

Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original

Número de Expediente: ECON/000237/2023

*SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE
MADRID DIGITAL – 4 LOTES*

LOTE 1

**Centro de Operaciones de Ciberseguridad
SOC-MD**

**Informe técnico de valoración de criterios cualitativos
cuya cuantificación depende de un juicio de valor.**

**SUBDIRECCIÓN GENERAL DE CIBERSEGURIDAD,
PROTECCIÓN DE DATOS Y PRIVACIDAD**



INFORME TÉCNICO DE VALORACIÓN DE CRITERIOS CUALITATIVOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

Contenido

1. Introducción	6
2. Criterios cualitativos cuya cuantificación depende de un juicio de valor	7
3. Valoración de la propuesta técnica: Hasta 45 puntos	9
3.1 CRITERIO NÚMERO 7: SOLUCIÓN TÉCNICA PROPUESTA PARA LOS SERVICIOS REQUERIDOS. HASTA 35 PUNTOS.	9
3.1.1 CRITERIO 7.1 - Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.	9
3.1.1.1 EVOLUTIO CLOUD ENABLER S.A.U.	9
3.1.1.2 ORANGE ESPAGNE S.A.U.	10
3.1.1.3 PROSEGUR CIBERSEGURIDAD S.L.	12
3.1.1.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	13
3.1.1.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	14
3.1.1.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	15
3.1.1.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	16
3.1.1.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	17
3.1.1.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	19
3.1.1.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	20
3.1.1.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	21
3.1.2 CRITERIO 7.2 - Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.	22
3.1.2.1 EVOLUTIO CLOUD ENABLER S.A.U.	22
3.1.2.2 ORANGE ESPAGNE S.A.U.	23
3.1.2.3 PROSEGUR CIBERSEGURIDAD S.L.	24
3.1.2.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	25
3.1.2.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	26
3.1.2.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	27

3.1.2.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	28
3.1.2.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	29
3.1.2.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	31
3.1.2.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	32
3.1.2.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	33
3.1.3	CRITERIO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.	34
3.1.3.1	EVOLUTIO CLOUD ENABLER S.A.U.	34
3.1.3.2	ORANGE ESPAGNE S.A.U.	35
3.1.3.3	PROSEGUR CIBERSEGURIDAD S.L.	36
3.1.3.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	37
3.1.3.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	38
3.1.3.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	39
3.1.3.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	40
3.1.3.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	41
3.1.3.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	42
3.1.3.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	43
3.1.3.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	44
3.1.4	CRITERIO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.	45
3.1.4.1	EVOLUTIO CLOUD ENABLER S.A.U.	45
3.1.4.2	ORANGE ESPAGNE S.A.U.	46
3.1.4.3	PROSEGUR CIBERSEGURIDAD S.L.	47
3.1.4.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	48
3.1.4.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	49
3.1.4.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	50
3.1.4.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	51
3.1.4.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	52
3.1.4.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	53
3.1.4.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	54
3.1.4.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	55

3.1.5	CRITERIO 7.5 – Servicio de orquestación, automatización y respuesta - SOAR. Hasta 3 puntos.....	56
3.1.5.1	EVOLUTIO CLOUD ENABLER S.A.U.....	56
3.1.5.2	ORANGE ESPAGNE S.A.U.	56
3.1.5.3	PROSEGUR CIBERSEGURIDAD S.L.	57
3.1.5.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	58
3.1.5.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.....	59
3.1.5.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.....	60
3.1.5.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	60
3.1.5.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	61
3.1.5.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	62
3.1.5.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	63
3.1.5.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	63
3.1.6	CRITERIO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis. Hasta 4 puntos.....	64
3.1.6.1	EVOLUTIO CLOUD ENABLER S.A.U.....	64
3.1.6.2	ORANGE ESPAGNE S.A.U.	65
3.1.6.3	PROSEGUR CIBERSEGURIDAD S.L.	66
3.1.6.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	67
3.1.6.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.....	68
3.1.6.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.....	69
3.1.6.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	69
3.1.6.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	70
3.1.6.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	71
3.1.6.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	72
3.1.6.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	73
3.2	CRITERIO NÚMERO 8: PLANES OPERATIVOS. HASTA 10 PUNTOS.....	73
3.2.1	CRITERIO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.	73
3.2.1.1	EVOLUTIO CLOUD ENABLER S.A.U.....	73
3.2.1.2	ORANGE ESPAGNE S.A.U.	74
3.2.1.3	PROSEGUR CIBERSEGURIDAD S.L.	75
3.2.1.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	76
3.2.1.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.....	76

3.2.1.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	77
3.2.1.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	78
3.2.1.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	79
3.2.1.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	79
3.2.1.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	80
3.2.1.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	81

3.2.2 CRITERIO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.82

3.2.2.1	EVOLUTIO CLOUD ENABLER S.A.U.	82
3.2.2.2	ORANGE ESPAGNE S.A.U.	82
3.2.2.3	PROSEGUR CIBERSEGURIDAD S.L.	83
3.2.2.4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	84
3.2.2.5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	84
3.2.2.6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.	85
3.2.2.7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	86
3.2.2.8	UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	86
3.2.2.9	UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.	87
3.2.2.10	UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	88
3.2.2.11	UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	88

4. Resumen de la valoración de los criterios cualitativos. Hasta 45 puntos 90

1. Introducción

Efectuada el martes 10 de septiembre de 2024 la apertura de proposiciones técnicas de los ofertantes admitidos a licitación del expediente número ECON/000237/2023 – SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL – 4 LOTES, A ADJUDICAR POR PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS, procede realizar la valoración del LOTE 1: CENTRO DE OPERACIONES DE CIBERSEGURIDAD, correspondiente a los criterios cualitativos cuya cuantificación depende de un juicio de valor, según lo establecido en el Pliego de Cláusulas Administrativas Particulares, cláusula 1, punto 8, criterios objetivos de adjudicación del contrato.

Las empresas que se han presentado a licitación son:

Nº	EMPRESA	CIF
1	EVOLUTIO CLOUD ENABLER S.A.U.	A80448194
2	ORANGE ESPAGNE S.A.U.	A82009812
3	PROSEGUR CIBERSEGURIDAD S.L.	B87602173
4	S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.	B96863444
5	SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.	B61588737
6	SOTHIS SERVICIOS TECNOLÓGICOS S.L.U	B98513260
7	TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.	A78053147
8	<u>UTE</u> NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.	B82387770 B62174842
9	<u>UTE</u> ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P	B79217790 B81644387 B81917858
10	<u>UTE</u> INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.	A28855260 B63647499
11	<u>UTE</u> SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.	A82733262 B01644558

A continuación, se desarrolla la valoración de las propuestas técnicas presentadas.

2. Criterios cualitativos cuya cuantificación depende de un juicio de valor

Tal y como se indica en el punto 8, de la cláusula 1 del Pliego de Cláusulas Administrativas Particulares para la valoración de los criterios cualitativos cuya cuantificación depende de un juicio de valor, criterios número 7 y 8 recogidos, se tendrá en cuenta lo siguiente:

CRITERIO NÚMERO	DESCRIPCIÓN DEL CRITERIO	PONDERACIÓN
7	SOLUCIÓN TÉCNICA PROPUESTA PARA LOS SERVICIOS REQUERIDOS	Hasta 35 puntos
7.1	<p>Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios.</p> <p>Se valorará la calidad, completitud e idoneidad de la solución propuesta para cada uno de los servicios, el equipo de trabajo, las herramientas puestas a disposición y los procesos y metodología propuesta para la gestión completa de cada servicio.</p>	Hasta 6 puntos
7.2	<p>Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM.</p> <p>Se valorará la calidad, completitud e idoneidad de la plataforma propuesta para la monitorización de eventos de seguridad, la arquitectura de la misma, su posición en el último cuadrante de Gartner (Cuadrante SIEM) y Forrester (Cuadrante de plataformas de analíticas de seguridad), las medidas de disponibilidad y continuidad planteadas, las capacidades de integración y adaptación con los sistemas de Madrid Digital, sus posibilidades de escalado, la disponibilidad de librerías de casos de uso de monitorización ya desarrollados, y la calidad de la propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.</p>	Hasta 10 puntos
7.3	<p>Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR.</p> <p>Se valorará la calidad, completitud e idoneidad de la plataforma propuesta para análisis del tráfico de red, arquitectura de la solución, su posición en el último cuadrante de Forrester (Cuadrante de visibilidad y análisis de red), escalabilidad y automatización, las medidas de disponibilidad y continuidad planteadas, las capacidades de integración y adaptación con los sistemas de Madrid Digital y equipos asociados, la disponibilidad de librerías de casos de uso de monitorización ya desarrollados, y la calidad de la propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.</p>	Hasta 8 puntos

CRITERIO NÚMERO	DESCRIPCIÓN DEL CRITERIO	PONDERACIÓN
7.4	Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Se valorará la calidad, completitud e idoneidad del servicio propuesto en base a la organización de los recursos, los procedimientos propuestos para la monitorización remota de las fuentes de eventos de seguridad, las plataformas SIEM/SOAR y NDR, y los procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad reportadas por cada uno de los servicios.	Hasta 4 puntos
7.5	Servicio de orquestación, automatización y respuesta – SOAR. Se valorará la calidad, completitud e idoneidad de la plataforma propuesta para orquestación, automatización y respuesta ante incidentes de seguridad, arquitectura de la solución, escalabilidad, las medidas de disponibilidad y continuidad planteadas, las capacidades de integración y adaptación con el resto de plataformas (SIEM/NDR), sistemas de Madrid Digital y equipos asociados; la disponibilidad de librerías de casos de uso de automatización ya desarrollados y la calidad de la propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.	Hasta 3 puntos
7.6	Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Se valorará la calidad, completitud e idoneidad de la metodología y procedimientos, capacidades y herramientas propuestas para cada uno de los servicios, para la gestión global de los incidentes de seguridad en todas sus fases: análisis de alcance, evaluación de impacto, medidas de contención, planes de recuperación y lecciones aprendidas; así como la propuesta de organización global de los recursos del proveedor y protocolos de activación de equipos adicionales.	Hasta 4 puntos
8	PLANES OPERATIVOS	Hasta 10 puntos
8.1	Plan de implantación de los servicios. Se valorará la calidad, completitud e idoneidad de la propuesta de implantación de cada uno de los servicios solicitados, detallando tareas, equipo humano dedicado y calendario de actividades propuesto, estrategia de mantenimiento y coexistencia de los servicios actuales/futuros durante esta fase, propuesta de procesos operativos a implementar y propuesta de despliegue de la plataforma SIEM/SOAR y NDR.	Hasta 6 puntos

CRITERIO NÚMERO	DESCRIPCIÓN DEL CRITERIO	PONDERACIÓN
8.2	Plan de operación y devolución de los servicios. Se valorará la calidad, completitud e idoneidad de la propuesta de modelo de gobierno de los servicios, las tecnologías y herramientas propuestas, la metodología de control y seguimiento de todo el proyecto (ANS, KPI), idoneidad de los procedimientos y documentación de seguimiento, calendario de puesta en marcha de cada servicio y transferencia de conocimiento, y medios humanos y materiales dedicados.	Hasta 4 puntos

A la hora de valorar cada criterio se ha tenido en cuenta el valor que aporta cada oferta respecto a lo exigido en pliego, conforme a la siguiente escala de valoración:

- Si la propuesta se limita a cumplir los requisitos del pliego, se considerará que NO APORTA VALOR, por lo que se puntuará con 0 puntos.
- En el caso en que la propuesta aporte poco valor, se considerará ADECUADA. Se puntuará con el 20% del máximo de los puntos asociados al criterio.
- Si aporta detalles que permitan identificar un valor claro respecto a lo requerido, se considerará que la propuesta es BUENA. Se puntuará con el 60% del máximo de los puntos asociados al criterio.
- Será considerada NOTABLE en el caso en que aporte beneficios para el servicio, de forma clara y significativamente por encima de lo requerido. Se puntuará con el 80% del máximo de los puntos asociados al criterio.
- Cuando la propuesta sea excepcional, será calificada como SOBRESALIENTE. Se puntuará con el máximo de los puntos asociados al criterio.

3. Valoración de la propuesta técnica: Hasta 45 puntos

Para el LOTE 1, y para cada criterio, se aporta la valoración de las propuestas técnicas presentadas y las puntuaciones obtenidas.

