CRÍTICO, al servicio de análisis y respuesta a incidentes.
- Actualizar las herramientas de actividad del SOC según sea necesario.
- Generar indicadores de compromiso (IOC's) asociados a las detecciones y consolidarlos en la MISP de Madrid Digital.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima de Técnico Superior en Administración de Sistemas Informáticos en red, o cualquier otra titulación de formación profesional de grado superior relacionada.
- Estar en disposición de alguna de las siguientes certificaciones de fabricantes de soluciones de seguridad: Cisco, PaloAlto, HP Fortify, Forcepoint, IBM, etc.

EXPERIENCIA PROFESIONAL

- Más de dos (2) años de experiencia demostrable en operación y mantenimiento de sistemas SIEM, análisis de logs de seguridad y tratamiento de eventos, o bien experiencia en labores de operación de cortafuegos, proxys de acceso a Internet, sistemas IPS, sistemas NDR, sistemas SOAR, o sistemas antimalware EDR.

ANALISTA DE SEGURIDAD/THREAT HUNTER - ÁREA DE MONITORIZACIÓN Y DETECCIÓN	**1 Persona**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Especialistas en la identificación de amenazas persistentes avanzadas.
- Identificar e investigar de forma proactiva las posibles amenazas de seguridad dentro de la red de Madrid Digital.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: eCTHP (eLearnSecurity Threat Hunting Professional), CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), ECSA (EC Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator), ECIH (Certified Incident Handler), CompTIA Security+ o conocimientos demostrables en herramientas de ingeniería inversa, tecnologías de sandboxing, vectores de ataque y herramientas tácticas ofensivas más comunes.
- 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 siete (7) años.

EXPERIENCIA PROFESIONAL:

- Más de dos (2) años de experiencia como analista de seguridad en tareas de Threat Hunting para grandes organizaciones, con experiencia demostrable en productos de seguridad como sistemas IDS/IPS/NDR, cortafuegos, SIEM/SOAR, DLP, WAF, etc.

ANALISTA DE SEGURIDAD – ÁREA DE ANÁLISIS Y RESPUESTA	**2 Personas**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Analistas de seguridad expertos en el análisis y gestión de incidentes de seguridad, determinación de impacto y ejecución del plan de acción.
- Análisis en profundidad y confirmación de incidentes de seguridad escalados del servicio de detección, completando los datos con información de contexto, inteligencia de amenazas o vulnerabilidades de seguridad asociadas.
- Determinación de peligrosidad e impacto de los incidentes, identificando activos afectados, valor para el negocio y nivel de compromiso.
- Proponer el plan de mitigación del incidente.
- Ejecutar los procedimientos de tratamiento de los incidentes elaborados al efecto.

- Automatizar procesos en la plataforma SOAR.
- Documentar todos los incidentes y elaborar el informe final de actividades realizadas.
- Proponer y coordinar todas las acciones de tratamiento de los incidentes con las áreas técnicas internas de Madrid Digital.
- En caso de gestión de incidentes críticos, colaborar con el Comité de Crisis de Madrid Digital en todo aquello que le requiera para la gestión de la crisis.
- Comunicar los incidentes a los CERT de referencia de Madrid Digital.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), CHFI (Computer Hacking Forensic Investigator), ECSA (EC Council Certified Security Analyst), ECIH (Certified Incident Handler), CompTIA Security+.
- 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 siete (7) años.

EXPERIENCIA PROFESIONAL:

- Más de dos (2) años de experiencia como analista de seguridad en tareas de análisis y gestión de incidentes de seguridad en grandes organizaciones.

ANALISTA DE SEGURIDAD – ÁREA DE PREVENCIÓN/CIBEREJERCICIOS	**-**
Dedicación al proyecto:	**A demanda**

FUNCIONES:

- Analistas de seguridad expertos en la ejecución y seguimiento de ciberejercicios orientados al entrenamiento de capacidades de seguridad.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), CHFI (Computer Hacking Forensic Investigator), ECSA (EC Council Certified Security Analyst), ECIH (Certified Incident Handler), CompTIA Security+.
- 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 siete (7) años.

EXPERIENCIA PROFESIONAL:

Más de dos (2) años de experiencia como analista de seguridad en la ejecución de ejercicios Table-top, y simulaciones de phishing en grandes organizaciones.

ANALISTA DE SEGURIDAD: ÁREA DE ANÁLISIS Y RESPUESTA	-
Dedicación al proyecto:	**A demanda**

FUNCIONES:

- Analistas de seguridad expertos en la gestión de incidentes críticos de seguridad/gestión de crisis.
- Apoyo en la ejecución de todas las actividades derivadas del tratamiento de la crisis: evaluación del ciberincidente, identificación de actores, coordinación y seguimiento de actividades, y, en general, cualquier actividad relacionada.
- Elaboración de informes a demanda del Comité de Crisis de Madrid Digital.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), CHFI (Computer Hacking Forensic Investigator), ECSA (EC Council Certified Security Analyst), ECIH (Certified Incident Handler), CompTIA Security+.
- 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 siete (7) años.

EXPERIENCIA PROFESIONAL:

Más de dos (2) años de experiencia como analista de seguridad en tareas de análisis y gestión de incidentes de seguridad en grandes organizaciones.

ANALISTA DE SEGURIDAD/FORENSE - ÁREA DE ANÁLISIS Y RESPUESTA	-
Dedicación al proyecto:	**A demanda**

FUNCIONES:

- Analistas de seguridad expertos en el análisis forense de incidentes de seguridad.
- Ejecución de análisis forense en sus distintas modalidades.
- Elaboración de informe forense asociado.
- Elaboración de indicadores de compromiso asociados.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), ECSA (EC Council Certified Security Analyst), CHFI (Computer

Hacking Forensic Investigator), ECIH (Certified Incident Handler), CompTIA Security+ o conocimientos demostrables en herramientas de ingeniería inversa, tecnologías de sandboxing, vectores de ataque y herramientas tácticas ofensivas más comunes. • 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 siete (7) años. **EXPERIENCIA PROFESIONAL:** • Más de dos (2) años de experiencia como analista de seguridad en tareas de análisis forense de incidentes de seguridad en grandes organizaciones.	
CONSULTOR LEGAL **Dedicación al proyecto**	**-** **A demanda**
FUNCIONES: • Asesor legal, especialista en derecho de las tecnologías de la información y de las comunicaciones y seguridad de la información. **TITULACIÓN Y FORMACIÓN:** • Titulación Universitaria de Grado en Derecho, Licenciado en Derecho, o equivalente. • Postgrado relacionado con derecho de Internet, derecho de las TIC, etc. **EXPERIENCIA PROFESIONAL:** • Más de cinco (5) años de experiencia en asesoría legal a empresas y administraciones públicas en relación a la legislación vigente en materia de seguridad de la información, aplicada a la protección de información, sistemas, redes e infraestructuras tecnológicas.	

4.2.4 Horario y lugar de prestación de los servicios

Los servicios objeto del presente pliego siguen el calendario laborable de Madrid Digital. El horario de este servicio será el comprendido dentro de la franja horaria de **lunes a viernes de 9:00 h a 18:00 h, los días laborables.**

Será excepción a este criterio aquellos servicios definidos específicamente en modalidad 24x7x365 (monitorización y detección, análisis y respuesta) o con horario extendido (detección).

Madrid Digital requiere el desempeño de estos servicios de forma prioritaria desde las instalaciones del proveedor o en modalidad tele-trabajo. En todo caso, en función de diferentes factores, como, por ejemplo, atención a reuniones que requieran trato directo, de cualquiera de los comités indicados en este contrato o bien, de cualquier otra reunión específica con personal de la Agencia, el lugar de la prestación de los servicios podría fijarse a criterio de Madrid Digital en las instalaciones de Madrid Digital y/o alguna de las dependencias de la Comunidad de Madrid. Este cambio del lugar de la prestación de los servicios deberá notificarse al menos con 24 horas de antelación.

Madrid Digital se reserva la potestad de solicitar al adjudicatario la prestación del servicio total o parcialmente en modo presencial en sus dependencias de, al menos, los perfiles de *Jefe de Proyecto*, *Arquitecto SOC* y responsables nombrados de áreas de actividad (prevención, detección, análisis y respuesta).

El personal del SOC-MD tendrá disponibilidad para desplazarse puntualmente a los distintos centros dependientes de la Comunidad de Madrid para la ejecución de actividades relacionadas con los servicios objeto del contrato.

Las tareas, planificadas o no, relacionadas con el mantenimiento y la operación de las herramientas del SOC y/o con sus integraciones con fuentes de datos de eventos, o relacionadas con la gestión de incidentes de seguridad que requieran realizar trabajos por parte del personal prestador del servicio fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, no serán objeto de ningún coste o compensación adicional por parte de Madrid Digital. Estos costes deberán ser asumidos siempre por el contratista.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

4.2.5 Acuerdos de nivel de servicio – ANS

El adjudicatario se comprometerá a cumplir unos niveles de calidad mínimos sobre los servicios prestados y plataformas suministradas. Para ello, se establecen los niveles de servicio recogidos a continuación, así como la política de penalizaciones ante incumplimientos de estos ANS, que el adjudicatario estará obligado a aceptar.

Para la definición de los ANS asociados a los distintos servicios, se aplicarán los siguientes conceptos:

- **Amenaza de seguridad**: toda aquella información de interés obtenida a través de fuentes externas a la organización, que pueda afectar a la seguridad de la información de los sistemas, y que pueda ser utilizada para una mejor protección de los mismos.
- **Vulnerabilidad de seguridad**: debilidad que puede ser aprovechada por una amenaza.
- **Evento de seguridad o alerta de seguridad**: una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Ciberincidente o incidente de seguridad**: acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta. Se clasificarán en:
    - **Incidente grave**: incidente de seguridad clasificado con un nivel de peligrosidad estimada de ALTO, MUY ALTO o CRÍTICO, según la clasificación recogida en la guía *CCN-STIC-817 – Esquema Nacional de Seguridad. Gestión de ciberincidentes.*
    - **Incidente normal**: incidente de seguridad clasificado con un nivel de peligrosidad estimada de BAJO o MEDIO, según la clasificación recogida en la guía *CCN-STIC-817 – Esquema Nacional de Seguridad. Gestión de ciberincidentes.*
- **Incidencia**: cualquier interrupción o degradación del servicio, ya sean de hardware, software, comunicaciones etc., que provoquen una pérdida parcial o total del mismo. Se clasificarán en:
    - **Incidencia grave**: incidencia que provoca una pérdida total del servicio.

- **Incidencia normal**: incidencia que provoca una degradación del servicio.

- **Tiempo de Respuesta**: tiempo transcurrido **desde la notificación fehaciente de una incidencia** o **evento de seguridad**, ya sea por Madrid Digital, por el equipo del SOC-MD (reactivo), o por el equipo de mantenimiento del adjudicatario (proactivo), hasta su aceptación y análisis por parte del adjudicatario.
- **Tiempo de Escalado**: tiempo transcurrido **desde el análisis del evento o incidente de seguridad hasta su escalado** al grupo de tratamiento correspondiente, ya sea el equipo de análisis y respuesta a incidentes del SOC-MD, ya sean equipos técnicos internos de Madrid Digital.
- **Tiempo de Resolución**: tiempo transcurrido **desde la aceptación de la incidencia hasta su resolución** por parte del adjudicatario.
- **Tiempo de Cierre**: tiempo transcurrido **desde que los equipos técnicos de Madrid Digital notifican al SOC-MD la resolución de un incidente, hasta que se produce su cierre**. Este cierre incluirá todas las acciones pertinentes a realizar en los sistemas de notificación y gestión de Madrid Digital y terceros (CCN-CERT, CNPIC, etc.).
- **Tiempo de entrega de informe de resolución**: **tiempo transcurrido desde que se resuelve la incidencia o el incidente de seguridad hasta que se entrega un informe completo de resolución** detallando causas del problema, acciones llevadas a cabo para su resolución, medidas preventivas adoptadas, conclusiones y acciones de mejora.

Los tiempos de respuesta, resolución y entrega de informes se contabilizarán en horario 24x7, alineado con el horario de prestación del servicio.

Para el cálculo de los ANS asociados a la disponibilidad de los servicios, entendiendo éstos como interrupciones o degradaciones en el acceso a las consolas de gestión, o en su operatividad básica, se entenderá ésta como el porcentaje de tiempo mensual en que se encontrará operativa cada plataforma, una vez en explotación.

El cálculo de la disponibilidad se obtendrá aplicando la siguiente fórmula:

$$D = \frac{Ttot - Tnodisp}{Ttot} * 100\ (\%)$$

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).

El adjudicatario deberá proporcionar los servicios de monitorización y gestión que permitan comprobar todos los ANS exigidos.

A continuación, se recogen los ANS aplicables a cada uno de los servicios demandados:

Servicio	Requisito	ID.	Nivel de servicio exigido
Identificación de amenazas y vigilancia digital	Implantación del servicio	ANS-1	T. Máximo= 30 días naturales
	Incorporación nuevo activo público al servicio	ANS-2	T. Máximo= 2 días naturales
Análisis de vulnerabilidades de seguridad de sistemas y redes	Implantación del servicio	ANS-3	T. Máximo= 30 días naturales
	Disponibilidad de la plataforma de escaneo de vulnerabilidades	ANS-4	Disponibilidad ≥ 99,5%
	Entrega de informes de resultados de análisis	ANS-5	T. Máximo= 7 días naturales
	Entrega informes mensuales de actividad	ANS-6	Antes del quinto día hábil de cada mes
Análisis de vulnerabilidades de seguridad de aplicaciones	Implantación del servicio	ANS-7	T. Máximo= 30 días naturales
	Entrega de informes de resultados de análisis	ANS-8	T. Máximo= 21 días naturales
	Entrega informes mensuales de actividad	ANS-9	Antes del quinto día hábil de cada mes
Ciberejercicios	Planificación de ciberejercicios	ANS-10	T. Máximo= 30 días naturales
Plataforma de gestión de eventos e información de seguridad - SIEM	Puesta en marcha de la plataforma SIEM	ANS-11	T. Máximo= 180 días naturales
	Entrega informe de solución desplegada	ANS-12	T. Máximo= 10 días naturales, desde la puesta en marcha.
	Disponibilidad de la plataforma SIEM	ANS-13	Disponibilidad ≥ 99,5%
	Incorporación de nuevas fuentes de eventos de seguridad	ANS-14	T. Máximo= 7 días naturales
	Incorporación de nuevo caso de uso de monitorización	ANS-15	T. Máximo= 2 días naturales
	Resolución de incidencias del servicio	ANS-16	T. Máximo Respuesta incidencia GRAVE= 30 minutos
		ANS-17	T. Máximo Respuesta incidencia NORMAL= 2 horas
		ANS-18	T. Máximo Resolución incidencia GRAVE= 4 horas
		ANS-19	T. Máximo Resolución incidencia NORMAL= 24 horas

Servicio	Requisito	ID.	Nivel de servicio exigido
		ANS-20	T. Máximo Informe incidencia= 24 horas
Servicio de monitorización avanzado de tráfico de red - NDR	Puesta en marcha de la plataforma NDR	ANS-21	T. Máximo= 180 días naturales
	Entrega informe de solución desplegada	ANS-22	T. Máximo= 10 días naturales, desde la puesta en marcha.
	Disponibilidad de la plataforma NDR	ANS-23	Disponibilidad ≥ 99,5%
	Resolución de incidencias del servicio	ANS-24	T. Máximo Respuesta incidencia GRAVE= 30 minutos
		ANS-25	T. Máximo Respuesta incidencia NORMAL= 2 horas
		ANS-26	T. Máximo Resolución incidencia GRAVE= 4 horas
		ANS-27	T. Máximo Resolución incidencia NORMAL= 24 horas
		ANS-28	T. Máximo Informe incidencia= 24 horas
Detección de ciberincidentes	Implantación del servicio	ANS-29	T. Máximo= 30 días naturales
	Gestión de eventos o alertas de seguridad	ANS-30	T. Máximo Respuesta evento= 1 hora
		ANS-31	T. Máximo Escalado evento= 30 minutos
	Entrega informes mensuales de actividad	ANS-32	Antes del quinto día hábil de cada mes
Búsqueda proactiva de amenazas - Threat Hunting	Implantación del servicio	ANS-33	T. Máximo= 90 días naturales
	Informe mensuales de actividad	ANS-34	Antes del día 5 de cada mes
Análisis y respuesta a incidentes de seguridad	Implantación del servicio	ANS-35	T. Máximo= 30 días naturales
	Incremento de caso de uso totales	ANS-36	10% por año
	Gestión de incidentes de seguridad	ANS-37	T. Máximo Respuesta incidente GRAVE= 30 minutos
		ANS-38	T. Máximo Escalado incidente GRAVE= 4 horas

Servicio	Requisito	ID.	Nivel de servicio exigido
		ANS-39	T. Máximo Respuesta incidente NORMAL= 2 horas
		ANS-40	T. Máximo Escalado incidente NORMAL= 24 horas
		ANS-41	T. Máximo Cierre incidente= 24 horas
		ANS-42	T. Máximo Informe incidente= 24 horas
	Entrega informes mensuales de actividad	ANS-43	Antes del quinto día hábil de cada mes
Automatización y orquestación	Puesta en marcha de la plataforma SOAR	ANS-44	T. Máximo= 180 días naturales
	Entrega informe de solución desplegada	ANS-45	T. Máximo= 10 días naturales, desde la puesta en marcha.
	Disponibilidad de la plataforma SOAR	ANS-46	Disponibilidad ≥ 99,5%
	Ratio SOAR: casos de uso automatizados/casos de uso totales	ANS-47	10% por año
	Resolución de incidencias del servicio	ANS-48	T. Máximo Respuesta incidencia GRAVE= 30 minutos
		ANS-49	T. Máximo Respuesta incidencia NORMAL= 2 horas
		ANS-50	T. Máximo Resolución incidencia GRAVE= 4 horas
		ANS-51	T. Máximo Resolución incidencia NORMAL= 24 horas
		ANS-52	T. Máximo Informe incidencia= 24 horas
Análisis forense	Peritaje informático	ANS-53	T. Máximo Informe = 21 días naturales desde solicitud
	Análisis DFIR	ANS-54	T. Máximo Informe= 7 días naturales
Gestión de cibercrisis	Tiempo de adscripción de perfiles	ANS-55	T. Máximo= 24 horas desde solicitud
Soporte a la operación	Puesta en marcha CMDB	ANS-56	T. Máximo= 90 días naturales
	Puesta en marcha portal de ciberseguridad y cuadros de mando	ANS-57	T. Máximo= 60 días naturales

Servicio	Requisito	ID.	Nivel de servicio exigido
	Actualización de datos para cuadros de mando	ANS-58	Antes del quinto día hábil de cada mes
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	ANS-59	T. Máximo Informe= 7 días naturales
	Nº Máximo de sustituciones permitidas por tipo de perfil	ANS-60	1 cambio anual

5. LOTE 2: SERVICIOS DE SUPERVISIÓN Y CONTROL DE LAS PROTECCIONES

Será objeto de este lote la creación de un servicio de Supervisión y Control de las Protecciones, en adelante SSCP-MD, que facilite un soporte especializado que permita realizar un seguimiento de las medidas de seguridad implementadas en los servicios TIC prestados por Madrid Digital a la Comunidad de Madrid.

El objetivo del servicio será, tomando como punto de partida las medidas de seguridad especificadas en el Anexo II del Esquema Nacional de Seguridad, realizar la elaboración de los controles automáticos que permitan revisar, verificar y comparar la evolución del nivel de aplicación de las medidas de seguridad mencionadas, así como cualquier otra medida de seguridad que se consideren necesarias o fundamentales lo largo de la duración del contrato.

El entorno tecnológico de referencia sobre el que se desarrollarán las actividades de soporte se recoge en el apartado ***10.1 Entorno tecnológico.***

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

5.1 SERVICIOS REQUERIDOS

Las actividades a desempeñar, tanto en soluciones on-premise como soluciones de nube, con carácter general, para este servicio de supervisión y control de las protecciones son las siguientes:

- Desarrollo y aplicación de los controles automáticos asociados a las medidas de seguridad correspondientes, recogidas en las declaraciones de aplicabilidad existentes de los servicios que ofrece Madrid Digital, priorizando aquellas medidas asociadas a servicios declarados como esenciales.

  Los trabajos que se deberán realizar son:

  - Definición y documentación concreta, en función de las tecnologías implicadas en cada uno de los servicios, de las medidas de seguridad especificadas como obligatorias en la declaración de aplicabilidad del servicio correspondiente.
  - Desarrollo y despliegue de los controles que permitan supervisar la implantación de las medidas de seguridad necesarias, así como su evolución temporal.
  - Propuesta de herramientas a suministrar e instalar que permitan la automatización de la gestión de los controles.
  - Implementación de un cuadro de mandos dedicado que muestre el nivel de cumplimiento de las medidas de seguridad supervisadas por los controles.
  - Integración de la información de supervisión en el cuadro de mandos de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad, basado en tecnología Power BI.