3.1 CRITERIO NÚMERO 7: SOLUCIÓN TÉCNICA PROPUESTA PARA LOS SERVICIOS REQUERIDOS. HASTA 35 PUNTOS.

3.1.1 CRITERIO 7.1 - Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

3.1.1.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **SOBRESALIENTE** debido al aporte de valor de su solución en la identificación de amenazas y vigilancia digital, en la que se ofrece una solución de inteligencia de amenazas que incorpora fuentes muy bien posicionadas

comercialmente y con gran aporte de valor. La solución ofrece funcionalidades adicionales, como una base de datos ya elaborada de vulnerabilidades asociadas a CPE's (*Common Platform Enumeration*) conocidos, o funcionalidades como poder identificar cambios no autorizados en el inventario de activos generado. La solución propuesta para el análisis de vulnerabilidades de sistemas y redes ofrece elementos extra a los requisitos solicitados en el pliego, como una suscripción adicional gratuita o capacidades de análisis de aplicaciones web y directorio activo. Por último, la propuesta de ciberejercicios detalla metodología, actividades y herramientas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la identificación de amenazas y vigilancia digital, se ofrece un amplio y completo catálogo de fuentes monitorizadas y consultadas. Se permite acceso ilimitado a feeds de fuentes comerciales, contando con fuentes muy bien posicionadas comercialmente y con gran aporte de valor. Además, es posible elaborar un inventario actualizado de activos para la identificación inmediata de cambios no autorizados. También se ofrece una base de datos ya elaborada de vulnerabilidades asociadas a CPE's para la identificación automática de vulnerabilidades que afecten a Madrid Digital.
- Sobre el análisis de vulnerabilidades de sistemas y redes, la solución propuesta, en nube, está dimensionada para 8.000 activos, localizados en infraestructura *on-premise* o en nube, permitiendo durante 45 días al año una sobresuscripción del número de activos, sin coste adicional. Como valor añadido se ofrecen capacidades adicionales de análisis de aplicaciones web y seguridad en directorio activo. Incluye la generación de una base de datos de activos, clasificados por criticidad empresarial y nivel de seguridad. También, se propone automatizar las alertas y notificaciones generadas a través del SOAR.
- En referencia al análisis de vulnerabilidades de aplicaciones, desarrolla las diferentes áreas de análisis a evaluar en una aplicación, sin comprometer en ningún caso su disponibilidad.
- La propuesta de ciberejercicios incluye metodología, tipología, ejemplos y herramientas de seguimiento, todo estructurado y relacionado.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

6 puntos

3.1.1.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **BUENA** debido al aporte de valor de la solución propuesta para la identificación de amenazas y vigilancia digital, donde se proporciona una descripción muy detallada de los tipos de activos a monitorizar y una metodología de obtención de información bien estructurada. Se detalla la metodología de gestión del servicio de análisis de vulnerabilidades de sistemas y redes, y se propone una herramienta específica con la que trabajar. Igualmente, se detalla la metodología y herramientas a utilizar para la realización del análisis de vulnerabilidades de aplicaciones. La propuesta de ciberejercicios refleja los tipos de ciberejercicios a realizar y un calendario con la planificación propuesta. Sin embargo, no se detalla la metodología del servicio de identificación de amenazas y vigilancia digital ni equipo de trabajo. Tampoco se detalla el

equipo de trabajo encargado de realizar los análisis de vulnerabilidades de sistemas y redes ni se especifica la metodología de gestión y seguimiento de las vulnerabilidades. Respecto de los ciberejercicios, falta concretar información sobre las herramientas empleadas y el equipo de trabajo.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la identificación de amenazas y vigilancia digital, se trata de un servicio facilitado a través del módulo de inteligencia de amenazas de la herramienta propuesta para el servicio de análisis de vulnerabilidades, complementado con otras fuentes de inteligencia de amenazas de uso público, y herramientas propias del licitador para vigilancia e inteligencia de amenazas en fuentes abiertas y para monitorización de la exposición digital en Internet. Se aporta una descripción muy detallada de los tipos de activos a monitorizar, a concretar durante la implantación. La metodología de obtención de información está bien estructurada, con detalle de fases, actividades y entregables a facilitar, aportando la tipología de información que suele detectarse más habitualmente.
- El servicio de análisis de vulnerabilidades de sistemas y redes describe detalladamente las actividades de análisis de la superficie de exposición, recogiendo una herramienta específica propuesta para la actividad. Se detalla profusamente la metodología de gestión del servicio, en base a fases, actividades de cada fase y responsables de su ejecución, así como los entregables resultantes de cada actividad. La herramienta propuesta permite la integración con directorio activo, la solución SIEM ofertada y FARO.
- La propuesta sobre análisis de vulnerabilidades de aplicaciones detalla el conjunto de herramientas a utilizar para el análisis y explotación de las vulnerabilidades. Además, queda bien reflejada la metodología a utilizar, indicando los estándares aplicados en los diferentes escenarios (aplicaciones web, infraestructura, redes inalámbricas).
- Respecto a los ciberejercicios se plasma la metodología a seguir para la realización y seguimiento de los ciberejercicios, se explican los tipos de ciberejercicios y se incluye un calendario que refleja el periodo de ejecución y duración de cada tipo de ejercicio, además del número de recursos dedicado en cada periodo.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Respecto de la identificación de amenazas y vigilancia digital, la propuesta no detalla la metodología de gestión del servicio, sólo habla de metodología de obtención de información y envío de informes mensuales. Tampoco menciona el equipo de trabajo encargado de desarrollar las actividades.
- En relación con el análisis de vulnerabilidades de sistemas y redes, no se menciona el modo de funcionamiento del equipo de trabajo, ni se proporcionan detalles sobre la gestión y seguimiento de las vulnerabilidades identificadas.
- Respecto a los ciberejercicios, faltan detalles sobre las herramientas a utilizar para llevar a cabo los diferentes tipos de ciberejercicios y especificaciones sobre el equipo de trabajo encargado de planificarlos, ejecutarlos y realizar un seguimiento de éstos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

3,6 puntos

3.1.1.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **NOTABLE** debido a la completitud e idoneidad de la solución propuesta para cada uno de los servicios. Describe con detalle el equipo de trabajo del servicio de análisis de vulnerabilidades de seguridad de sistemas y redes como el de ciberejercicios, faltando, sin embargo, su definición en el resto. Propone herramientas específicas para todos los servicios salvo para los ciberejercicios. Por último, desarrolla una metodología bien detallada para todos los servicios salvo para el de identificación de amenazas y vigilancia digital.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación con la identificación de amenazas y vigilancia digital, propone un servicio basado en herramientas comerciales y plataforma propietaria del licitador basada en IA y ML y configurada para 500 *assets* (IP's, dominios). Define de forma estructurada los objetivos del servicio. Incluye un conjunto de herramientas completo de soporte del servicio, con herramientas específicas para la gestión de *takedowns* en redes sociales. Por último, incluye una propuesta de reuniones periódicas con el equipo de ciberinteligencia.
- Respecto al análisis de vulnerabilidades de seguridad de sistemas y redes, clasifica los activos por niveles de exposición y las vulnerabilidades según su relevancia para Madrid Digital. Propone un inventario de activos que estará disponible para su consulta y descarga y alimentará la CMDB mantenida por la empresa. Describe una plataforma de análisis de vulnerabilidades complementada con una plataforma específica de información de vulnerabilidades conocidas que le permite conocer y priorizar los CVE's (*Common Vulnerabilities and Exposures*) que se estén atacando en cada momento, además de ser integrable con la solución SIEM ofertada. La herramienta incluye varios motores de análisis, y permite el escaneo de redes IT, OT e IoT. La metodología está bien detallada, dividida por fases y actividades asociadas, proponiendo un plan personalizado de priorización de las remediaciones. Se detallan los entregables y el equipo de trabajo, que consta de un *Customer Success Manager* (CSM) más un analista.
- En cuanto al análisis de vulnerabilidades de seguridad de aplicaciones, define claramente las metodologías de análisis, tácticas, técnicas y procedimientos aplicados para la prestación del servicio; así como los criterios de valoración de las vulnerabilidades encontradas y las herramientas de análisis y explotación utilizadas. Propone una metodología de análisis basado en OWASP para aplicaciones web y OSSTMM y NIST para infraestructura. Recoge propuesta concreta de auditoría sobre DA. Recoge un amplio catálogo de herramientas para auditoría de aplicaciones web y perimetrales.
- En relación con los ciberejercicios, plantea un desarrollo claro y estructurado de las metodologías y procedimientos a utilizar. Propone la ejecución de un ciberejercicio anual compuesto a su vez por un ejercicio Table-top y dos campañas de simulación de *phishing*,

detallando duración de cada actividad. Además, detalla el equipo de trabajo dedicado al servicio.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en relación con lo siguiente:

- No detalla el equipo de trabajo en el servicio de vigilancia digital ni en el de vulnerabilidades de seguridad de aplicaciones. Respecto a vigilancia digital, no describe la metodología a desarrollar. Por último, en cuanto a los ciberejercicios, falta definir las herramientas que va a utilizar.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

4,8 puntos

3.1.1.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **BUENA** ya que en general la propuesta es ordenada y describe con detalle la metodología para casi todos los servicios, salvo el de análisis de vulnerabilidades de seguridad de aplicaciones que está poco desarrollada. En cuanto a las herramientas, explica pormenorizadamente las utilizadas por cada servicio. Sin embargo, no describe el equipo de trabajo para ninguno de los servicios, salvo para el caso de ciberejercicios. Tampoco desarrolla la gestión del ciclo de vida de las vulnerabilidades.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación con la identificación de amenazas y vigilancia digital describe una plataforma propietaria de monitorización y detección de amenazas que integra fuentes de inteligencia externas públicas e inteligencia propia del licitador, con conectores a fuentes de enriquecimiento de información. Propone con detalle una herramienta igualmente propietaria, con módulos de IA, que facilita procesamiento de datos mediante técnicas de *Big Data* y que está integrada con el SIEM. Desarrolla en profundidad la metodología aplicada, mediante fases y actividades, y el proceso de *takedown*, en el que se incluye, de ser necesario, su escalado a las autoridades competentes.
- En cuanto al análisis de vulnerabilidades de seguridad de sistemas y redes, plantea de forma detallada una herramienta integrada de forma nativa con el SIEM propuesto, con una amplia variedad de módulos de análisis. Describe una metodología de análisis según OWASP y OSSTM, detallada por fases, plan de pruebas y entregables.
- En referencia a los ciberejercicios, describe un equipo de trabajo ampliamente cualificado. Desarrolla en profundidad la metodología de ejecución de cada ejercicio, destacando el enfoque por gamificación, cuya principal ventaja es que cambia la percepción de la actividad, mejorando sensiblemente su aceptación por parte del personal involucrado. Enumera los ejercicios propuestos y elabora píldoras formativas para consolidar la acción de concienciación. Por último, plantea una herramienta específica de seguimiento de ejercicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en relación con lo siguiente:

- No describe el equipo de trabajo para el servicio de identificación de amenazas y vigilancia digital.
- En cuanto al servicio de vulnerabilidades de seguridad de sistemas y redes, no indica auditorías específicas ni profundiza en la gestión del ciclo de vida de las vulnerabilidades, especificando el registro y la tipología de vulnerabilidades a tratar. Tampoco detalla el criterio de valoración que utilizará el equipo técnico y el sistema de *ticketing* utilizado. Por último, no menciona el equipo de trabajo.
- Servicio de análisis de vulnerabilidades de seguridad de aplicaciones poco desarrollado. Indica el uso de la misma herramienta que en el servicio de análisis de vulnerabilidades de seguridad de sistemas y redes sin detallar cómo realizará el servicio. Se limita a comentar que se realizarán análisis DAST (Test de Seguridad de Aplicación Dinámico). No describe la metodología ni el equipo de trabajo.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

3,6 puntos

3.1.1.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** este criterio se considera **SOBRESALIENTE** ya que plantea una solución detallada para cada uno de los servicios, poniendo el foco en la integración y automatización de estos servicios a través de la plataforma de IA que expone. Desarrolla con gran nivel de profundidad el uso de las distintas herramientas y equipos de trabajo.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Propone una arquitectura integral para todo el ciclo de prevención, destacando el disponer de un SOAR específico para la parte preventiva que ofrece un entorno concreto más adaptado a resolver las vulnerabilidades, propiciando una investigación proactiva de las alertas antes de incorporarlas al SIEM. Este SOAR está basado en IA y para su gestión propone un recurso específico denominado analista IA.
- En relación con la identificación de amenazas y vigilancia digital, propone una solución dimensionada inicialmente para 300 activos, detallando tipología de alertas y componentes clave del servicio en cada una de sus fases de ejecución (recopilación, análisis, contextualización...). Se aporta relación muy detallada de tipos de activos a vigilar, integrada con la plataforma de IA para enriquecimiento y contextualización. Plantea una herramienta integrada de forma nativa con la herramienta de análisis de vulnerabilidades propuesta para correlar vulnerabilidades internas con amenazas externas. La metodología de gestión del ciclo de vida de las amenazas es adecuada.

- En cuanto al análisis de vulnerabilidades de seguridad de sistemas y redes, propone una herramienta, licenciada para 8.000 activos, cuyo valor fundamental es que no solo proporciona visibilidad de las vulnerabilidades en el entorno TI (redes y sistemas) sino cómo se traducen en riesgo empresarial y probabilidades de ser objetivo de los atacantes, permitiendo la remediación basada en impacto. Indica que está complementada con módulos de SOAR orientados a la orquestación y gestión de vulnerabilidades detectadas. Además, está integrada con el SIEM propuesto, la plataforma de IA y la plataforma de recolección y generación de BBDD de activos propuesta.
- Respecto al análisis de vulnerabilidades de seguridad de aplicaciones, mejora las capacidades de las auditorías de DDoS que se soliciten bajo demanda gracias a su especialización en esos casos (ataques de capa de aplicación, *http flood*, *slowloris*, *tsunami webDDoS*). Igualmente, describe una arquitectura altamente integrable con ITSM-FARO. Se incluye en la oferta herramienta para análisis DAST/SAST/IAST, como complemento a las herramientas específicas de hacking utilizadas por los analistas, integrada también con el resto de las plataformas propuestas.
- Por último, respecto a los ciberejercicios, plantea un amplio abanico de tipologías de ellos: campañas de *phishing*, torneos *Capture The Flag (CTF)*, entrenamientos bajo el esquema *CyberRange* y ejercicios basados en *table-top* para valorar el correcto funcionamiento de los comités de crisis y procedimientos. Incluye, asimismo, ciberejercicios propios de las herramientas de SIEM y NDR propuestas. Describe con amplio detalle el uso de las herramientas utilizadas en cada ejercicio y la herramienta específica para la gestión de ciber crisis. Se recoge propuesta de calendario de ejecución y duración de cada uno de ellos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

6 puntos

3.1.1.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA** dado que describe la metodología y herramientas a utilizar en la identificación de amenazas, el análisis de vulnerabilidades de seguridad tanto de sistemas y redes como de aplicaciones; sin embargo, de manera general, no profundiza en el desarrollo de los puntos más relevantes de cada uno de estos elementos ni describe los equipos de trabajo de los servicios. En cuanto al servicio de vulnerabilidades de seguridad de aplicaciones, la descripción está enfocada al análisis de la superficie de exposición más que al análisis a demanda de aplicaciones.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la identificación de amenazas y vigilancia digital, describe con mucho detalle la herramienta que sustenta el servicio, integrada con el SIEM/SOAR propuesto y la MISP de Madrid Digital. Se recoge la relación de fuentes de información y actores relevantes.
- Respecto al análisis de vulnerabilidades de seguridad de sistemas y redes, propone una herramienta totalmente integrada y bidireccional con la solución de SIEM escogida que le

permite despertar alertas, enriquecer la información de contexto de los activos involucrados, etc.

- En relación con el análisis de vulnerabilidades de seguridad de aplicaciones, enumera de forma clara y concisa la metodología a utilizar y las acciones a realizar en el servicio.
- Respecto a los ciberejercicios, describe una propuesta detallada de ejercicios entre los que destacan dos simulacros por año estilo table-top y doce simulaciones de *phishing*.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- En relación con la identificación de amenazas y vigilancia digital, falta profundidad en la descripción del equipo de trabajo que realizará el servicio. La metodología de gestión propuesta es demasiado genérica. Por último, solo se considera como fuente de inteligencia de amenazas la facilitada por la propia herramienta propuesta.
- En cuanto al análisis de vulnerabilidades de sistemas y redes, existe divergencia entre el número de activos simultáneos ofertados (8.000 activos) y lo propuesto (1.275 IP's públicas). La descripción del equipo de trabajo es genérica, la metodología es igualmente poco concreta y no detalla las características técnicas de la herramienta a utilizar.
- Respecto al análisis de vulnerabilidades de seguridad de aplicaciones, la descripción está muy orientada al análisis de superficie de exposición, no al objetivo de pentesting de aplicaciones. No se detallan las herramientas de *hacking*, solo la asociada a la herramienta propuesta en el servicio de análisis de vulnerabilidades de seguridad de sistemas y redes. Por último, tampoco se detalla el equipo de trabajo.
- Referente a los ciberejercicios, resume de manera escueta los tipos de ciberejercicios que va a realizar junto a un calendario confuso, sin detallar los objetivos generales: equipo de trabajo, herramientas y metodología (de la que únicamente se mencionan los tipos de ejercicios y los informes de resultados).

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

1,2 puntos

3.1.1.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **NOTABLE** debido a que describe de forma clara y completa la solución propuesta destacando, para el servicio de identificación de amenazas y vigilancia digital, la metodología propuesta, el equipo de trabajo y la amplia relación de fuentes de inteligencia de amenazas y de indicadores de compromiso manejados. Del servicio de análisis de vulnerabilidades de seguridad de sistemas y redes mencionar el desarrollo completo de la metodología de gestión propuesta en fases, actividades y herramientas. En cuanto a la propuesta para el servicio de vulnerabilidades de seguridad de aplicaciones, destaca la tipología de análisis a desarrollar y el

completo conjunto de herramientas. Por último, si bien de la oferta de ciberejercicios destaca la propuesta de una herramienta específica para su ejecución falta profundidad en su desarrollo.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la identificación de amenazas y vigilancia digital, detalla de manera exhaustiva los indicadores de compromiso (*feeds* de Telefónica, propietarios, Red Nacional de SOC y CTA, y públicos), los protocolos de integración con la MISP de Madrid Digital (*feeds* vía TAXII en formato STIX) o URL, las amenazas monitorizadas, así como las tareas de mitigación, entre las que se encuentra el cierre técnico de dominios que destaca como objetivo prioritario. Describe con detalle el equipo de trabajo y la metodología utilizada.
- Con relación al análisis de vulnerabilidades de seguridad de sistemas y redes, describe en profundidad el equipo de trabajo y la metodología de gestión propuesta, fases y actividades a desarrollar y herramientas a utilizar. Destaca la funcionalidad de alerta temprana de vulnerabilidades por la que el equipo de analistas de seguridad enviará mediante ITSM-FARO cualquier vulnerabilidad alta o crítica (CVSS > 7.0) que pueda afectar a Madrid Digital, realizando para ello una prueba de concepto para verificar el alcance real de la amenaza y su posible afectación en los sistemas de Madrid Digital.
- Referente al análisis de vulnerabilidades de seguridad de aplicaciones, enumera de manera clara, sencilla y completa la tipología de análisis a realizar (web, móviles y de sobremesa) así como el conjunto de herramientas a utilizar por el analista de seguridad de vulnerabilidades de aplicaciones, del que se menciona su alta cualificación y exclusiva dedicación a Madrid Digital.
- Respecto a los ciberejercicios, propone dos ejercicios de *table-top* y doce ejercicios de *phishing* al año. Plantea una herramienta especializada de formación y concienciación licenciada para 700 usuarios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en relación con lo siguiente:

- En referencia a los ciberejercicios, falta profundidad en la descripción de la solución respecto al equipo de trabajo, los informes de resultados, las fortalezas, debilidades y puntos de mejora correspondientes, la mejora de la comunicación y los planes de respuesta.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

4,8 puntos

3.1.1.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **NOTABLE**, dada la completitud, calidad técnica y buena exposición de los servicios. Las soluciones de identificación de amenazas y vigilancia digital y de análisis de vulnerabilidades son completas y están bien explicadas, aportando elementos diferenciadores. Se indican las herramientas utilizadas en los servicios de identificación de amenazas

y vigilancia digital y ambos servicios de análisis de vulnerabilidades. En el apartado de ciberejercicios, destaca la propuesta de tipos y el calendario de ejecución. Sin embargo, falta detallar la metodología de gestión para cada uno de los servicios, así como aportar detalles sobre el funcionamiento y coordinación del equipo de trabajo asociado a cada servicio. En el caso de los ciberejercicios no se especifica la estimación de horas para cada tipo de ciberejercicio a realizar.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En referencia a la identificación de amenazas y vigilancia digital se aporta una metodología completa, que incluye el seguimiento de las amenazas descubiertas y prioriza las amenazas en función de probabilidad de impacto y gravedad. Las fuentes de inteligencia integradas son diversas y de variada naturaleza. Se incluye la incorporación de IOC's en la MISP y la herramienta seleccionada permite desarrollar adaptaciones de la solución.
- Respecto al análisis de vulnerabilidades de sistemas y redes, se cubre tanto el descubrimiento de activos como el análisis de vulnerabilidades. La solución permite realizar análisis de rutas de ataque asociadas a la superficie de exposición y para la priorización de las vulnerabilidades, además de variables estáticas, se utilizan factores dinámicos como la criticidad del activo para Madrid Digital, el nivel de exposición, la facilidad de explotación, el interés del atacante o la facilidad de descubrimiento de la vulnerabilidad. La metodología de gestión de las vulnerabilidades incluye fases de seguimiento para resolución de las vulnerabilidades encontradas, con soporte experto y una fase de mejora continua con indicadores que permitan incrementar la madurez del servicio. También se explican las herramientas utilizadas y se dan detalles técnicos sobre su funcionamiento.
- El servicio de análisis de vulnerabilidades de aplicaciones se realiza bajo un enfoque de evaluación manual detallada, con la ayuda de la utilización de un conjunto de herramientas, tanto comerciales como arsenal propio, que permiten cubrir aproximadamente el 80% de las tácticas, técnicas y procedimientos (TTP's) incluidas en la matriz *MITRE ATT&CK*. Además, se incluyen planes de pruebas diferenciados para la evaluación de aplicaciones móviles.
- Los ciberejercicios están descritos de forma clara, indicando su tipología, número de ejercicios al año, fases, informes y un calendario propuesto para la realización de los diferentes tipos de ciberejercicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- En general faltan detalles sobre el equipo de trabajo encargado de llevar a cabo las diferentes actividades de cada servicio, así como exponer de manera completa y clara la metodología de gestión y seguimiento de los servicios. En el apartado de ciberejercicios no se especifica la estimación de horas para cada tipo de ciberejercicio.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

4,8 puntos

3.1.1.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **BUENA** debido al aporte de valor de la propuesta de identificación de amenazas y vigilancia digital, donde se incluyen fuentes de inteligencia muy bien posicionadas comercialmente y con gran valía. Tanto en el servicio de identificación de amenazas como en el de análisis de vulnerabilidades de sistemas y redes se indican las herramientas a utilizar para realizar las actividades asociadas al servicio correspondiente. En el apartado de ciberejercicios, se relacionan los tipos de ejercicios a llevar a cabo, propuesta de calendario y elementos diferenciadores a considerar como la grabación de los simulacros para extraer lecciones aprendidas. Sin embargo, hay una limitación de activos a monitorizar en el servicio de identificación de amenazas y vigilancia digital, no se detalla suficientemente el equipo de trabajo en ninguno de los dos servicios de análisis de vulnerabilidades ni en los ciberejercicios. En los servicios de análisis de vulnerabilidades se echa en falta una descripción completa de la metodología de gestión del servicio y en los ciberejercicios faltan detalles sobre la metodología de seguimiento de los ciberejercicios realizados, incluyendo la notificación y seguimiento del estado de resolución de las debilidades encontradas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la identificación de amenazas y vigilancia digital, se incluye una amplia batería de fuentes de inteligencia procedente de diversos orígenes, entre las que se incluyen fuentes de inteligencia muy bien posicionadas comercialmente y con gran aporte de valor. Se incluye una herramienta propia para la gestión de los casos de amenazas, la cual se puede integrar con el SIEM ofertado.
- Se propone que el análisis de vulnerabilidades de sistemas y redes se realice con periodicidad mensual, siendo posible priorizar las vulnerabilidades en función del impacto que puedan tener en el negocio. Se menciona también la herramienta concreta, en nube, que se utilizará para el servicio.
- En cuanto al análisis de vulnerabilidades de aplicaciones, se incluye la posibilidad de realizar simulaciones de ataques de DDoS.
- En cuanto a los ciberejercicios, se especifica el tipo de ciberejercicios a realizar, proponiendo la figura del moderador y grabar el simulacro para hacer sugerencias de mejora. Se incluye un ejemplo de calendario de ejecución para cada uno de los ciberejercicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- En el servicio de identificación de amenazas y vigilancia digital se especifica el número de activos de cada tipo a monitorizar, lo que supone una limitación en la cantidad de activos que se pueden supervisar.
- Con relación al análisis de vulnerabilidades de sistemas y redes falta concretar el equipo de trabajo encargado de realizar todas las tareas indicadas. Tampoco se detalla la metodología de gestión del servicio de forma diferenciada a la metodología de ejecución de los escaneos.

- Sobre el análisis de vulnerabilidades de aplicaciones no se desarrolla la metodología de gestión del servicio ni se concreta el equipo de trabajo. Aparte de los ataques de DDoS, no se detallan otros tipos de pruebas que deben estar incluidas en el alcance.
- En el caso de los ciberejercicios, falta precisar información sobre el equipo de trabajo, estimación de horas de duración de cada tipo de ciberejercicio, así como profundizar en el desarrollo de la metodología de seguimiento del servicio.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.

3,6 puntos

3.1.1.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **ADECUADA** destacando la variedad de fuentes de inteligencia incluidas en el servicio de vigilancia digital, la herramienta a utilizar para el análisis de vulnerabilidades de sistemas y redes y el procedimiento de seguimiento y certificación de las vulnerabilidades. En los ciberejercicios se incluyen varios escenarios de *phishing* y se aporta un ejercicio que complementa los solicitados. Sin embargo, no se aporta la metodología a seguir en el servicio de identificación de amenazas y vigilancia digital ni en el de ciberejercicios. No se especifica un equipo de trabajo dedicado en el análisis de vulnerabilidades de aplicaciones ni en el de ciberejercicios. En el análisis de vulnerabilidades de aplicaciones no se explica detalladamente el proceso de pruebas manuales a realizar ni las herramientas utilizadas. Faltan detalles sobre la estimación de horas de cada tipo de ciberejercicio propuesto.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Sobre la propuesta de identificación de amenazas y vigilancia digital, destacan como aspectos positivos la variedad de fuentes de información y la propuesta para la gestión del ciclo de vida de las amenazas.
- En cuanto al análisis de vulnerabilidades de sistemas y redes, se especifica la herramienta propuesta para el servicio, la cual permite registrar y priorizar las vulnerabilidades, integrada con el SIEM y el SOAR propuestos. Se incluye una fase de seguimiento y validación de las remediaciones asociadas a cada vulnerabilidad descubierta.
- La propuesta de ciberejercicios detalla los diferentes tipos de ciberejercicios a llevar a cabo, incluyendo varios tipos de escenarios de *phishing*, sugiriendo algún ejercicio adicional a los solicitados. Se especifican herramientas a utilizar durante la ejecución de los ciberejercicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- En el servicio de identificación de amenazas y vigilancia digital faltan detalles sobre la metodología a seguir y no se hace mención del equipo de trabajo.
- Con relación al análisis de vulnerabilidades de sistemas y redes falta detallar información sobre el descubrimiento de activos y la base de datos de activos.