- Mejora de la seguridad de las arquitecturas técnicas de Madrid Digital mediante el control y supervisión de las medidas de seguridad de los elementos que conforman los sistemas de información de Madrid Digital, incluidos los equipos de usuarios, considerando la legislación,

normativa de seguridad de Madrid Digital, buenas prácticas y referencias de arquitecturas seguras, como son las del CCN-CERT o del NIST (National Institute of Standards and Technology del Gobierno de EEUU), teniendo en cuenta la arquitectura técnica implantada. Básicamente deberán trabajar en la realización de:

  - Procedimientos e instrucciones técnicas de bastionado seguro de los componentes TIC presentes en cada arquitectura analizada.
  - Recomendaciones de soluciones y tecnologías adicionales que puedan complementar la seguridad del servicio, sistema y/o infraestructura tecnológica.
  - Revisiones de estado de seguridad y propuesta de mejoras.
  - La definición de nuevos controles, creación de scripts y herramientas que los implementen y que sean capaces de detectar y comprobar si las medidas de seguridad supervisadas por dichos controles están aplicadas.
  - Integración de resultados obtenidos en el cuadro de mandos del servicio y cuadro de mandos de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad, todo ello basado en tecnología Power BI.

- La creación de una base de datos de configuraciones de seguridad, que complemente los procesos de gestión de configuraciones existentes en Madrid Digital.
- Definición de los criterios para la normalización de nombres y definición de reglas y objetos en las políticas de los elementos de seguridad gestionados por Madrid Digital (cortafuegos, proxy, sistemas de redes definidas por software SDN, etc.), y elaboración de manuales de operación de elementos de seguridad, que recojan para cada elemento solicitado cómo:
  - Normalizar la definición (nombre y atributos) de los objetos en las políticas.
  - Normalizar los atributos, características y restricciones que deben cumplir las reglas.
- Servicio de revisión de reglas y objetos que componen las políticas de los elementos de filtrado.

  En el ciclo de vida de explotación de los dispositivos de filtrado, dentro de los procedimientos de gestión de sus reglas deben existir procesos de revisión periódica y optimización de las mismas. Estos procesos de revisión deberían de cubrir al menos los siguientes puntos:
  - Analizar las anomalías en las reglas que afectan al rendimiento.
  - Reordenar las reglas existentes para mejorar el rendimiento del servicio.
  - Identificar y eliminar las reglas no utilizadas o redundantes.
  - Detección de objetos duplicados o no utilizados.
  - Detección y eliminación de reglas potencialmente perjudiciales y peligrosas que puedan comprometer la seguridad y que no se ajusten a los indicado en el ENS
  - Definición del procedimiento de revisión de los elementos indicados, con calendario periódico e informe de resultados para cada interacción
  - Revisión del cumplimiento de los criterios de normalización definidos en el punto anterior.

El objetivo de esta actividad consiste en:

- La definición de los procesos de revisión, con su calendario periódico de aplicación e informe de resultados para cada interacción.
- Elaborar las guías asociadas a cada proceso que permitan aplicar de forma ordenada los puntos de control enumerados.
- Elaborar y desplegar los controles de supervisión de los mismos, permitiendo una revisión y control periódicos, a ser posible de forma automática, del nivel de cumplimiento.
- Implementación de un cuadro de mandos dedicado que muestre el nivel de cumplimiento normalización y de las medidas de revisión de las reglas.
- Integración de la información de supervisión en el cuadro de mandos de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad, basado en tecnología Power BI.

- Consultoría en materia de seguridad en las fases de definición de proyectos tecnológicos y de desarrollo en el ámbito de Madrid Digital.

Las actividades descritas se desarrollarán en dos entornos diferenciados: ciberseguridad perimetral y comunicaciones y ciberseguridad de los sistemas, requiriéndose perfiles profesionales especializados en cada uno de ellos.

Para la ejecución de estas actividades, el adjudicatario deberá considerar la provisión, diseño, operación y mantenimiento de todas las herramientas, equipos, plataformas y activos necesarios para el servicio SSCP-MD, tanto de gestión como de soporte a sus actividades. Preferentemente se optará por soluciones Open Source, 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 las herramientas pasarán a ser propiedad de Madrid Digital, así como el código fuente desarrollado a medida para la ejecución de las tareas relacionadas con el proyecto. El licitador detallará en su propuesta el hardware necesario para cada herramienta adquirida o utilizada en el proyecto y que será provisionado por Madrid Digital (salvo herramientas que solo funcionen en appliance dedicados).

5.2 MODELO OPERATIVO Y DE ORGANIZACIÓN

5.2.1 Equipo de trabajo

El adjudicatario estará obligado a observar las condiciones generales del equipo de trabajo que pondrá a disposición del contrato, recogidas en el apartado ***8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO.***

En la siguiente tabla se recoge la dimensión del equipo de trabajo mínimo requerido por Madrid Digital para el desarrollo de los servicios.

Perfil – Función	Nº de personas	% Dedicación	Horas estimadas
Ingeniero de Seguridad especialista en Comunicaciones	2	100	7.680 horas
Ingeniero de Seguridad especialista en Sistemas	2	100	7.680 horas
Ingeniero de Seguridad especialista en tecnologías emergentes	1	-	720 horas

Para el cálculo de horas estimadas se considera como 100% de dedicación al proyecto un esfuerzo de 160 horas mensuales, 24 meses de duración del contrato.

Todos los perfiles identificados con un 100% de dedicación están asociados a servicios continuos facturables en modalidad de cuota fija.

Los perfiles en los que no se detalla un porcentaje de dedicación están asociados a servicios a demanda, facturables en concepto cuota variable.

A continuación, se recogen el perfil profesional, funciones y requisitos de titulación, formación y experiencia, del equipo de trabajo que prestará los servicios exigidos.

INGENIERO DE SEGURIDAD PERIMETRAL Y DE LAS COMUNICACIONES	**2 Personas**
Dedicación al proyecto:	**100%**

FUNCIONES:

- Expertos en el despliegue de las medidas de seguridad especificadas en el ENS con experiencia en labores de supervisión, control e implantación de dichas medidas de seguridad desde el punto de vista de las de tecnologías de seguridad perimetral y de las comunicaciones de voz y datos.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: ISSP (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.
- 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 siete (7) años en los entornos requeridos para este perfil.

EXPERIENCIA PROFESIONAL:

- Más de 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).

INGENIERO DE SEGURIDAD DE SISTEMAS	2 Personas
Dedicación al proyecto:	100%

FUNCIONES:

- Expertos en el despliegue de las medidas de seguridad especificadas en el ENS con experiencia en labores de supervisión, control e implantación de dichas medidas de seguridad desde el punto de vista de sistemas operativos de servidor UNIX y Windows, bases de datos Oracle, SQL Server y MySQL.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) de la organización EC-Council, OCSP (Offensive Security Certified Professional) de Offensive Security, certificaciones de seguridad en sistemas operativos de servidor y bases de datos.
- 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 siete (7) años en los entornos requeridos para este perfil.

EXPERIENCIA PROFESIONAL:

- Más de cinco (5) años de experiencia como arquitecto de seguridad, con experiencia demostrable en diseño seguro de servidores y bases de datos.

INGENIERO DE SEGURIDAD EN TECNOLOGÍAS EMERGENTES	-
Dedicación al proyecto:	A demanda

FUNCIONES:

- Expertos en seguridad de tecnologías emergentes, 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.
- 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.
  - Elaboración de cuadros de mando: Power BI.
  - 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.
  - Arquitecturas de seguridad de comunicaciones en la nube (Azure, AWS, Google Cloud).
  - Arquitecturas de virtualización de comunicaciones: SDN, HCI, Vmware NSX etc.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones 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, OCSP (Offensive Security Certified Professional) de Offensive Security, y certificaciones de seguridad de Microsoft.
- 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 siete (7) años en los entornos requeridos para este perfil.

EXPERIENCIA PROFESIONAL:

- 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.

5.2.2 Horario y lugar de prestación de los servicios

Los servicios objeto del presente pliego siguen el calendario laborable de Madrid Digital. El horario de este servicio será el comprendido dentro de la franja horaria de **lunes a viernes de 9:00 h a 18:00 h, los días laborables.**

Madrid Digital requiere el desempeño de estos servicios de forma prioritaria desde las instalaciones del proveedor o en modalidad tele-trabajo. En todo caso, en función de diferentes factores, como, por ejemplo, atención a reuniones que requieran trato directo, de cualquiera de los comités indicados en este contrato o bien, de cualquier otra reunión específica con personal de la Agencia, el lugar de la prestación de los servicios podría fijarse a criterio de Madrid Digital en las instalaciones de Madrid Digital y/o alguna de las dependencias de la Comunidad de Madrid. Este cambio del lugar de la prestación de los servicios deberá notificarse al menos con 24 horas de antelación.

El personal del SSCP-MD tendrá disponibilidad para desplazarse puntualmente a los distintos centros dependientes de la Comunidad de Madrid para la ejecución de actividades relacionadas con los servicios objeto del contrato.

Las tareas, planificadas o no, relacionadas con el mantenimiento y la operación de las herramientas usadas en el contrato y/o con sus integraciones con los elementos de la arquitectura de Madrid Digital que requieran realizar trabajos por parte del personal prestador del servicio fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, no serán objeto de ningún coste o compensación adicional por parte de Madrid Digital.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

5.2.3 Acuerdos de nivel de servicio – ANS

El adjudicatario se comprometerá a cumplir unos niveles de calidad mínimos sobre los servicios prestados. Para ello, se establecen los niveles de servicio recogidos a continuación, así como la política de penalizaciones ante incumplimientos de estos ANS, que el adjudicatario estará obligado a aceptar.

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido.	T. Máximo = 7 días naturales
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual
Informes de seguimiento del servicio y actas de reuniones	Tiempo de entrega de informes mensuales y actas de seguimiento del servicio de la SSCP-MD	Quinto día hábil del mes siguiente a la fecha de la reunión de seguimiento mensual
Cuadro de mando	Tiempo de actualización del cuadro de mando cumplimiento de los controles	Quinto día hábil del mes siguiente

Los tiempos de entrega de informes se contabilizarán alineado con el horario de prestación del servicio

6. LOTE 3: SERVICIOS DE CIBERSEGURIDAD OFENSIVA

El objeto de este lote es la prestación de un servicio de ciberseguridad ofensiva basado en la ejecución de ciberataques controlados y dirigidos, simulando ser un atacante, (Red Team), para poner en prueba las capacidades del equipo de detección y respuesta de la organización (Blue Team).

A continuación, se describirán los principales aspectos del servicio a tener en cuenta por los licitadores en sus propuestas técnicas.