- Respecto del análisis de vulnerabilidades de aplicaciones falta profundizar sobre la realización de análisis manuales y las herramientas de pentesting a utilizar en el proceso de realización de las pruebas de seguridad de las aplicaciones analizadas. Tampoco se hace referencia a los detalles sobre el equipo de trabajo.
- Respecto a los ciberejercicios, se echa en falta una explicación más detallada sobre la metodología para la gestión del servicio, la estimación de horas para cada tipo de ejercicio y detalles sobre la composición y cualificación del equipo de trabajo.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.	1,2 puntos
--	-------------------

3.1.1.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **NOTABLE** dado que describe con detalle la metodología y herramientas a utilizar en los ciberejercicios y en el análisis de vulnerabilidades de seguridad de aplicaciones, así como las herramientas a utilizar en el escaneo de vulnerabilidades; sin embargo, no profundiza en la identificación de amenazas y vigilancia digital, identificando únicamente las fuentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Respecto al servicio de identificación de amenazas y vigilancia digital se detallan las fuentes de información desde donde se recogerán los datos a analizar.
- En cuanto al análisis de vulnerabilidades de seguridad de sistemas y redes, describe de manera detallada la gestión de vulnerabilidades y la herramienta de escaneo de vulnerabilidades incluyendo la justificación de cada característica solicitada, además de asegurar su integración con el SIEM y el SOAR propuesto.
- Respecto al análisis de vulnerabilidades de seguridad de aplicaciones se indica una metodología clara de análisis a seguir, que incluye un detalle de las actividades y herramientas a emplear en cada fase y actividad, así como la elaboración de un informe final que recoja de forma completa los resultados obtenidos.
- Detalla de manera clara y concisa los ciberejercicios que se van a realizar, describiendo los distintos escenarios y facilitando la comprensión de estos, así como los informes obtenidos de su ejecución para evaluar el grado de madurez de la organización en materia de ciberseguridad.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- En cuanto a la identificación de amenazas y vigilancia digital, no se hace referencia a los actores intervinientes, tampoco se especifican las actividades de recopilación de IOC's para su integración con la MISP, ni las actividades necesarias para cerrar dominios maliciosos, ni qué metodología y/o procesos se usarán para la gestión del servicio.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.1 – Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios. Hasta 6 puntos.	4,8 puntos
--	-------------------

3.1.2 CRITERIO 7.2 - Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

3.1.2.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **SOBRESALIENTE** debido a que detalla exhaustivamente la arquitectura de la solución, capacidades de conectividad y comunicaciones entre elementos *on-premise* y entre CPD's y nubes, dimensionamiento con capacidad de correlación mejorada con 12 meses de datos online, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de Madrid Digital, detallando librerías de casos de uso de monitorización disponibles ya predefinidos y mapeados con la matriz *MITRE ATT&CK*. Incorpora amplia propuesta de operación, mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, bien posicionada en el cuadrante mágico de Gartner, configurada con capacidad suficiente para soportar 3 terabytes de ingesta diaria y compromiso de asunción de picos que sobrepasen el límite, como mejora ofrece 12 meses de correlación con datos online sin coste adicional.
- Detallada y completa propuesta de arquitectura SIEM en nube, escalable y redundada, de uno de los principales proveedores de soluciones de nube hiperescalares del mercado, que únicamente precisa desplegar *on-premise* recolectores y/o agentes. Todos los elementos de recolección se proveen configurados en alta disponibilidad hardware y software, y se dimensiona para todos los CPD's indicados en el PPT. Se describe en detalle la solución de conectividad y comunicaciones específica, redundada y cifrada para el servicio, tanto para los elementos *on-premise* como para la subida de logs a la nube del servicio e incluso arquitectura de conectividad con otras nubes que alberguen servicios de Madrid Digital. Destaca la capacidad de recolección, ingesta, normalización, enriquecimiento de logs, análisis e investigación que ofrece. Amplia capacidad de integración con multitud de sistemas, fuentes de logs, incluido EPDR actual de Madrid Digital. Integrada con fuentes de datos de inteligencia del fabricante del SIEM, además de otras fuentes comerciales de amplio reconocimiento en el mercado que ofrece sin coste, y con REYES del CCN-CERT. Se oferta también capacidades de aprendizaje automático e inteligencia artificial (IA) continuos y transversales para detectar anomalías y ataques, incorporando modelado de comportamiento de usuarios. Se indica que soporta acceso remoto con capacidades de autenticación con 2FA, SSO y modelado de autorización RBAC.
- Se recoge y describe la capacidad de integración con sistemas de Madrid Digital ITSM-FARO (conector nativo) y LUCIA (herramienta de gestión de incidentes con el CCN-CERT).

- Amplia librería de casos de uso desarrollada por el fabricante del SIEM, a disposición, mapeados con *MITRE ATT&CK*.
- En cuanto a las actividades de operación, mantenimiento, administración y monitorización de la plataforma, se indican las actividades a realizar por el fabricante del SIEM al ser un servicio SaaS y se recogen también las que va a realizar el licitador, centradas en la gestión del ciclo de vida de fuentes de datos y casos de uso, y soporte centralizado.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

10 puntos

3.1.2.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **SOBRESALIENTE** debido a que detalla exhaustivamente la arquitectura de la solución, capacidades de conectividad y comunicaciones de forma completa, dimensionamiento, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y con sistemas de *ticketing* requeridos, aportando completa librerías de casos de uso de monitorización predefinidos y mapeados con la matriz *MITRE ATT&CK*. Incorpora amplia propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, muy bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, configurada con capacidad suficiente para soportar 3 Terabytes de ingesta diaria, tres meses de retención en caliente y 12 meses de almacenamiento para búsquedas en frío, sin restricción ni pérdida de eventos en picos de tráfico. Se indica que los logs de Microsoft 365 y Azure, así como las alertas de productos de seguridad no tienen coste.
- La arquitectura SIEM se presenta profusamente descrita, destacando su propuesta de despliegue automático en nube de unos de los principales proveedores hiperescalares cloud del mercado, requiriendo únicamente *on-premise* despliegue de recolectores de eventos y/o agentes. Se indica que también se contará con recolectores en nube para ingesta de logs de otras nubes. Se incluye descripción y dimensionamiento hardware y software de los recolectores a desplegar en los CPDs requeridos, incluyendo su redundancia. Destaca el detalle de la solución de conectividad de elementos *on-premise* y de ingesta en nube, indicando tipología de redes, conexiones a utilizar, capacidad y redundancia, asegurando que esta conectividad llegue a todos los CPD's requeridos. Los procesos de recolección, ingesta, correlación, análisis y respuesta que ofrece el SIEM se detallan y relacionan. Asegura integración con multitud de fuentes de datos de eventos que enumera y detalla forma de integración. Ofrece integración con fuentes de inteligencia y oferta integración con fuente comercial reconocida sin coste. Capacidades disponibles de IA transversales a la plataforma para análisis de anomalías, amenazas y ayuda al modelado de casos de uso. Se indica que soporta acceso remoto con capacidades de autenticación con 2FA, SSO y modelado de autorización RBAC.

- Se recoge y describe la capacidad de integración con sistemas de Madrid Digital ITSM-FARO LUCIA y MISP existen en Madrid Digital.
- Extensa librería de casos de uso desarrollada por el fabricante del SIEM, a disposición, basados en *MITRE ATT&CK* complementados con casos de uso base de monitorización que ofrece el SIEM.
- En cuanto a las actividades de operación, mantenimiento, administración y monitorización de la plataforma, se indica las actividades a realizar por el fabricante de la solución SaaS, indicando que en todo caso el licitador lo asume como servicio gestionado, recogiendo las tareas que realizará de monitorización, mantenimiento y salud de la plataforma de forma continua, todo ello organizado en 5 fases.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

10 puntos

3.1.2.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **NOTABLE** debido a la arquitectura de la solución, dimensionamiento mejorado de ingesta excepcional, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de *ticketing*, amplia propuesta de casos de uso de monitorización predefinidos y mapeados con la matriz *MITRE ATT&CK*; sin embargo, no desarrolla la arquitectura de recolectores ni la solución de conectividad de elementos *on-premise* ni de subida de logs a la nube.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, muy bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, configurada con capacidad suficiente para soportar hasta 5 Terabytes de ingesta diaria (2 más de los requeridos), tres meses de retención en caliente y 12 meses offline, sin restricción y con soporte de picos de tráfico. Se indica que los logs de Microsoft 365 y Azure, así como las alertas de productos de seguridad no tienen coste.
- La arquitectura propuesta de SIEM se aloja en nube de uno de los principales proveedores hiperescalares de soluciones en nube y no requiere ninguna instalación de componentes en CPD's a excepción de capa de recolección compuesta por recolectores y agentes *on-premise* y recolectores en nube. Se garantiza el cifrado de toda la información, en tránsito, reposo y almacenada. Capacidades de ingesta automatizada, integración, filtrado y enriquecimiento con información de contexto de los logs. Integración con multitud de fuentes de datos de eventos. e integración con fuentes de inteligencia y oferta integración con fuente comercial reconocida sin coste. Capacidades disponibles de IA transversales a la plataforma, aporte de IA tipo copiloto, asistente inteligente para análisis de anomalías y casos de uso. Se indica que soporta acceso remoto con capacidades de autenticación con 2FA, SSO y modelado de autorización RBAC.
- Se recoge y describe la capacidad de integración con sistemas de Madrid Digital ITSM-FARO y LUCIA mediante API y conectores específicos.

- Amplia librería de casos de uso desarrollada por el fabricante, a disposición, basados en *MITRE ATT&CK*.
- En cuanto a las actividades de operación, mantenimiento, administración y monitorización de la plataforma, se indica las actividades a realizar por el fabricante de la solución SaaS, y también se indica las tareas a realizar por parte del licitador desarrollando tareas de soporte y administración.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detalla la solución de comunicaciones para la interconexión de CPD's y para la subida a las nubes de la información de eventos. Solo se indica la tecnología utilizada sin aportar detalle de arquitectura de conectividad por cada CPD, ni número, capacidad, redundancia de las líneas necesarias. Adicionalmente no se especifica la arquitectura, dimensionamiento y capacidad de los recolectores.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

8 puntos

3.1.2.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **BUENA** destacando de su oferta la completa descripción de los módulos de su arquitectura de plataforma SIEM, dimensionamiento, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de *ticketing*, amplia propuesta de librerías de casos de uso de monitorización disponibles predefinidos y mapeados con la matriz *MITRE ATT&CK*; sin embargo, la solución SIEM carece de posicionamiento en los cuadrantes de Gartner y Forrester, no se ha descrito la arquitectura de los recolectores, la solución de conectividad está poco detallada y la propuesta de operación, mantenimiento y monitorización no está desarrollada.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Proponen una plataforma SIEM en modalidad SaaS desplegada en nube privada del licitador, y configurada para asumir la capacidad requerida y absorber picos de ingesta sin pérdida de servicio. Como valor diferencial se indica que la solución SIEM no tiene coste por producto, por licenciamiento de solución.
- Se detallan los módulos de la arquitectura de la plataforma: módulo de gestión, normalización y almacenamiento, módulo de correlación que proporciona inteligencia, motor de correlación, consola de gestión de eventos e incidentes y módulo de cuadros de mandos. Se indica que se instalaran 4 recolectores en los CPDs, todos redundados, sin indicar información de arquitectura. También se dispone de agente para instalar en endpoints y recolectar información de seguridad. Integrada con fuentes de datos de inteligencia del múltiples feeds públicos, además de otras fuentes comerciales de amplio reconocimiento en el mercado, y con REYES del CCN-CERT. Permite una correlación en tiempo real de logs, flujos de red y vulnerabilidades, utilizando algoritmos de inteligencia artificial y aprendizaje automático, con enriquecimiento de

contexto. Dispone de capacidades de detección de anomalías en logs basada en el análisis de registros de eventos generados por sistemas y aplicaciones, mediante técnicas de procesamiento de lenguaje natural y algoritmos de Machine Learning. Posee capacidades UEBA de análisis de comportamiento. Disponible módulo SOAR e Integración nativa con SIEM. Se indica que soporta acceso remoto con capacidades de autenticación con 2FA, SSO y modelado de autorización RBAC

- Se describe y detalla la integración con ITSM-FARO (vía API) y LUCIA (integración bidireccional).
- Incorpora más de 200 casos de uso específicos de seguridad y más de 700 reglas de correlación, clasificadas según la matriz *MITRE ATT&CK*. Es de destacar también la prolija lista de fabricantes por tipología de fuentes de eventos que soporta.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- La solución SIEM no está en los cuadrantes de Gartner y de Forrester, carece de posicionamiento en ellos.
- Respecto a la arquitectura, no se detalla la solución de comunicaciones para la interconexión de CPD's y para la subida a las nubes de la información de eventos, solo se menciona una línea de conexión. Tampoco se indica cómo está previsto conectar y poder acceder a los logs de M365 (Office365) y a otros servicios de Madrid Digital que estén en nube. Por último, respecto a los recolectores no se describe su arquitectura, ni software ni hardware.
- Escasa y generalista propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes, solo se detalla los horarios de soporte de consultas e incidencias (en este caso 24x7) y las vías de acceso (portal, web, teléfono, mail).