6.1 SERVICIOS REQUERIDOS

Este servicio facilitará a Madrid Digital capacidades específicas para la evaluación de su nivel de seguridad real frente a ataques externos, mediante la ejecución de ciberataques controlados cuyo principal objetivo será detectar el mayor número de brechas o debilidades de los sistemas gestionados por Madrid Digital, utilizando el mayor número posible de vectores de ataque.

Los ejercicios de Red Team deben simular ataques reales, empleando las tácticas y técnicas que los ciberatacantes aplican en escenarios reales, haciendo uso de todos los recursos posibles contra la organización, con el objeto de exfiltrar activos e información.

Estas actividades deben diferenciarse claramente de los análisis de vulnerabilidades de seguridad de aplicaciones, redes y sistemas (test de intrusión).

Cada uno de los ciberataques realizado por el equipo Red Team será informado exclusivamente al equipo que Madrid Digital defina al respecto, nunca al equipo de detección y respuesta, pudiendo realizarse en horario 24x7x365, si así se acuerda. Al principio de cada año el adjudicatario hará una recomendación de los ejercicios a realizar, para su aprobación por parte de Madrid Digital.

Cada ejercicio se finalizará con la presentación de un informe que detalle la información corporativa obtenida, el método utilizado para su obtención, y las sugerencias de mejora a facilitar en protecciones, procedimientos, etc., al equipo de detección y respuesta de Madrid Digital, con el objetivo de puesta en marcha de medidas de mejora de las defensas.

Los licitadores facilitarán en su propuesta de servicios la metodología aplicada para la realización de los ejercicios de Red Team. En cuanto a las técnicas, tácticas y procedimientos utilizados, se seguirán las recogidas en el framework MITRE ATT&CK. Los licitadores recogerán en su respuesta técnica la relación de tácticas y técnicas que utilizarán.

Las actividades a desarrollar serán las siguientes:

- Realización de ejercicios, sin conocimiento de la arquitectura, funcionalidad o activos soporte, consistentes en pruebas de penetración sobre los sistemas.
- Los ejercicios se realizarán sin conocimiento de los equipos de respuesta a incidentes de Madrid Digital. Únicamente serán conocedores de su ejecución los responsables del lote.

Los ejercicios contemplarán como mínimo ataques desde Internet, a través de acceso físico la red, a través de conexiones inalámbricas y simulando un atacante interno.

Los ejercicios se realizarán de acuerdo con las siguientes fases:

- **FASE 1 - Diseño del ejercicio**: con el asesoramiento del adjudicatario, se fijarán los parámetros globales del mismo: autorizaciones, comunicaciones, miembros de los distintos

equipos (White Team, Red, Team), alcance y duración, límites aceptables, objetivos específicos, tareas a realizar, etc. En la definición del ejercicio deberá asegurarse que no se pone en peligro el servicio analizado, ni se producen daños en las infraestructuras o aplicaciones.

El objetivo final de cada ejercicio será siempre detectar el mayor número posible de debilidades de seguridad y que efectivamente son explotables, por lo que cada ejercicio no finalizará cuando se consiga comprometer un sistema, sino que debe explotar, durante el plazo de ejecución acordado, si hay más formas de comprometerlo y, por tanto, más debilidades de seguridad explotables.

Con carácter obligatorio, Madrid Digital deberá autorizar previamente cada ejercicio.

- **FASE 2 - Ejecución del ejercicio**: el adjudicatario podrá utilizar todos los medios que estén a su alcance para analizar el mayor número de brechas de seguridad y explotarlas. Como mínimo deberá aplicar un 20% de las técnicas y tácticas recogidas en la matriz para empresas MITRE ATT&CK. Se realizarán reuniones de seguimiento para corregir los resultados y velar por la ejecución de la misión.

  El adjudicatario deberá asegurarse de que dispone de todas las autorizaciones previas necesarias antes de iniciar la ejecución del ejercicio.

- **FASE 3 - Análisis de resultados**: finalizado el plazo de ejecución del ejercicio de Red Team, el adjudicatario elaborará un informe que describa en detalle las vulnerabilidades y debilidades encontradas, las veces que ha conseguido comprometer los sistemas de Madrid Digital durante el ejercicio, así como las técnicas y tácticas que han utilizado para conseguirlo, cómo han sido aplicadas y el resultado obtenido en cada una de ellas. Se incluirá además un reporte de auditoría, que será entregado al servicio de auditorías de seguridad para su seguimiento.

- **FASE 4 – Recomendaciones de seguridad**: una vez identificadas las brechas de seguridad encontradas, el adjudicatario elaborará una relación de recomendaciones e indicaciones que permitan a Madrid Digital corregir estas debilidades.

- **FASE 5 – Elaboración de informe de auditoría**: el adjudicatario facilitará un informe completo con el detalle suficiente de todo el trabajo realizado. La estructura de este informe de auditoría deberá ser validada previamente con Madrid Digital.

- **FASE 6 – Revisión de auditoría**: una vez implementadas las medidas de corrección de los problemas detectados por parte de los equipos técnicos correspondientes de Madrid Digital, ésta podrá solicitar al adjudicatario la revisión de la efectividad de las mismas. El adjudicatario entregará en esta fase el correspondiente informe de revisión con los resultados obtenidos.

Los licitadores presentarán en su respuesta al pliego una propuesta inicial de ejercicios a realizar a lo largo del contrato, con estimación de esfuerzos (horas/hombre) de los perfiles recogidos en el apartado ***6.2.2 Equipo de trabajo.***

6.2 MODELO OPERATIVO Y DE ORGANIZACIÓN

6.2.1 Modelo de provisión del servicio

El servicio se prestará a demanda de Madrid Digital, mediante peticiones concretas de ejercicios de Red Team. Cada petición requerirá la valoración de esfuerzos en horas/hombre y perfiles, que deberá ser aprobada por Madrid Digital.

6.2.2 Equipo de trabajo

Las actividades de Red Team objeto de este lote se prestarán de forma completamente gestionadas por el adjudicatario, siendo éste responsable extremo a extremo de todo el servicio. Así, el adjudicatario será responsable de dimensionar adecuadamente el equipo de trabajo y cualificación correspondiente entre su personal técnico en función de la tipología de ejercicio a realizar.

En todo caso, el adjudicatario estará obligado a observar las condiciones generales del equipo de trabajo que pondrá a disposición del contrato, recogidas en el apartado ***8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO.***

El adjudicatario nombrará un Jefe de Proyecto/ Jefe de Equipo Red Team, como interlocutor principal entre Madrid Digital y el resto del equipo de trabajo, analistas de seguridad del contratista con perfiles diversos encargados de la ejecución de los análisis, que deberá estar localizable a lo largo de todo el contrato.

El Jefe de Proyecto será responsable de las siguientes funciones:

- Coordinación y seguimiento de las actividades de su equipo técnico.
- Coordinación e interlocución con los equipos de Madrid Digital (White Team, Blue Team).
- Gestión del servicio y seguimiento de los ANS.
- Elaboración del cuadro de mando, informes agregados que reflejen toda la actividad realizada.
- Elaboración de propuesta de ejercicios a realizar para su aprobación por parte de Madrid Digital.
- Seguimiento y supervisión de las peticiones de ejecución de ejercicios por parte de Madrid Digital.
- Elaboración de informes técnicos y ejecutivos solicitados por Madrid Digital.

Perfil – Equipo de Trabajo	N° de personas	N° Horas/mes	Horas estimadas (24 meses)
Jefe de Proyecto	1	40	960 horas
Analista de seguridad	2	80	3.840 horas

Todos los perfiles identificados están asociados a servicios a demanda facturables en modalidad de cuota variable.

A continuación, se recogen los perfiles profesionales, funciones y requisitos de titulación, formación y experiencia, de cada uno de los recursos que conformarán el equipo de trabajo.

JEFE DE SERVICIO – PROYECTO	**1 Persona**
Dedicación al proyecto:	**A demanda**

FUNCIONES:

- Coordinación del todo el proyecto y responsable, en último término, de la buena marcha de los trabajos.
- Responsable de proponer, coordinar y ejecutar con el equipo técnico apropiado, los diferentes ejercicios de Red Team, objeto del contrato.
- Ejercer el mando y la responsabilidad sobre el equipo completo de Red Team
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Asegurar la ejecución de las operaciones acordadas.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), y formación en gestión de proyectos y/o gestión de servicios TI con certificaciones en ITIL, CoBIT, PRINCE2, PMP o equivalentes.

EXPERIENCIA PROFESIONAL:

Más de cinco (5) años de experiencia como responsable de equipos de Red Team, o bien como jefe de proyecto de operaciones de seguridad TIC.

ANALISTA DE SEGURIDAD –RED TEAM	**-**
Dedicación al proyecto:	**A demanda**

FUNCIONES:

- Ejecución de ciberataques controlados contra las infraestructuras TIC de Madrid Digital, para la identificación de brechas de seguridad y vulnerabilidades.

TITULACIÓN Y FORMACIÓN:

- Titulación mínima universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CHEE CCNA (Certified Network Associate Security), CSX (Cybersecurity Fundamentals Certificate), OCSP (Offensive Security Certified Professional), ECSA – EC Council Certified Security Analyst), LPT (Licensed Penetration Tester), CompTIA Pentest+, eJPT (eLearning Junio Penetration Tester), eCPPT (eLearnSecurity Certified Professional Penetration Tester).
- 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 cinco (5) años.

EXPERIENCIA PROFESIONAL:

Más de dos (2) años de experiencia como analista de seguridad en tareas de seguridad ofensiva/Red Team.

6.2.3 Horario y lugar de prestación de los servicios

Los servicios objeto del presente pliego siguen el calendario laborable de Madrid Digital. El horario de este servicio será con carácter general de 8x5 en la franja horaria de **lunes a viernes de 9:00 h a 18:00 h, los días laborables,** si bien la ejecución de los ejercicios podrá realizarse en horario 24x7x365, si así se acuerda previamente.

El lugar de prestación de los servicios será habitualmente en las dependencias del adjudicatario, si bien el equipo estará en disposición de personarse en cualquier dependencia de la Comunidad de Madrid, si el ejercicio así lo requiriera.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

6.2.4 Acuerdos de nivel de servicio - ANS

El adjudicatario se comprometerá a cumplir unos niveles de calidad mínimos sobre los servicios prestados. Para ello, se establecen los niveles de servicio recogidos a continuación, así como la política de penalizaciones ante incumplimientos de estos ANS, que el adjudicatario estará obligado a aceptar.

A continuación, se describen los acuerdos de nivel de servicio exigidos para este lote:

Servicio	Requisito	Nivel de servicio exigido
Ejercicios de Red Team	Valoración de nuevo ejercicio	T. Máximo = 48 horas
	Inicio de ejercicio de Red Team	T. Máximo = 48 horas
	Entrega de informe de resultados	T. Máximo = 48 horas, desde finalización de ejercicio
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido.	T. Máximo = 7 días naturales
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual
Informes de seguimiento del servicio y actas de reuniones	Tiempo de entrega de informes mensuales y actas de seguimiento del servicio	Quinto día hábil del mes siguiente a la fecha de la reunión de seguimiento mensual
Cuadro de mando	Tiempo de actualización del cuadro de mando	Quinto día hábil del mes siguiente

7. LOTE 4: OFICINA TÉCNICA DE SEGUIMIENTO Y CONTROL DE LOS SERVICIOS GESTIONADOS DE CIBERSEGURIDAD

Este lote prestará servicios de Oficina Técnica de apoyo a la Subdirección General de Ciberseguridad para el de seguimiento y control de los servicios gestionados de ciberseguridad, en adelante servicios OTSC-Ciber, prestados por dicha subdirección, teniendo dos objetivos:

- **Dotar de capacidad extendida para poder asumir la carga de trabajo para el seguimiento, supervisión y control** en todas las tareas relativas al gobierno de los servicios y de los contratos recogidos en los lotes 1, 2 y 3 del presente Pliego de Prescripciones Técnicas, y de cualquier otro contrato cuyo responsable sea la Subdirección General de Ciberseguridad (aproximadamente 12 contratos en total).
- **Asesorar, dar soporte al Responsable de Seguridad de Madrid Digital** en relación a la gobernanza y control de la ciberseguridad en su ámbito de actuación.

La prestación de estos servicios se realizará **en modalidad de asistencia técnica**.

7.1 SERVICIOS REQUERIDOS

El objeto de este servicio es la realización de las actividades necesarias para dar soporte al gobierno de los servicios y control de los contratos. A modo informativo, y no limitativo, pueden ser las siguientes:

- Normalización, homogenización y puesta en marcha de buenas prácticas en el modelo de seguimiento y control de los contratos del lote 1, 2 y 3 del presente pliego, y de otros contratos que se determinen, cuyo responsable sea la Subdirección General de Ciberseguridad.
- Elaboración de buenas prácticas para facilitar y homogeneizar el modelo de gestión del servicio entre el personal de Madrid Digital y los proveedores de los lotes 1, 2 y 3 del presente pliego, y de otros contratos que se determinen, cuyo responsable sea la Subdirección General de Ciberseguridad.
- Velar por la prestación del servicio de forma eficaz y eficiente, y, alertar de forma temprana de la evolución de los servicios para tomar las medidas de corrección oportunas: necesidad de recursos, cambios en la gestión, cambios en el presupuesto disponible, etc.
- Seguimiento de los contratos, del servicio y de los proyectos y actividades relacionados, revisando y supervisando:
    - Grado de avance de las planificaciones.
    - Visión integral y supervisión del estado de las actividades.
    - Visión integral y seguimiento de los proyectos.
    - Gestión de riesgos en el servicio y propuestas de mitigación de los riesgos.
    - Seguimiento presupuestario del contrato.
    - Seguimiento y control de la calidad de los entregables.
    - Visión integral del servicio de los diferentes ámbitos basado en indicadores de negocio y tecnológicos.

- Participar en el modelo de seguimiento y consecuentemente en los comités establecidos.
- Generar y mantener la documentación relacionada con los procesos de gestión del servicio y del contrato.
- Organización de la documentación generada por la oficina técnica para el seguimiento del servicio y de los contratos responsables de la Subdirección General de Ciberseguridad.
    - Asesorar, dar soporte al Responsable de Seguridad de Madrid Digital (titular de la Subdirección General de Ciberseguridad) en labores de:
    - Gobernanza en materia de ciberseguridad.
    - Control y supervisión de la correcta ejecución de todos los contratos y proyectos bajo su responsabilidad.
    - Gestión de toda la demanda en materia de ciberseguridad tanto interna, proveniente de la Comunidad de Madrid y de la Agencia, como externa, proveniente de supervisores públicos en materia de ciberseguridad (CCN-CERT, OCC, CNPIC), Cuerpos y Fuerzas de seguridad del Estado, otras AAPP, empresas contratistas y proveedoras de Madrid Digital, etc.
    - Cuadros de mando, informes agregados que reflejen toda la actividad realizada, que deberán realizarse en PowerBI, herramienta corporativa de Madrid Digital para la elaboración de cuadros de mando.
    - Estudio de impacto en Madrid Digital ante nuevas legislaciones, regulaciones que afecten a la ciberseguridad de la organización.
    - Asesoramiento sobre estado del arte y evolución de la ciberseguridad. Estudios de tendencias en mejora de procesos y nuevas tecnologías de ciberseguridad, actores relevantes del sector, evolución de amenazas, ataques, y predicciones en cualquier área relacionada con la ciberseguridad, etc.
    - Realización con carácter general de informes, estudios que tengan que ver con la función del responsable de seguridad.
- Asistir al responsable de seguridad en situaciones de crisis ante incidentes de seguridad de nivel crítico o muy alto. Esta asistencia se centrará sobre todo en actividades de coordinación y comunicación.
- Dar apoyo al responsable de seguridad en los procesos de contratación de Madrid Digital, incluido la gestión de fondos europeos, si así se requiere.

Toda esta actividad será realizada en colaboración y coordinación con todas las áreas dependientes de la Subdirección General de Ciberseguridad, y si se requiere con cualquier organización de la Agencia y/o de la Comunidad de Madrid, dentro del ámbito de actuación de la Agencia.

7.2 MODELO OPERATIVO Y DE ORGANIZACIÓN

7.2.1 Equipo de trabajo

El adjudicatario estará obligado a observar las condiciones generales del equipo de trabajo que pondrá a disposición del contrato, recogidas en el apartado ***8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO.***

En la siguiente tabla se recoge la dimensión del equipo de trabajo mínimo requerido por Madrid Digital para el desarrollo de los servicios. La facturación de estos recursos se realizará

	Nº de personas	% Dedicación	Horas estimadas
Consultor de ciberseguridad, seguridad de la información	2	100	7.680 horas

Para el cálculo de horas estimadas se considera como 100% de dedicación al proyecto un esfuerzo de 160 horas mensuales, 24 meses de duración del contrato.

Todos los perfiles identificados con un 100% de dedicación están asociados a servicios continuos facturables en modalidad de cuota fija.

Los requisitos mínimos en cuanto a titulación, formación y experiencia por perfiles, exigida para los miembros del equipo prestador del servicio, son los siguientes:

CONSULTOR CIBERSEGURIDAD	**2 Personas 100%**
TITULACIÓN Y FORMACIÓN: • Titulación mínima universitaria de Grado de al menos 240 ECTS, Licenciado o Ingeniero superior, preferentemente en cualquiera de las áreas de ingeniería, informática o ciencias. • Estar en disposición de alguna de las siguientes certificaciones de seguridad: CISM (Certified Information Security Manager) o CISA (Certified Information Systems Auditor) de ISACA, o CISSP (Certified Information Systems Security Professional) de ISC2, o equivalentes. **EXPERIENCIA PROFESIONAL:** • Haber realizado tareas de consultoría en materia de ciberseguridad y/o seguridad de la información, al menos, durante cinco (5) años.	

7.2.2 Horario y lugar de prestación de los servicios

Los servicios objeto del presente pliego siguen el calendario laborable de Madrid Digital. El horario de este servicio será el comprendido dentro de la franja horaria de **lunes a viernes de 9:00 h a 18:00 h, los días laborables.**

Madrid Digital requiere el desempeño de estos servicios de forma prioritaria desde las instalaciones del proveedor o en modalidad tele-trabajo. En todo caso, en función de diferentes factores, como, por

ejemplo, atención a reuniones que requieran trato directo, de cualquiera de los comités indicados en este contrato o bien, de cualquier otra reunión específica con personal de la Agencia, el lugar de la prestación de los servicios podría fijarse a criterio de Madrid Digital en las instalaciones de Madrid Digital y/o alguna de las dependencias de la Comunidad de Madrid. Este cambio del lugar de la prestación de los servicios, deberá notificarse al menos con 24 horas de antelación.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

7.2.3 Acuerdos de nivel de servicio – ANS

El adjudicatario se comprometerá a cumplir unos niveles de calidad mínimos sobre los servicios prestados. Para ello, se establecen los niveles de servicio recogidos a continuación, así como la política de penalizaciones ante incumplimientos de estos ANS, que el adjudicatario estará obligado a aceptar.

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO
Personal adscrito a los servicios	Sustitución de recurso asignado por detección de incumplimiento de perfil exigido	T. Máximo = 7 días naturales
	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio anual
Informes de seguimiento del servicio y actas de reuniones	Tiempo de entrega de informes mensuales y actas de seguimiento del servicio de la OTSC	Quinto día hábil del mes siguiente a la fecha de la reunión de seguimiento mensual
Cuadro de mando	Tiempo de actualización del cuadro de mando de la OTSC	Quinto día hábil del mes siguiente

Los tiempos de entrega de informes se contabilizarán alineado con el horario de prestación del servicio.

8. MODELO DE GESTIÓN COMÚN A TODOS LOS LOTES

8.1 SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO

Madrid Digital requiere establecer un Modelo de Seguimiento y Control de la ejecución del contrato para asegurar el correcto desarrollo de todo el servicio definido en el objeto y alcance del contrato

El *Responsable del Contrato* por parte de Madrid Digital designará un *Responsable del Servicio* de la Agencia que se relacionará con el *Responsable del Servicio y con el equipo del servicio* del contratista.

La Agencia podrá revisar y ajustar el Modelo de Seguimiento en cualquier momento durante la vida del contrato, siempre con el objetivo de obtener alguna mejora en su ejecución. El contratista podrá proponer a la Agencia modificaciones al modelo (procedimientos, plantillas, herramientas, etc.) con el

objetivo de mejorar la eficiencia y la calidad del servicio. Cualquier cambio en los procedimientos vigentes necesitará la aprobación por parte de Madrid Digital.

La Agencia distingue los siguientes niveles en el modelo de seguimiento:

- **Nivel Estratégico, de Dirección**: en el que se realiza el seguimiento y control de los aspectos contractuales, del cumplimiento y consecución de hitos del proyecto y de la gestión de sus riesgos.
- **Nivel Táctico y Operativo**: en el que se realiza el seguimiento, el control y la coordinación de las actividades a realizar al amparo del objeto del contrato, en su día a día.

Asociados a estos niveles de seguimiento, se configuran los siguientes Comités:

- **Nivel Estratégico – Comité de Dirección del Contrato.**
- **Nivel Táctico y Operativo – Comité de Operación del Contrato**

La composición y funciones de cada comité se indican a continuación.