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

6 puntos

3.1.2.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **SOBRESALIENTE** debido a que detalla exhaustivamente la arquitectura de la solución, dimensionamiento, escalado, solución completa de comunicaciones y conectividad, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas, y librerías de casos de uso de monitorización disponibles ya predefinidos y mapeados con la matriz *MITRE ATT&CK*. Adicionalmente describe en detalle el modelo de operación, mantenimiento, administración y monitorización.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, configurada con capacidad suficiente para soportar 3 Terabytes de ingesta diaria, tres meses de retención en caliente y 12 meses de almacenamiento para búsquedas en frío, sin restricción ni pérdida de eventos en picos de tráfico.

- La arquitectura propuesta consta de una capa intermedia de recolección, muy potente, que incluye el archivado de todos los eventos sin tratar en nube de uno de los principales hiperescalares del mercado, el enriquecimiento con información de contexto de los logs mediante su tratamiento en la nube del proveedor y una CMDB confiable de activos generada a partir de la información recogida, y una capa de centralización, análisis y correlación de eventos de seguridad propiamente dicha, que recoge para su procesamiento los logs enriquecidos. Esta solución de recolección reduce el nº de equipos a instalar *on-premise* frente a la solución nativa del SIEM propuesto. Todo el equipamiento local se despliega en alta disponibilidad. Se detalla la solución de conectividad *on-premise*, la necesaria para la subida de información a la nube y con otras nubes. Integrada con fuentes de datos de inteligencia del fabricante del SIEM, además de otras fuentes comerciales de amplio reconocimiento en el mercado, y con REYES del CCN-CERT. Capacidades de aprendizaje automático para la detección de anomalías, prevención de eventos y detección de anomalías en el rendimiento y en el comportamiento operativo. La solución facilita también capacidades para la mejora de la gestión de alertas y detección de amenazas basadas en la gestión del riesgo y capacidades transversales de inteligencia artificial (IA) a través de una plataforma complementaria a la funcionalidad principal de SOAR ofertada, para mejora de las tareas de ingesta, personalización de casos de uso o normalización de datos, entre otras actividades.
- Se detalla la integración con ITSM-FARO y LUCIA vía API.
- Amplia librería de casos de uso desarrollada por el fabricante, a disposición, basados en *MaGMA* y *MITRE ATT&CK*, ordenados por categoría. La oferta recoge casos de uso y fuentes de eventos más comunes aportando ejemplos concretos de posibles casos a implementar.
- En cuanto a las actividades de operación, mantenimiento, administración y monitorización de la plataforma, se destaca que en un modelo SaaS se elimina una gran parte de las actividades de gestión que quedan cubiertas por el fabricante, obteniendo un SLA de tiempo de actividad del 100%. También se listan y describen las tareas de monitorización, mantenimiento y salud de la plataforma a realizar por el licitador.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

10 puntos

3.1.2.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA** debido a que oferta una solución de SIEM en modalidad SaaS bien posicionada en el mercado, que centraliza todas las actividades de recogida, enriquecimiento y proceso, detección de anomalías, respuesta a incidentes y vulnerabilidades; sin embargo, no concreta varios aspectos de la arquitectura propuesta como son el equipamiento y las comunicaciones a instalar en los CPD's objeto del servicio, las capacidades de integración con sistemas de Madrid Digital, la información detallada de librerías de casos de uso propuestas, ni se especifica la propuesta de operación, mantenimiento y administración de la plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma bien posicionada en los cuadrantes de Gartner y Forrester, desplegada en modalidad SaaS en la nube de uno de los principales hiperescalares del mercado, que concentra en una única arquitectura el análisis de registros de sucesos, flujos de red, paquetes de red, vulnerabilidades, usuarios y datos de activos, configurada para soportar 3 Terabytes de ingesta diaria, tres meses de almacenamiento en caliente y 12 meses de almacenamiento de datos más antiguos. La plataforma consta de una capa de recogida de información compuesta por sondas y agentes instalados en los diferentes servidores, y una capa de proceso en la nube.
- La plataforma integra la gestión de sucesos e información de seguridad, la gestión de registros, la detección de anomalías, la investigación y respuesta a incidentes y la gestión de la configuración y de las vulnerabilidades, disponiendo también de un motor avanzado de detección de amenazas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detalla el comportamiento de la plataforma frente a picos de ingesta, los elementos concretos a instalar en los CPD's ni la infraestructura de comunicaciones propuesta para la subida de datos a la nube. Se describen las capacidades UBA (*User Behavior Analytics*) de la plataforma de forma completa pero no se mencionan capacidades específicas de inteligencia artificial. Tampoco queda claro la propuesta de integración de fuentes de inteligencia de amenazas en la plataforma, recogiendo fuentes disponibles en el SOC del licitador.
- No se mencionan capacidades específicas de la plataforma de integración con FARO y LUCIA, recogiendo únicamente el compromiso de realizarlo, y para el caso de LUCIA, alojarlo en la infraestructura IaaS centralizada propuesta para el servicio.
- Dispone de librerías de casos de uso mapeados con la matriz *MITRE ATT&CK*, pero no se facilita detalle de la cantidad o tipología de los casos predefinidos.
- Tampoco se detallan actividades de operación, mantenimiento, administración y monitorización a realizar en la plataforma.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

2 puntos

3.1.2.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **ADECUADA** debido a que la solución SaaS ofertada está bien posicionada en el mercado y el diseño de arquitectura propuesto es conforme con los requisitos mínimos exigidos; sin embargo, no concreta aspectos importantes como la infraestructura local a instalar en los CPD's objeto del servicio, las capacidades avanzadas de la plataforma en materia de IA, *Machine Learning* o UEBA, la estrategia y tipología de casos de uso de monitorización a definir, ni menciona cómo se va a operar, mantener y monitorizar la plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, configurada para asegurar que no hay pérdida de eventos en picos de tráfico, compuesta por una capa de recolección *on-premise* e integraciones nativas vía API para la recolección de datos en la nube.
- Todos los elementos de la plataforma cuentan con medidas de redundancia ante fallos, ofreciendo cifrado TLS para el acceso de usuarios y transmisión de datos, autenticación SSO con el directorio corporativo y modelo de control de acceso basado en roles. La arquitectura de la plataforma permite un crecimiento modular y progresivo, asegurando su escalabilidad. Integra fuentes de inteligencia de amenazas propios del licitador, integraciones ya desarrolladas con las fuentes de datos más habituales y desarrolla de forma adecuada la propuesta de monitorización integral proactiva de todos los componentes, y tareas específicas de ajustes de la plataforma, afinado de casos de uso y revisión de rendimiento, capacidad y funcionalidades.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- La descripción del equipamiento local para recogida de información es muy somera, limitándose a indicar el número de appliances locales previstos, sin detallar capacidad, ni estrategia de alta disponibilidad. No se menciona tampoco la infraestructura de comunicaciones prevista para el envío de información a la capa de procesamiento en nube ni cómo se ingestará la información de nubes de hiperescalares habituales del mercado.
- Se recoge que la plataforma dispone de capacidades avanzadas de inteligencia de amenazas, análisis de usuario y entidad, detección de anomalías basadas en machine learning, o investigación guiada, sin aportar detalle suficiente que permita su valoración. Tampoco se recoge la propuesta de integración de la solución con la plataforma ITSM-FARO de Madrid Digital.
- Se pone a disposición un catálogo de casos de uso propios del licitador, sin detallar tipología de los mismos.
- Tampoco se detallan actividades de operación, mantenimiento, administración y monitorización a realizar en la plataforma.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.	2 puntos
---	-----------------

3.1.2.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **NOTABLE** proponiendo una plataforma ajustada a los requisitos del pliego, con capacidad adicional sin coste para logs de eventos en nube de Microsoft365, solución de conectividad *on-premise* y con nube especificada, aportando diseño detallado de la

infraestructura de recolección prevista, fuentes de datos de eventos y capacidades avanzadas de la plataforma relacionadas con IA, *Machine Learning* o UEBA, complementado con propuesta de valor de reutilización de la plataforma actual para copia de logs; sin embargo, no presenta la propuesta de integración con los sistemas de *ticketing* recogidos (FARO y LUCIA), y aunque menciona actividades de operación y mantenimiento, no especifica soporte y monitorización.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, desplegada en la nube de uno de los principales hiperescalares existentes, bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, que se oferta con capacidad para recolectar y procesar todos los logs de eventos en nube de Microsoft365 sin coste adicional.
- Se desarrolla pormenorizadamente la solución propuesta para la recolección de los datos a tratar, mediante instalación de agentes en servidores y colectores en cada CPD cuyo dimensionamiento se especifica; la arquitectura de conexión; el canal de comunicaciones mediante línea dedicada y privada en alta disponibilidad entre el SIEM y los CPD's, y el cifrado de datos tanto en tránsito como en reposo con control de acceso basado en roles. Se ofrece como mejora la posibilidad de realización de copias de los eventos en sistemas *on-premise*, proponiendo reutilizar la plataforma actual del SIEM para este cometido. Destaca de la descripción de la plataforma, el soporte amplio de fuentes de eventos, el uso de soluciones de IA generativa integrada para ampliar las capacidades de análisis y respuesta a incidentes, además de capacidades de correlación automática de casos para ataques no conocidos y detección de anomalías, y capacidades UEBA para análisis de comportamiento de usuarios y entidades, detección de amenazas y anomalías. El diseño contempla la integración como fuente de inteligencia de amenazas la propia del fabricante e información de la MISP del licitador.
- Se pone a disposición del proyecto completa biblioteca de casos de uso desarrollados por el proveedor, además de la colección de reglas analíticas y búsquedas de *hunting* predefinidas por el fabricante.
- La propuesta de operación, mantenimiento y administración remota se limita a indicar el ciclo de incorporación de fuentes de eventos y casos de uso.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detalla las capacidades de integración con FARO y LUCIA y no se especifica las actividades de monitorización, soporte ni gestión de incidencias.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

8 puntos

3.1.2.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **NOTABLE** proponiendo una plataforma bien posicionada en el mercado, detallando claramente los elementos a instalar en modo local, capacidades de integración de fuentes correlación de eventos, biblioteca de casos de uso disponibles, capacidades avanzadas de inteligencia artificial, aprendizaje automático y análisis de comportamiento de usuarios y entidades; sin embargo, no concreta el dimensionamiento propuesto de la infraestructura de comunicaciones que se instalará para envío de los datos a la nube ni detalla la propuesta de operación, mantenimiento y administración.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, desplegada en la nube de uno de los principales hiperescalares existentes, bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, sin límite diario de ingesta, escalable y bien dimensionado con 3 meses en caliente y 12 de archivado.
- Se describen de forma completa las posibilidades ofrecidas por la plataforma en el apartado de ingesta de datos mediante agentes recolectores instalables en servidores, conexiones nativas y máquinas dedicadas, disponiendo de multitud de conectores oficiales, ya desarrollados, y detallando en la solución las fuentes de eventos y formatos de flujo soportados y el método de recolección idóneo para cada fuente. Se identifican los elementos a desplegar en cada uno de los CPD's requeridos en alta disponibilidad, y la solución de comunicaciones propuesta, para el envío de fuentes de eventos o logs *on-premise* a la nube. Accesos a la plataforma, basada en roles RBAC, modelo de delegación de permisos potente basado en la premisa de mínimo privilegio en el acceso a los recursos, y mecanismos de seguridad mediante autenticación MFA. La plataforma permite la correlación histórica de eventos contra indicadores de compromiso y reglas nuevas, así como la correlación automática mediante técnicas de inteligencia artificial y capacidades de detección de anomalías basadas en tiempo real o estacionales, y algoritmos de aprendizaje automático (*Machine learning*) para modelar el comportamiento habitual de entidades y usuarios (UEBA). Se oferta también la utilización de IA generativa integrada en la plataforma.
- Detalla biblioteca de casos de uso desarrollados por el proveedor, además de la colección de reglas analíticas y búsquedas de *hunting* predefinidas por el fabricante. Todos los casos de uso se mapean sobre el framework *MITRE ATT&CK* para su categorización.
- Extensa descripción de las capacidades de integración con FARO y LUCIA a través de API propia de estos sistemas y del que ofrece el SIEM, aportando gráfico conceptual.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se presenta dimensionamiento detallado de las comunicaciones a instalar en cada uno de los CPD's objeto del servicio y se aporta escasa información sobre las actividades de operación, administración y monitorización de la plataforma, que se limita a enumerar lo que realizará el fabricante del SIEM, y solo especificando que realizará monitorización 24x7.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

8 puntos

3.1.2.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **BUENA** destacando de su oferta de plataforma SIEM en modalidad SaaS su descripción precisa del equipamiento local *on-premise* a instalar, las capacidades de la plataforma relacionadas con la integración de fuentes de eventos, aprendizaje automático, incorporación de inteligencia artificial en el proceso, o análisis de comportamiento; sin embargo, no concreta la propuesta de integración de la plataforma con los sistemas de *ticketing* de Madrid Digital, se valora de forma negativa no disponer de un catálogo de fuentes de inteligencia de amenazas más amplio y falta concretar y detallar la propuesta de operación, mantenimiento, y administración .

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Proponen una plataforma SIEM en modalidad SaaS desplegada en nube de uno de los principales hiperescalares del mercado, bien posicionada en el cuadrante mágico de Gartner y en el informe de Forrester, y configurada para asumir la capacidad requerida y absorber picos de ingesta sin pérdida de servicio.
- Respecto a la arquitectura, se detalla de forma precisa y completa la propuesta de capa de recolección de los diferentes logs, especialmente los localizados *on-premise*, así como el equipamiento a instalar, en alta disponibilidad, y las opciones y propuesta concreta de infraestructura de comunicaciones y dimensionamiento para envío de los datos a la nube donde se alojará el SIEM. La comunicación con otros hiperescalares no requerirá provisión de infraestructura en Madrid Digital. Permite una correlación en tiempo real de logs, flujos de red y vulnerabilidades, utilizando algoritmos de inteligencia artificial y aprendizaje automático para modelado de comportamiento de usuario y entidades, y detección de desviaciones y anomalías. Facilita también *frameworks* específicos para la identificación de incidentes destacables, correlación de activos e identidades, consumo y gestión de feeds de amenazas, gestión de perfil de riesgo de usuarios y activos, o ejecución de acciones preconfiguradas.
- Más de 900 fuentes predefinidas de datos a ingestar, disponibilidad de librería de casos de uso del fabricante alineados con el esquema *MITRE ATT&CK*.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se especifica la propuesta de integración de la plataforma con la herramienta de *ticketing* ITSM-FARO, proponiendo la utilización de una herramienta de *ticketing* distinta para uso interno del servicio.
- Únicamente se menciona que la solución viene con listas de inteligencia públicas y gratuitas integradas en la plataforma sin especificar cuales, estando previsto a corto plazo la incorporación de fuente comercial que se menciona sin especificar valor.

- Respecto a la propuesta de operación mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes, se menciona herramienta propia de monitorización y centralización de análisis y respuesta, no especificando procesos y actividades.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

6 puntos

3.1.2.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, - S.L.U** a este criterio se considera **SOBRESALIENTE** debido a que detalla la arquitectura de la solución, infraestructura de conectividad *on-premise* y en nube, dimensionamiento con capacidad de correlación mejorada, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de *ticketing*, amplia librerías de casos de uso de monitorización ya predefinidos y mapeados con la matriz *MITRE ATT&CK*, aportando descripción detallada de las capacidades de operación, administración y monitorización.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plataforma SIEM en modalidad SaaS, bien posicionada en el cuadrante mágico de Gartner, configurada con capacidad suficiente para soportar 3 Terabytes de ingesta diaria, soportando incremento de picos de ingesta sin afectar al rendimiento, y como mejora ofrece 12 meses de correlación con datos online sin coste adicional.
- Detallada y completa propuesta de arquitectura SIEM en nube, escalable y redundada, de uno de los principales proveedores de soluciones de nube hiperescalares del mercado, que únicamente precisa desplegar *on-premise* recolectores y/o agentes. Todos los elementos de recolección se proveen configurados en alta disponibilidad. Propuesta completa de conectividad *on-premise* y en nube. Destaca la capacidad de recolección, ingesta, normalización, enriquecimiento de logs, análisis e investigación que ofrece. Amplia capacidad de integración con multitud de sistemas, fuentes de logs, especificando los sistemas actuales de Madrid Digital. Integrada con fuentes de datos de inteligencia del fabricante del SIEM, además de otras fuentes comerciales de amplio reconocimiento en el mercado que ofrece sin coste, y con REYES del CCN-CERT. Se oferta también capacidades de aprendizaje automático e inteligencia artificial (IA) continuos y transversales para detectar anomalías y ataques, incorporando modelado de comportamiento de usuarios. Se indica que soporta acceso remoto con capacidades de autenticación con 2FA, y capacidades de federación con IdP de terceros que admitan *OpenID Connect*, *Okta* o *SAML 2.0*.
- Descrita integración con ITSM-FARO y LUCIA. Se prevé la integración de ITSM-FARO con sistema interno de incidencias y peticiones JIRA.
- Amplia librería de casos de uso desarrollada por el fabricante del SIEM, a disposición, basados framework *MaGMA* y en *MITRE ATT&CK* que se presentan mapeados y explicados.

- En cuanto a las actividades de operación, mantenimiento, administración y monitorización de la plataforma, se recoge que la UTE realizará todas las actividades de soporte especificando acciones, parcheo, mantenimiento, monitorización de disponibilidad y salud, gestión de incidencias y consultas. Respecto a la solución SaaS SIEM se indica que es el fabricante el que supervisa su rendimiento, siendo supervisado a su vez por la UTE.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.2 – Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM. Hasta 10 puntos.

10 puntos

3.1.3 CRITERIO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

3.1.3.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **NOTABLE**, ya que describe de forma idónea y completa la plataforma propuesta. La herramienta está bien posicionada dentro del último cuadrante de Forrester de soluciones de análisis y visibilidad de red, es escalable y permite la automatización. Detalla las medidas de disponibilidad, continuidad y las capacidades de integración. Sin embargo, no propone de forma clara la propuesta de operación y mantenimiento de la plataforma ni desarrolla ejemplos de casos de uso de monitorización.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación con la arquitectura, en lugar de implementar cientos de sensores en toda la red, la solución se basa en agregar y analizar la telemetría de la red para convertirla en un sensor en sí misma. La propuesta combina la inspección profunda de paquetes mediante detección basada en firmas con otras técnicas de análisis de comportamiento de tráfico, inteligencia de amenazas, machine learning e inteligencia artificial, para análisis del tráfico cursado sin necesidad de descifrado, así en la detección la detección de ataques desconocidos (zero-day). Integra como fuente de inteligencia de amenazas la propia del fabricante.
- Detalla adecuadamente las capacidades de integración con otras herramientas. La solución se puede conectar con el SIEM a tres niveles: sondas, NDR local y sistema XDR, puesto que dispone de conectores nativos para ello. La filosofía propuesta para el proyecto se basa en convertir al sistema XDR en el elemento principal de la detección de anomalías de red.
- El sistema propuesto permite obtener telemetría de las nubes (Azure, AWS, GCP) sin necesidad de desplegar sondas. Además, se detalla que el dimensionamiento HW proporcionado permite un crecimiento de hasta el 30% solamente aumentando el licenciamiento, sin cambios en la infraestructura desplegada, lo que garantiza la escalabilidad y disponibilidad del servicio, además de no descartar tráfico en caso de superación puntual del licenciamiento. La solución está dimensionada para permitir un almacenamiento de hasta 3 meses de los datos en bruto de capturas de tráfico y otros elementos de análisis, para fines forenses.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta concreción en la propuesta de operación y mantenimiento de la plataforma: soporte hardware y software de la plataforma, actualizaciones y parches de producto, gestión de incidencias, cambios, parches y actualizaciones, control de acceso, usuarios y permisos, etc.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.	6,4 puntos
---	-------------------

3.1.3.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **NOTABLE**, ya que describe de forma idónea y completa la plataforma propuesta, siendo una de las soluciones líder en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. La solución permite automatización, se detalla en profundidad la propuesta de operación y mantenimiento, y se recogen de forma clara las medidas de disponibilidad, escalabilidad, rendimiento, funcionalidad y cumplimiento normativo de la solución; sin embargo, no propone casos de uso de monitorización del servicio ya desarrollados.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la plataforma propuesta, está diseñada para manejar volúmenes de datos de red de hasta 100 Gbit/s garantizando así el crecimiento de la solución. Como características diferenciadoras, destaca su potencia en la monitorización en tiempo real de más de 90 protocolos diferentes incluyendo protocolos de Microsoft. Posibilita el descifrado pasivo de esquemas complejos de cifrado, como TLS v1.3 con PFS y protocolos de Microsoft e integra fuentes de inteligencia contextual de reconocido prestigio además de la propia del fabricante. Como valor añadido, detalla que la solución permite almacenar los datos más recientes en el disco de los sensores o en *Data Lakes* externos. Esta configuración facilita la investigación diaria de incidentes, y permitiendo extender el almacenamiento de datos durante periodos de retención más prolongados o para otros casos de uso, solamente aumentando el licenciamiento, sin cambios en la infraestructura desplegada.
- En relación con la disponibilidad, la solución propuesta de sensores es robusta, implementándose fuera de banda para la recopilación pasiva del tráfico de red para su análisis. Cualquier fallo no tendrá impacto en la disponibilidad para los usuarios finales ni en las operaciones del negocio. Están dimensionados para asumir 5 Gbit/seg adicionales de throughput sobre los requisitos iniciales, para evitar la pérdida de eventos.
- En cuanto a automatización, hay que destacar que, adicionalmente a las reglas *Snort/Yara*, se pueden crear detecciones personalizadas en su lenguaje de triggers basado en *Javascript*. Un estándar que, según indica, es más sencillo y flexible que implementar reglas YARA.
- Describe con detalle la propuesta de operación y mantenimiento, garantizando el funcionamiento óptimo de la plataforma NDR durante la totalidad del contrato. También indica cómo realizar una evolución de las capacidades de la misma.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No se detalla la librería de casos de uso que cubre la solución.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

6,4 puntos

3.1.3.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **BUENA**; en términos generales plantea una solución clara y una arquitectura correcta, basada en una herramienta bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. Se detallan características enfocadas a la disponibilidad, escalabilidad y automatización. Sin embargo, no desarrolla la librería de casos de uso para su utilización ni describe la propuesta de operación y mantenimiento.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la arquitectura, propone una consola en cloud que unifica todas las sondas en un único punto de acceso. La solución propuesta se licencia por tráfico procesado, en lugar de por activo protegido, conservando los metadatos de red enriquecidos durante 365 días, para investigaciones posteriores. Estos datos garantizan que las herramientas, tácticas y procedimientos descubiertos puedan investigarse retroactivamente para descubrir si las amenazas pueden haberse infiltrado en la red del cliente y cuándo. La captura de tráfico se realizará a través de los puertos de las sondas físicas ofertadas y que aparecen en la arquitectura en los CPDs, y a través del despliegue de máquinas virtuales (sin límite), en la parte de infraestructura desplegada en hiperescalares.
- En relación con la disponibilidad y escalabilidad, indica que se dispone de mecanismos para evitar la pérdida de eventos en caso de superación puntual de la capacidad máxima soportada o licenciada, no cortando el análisis cuando puntualmente se producen excesos de throughput licenciado. Además, menciona que tiene la posibilidad de configuración independiente de detección en cada sensor, permitiendo realizar una configuración multitenant, repartiendo los sensores en cada tenant para poder tener reglas de detección diferentes para cada grupo de sensores.
- Referente a la integración con otros sistemas, la solución se integra con los SIEM/SOAR más desplegados del mercado, y, para el caso de Madrid Digital, indica que se integra de forma nativa con ellos mediante conectores API y creación de resources groups.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No detalla el uso de casos de uso para monitorización del servicio.
- A pesar de indicarse que la solución está basada en nube, apoyada por un despliegue de sondas físicas y virtuales, no se desarrolla la propuesta de operación y mantenimiento de la misma.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

4,8 puntos

3.1.3.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **SOBRESALIENTE**, ya que describe de forma idónea y completa la plataforma propuesta, incluyendo un esquema de arquitectura claro. La solución es escalable y permite la automatización, estando la herramienta propuesta bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. Se detallan perfectamente las medidas de disponibilidad y continuidad y las librerías de casos de uso de monitorización ya desarrollados. La oferta recoge de forma clara y completa la propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación con la plataforma y arquitectura, indica que las sondas propuestas superan la capacidad de rendimiento prevista, llegando a una capacidad de procesamiento de hasta 50Gbps. La solución no necesita descifrar tráfico SSL/TLS para la detección de ataques, sino que utiliza técnicas de IA para la identificación de comportamientos maliciosos. Los algoritmos de IA aplicados no necesitan aprender de la red, ya que están previamente entrenados en las TTP's utilizadas comúnmente por los atacantes, aspecto que mejora los tiempos de despliegue y puesta en funcionamiento y reduce los falsos positivos. La solución monitoriza tráfico este-oeste y norte-sur identificando múltiples comportamientos de atacantes, como movimientos laterales asociados a técnicas *live off the land* como: ejecución remota sospechosa, escritorio remoto sospechoso, administración sospechosa, *port knocking/hijacking*, replicación automatizada, fuerza bruta, fuerza bruta SMB, fuerza bruta Kerberos y actividad de *ransomware*.
- En cuanto a la disponibilidad, el licenciamiento se basa en el número de IP's, pero la plataforma seguirá funcionando incluso si se excede el número máximo de IP's soportadas.
- Describe con detalle el proceso de mantenimiento, administración y operación de la plataforma describiendo las principales tareas en las que consistirá el proceso: revisión y comprobación del estado de la plataforma, comprobación de actualizaciones, comunicación, resolución de incidencias, etc.
- Respecto a los casos de uso, se ponen a disposición más de 100 modelos de detección y casos de uso que abordan una amplia variedad de ataques y comportamientos anómalos en la red. Incluyen una breve descripción de los principales ejemplos.
- Referente a las integraciones con otros sistemas, el servicio se integra con la solución SIEM propuesta y con capacidades y herramientas adicionales que se consideren necesarias, tales como herramientas del CCN-CERT que puedan desplegarse en el caso de incidentes críticos para el análisis de compromisos por APT.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