8.1.1 Comité de Dirección del Contrato

El Comité de Dirección del Contrato estará compuesto por el Responsable del Contrato y el Responsable del Servicio objeto del contrato de Madrid Digital, y las figuras que estos definan al respecto, y por parte del adjudicatario, el Responsable del Servicio y quien él determine, siempre que sea parte del equipo de trabajo.

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

- Definir las líneas estratégicas de acción del proyecto y validar sus resultados.
- Impulsar y promover el proyecto en cada una de las áreas implicadas.
- Controlar y garantizar que todos los trabajos se ejecutan y ajustan a los niveles de calidad requeridos por la Agencia.
- Asegurar que la ejecución del proyecto se ajusta al marco contractual.
- Hacer un seguimiento periódico del grado de avance del proyecto, haciendo especial hincapié en los hitos establecidos.
- Tomar las decisiones que sean necesarias para facilitar la consecución de los objetivos del proyecto (contenido y plazos).
- Determinar la medición del nivel de servicio conforme a los ANS establecidos, de los que derivarán las correspondientes penalidades en los casos de incumplimiento.
- 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 y resolver cualquier incidencia o problema relacionado con la facturación de los servicios.
- Cualquier otro asunto que el propio Comité considere de interés.

El Comité de Dirección del Contrato se celebrará con la periodicidad que él mismo determine o, en ausencia de otras indicaciones al respecto, a propuesta del Responsable del Contrato de Madrid Digital.

Los acuerdos adoptados en el seno de este comité deberán ser de mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable 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.

8.1.2 Comité de Operación

El Comité de Operación estará formado por el Responsable del Servicio de Madrid Digital, y las figuras que éste defina al respecto, y por parte del adjudicatario, asistirá el Responsable del Servicio designado y las personas del equipo de trabajo que él decida.

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

- Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades del proyecto y evaluación de sus 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).
- 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 varias fases del proyecto, o tengan impacto o importancia estratégica, serán elevadas al Comité de Dirección del Contrato.
- 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. El adjudicatario será responsable 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.

8.1.3 Responsable del Servicio

Además del equipo adscrito a la ejecución del servicio, el contratista designará un *Responsable del Servicio* ante Madrid Digital.

El licitador propuesto como adjudicatario, con carácter previo a la adjudicación del contrato, deberá aportar el ***Curriculum Vitae*** del mismo, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando su cualificación profesional (con detalle de categoría, titulación, formación y actividad profesional).

Este responsable se encontrará en permanente contacto con el personal que la Dirección de Madrid Digital designe, a los efectos que se señalan en la cláusula correspondiente del Pliego de Cláusulas Administrativas.

El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que en cada fase del mismo 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 realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y la formación necesaria que el adjudicatario suministrará al equipo humano que realice los servicios objeto del contrato, en todas aquellas materias que sean necesarias para el perfecto desempeño de dichos trabajos.
- Impartir, con exclusividad, instrucciones específicas sobre el trabajo a realizar al personal que el adjudicatario adscriba a la ejecución del contrato, siempre teniendo en cuenta la base de las instrucciones genéricas que se desprendan de lo establecido en el presente Pliego y encaminadas al buen término del servicio.
- Supervisar y controlar el trabajo y las actividades realizadas, e informar a Madrid Digital de las posibles incidencias y seguimiento o desviaciones de plazos.
- Ejercer el mando y el poder organizativo sobre el equipo humano del adjudicatario destinado a atender los servicios objeto del presente contrato, que estará siempre bajo la disciplina laboral y el poder de dirección del adjudicatario, con independencia de que, para el mejor cumplimiento del servicio, en determinados momentos, pueda el adjudicatario destacar personal del equipo prestador del servicio en cualquier centro de trabajo, oficinas o ubicaciones de la Comunidad de Madrid.
- Informar a Madrid Digital, con la periodicidad que ésta defina, sobre el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas.
- Mantener con el *Responsable del Contrato* designado por Madrid Digital reuniones periódicas de seguimiento del contrato y de los trabajos realizados.

8.2 CONDICIONES GENERALES APLICABLES A LOS EQUIPOS DE TRABAJO

Los adjudicatarios asumirán la organización de los trabajos contratados, dentro del marco fijado por la Agencia, y, por tanto, ejercerán el poder organizativo y de dirección de los recursos humanos que constituyan el equipo prestador del servicio de cada uno de los lotes, para el cumplimiento de los fines que se le encomiendan. Para tal fin, los adjudicatarios designarán un Responsable del Servicio ante Madrid Digital, que tendrá una visión completa del servicio y se responsabilizará de su gestión y coordinación.

Los proveedores asumen la responsabilidad de dimensionar adecuadamente el equipo de trabajo necesario para atender cada uno de los servicios y entregables señalados en cada lote, con el nivel de especialización, calidad y tiempo que requiere cada uno.

Para configurar su oferta técnica en relación con la organización y descripción del equipo de trabajo, los adjudicatarios deberán garantizar y justificar la capacidad de disponer de un número de personas suficiente para realizar todos los trabajos objeto del contrato en los plazos indicados en el presente pliego.

El licitador podrá aportar otros perfiles que considere necesarios para la ejecución del contrato.

El equipo de trabajo ofertado deberá estar formado por personal técnico con capacitación suficiente para el desarrollo de los trabajos descritos en el presente pliego. Asimismo, contarán con la formación, categoría profesional y nivel de especialización adecuados.

En cada uno de los lotes se recoge la dimensión requerida mínima por Madrid Digital de los equipos de trabajo.

Los licitadores deberán aportar, un 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.

El licitador propuesto como adjudicatario, con carácter previo a la adjudicación del contrato, 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 apartado ***10.4 Modelo de currículum vitae del equipo prestador del servicio,*** 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.

8.3 DOCUMENTACIÓN DE LOS SERVICIOS

El adjudicatario deberá entregar, como parte de los trabajos objeto del contrato, toda la documentación generada durante la ejecución del contrato.

La documentación generada durante la ejecución del contrato será propiedad exclusiva de Madrid Digital sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de Madrid Digital.

Toda la documentación se entregará en castellano en el soporte electrónico que se acuerde para facilitar el tratamiento y reproducción de los mismos.

El adjudicatario deberá suministrar a Madrid Digital las nuevas versiones de la documentación que se vayan produciendo. También se entregarán, en su caso, documentos de trabajo previos, informes de referencia, etc. en idéntico soporte a los anteriores.

Madrid Digital supervisará la calidad de todos los trabajos entregados.

Toda la documentación generada deberá ser remitida al equipo designado de Madrid Digital para su validación antes de que se considere como finalizada. El adjudicatario completará las carencias detectadas y corregirá los defectos que le sean notificados por Madrid Digital como condición previa a la aprobación de cada entregable.

El modelo de documentación, si no se indica uno expreso, se acordará con el equipo designado de Madrid Digital. Los entregables deberán ajustarse, en formato y contenido mínimo, a lo indicado por Madrid Digital, y deberán ser aportados en formato electrónico.

Se contará con una carpeta digital de documentación, adecuadamente estructurada, en la que se recopilará toda la información relativa a la realización de los trabajos. La carpeta contará con un índice estructurado temáticamente que permita localizar fácilmente la documentación disponible de forma integral.

8.4 DISPONIBILIDAD DE MEDIOS

En relación a los medios que el equipo de trabajo del proveedor requiera para desarrollar los trabajos objeto del contrato, todos ellos serán provisionados y gestionados por el proveedor, incluido el pc puesto de trabajo, con todas las licencias requeridas de software ofimático, servicios de correo, entornos de colaboración, conexión a Internet, acceso vpn, etc.

Para las reuniones que se realicen de manera virtual, Madrid Digital emplea la herramienta colaborativa de Microsoft TEAMS, herramienta que también se usa para trabajo colaborativo. Debido a ello, es necesario que el adjudicatario cuente con las licencias pertinentes para su utilización.

Por cuestiones de ciberseguridad de las redes y sistemas de Madrid Digital, el adjudicatario deberá responsabilizarse que los puestos de su equipo de trabajo, contemplen las siguientes medidas de seguridad de manera obligatoria:

- Sistema operativo con versión de parcheado de seguridad permanentemente actualizado.
- Software de protección antimalware actualizado y supervisado 24x7, con capacidades de prevención, detección y respuesta ante amenazas e incidentes de seguridad, todo ello garantizado por la empresa adjudicataria y sus servicios de ciberseguridad

La información, documentación, que se genere durante la ejecución de los servicios objeto de este pliego técnico será en formato Microsoft365. Las licencias que a tal efecto requiera el adjudicatario para sus empleados, serán provisionadas por su parte y, en consecuencia, sin coste para Madrid Digital

En todo lo relativo a conectividad de los equipos de trabajo del proveedor y necesidades de acceso remoto a la sede de Madrid Digital y/o a los CPDs incluidos dentro del alcance de este pliego técnico, se seguirá lo indicado en el apartado ***10.2 Requisitos para acceso remoto de proveedores***

9. CONTENIDO DE LAS OFERTAS TÉCNICAS

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

Resulta obligatorio, para facilitar la valoración de las ofertas, que la documentación presentada, ***"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.

9.1 CONTENIDO DE LAS OFERTAS PARA EL LOTE 1

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 100 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. El tamaño de letra a emplear será equivalente al tipo “Arial” de 11 puntos, y con espaciado de interlineado múltiple de al menos1,15.

9.1.1 Resumen ejecutivo

En este documento se expondrá el planteamiento de la solución global y aquellos aspectos relevantes de la oferta que el licitador quiera destacar. Este resumen permitirá valorar de forma general e integrada la oferta presentada, siendo libre tanto el contenido como la estructura del documento. **El número máximo de páginas previsto para este apartado es de diez (10) páginas**.

9.1.2 Solución técnica propuesta para los servicios requeridos

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

- Servicios de prevención:
  - Identificación de amenazas y vigilancia digital.
  - Análisis de vulnerabilidades de seguridad de sistemas y redes.
  - Análisis de vulnerabilidades de seguridad de aplicaciones.
  - Ciberejercicios.
- Servicios de monitorización y detección:
  - Monitorización de eventos e información de seguridad:
    - Plataforma de gestión de eventos e información de seguridad – SIEM.
  - Servicio de monitorización de tráfico de red.
  - Detección de ciberincidentes.
  - Búsqueda proactiva de amenazas – Threat Hunting.
- Servicios de análisis y respuesta:
  - Análisis y respuesta a incidentes de seguridad.
  - Sistema de orquestación, automatización y respuesta.
  - Análisis forense.

- Servicios de apoyo a la gestión de cibercrisis.