8 puntos

3.1.3.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **NOTABLE**, ya que describe de forma idónea y completa la plataforma propuesta, incluyendo un esquema de arquitectura muy claro que facilita su comprensión. La solución está bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red, es escalable y permite la automatización. Se describen perfectamente las medidas de disponibilidad y continuidad y las capacidades de integración de la solución con otras plataformas y servicios. En el apartado de casos de uso de monitorización, se aporta una tabla muy completa con ejemplos de casos. Sin embargo, la propuesta no describe las actividades de operación y mantenimiento.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la plataforma y arquitectura, indica que la solución no necesita descryptar los datos para su análisis utilizando técnicas de IA para identificar comportamientos maliciosos. Se destaca que los modelos de detección mediante IA aplican a todos los dispositivos conectados a la red interna del cliente (cualquier sistema operativo, BYOD, IOT), asegurando toda la infraestructura, física y virtual. Además, la solución propuesta es la que dispone de más patentes referenciadas en D3FEND, siendo el único proveedor de NDR que cuenta con detecciones de network.
- Respecto a las medidas de continuidad del servicio, hace especial mención a la capacidad de la solución para gestionar el entorno de sondas IDS actuales de Madrid Digital. Indica que la solución de IDS está soportada de forma nativa, pudiéndose desplegar como microservicio en las propias sondas, lo que hace especialmente ágil la migración de las sondas actuales. Además, añade que ofrece capacidades mejoradas para la detección y la respuesta mediante la incorporación del contexto de la firma de detección de intrusos, para una búsqueda e investigación de amenazas más eficiente y efectiva.
- Respecto a la escalabilidad, la plataforma no tiene limitaciones en arquitectura para la escalabilidad de activos a monitorizar. En cuanto a la disponibilidad, aunque menciona que las soluciones NDR habitualmente no se despliegan en HA, debido al gran volumen de tráfico, para dotar de alta disponibilidad al servicio de monitorización se propone varias alternativas.
- Presenta una tabla con numerosos casos de uso cubiertos, clasificados según el tipo de técnica avanzada usada por los atacantes. Destaca que la solución identifica de forma determinista las técnicas fundamentales de un ciberataque como el uso de herramientas de acceso remoto, túneles ocultos, comportamientos de botnet y herramientas de reconocimiento gracias a modelos de IA entrenados, independientemente de que sea un comportamiento anómalo.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No describe las actividades de operación y mantenimiento de la plataforma.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

6,4 puntos

3.1.3.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **BUENA**, ya que se describe de forma adecuada la arquitectura de la solución propuesta. La herramienta está bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. Se detallan las medidas de disponibilidad y escalabilidad y se mencionan las capacidades de integración. Sin embargo, no propone casos de uso de monitorización ni se define una propuesta de operación y mantenimiento de la plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En cuanto a la arquitectura, la solución propuesta se licencia por tráfico procesado en lugar de por activo protegido y conserva los metadatos de red enriquecidos durante 365 días, para investigaciones posteriores. La combinación de investigación automatizada en tiempo real de los incidentes de seguridad de la red y la visibilidad histórica ampliada facilita una respuesta más rápida y completa a las amenazas. La captura de tráfico se realiza a través de los puertos de las sondas físicas ofertadas para los CPD's, y a través del despliegue de sondas virtuales (sin límite), en la parte de infraestructura desplegada en hiperescalares o en centros remotos.
- Respecto a las medidas de disponibilidad, la solución mantiene el de tráfico ante excesos de throughput licenciado puntuales, asegurando que no hay pérdida de servicio. Solo cuando la superación de este throughput es mantenida en el tiempo, se requerirá la regularización del licenciamiento.
- En cuanto a escalabilidad, menciona que, dado que no es necesario licenciar las sondas virtuales, se pueden desplegar tantas como se considere, teniendo en cuenta que el límite lo pone el tráfico total (*throughput*) licenciado.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta definición en la propuesta de operación y mantenimiento de la plataforma: soporte hardware y software de la plataforma, actualizaciones y parches de producto, gestión de incidencias, cambios, parches y actualizaciones, control de acceso, usuarios y permisos, etc.
- No incorpora ejemplos de casos de uso de monitorización de la herramienta.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

4,8 puntos

3.1.3.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **NOTABLE**, ya que describe de forma muy completa la plataforma propuesta, que está bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red, incluyendo un listado de equipos con sus capacidades, así como un esquema de la arquitectura detallado y claro. Todo ello se acompaña con una lista descriptiva de todas las tareas implicadas en la operación y mantenimiento de la solución, además de indicar las tareas que van a reforzar su disponibilidad y continuidad. Por último, se indican las posibles integraciones con otras herramientas y sistemas de seguridad de Madrid Digital; sin embargo, no se mencionan las posibilidades de escalado, ni se detallan los posibles casos de uso.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se describe con bastante detalle la arquitectura y los equipos que formaran parte de la solución, así como la interacción entre todos ellos. Se propone una solución de *Network Detection and Response* (NDR) robusta y avanzada para proteger los activos críticos de la organización contra amenazas cibernéticas avanzadas, mediante la utilización de técnicas de inteligencia artificial, redes neuronales y aprendizaje profundo, que permitirán realizar un análisis del comportamiento del tráfico cifrado, pudiendo encontrar actividades maliciosas de los atacantes sin necesidad de descifrarlo.
- Se propone un modelo operativo 24x7 que garantizará una cobertura continua, con un equipo de ingenieros y analistas certificados en la tecnología subyacente, dimensionado para proporcionar una respuesta rápida y eficiente.
- Las tareas de soporte hardware y software, gestión de actualizaciones y parches, monitorización de la disponibilidad, y mantenimiento preventivo y correctivo, se realizan de forma transparente, asegurando que la plataforma siempre esté operativa y actualizada.
- La solución propuesta permite la integración con otras soluciones de seguridad que pudieran estar desplegadas en Madrid Digital, permitiendo el uso de firmas e indicadores específicos de compromiso (IOC) que el licitador ofrece en feeds de inteligencia propios, alimentados por detecciones que se dan en el resto de clientes a nivel mundial, investigaciones de sus propios analistas, así como en feeds propietarios procedentes de sus acuerdos de compartición de inteligencia de amenazas como la Cyber Threat Alliance, la Red Nacional del SOC's, o *feeds* públicos, incluyendo los principales *feeds open source*.
- El servicio propuesto permite, mediante la automatización, la reducción de falsos positivos ajustando los umbrales de detección, ya que aplica su IA para priorizar los activos que son importantes y están siendo atacados y mostrarlos en un cuadrante de amenaza y certeza de forma automática. Esto ayuda a mantener al equipo de analistas centrados en los ataques realmente positivos

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Aunque se indica que la solución dispone de mecanismos para evitar la pérdida de eventos en caso de que se supere de forma puntual la capacidad máxima soportada o autorizada, no se ofrece una descripción de que como escala la plataforma propuesta en caso de que dicho desbordamiento se sostenga en el tiempo y haya que aumentar de forma permanente la capacidad total de la plataforma.
- No se detallan los casos de uso que puede llegar a cubrir la solución y que permitirán explotar la funcionalidad de la herramienta desde el primer momento.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

6,4 puntos

3.1.3.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de la **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **SOBRESALIENTE**, ya que describe de forma completa la plataforma, incluyendo un listado de equipos con sus capacidades y licencias. Se explica de forma detallada la gestión y operación de la plataforma, así como las propuestas para garantizar la disponibilidad y continuidad del servicio. Se muestra en una tabla, a modo de ejemplo, los casos de uso que se pueden llegar a cubrir, así como, posteriormente, los niveles de automatización que se pueden alcanzar y algunos ejemplos de escalabilidad de la plataforma. La solución elegida está bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- La detallada descripción del servicio, los elementos que lo componen y que formarán parte de la arquitectura propuesta, indicando sus interrelaciones, ubicaciones físicas y el nivel de licenciamiento.
- La propuesta del servicio de soporte y mantenimiento de la solución en modalidad 7x24, que incluye equipamiento en cold standby para cumplir con los requerimientos de la solicitud en relación con la disponibilidad y continuidad de la solución y cumplimiento de SLA's.
- La descripción de la gestión y operación del servicio, incluyendo la mediación en los conflictos entre fabricantes que pudieran surgir en las integraciones mediante la gestión completa y coordinada de las posibles incidencias, así como sus capacidades de integración con EDR, SIEM y herramientas SOAR, que permiten facilitar la gestión y visibilidad de amenazas desde el endpoint hasta la nube.
- La presentación en una tabla de los múltiples casos de uso cubiertos, clasificados según el tipo de técnica avanzada usada por los atacantes.

- A nivel evolutivo, indican que la solución puede escalar y extenderse hacia entornos de nube pública ubicando sensores en los diferentes hiperescalares, extendiendo de esta manera las capacidades de detección y respuesta ante ciberamenazas

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.	8 puntos
---	-----------------

3.1.3.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de la **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **NOTABLE**, ya que describe de forma bastante completa la solución elegida, incluyendo un listado de los elementos que la componen, con sus capacidades y su posible integración con los sistemas de seguridad de Madrid Digital y equipos asociados. La herramienta ofertada se encuentra bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. El desarrollo de la solución incluye una descripción detallada de las actividades relacionadas con la operación, así como las medidas de disponibilidad, continuidad, escalabilidad y procesos de automatización disponibles; sin embargo, no se llegan a indicar los posibles casos de uso que la propia herramienta puede llegar a implementar en el tiempo de vida del servicio.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- La descripción exhaustiva de los elementos desplegados en la red de Madrid Digital, fundamentalmente sondas y su integración con la solución de nube (SaaS) propuesta, en la que se detallan su capacidad, posibles ubicaciones y características físicas, que en conjunto definen la capacidad total de análisis de la solución. Se indica la posibilidad de que, aunque se superen de forma puntual los límites ofertados, este desbordamiento se verá atendido y absorbido sin problemas.
- La integración y respuesta orquestada a través de desarrollos, tanto con herramientas de seguridad terceros, mediante API, como con otros productos de los principales líderes del mercado.
- Un listado con las principales tareas que se realizarán en la operación del servicio, respaldadas por personal técnico del fabricante que permitirá ajustar las configuraciones y optimizar las implementaciones.
- Como toda solución SaaS la escalabilidad, disponibilidad y continuidad están completamente garantizadas, entre otras razones por los correspondientes SLA's del propio servicio. La escalabilidad se ve reforzada en la red del cliente por la posibilidad de poder desplegar sondas virtuales ilimitadas, además se asegura una retención de los datos capturados y procesados durante 365 días para poder realizar análisis retrospectivos y búsqueda de amenazas.
- La automatización del análisis de la información recogida por las sondas puede llegar incluso a la detección de amenazas en el tráfico SSL/TLS sin necesidad de descifrarlo, mediante la utilización de algoritmos *Machine Learning* e inteligencia artificial, detectando, por ejemplo,

canales de *command and control* (C2) cifrados, mirando única y exclusivamente el comportamiento del túnel.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- A pesar de que se mencionan de la existencia de una librería de *playbooks* guiados, estos no se detallan, ni se listan por lo que no podemos valorar los casos de usos más habituales soportados por la solución.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