- Servicios de soporte a la gestión, operación y procesos:
  - CMDB.
  - Plataforma MISP.
  - Portal de ciberseguridad y cuadros de mando.
  - Herramientas.
  - Sala física del SOC-MD
- Servicios de capacitación y formación en ciberseguridad.
- Servicios de asesoría y asistencia legal.

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.

9.1.3 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:

9.1.3.1 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 la puesta en marcha de cada uno de los servicios requeridos, como son datos críticos, información de infraestructuras y sistemas a supervisar, capacidades de seguridad actuales, procedimientos vigentes para la gestión de la seguridad, etc.
- Propuesta de puesta en marcha de cada uno de los servicios, con detalle de recursos técnicos y humanos dedicados, calendario de actividades y plazos estimados.
- Propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital, hasta su sustitución por los nuevos servicios demandados.
- Propuesta de procesos operativos a implementar en el SOC-MD para la prestación de los distintos servicios.

- Organización del SOC, con detalle de actividades y recursos operativos dedicados a cada uno de los servicios.
- Organización de los servicios de soporte 24x7, detallando interrelaciones entre los equipos dedicados y equipos no dedicados del adjudicatario, y sistemas de ticketing/seguimiento propuestos.
- Propuesta de despliegue de la plataforma SIEM/SOAR, con detalle de los recursos técnicos puestos a disposición para el proyecto, actividades a desarrollar y calendario de puesta en marcha.
- Propuesta de despliegue de la plataforma NDR, con detalle de los recursos técnicos puestos a disposición para el proyecto, actividades a desarrollar y calendario de puesta en marcha.

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 las fases y plazos recogidos en la cláusula correspondiente del **Pliego de Cláusulas Administrativas.**

9.1.3.2 Plan de operación 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.
- Procedimientos operativos propuestos para prestación de todos los servicios, detallando recursos técnicos y humanos.
- Modelo de relación entre los recursos del adjudicatario, ya sean dedicados en exclusividad o no al proyecto, y Madrid Digital, detallando los procedimientos de notificación de incidencias y peticiones y los sistemas de seguimiento y control propuestos.
- Propuesta de métricas (KPI's y KRI's) a facilitar para control de los servicios, metodología de obtención y sistemas puestos a disposición de Madrid Digital para su revisión.
- Metodología y herramientas propuestas para el reporte y seguimiento del cumplimiento de los ANS requeridos en este pliego.

9.1.3.3 Plan de devolución de servicios

El plan de devolución de los servicios deberá garantizar 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.

9.2 CONTENIDO DE LAS OFERTAS PARA EL LOTE 2

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 35 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. El tamaño de letra a emplear será equivalente al tipo "Arial" de 11 puntos, y con espaciado de interlineado múltiple de al menos1,15.

9.2.1 Resumen ejecutivo

En este documento se expondrá el planteamiento de la solución global y aquellos aspectos relevantes de la oferta que el licitador quiera destacar. Este resumen permitirá valorar de forma general e integrada la oferta presentada, siendo libre tanto el contenido como la estructura del documento. **El número máximo de páginas previsto para este apartado es de cinco (5) páginas.**

9.2.2 Solución técnica propuesta para los servicios requeridos

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

- Controles de las medidas de seguridad recogidas en las declaraciones de aplicabilidad de los diferentes servicios de Madrid Digital, detallando herramientas, metodología de trabajo para la implementación de los controles, tiempo estimado de ejecución de la tarea y número de personas involucradas en la actividad.
- Propuesta de nuevos controles técnicos de seguridad a definir e implementar por cada uno de los entornos tecnológicos recogidos en el punto **10.1 Entorno tecnológico**, considerando la legislación vigente y las buenas prácticas en seguridad, detallando herramientas y/o aproximación a la metodología de trabajo para la implementación de los controles, tiempo estimado de ejecución y número de personas involucradas en la actividad
- 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 medidas de seguridad supervisados por los controles.
- Procedimiento de normalización de nombres, y definición de reglas y objetos en las políticas de los elementos de seguridad, detallando metodología de trabajo propuesta, tiempo estimado de ejecución y número de personas involucradas en la actividad.
- Servicio de revisión de reglas y objetos que componen las políticas de los elementos de filtrado, herramientas y/o aproximación a la metodología de trabajo, tiempo estimado de ejecución y número de personas involucradas en la actividad.

9.3 CONTENIDO DE LAS OFERTAS PARA EL LOTE 3

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 25 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. El tamaño de letra a emplear será equivalente al tipo “Arial” de 11 puntos, y con espaciado de interlineado múltiple de al menos1,15.

9.3.1 Resumen ejecutivo

En este documento se expondrá el planteamiento de la solución global y aquellos aspectos relevantes de la oferta que el licitador quiera destacar. Este resumen permitirá valorar de forma general e integrada la oferta presentada, siendo libre tanto el contenido como la estructura del documento. **El número máximo de páginas previsto para este apartado es de cinco (5) páginas**.

9.3.2 Solución técnica propuesta para los servicios requeridos

El documento de solución técnica propuesta tendrá una extensión máxima de 25 páginas, y contendrá los siguientes apartados:

- Plan de gestión del servicio y modelo organizativo propuesto.
- Composición y cualificación del equipo de trabajo puesto a disposición del servicio.
- Propuesta de ejercicios de Red Team a ejecutar a lo largo del contrato, detallando equipo de trabajo dedicado, esfuerzo estimado en horas/hombre, vectores de ataque utilizados, tácticas y técnicas de la matriz de MITRE ATT&CK aplicadas, y, en general, cualquier valor añadido ofrecido por el licitador para el servicio.
- Propuesta de KPI de seguimiento del servicio.
- Propuesta de sistema de seguimiento de cada ejercicio, desde su planificación, solicitud y ejecución, hasta gestión de las debilidades encontradas y acciones de mejora propuestas.

9.4 CONTENIDO DE LAS OFERTAS PARA EL LOTE 4

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos, **no debiendo exceder en ningún caso las 25 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. El tamaño de letra a emplear será equivalente al tipo “Arial” de 11 puntos, y con espaciado de interlineado múltiple de al menos 1,15.

9.4.1 Resumen ejecutivo

En este documento se expondrá el planteamiento de la propuesta requerida y aquellos aspectos relevantes de la oferta que el licitador quiera destacar. Este resumen permitirá valorar de forma general e integrada la oferta presentada, siendo libre tanto el contenido como la estructura del documento. **El número máximo de páginas previsto para este apartado es de cinco (5) páginas**.

9.4.2 Propuesta Modelado de servicios y Organización de la Oficina Técnica

Se valorará la memoria técnica presentada en la que se describa lo siguiente:

- Modelo de prestación de servicios y organización de la oficina técnica considerando el alcance de lo requerido en el apartado ***7.1 SERVICIOS REQUERIDOS***
- Propuesta de buenas prácticas para el seguimiento y control de los contratos del lote 1, 2 y 3 del presente pliego.
- Propuesta de contenido y organización de la documentación de la OTSC-Ciber, considerando que Microsoft365 es la herramienta corporativa de Madrid Digital para la elaboración, compartición de documentación y de colaboración de equipos. Se presentarán ejemplos de documentación de los contenidos propuestos.
- Propuesta de contenido y estructura de cuadro de mando de prestación del servicio de la OTSC-Ciber, considerando que PowerBI es la herramienta corporativa de Madrid Digital para

la elaboración de cuadros de mando. Se presentarán ejemplos de cuadro de mando con los contenidos propuestos.

10. INFORMACIÓN RELEVANTE PARA LOS LICITADORES

10.1 ENTORNO TECNOLÓGICO

El entorno tecnológico sobre el que se prestarán los servicios definidos en el pliego es el siguiente:

SISTEMAS OPERATIVOS	
Servidor	Red Hat, SUSE, CenTOS, Solaris, AIX, Tru64, Ubuntu, Oracle Linux, Debian, Solaris, 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, Palo Alto
Proxy	Forcepoint, Squid
COMUNICACIONES	
Routers	Cisco, Huawei
Switches	Cisco, Extreme Networks, HP, Huawei
WIFI	Extreme, Cisco, Aruba
DNS, DHCP	Infoblox
Balanceadores	Citrix (Netscaler), A10 y F5
VPN	Checkpoint , Palo Alto
SOFTWARE NEGOCIO	
Gestión documental	Documentum, Alfresco
Colaboración	Sharepoint, Teams, Office 365
ERP's	SAP
Gestores de contenido	Fatwire, Joomla, Drupal

Correo electrónico	MS Exchange
Servicios de autenticación	Active Directory, LDAP SunOne, SAP. OAut, SAML

Volumetrías:

- 126.0000 endpoints (PC's de usuario de sobremesa y portátiles).
- 4.000 servidores, alojados en los dos CPD's de Madrid Digital.
- 3.000 servidores alojados en los dos CPD's de la Consejería de Sanidad – SERMAS y en el CPD principal de EducaMadrid.

Madrid Digital notificará puntualmente cualquier evolución tecnológica en sus sistemas que pueda afectar a los servicios objeto del contrato.

10.2 REQUISITOS PARA ACCESO REMOTO DE PROVEEDORES

El servicio de conectividad entre la empresa adjudicataria y la Comunidad de Madrid se considerará incluido dentro del servicio prestado por el adjudicatario y seguirá las siguientes premisas:

- El adjudicatario será responsable de dar adecuada conectividad a sus trabajadores para poder ejecutar el contrato, esto incluye las necesidades de conexión a internet, acceso a correo electrónico, aplicaciones corporativas, accesos VPN, etc.
- El adjudicatario realizará los controles necesarios para asegurar que los accesos a través de su línea de comunicaciones a los CPDs de la Comunidad de Madrid son realizados por los usuarios y máquinas debidamente autorizados.
- En consecuencia, el adjudicatario deberá proporcionar un acceso seguro a su propia red (VPN, extensión de VLAN etc.), de manera que, a los efectos de acceso a los recursos situados en los CPD de la Comunidad de Madrid, cualquier tipo de empleado que se conecte, por cualquier medio y desde cualquier ubicación, aparezca como un usuario del equipo de trabajo y con un direccionamiento IP compatible con el rango reservado por Madrid Digital al contrato del adjudicatario.
- Los trabajadores del adjudicatario que presten sus servicios en edificios de la Comunidad de Madrid no estarán directamente conectados a la red corporativa, sino que, de forma lógica, se encontrarán en un segmento de red que se considera una extensión de la red de su empresa.
- Independientemente de la ubicación de los empleados del adjudicatario, para el acceso lógico a los distintos entornos de la Comunidad objeto del contrato usarán el servicio de conectividad descrito en este apartado.
- Los usuarios que trabajen en las instalaciones de la Comunidad de Madrid dispondrán de un direccionamiento IP en una red diferenciada, asignado por Madrid Digital.
- El adjudicatario debe ofrecer directamente a sus empleados desplazados en sedes de la Comunidad de Madrid los siguientes servicios mínimos, para los que Madrid Digital asignará otro rango IP diferenciado:

- Servicio de nombres (DNS), en el caso de que los trabajadores en las instalaciones de Madrid Digital deban acceder a servicios locales a su empresa. Este servicio de nombres servirá para acceder a los recursos ubicados en los CPD de la Madrid Digital o a los servicios digitales ofrecidos por su empresa. Para ello, la empresa deberá proporcionar servidores de nombres (DNS), bien haciendo *forwarding DNS* para los dominios que Madrid Digital determine (si el direccionamiento es compatible con el de la red de la empresa), bien publicando dichos nombres en la red interna mediante técnicas de NAT. En el caso de que no sea preciso acceder por nombre a servicios de su empresa, los puestos de trabajo del adjudicatario podrán utilizar los servidores DNS proporcionados por Madrid Digital.
- Proxy de navegación a internet, con el fin de que puedan acceder a internet a través de la conectividad entre el CPD de Madrid Digital y las instalaciones del adjudicatario.
- Servicio de correo electrónico, vía webmail u otras direcciones IP del rango reservado

- El adjudicatario pondrá en marcha una conexión dedicada desde su empresa a CPDs de la Comunidad de Madrid, contratada y sufragada por la empresa adjudicataria. La comunicación podrá realizarse mediante línea punto a punto o RPV-IP sobre red de operador, siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en los CPDs de la Comunidad de Madrid se instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.
- La compatibilidad de direccionamiento (mediante NAT), si fuera necesaria, se realizará en los equipos del adjudicatario que empiezan y terminan la línea dedicada.
- Para la conexión de personal externo desde sedes de la Comunidad de Madrid a sistemas de información de la Comunidad o a su propia empresa, el adjudicatario deberá instalar, a su cargo, una conexión dedicada en configuración de alta disponibilidad (doble línea, doble equipo) desde la empresa prestadora a cada una de las sedes de la Comunidad de Madrid. Al igual que en el caso de la conexión con el CPD, la comunicación puede realizarse mediante línea punto a punto o RPV-IP sobre red de operador siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en las sedes de la Comunidad de Madrid se instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.
- Caudales de la conexión con la empresa: el necesario en cada sentido para la prestación de los servicios objetos del contrato.
- Respecto a los trabajadores del adjudicatario que presten sus servicios en edificios de la Comunidad de Madrid descritos anteriormente, el adjudicatario será responsable de proporcionar por sus propios medios la conectividad entre su segmento de red, los servicios y herramientas de su empresa necesarias para su trabajo, y la conexión dedicada con el CPD citada anteriormente.
- En consecuencia, los trabajadores de la empresa prestataria, ya estén ubicados en instalaciones de la misma o en instalaciones de la Comunidad de Madrid, se conectarán

siempre a través de un punto de entrega en un CPD de la Comunidad de Madrid, desde donde podrá acceder a los sistemas de información necesarios para realizar su trabajo.

- La responsabilidad de Madrid Digital con este equipo es:
    - Ofrecer la conectividad física de los equipos a los conmutadores LAN de la sede de la Comunidad de Madrid objeto del contrato para poder alcanzar al router de salida del adjudicatario que conecta con la sede de su empresa (ya sea mediante una línea dedicada o mediante un servicio RPV-IP contratado por dicha empresa).
    - Servicio de DHCP para asignar a cada puesto de trabajo del Adjudicatario en la sede de la Comunidad de Madrid objeto del contrato una dirección IP dentro del rango reservado al Adjudicatario. En su caso, la empresa adjudicataria deberá informar de los servidores DNS que desea que se entreguen a estos puestos.

10.2.1 Equipo de trabajo en instalaciones de la empresa adjudicataria

Este equipo de trabajo se encontrará físicamente en las instalaciones y en la red de la empresa adjudicataria del contrato.

Dicha empresa deberá tener una línea punto a punto dedicada, del caudal y simetrías necesarios que termine en el CPD de Madrid Digital.

Todos los usuarios que estén en este emplazamiento usarán los servicios que la empresa adjudicataria estime oportuno para la ejecución de su trabajo en la propia red de la empresa (acceso Internet, DNS, correo, ERP, etc.).

10.2.2 Equipo de trabajo en las instalaciones de Madrid Digital

En el caso de que Madrid Digital determine que el equipo, o parte del equipo, deben estar físicamente en las instalaciones de Madrid Digital, lógicamente se encontrarán en una extensión de la red de su empresa, en un segmento de red completamente aislado al del resto de trabajadores de la CM y al de otras empresas adjudicatarias.

El adjudicatario necesitará una conexión dedicada con cada una de las sedes de Madrid Digital donde estén ubicados los equipos de trabajo del caudal y características requeridos. Madrid Digital indicará el equipo de dicha ubicación en el que terminará la conexión dedicada.

La responsabilidad de Madrid Digital con este equipo es:

- Ofrecer la conectividad física de los equipos a los conmutadores LAN de la sede de Madrid Digital edificio para poder alcanzar al router de salida del adjudicatario que conecta con la sede de su empresa (ya sea mediante una línea dedicada o mediante un servicio RPV-IP contratado por dicha empresa).
- Servicio de DHCP para asignar a cada puesto de trabajo del adjudicatario en la sede de Madrid Digital una dirección IP dentro del rango reservado al adjudicatario.

10.2.3 Equipo de trabajo remoto

Este equipo de trabajo se encontrará físicamente en cualquier punto distinto de los anteriormente mencionados y en una red externa a la del adjudicatario del contrato o de Madrid Digital.

El adjudicatario deberá proporcionar un acceso seguro a su propia red (VPN, extensión de VLAN etc.), de manera que a los efectos de acceso a los recursos situados en los CPD de la Agencia aparezcan como un usuario más del equipo de trabajo en las instalaciones de la empresa. La compatibilidad de direccionamiento (mediante NAT) se realizará en los equipos que empiezan y terminan la línea dedicada si fuera necesario.

10.2.4 Informes de monitorización de las líneas de comunicaciones

El adjudicatario deberá realizar informes de monitorización de línea. Dicho informe debe contener como mínimo para cada una de las líneas, información relativa a tráfico, latencia y pérdida de paquetes.

Igualmente, el Adjudicatario realizará los controles necesarios para asegurar que los accesos a través de su línea de comunicaciones al CPD de Madrid Digital son realizados por los usuarios y máquinas debidamente autorizados.

Los informes se generarán con una periodicidad mensual y deberán estar a disposición de Madrid Digital para cuando le sea necesario. Adicionalmente, se generarán puntualmente cuando se requiera para asegurar la continuidad del servicio.

10.3 PLATAFORMA SIEM ACTUAL DE MADRID DIGITAL

La plataforma SIEM actual de Madrid Digital está basada en la solución Exabeam (Exabeam SIEM versión 156.13) sobre un motor de Elasticsearch (Elasticsearch versión 7.15.2) que actúa de Datalake y correlador de eventos.

Toda la infraestructura de almacenamiento de logs se encuentra en los nodos ELK. La ingesta de logs desde las diferentes fuentes de eventos se realiza sobre nodos Logpro.

La plataforma consta de 21 servidores físicos, que albergan 53 máquinas virtuales, para las diferentes funciones (Logpro (6), nodos master (3), hot (14), warm (22), Exabeam (2), Kibana (2), balanceadores (4)).

Para la visualización de los casos de uso de monitorización se utiliza Kibana. Están desarrollados más de 170 casos de uso de monitorización que cubren 11 tácticas y 29 técnicas de la matriz de MITRE ATT&CK. Frente a una detección, cada caso de uso genera una alerta, y cada alerta un ticket en el sistema de ticketing OTRS del SOC-MD, desplegado al efecto.

Toda la infraestructura está montada en los dos Centros de Proceso de Datos (CPD) de Madrid Digital, aunque el grueso de servidores de recolección y proceso reside en el CPD principal.

A nivel de hardware, se dispone de:

- 12 servidores Dell Poweredge R740XD, para nodos Data Lake.
- 2 servidores Dell Poweredge R440, para nodos Exabeam.
- 4 servidores Dell Poweredge R440, para sondas IDS.

- 2 servidores HPE DL360 GEN10 8SFF NC CTO, para sondas IDS.
- 2 servidores HPE DL360 GEN10 8SFF NC CTO, para sondas SAT-INET.

A nivel de software y subscripciones, se dispone de:

- Suscripción Exabeam, SIEM-UEBA: Advanced Analytics and Threat Hunter Subscription Software License for 1.001 users. Esta suscripción está contratada hasta 30/06/2024.
- Suscripción Exabeam, SIEM-UEBA: Entity Analytics Software License for 1.001 users. Esta suscripción está contratada hasta 30/06/2024.
- Elastic – SIEM-DATALAKE: Platinum suscription for 39 nodes. Esta suscripción está contratada hasta 30/06/2024.

La relación de fuentes de eventos de seguridad integrados es la siguiente:

- Cortafuegos de red.
- Servicios de directorio (DA).
- Servicios de redes privadas VPN.
- Proxies de navegación.
- Protección antispam/antimalware de correo.
- Protección AntiDDoS.

En cuanto a la infraestructura de sondas de red IDS, se dispone de los siguiente:

- 6 sondas de red IDS, para análisis del tráfico cursado de entrada/salida a Internet y de tráfico interno de entrada/salida a los CPD's de Madrid Digital. Los dos tráficos analizados son actualmente del orden de 10 Gbps.
- 2 sondas de red NSM/IDS SAT-INET del CCN-CERT, una en cada CPD de Madrid Digital, para análisis del tráfico de entrada/salida a Internet.
- 4 sondas de red IDS para análisis de tráfico cursado de entrada/salida a los CPD's de Sanidad.
- 2 sondas de red NSM/IDS SAT-INET y NSM/IDS SAT-ICS del CCN-CERT, en el Hospital Universitario 12 de Octubre.
- 37 sondas de red IDS para análisis del tráfico cursado de entrada/salida local, en centros hospitalarios.
- 22 sondas de red IDS para análisis del tráfico cursado de entrada/salida local, en centros sanitarios.

10.4 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.

11. CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS

Durante el periodo de presentación de la oferta y, ante cualquier duda o necesidad de aclaración referida a las especificaciones del Pliego de Prescripciones Técnicas, el licitador podrá dirigirse a:

Agencia para la Administración Digital de la Comunidad de Madrid

Subdirección General de Ciberseguridad, Protección de Datos y Privacidad

E-mail: md_ciberseguridad_soc@madrid.org

La Subdirectora de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2024 06 12 12:33

Fdo.: Esther Muñoz Fuentes