6,4 puntos

3.1.3.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de la **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **BUENA**, ya que describe de forma completa la plataforma elegida, muy bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red, y su arquitectura incluyendo una descripción detallada de cada componente implicado, las automatizaciones que se pueden conseguir, así como su escalabilidad, y su posible integración con otras herramientas de seguridad. Sin embargo, no se aporta una relación de casos de uso concretos, ni las actividades detalladas de operación y mantenimiento, ni planes de disponibilidad y continuidad del servicio propuesto.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- El planteamiento y descripción de la solución, mediante la inclusión de una detallada información sobre las características y funciones de cada componente, completado con una arquitectura que muestra la interacción y los flujos de información que hay entre todos ellos
- El descubrimiento de activos y el análisis de la información se realiza de forma automática en base al flujo de datos mediante el descifrado en tiempo real de forma pasiva a velocidad de línea del tráfico SSL/TLS incluido el *Perfect Forward Secrecy (PFS)* y la aplicación de *Machine Learning* e Inteligencia artificial a toda la información recopilada.
- La API bidireccional que facilita la integración, automatización y orquestación con otras tecnologías como SOAR, firewall, NAC, EDR. Además, es posible realizar integraciones completamente personalizables mediante una API REST abierta y un motor de análisis programable.
- La solución planteada es reconocida en el mercado como una de las soluciones más avanzadas y potentes, lo que asegura un rendimiento superior y confiable a largo plazo, proporcionando una visibilidad de 360 grados (Norte, Sur, Este y Oeste) y continua del tráfico de red, incluidas las comunicaciones cifradas, estando posicionada por todo ello en la parte más alta, del último cuadrante de Forrester de visibilidad y análisis de red.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Aunque se nombran ciertos casos de uso en la integración con otras herramientas, no se detallan de forma adecuada los casos de uso más habituales que permitirán explotar las funcionalidades de la plataforma ofertada.
- No recoge ninguna propuesta de aseguramiento de disponibilidad y continuidad del servicio, así como tampoco contempla el mantenimiento y operación, hasta el fin del contrato, de las sondas de análisis de tráfico SAT-INET y SAT-ICS desplegadas en la red interna por el Centro Criptológico Nacional (CCN-CERT).
- No se describen las actividades de operación y mantenimiento de la plataforma, además de solo incluir licenciamiento para el análisis del tráfico de servidores, dejando sin cubrir los equipos de usuarios en la red interna.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

4,8 puntos

3.1.3.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de la **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **SOBRESALIENTE**, ya que describe de forma muy completa la plataforma presentada, incluyendo un esquema detallado de la arquitectura, así como un listado de los equipos empleados con sus correspondientes capacidades y redundancias, que, unidas a la propuesta de la monitorización constante, confieren a la solución un alto grado de disponibilidad y escalabilidad. La solución dispone entre otras características, de diversos mecanismos de automatización, que, junto a sus capacidades de integración con otros sistemas de seguridad, la posicionan en un buen lugar el ultimo cuadrante Forrester de soluciones de análisis y visibilidad de red. Por último, la propuesta presenta distintas librerías de casos de uso.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- La arquitectura redundante propuesta se describe de forma detallada, listando cada uno de los elementos que la componen, y describiendo su capacidad y funcionalidad. Además, la propuesta está diseñada para cubrir más centros de los inicialmente pedidos en el pliego.
- Se plantea realiza una monitorización continua para supervisar el estado de la red y los componentes de la plataforma, permitiendo detectar y resolver problemas antes de que afecten a la disponibilidad, así como la realización de copias de seguridad regulares de las configuraciones y la definición de un plan de recuperación para restaurar rápidamente el servicio en caso de una interrupción significativa de este o indisponibilidad de un componente. Se plantea realizar un mantenimiento preventivo y correctivo continuo, así como se ofrece una atención de consultas en horario 8x5 e incidencias en horario 24x7.
- Se integra fácilmente con el SIEM propuesto, lo que permite una escalabilidad sin interrupciones. La inteligencia artificial y el aprendizaje automático permiten a la plataforma adaptarse y escalar según el volumen de datos y la complejidad de las amenazas, sin

necesidad de una intervención manual constante. Se presentan una lista de integraciones nativas soportadas, incluyendo los principales proveedores de NAC y firewalls, así como la disponibilidad de scripts a medida para otras soluciones de seguridad. Se destaca también la integración nativa con *Active Directory* para poder bloquear de forma rápida y automática las cuentas comprometidas.

- La plataforma presentada acelera la detección de amenazas y reduce el tiempo de investigación mediante la captura de metadatos, a escala, en toda la infraestructura de la organización. Recopila y enriquece de forma automática los metadatos de seguridad con conocimientos profundos y contexto para permitir a los analistas detener una amplia gama de ataques de forma temprana y consistente. Automatiza las tareas manuales asociadas a los análisis de nivel 1 y 2 para reducir la carga de trabajo global de las operaciones de seguridad. Utiliza inteligencia artificial para puntuar, clasificar y revelar automáticamente las amenazas más críticas, reduciendo el ruido de alertas en un 80% o más.
- La herramienta propuesta ofrece una amplia gama de librerías de casos de uso de monitorización, ya desarrollados, que ayudan a detectar y responder a una amplia variedad de amenazas de manera eficiente, entre las que se pueden destacar: la detección de amenazas internas, casos de ransomware, exfiltración de datos, detección de movimientos laterales o protección contra *malware* en general.
- Como valor añadido ofrece licencias para la supervisión y defensa de un número de usuarios en la plataforma Office 365 de Microsoft, mediante el análisis de las conexiones generadas en sus cuentas.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.3 – Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR. Hasta 8 puntos.

8 puntos

3.1.4 CRITERIO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

3.1.4.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **NOTABLE**; destacando de su oferta los procedimientos y actividades de operación SIEM, NDR y sondas, los procedimientos propuestos para la integración de fuentes de eventos y los recursos específicos para el desarrollo de casos de uso de monitorización; los procedimientos asociados al servicio de detección de identificación, tratamiento y escalado de incidentes y amenazas de seguridad, y para el servicio de búsqueda proactiva de amenazas, la tipología y detalle de informes propuesta y herramientas propuestas; sin embargo, no aporta ninguna propuesta de valor en cuanto a la organización de los recursos y funciones de cada uno de ellos para los distintos servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se describen los procedimientos y actividades de operación y administración de las plataformas SIEM, sondas IDS y NDR de forma completa.

- En el servicio de monitorización, la descripción del proceso de integración de fuentes de eventos de seguridad es detallada, haciendo foco en los pasos a seguir para incluir fuentes de eventos ubicadas en cloud, así como el EDR. Se propone la asignación de un recurso experto en *DevSecOps* dedicado en exclusiva a las tareas de integración de nuevas fuentes, nuevas reglas, casos de uso de monitorización, *playbooks* y desarrollo de conectores personalizados.
- La propuesta de actividades del servicio de detección de incidentes relativas a la identificación, tratamiento y escalado de incidentes y amenazas recoge, para cada una de las tareas, triaje, primer nivel de investigación y escalado de incidentes, las herramientas de apoyo que se utilizarán.
- La propuesta de metodología a aplicar, documentación e informes asociada al servicio de *hunting* es detallada, proponiendo tipología de informes y documentos a facilitar, y capacidades de la herramienta de consola unificada de trabajo y de la herramienta de análisis de relaciones entre activos propuestas para el servicio.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Respecto a los recursos técnicos, no detalla cómo será la organización de los mismos. Se limita a enumerar los técnicos que componen el servicio tal y como los describe el pliego, sin especificar dedicación y funciones asociadas a las actividades de monitorización, detección y *hunting*. Tampoco se mencionan protocolos de relación entre ellos y con otros equipos involucrados en el servicio, como pueden ser los fabricantes de las distintas plataformas o proveedores de cloud.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

3,2 puntos

3.1.4.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **NOTABLE** ya que desarrolla de forma detallada y muy completa los procedimientos de administración y operación de las distintas plataformas, el servicio ofrecido de modelado de amenazas a partir del cual se definirán los casos de uso de monitorización a desarrollar, y los procedimientos de monitorización de eventos y alertas, y de identificación, tratamiento y escalado de incidentes y amenazas de seguridad reportadas por cada uno de los servicios. Destaca también la propuesta metodológica del servicio de *hunting*, así como los entregables del servicio previstos; sin embargo, falta concreción en la organización de los recursos y funciones de cada uno de ellos para los distintos servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Descripción muy detallada y completa de los procedimientos asociados a las actividades de operación y administración de las plataformas SIEM, sondas IDS y NDR, así como de las distintas actividades contempladas para la gestión integral del servicio: control de incidencias y cambios, control de permisos, monitorización de disponibilidad, etc.

- Propuesta de servicio específico de modelado de amenazas, estructurado, para la identificación de amenazas y vulnerabilidades de seguridad, cuantificación de su gravedad, priorización de técnicas de mitigación y protección, y propuesta final de casos de uso de monitorización a generar en el SIEM. Se desarrolla muy detalladamente la metodología aplicada para el perfilado de amenazas, basada en *NIST 800-154*, *MITRE ATT&CK* y la *Cyber Kill Chain*, y para la elaboración de los casos de uso de monitorización.
- Se desarrollan exhaustivamente las actividades, metodología propuesta y proceso completo del servicio de monitorización y gestión de alertas de ciberseguridad. Destaca especialmente el detalle de las fases y actividades para la evaluación y la clasificación de incidentes de seguridad.
- Metodología propuesta para el servicio de búsqueda de amenazas muy completa y detallada, basada en inteligencia de amenazas (IOC's y TTP's), hipótesis de analistas y análisis de valores atípicos. Se valora también muy positivamente la relación de entregables a generar, en forma de informes periódicos, informes de progreso, de nuevos casos de búsqueda, de incidentes identificados, de recomendaciones, o de integración de nuevas IOC's y TTP's, entre otros.
- Se identifica herramienta específica para el servicio de *hunting*, integrada de forma nativa con el SIEM y la solución EDR corporativa de Madrid Digital, Watchguard, para la construcción de misiones de *hunting* recurrentes y automatizadas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Respecto a los recursos técnicos, no se detalla adecuadamente la organización de los mismos, funciones y protocolos de relación entre ellos y con otros equipos involucrados en el servicio, como pueden ser los fabricantes de las distintas plataformas o proveedores de cloud.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

3,2 puntos

3.1.4.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **ADECUADA**; describe la organización de los recursos y los procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad. Sin embargo, no detalla el servicio de monitorización de eventos de seguridad ni profundiza en la detección de incidentes en relación con la monitorización continua de los eventos o alertas generados por los servicios de prevención, monitorización, y vigilancia digital.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Propone una plataforma tecnológica propia utilizada por todos sus analistas en la operación y entrega de servicios de monitorización y detección, lo que permite generar sinergias, compartir mejores prácticas y enriquecer el conocimiento para la anticipación de incidentes.

- Mediante técnicas de procesado inteligente de alertas, se enriquece la investigación con datos de reputación y de otros incidentes registrados. De este modo, de forma unificada y centralizada, se alcanza una comprensión mayor sobre los ataques y se pueden tomar decisiones más rápidas y fiables, reduciendo significativamente las alertas y falsos positivos.
- Para el servicio de *hunting*, destaca la metodología aplicada en la plataforma unificada, aplicando distintos enfoques de búsqueda de amenazas: a través de reglas y firmas, análisis de datos en tiempo real, caza de comportamientos anómalos, etc.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Muy poco detalle en la descripción del servicio de monitorización de eventos de seguridad, faltando información sobre la implementación, administración y operación del SIEM/SOAR, sondas IDS y NDR. Menciona que integrará fuentes, pero no propone cuales ni cómo. Habla del equipo de trabajo, sin especificar roles y funciones.
- En cuanto al servicio de detección, poco detalle en la explicación de la monitorización continua de eventos, en los procedimientos de detección de incidentes, o en la documentación, informes y ANS que se generarán y utilizarán en el servicio.
- Relativo al servicio de *hunting*, no se desarrolla adecuadamente la propuesta de casos de uso de búsqueda a elaborar, los sistemas finales sobre los que se actuará, ni los procedimientos de notificación y escalado de hallazgos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.	0,8 puntos
--	-------------------

3.1.4.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **NOTABLE** destacando de la propuesta los procedimientos de administración y operación de las plataformas SIEM y NDR, el proceso para la integración de fuentes a monitorizar, la organización de los recursos para el servicio, los procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad, y la descripción metodológica del servicio de *hunting*; sin embargo, falta propuesta de casos de búsqueda a implementar en el servicio de búsqueda proactiva de amenazas, clasificados en base a la tipología de la búsqueda implementada.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En el servicio de monitorización, destaca la propuesta de administración y operación de las plataformas SIEM y NDR, y los procedimientos de integración de fuentes en la plataforma de monitorización.
- La metodología del servicio de detección y gestión de alertas es muy detallada, al igual que la solución propuesta para la monitorización de eventos de seguridad, basada en un triaje y priorización automatizada que permite enfocarse en lo más relevante. Los algoritmos aplicados entienden el comportamiento del atacante, lo que reduce el número de alertas al relacionar

eventos con comportamientos maliciosos, proporcionando un impacto más real. Destaca también la propuesta de elaboración de hipótesis de detección para su transformación posterior en casos de uso de monitorización, reglas de correlación e indicadores de compromiso.

- Respecto a la organización de recursos, aparte de los niveles 1 a 3 solicitados, describe un nivel 0, automatizado. Este nivel de servicio proporciona, de manera completamente automática y sin intervención humana, capacidades de análisis de eventos y respuesta ante alertas de seguridad.
- En relación con la implementación de alertas, no se limita a la simple detección de eventos sospechosos, menciona también que incorporará inteligencia de amenazas en tiempo real, obtenida de fuentes internas y externas, como *feeds* de amenazas, informes de vulnerabilidades y análisis de comportamiento de usuarios. Indica que esta inteligencia contextual enriquecerá las alertas, proporcionando información detallada sobre la naturaleza de la amenaza, su origen y las posibles implicaciones para la infraestructura de la organización.
- En la descripción del servicio de hunting, se explican las capacidades técnicas del equipo multidisciplinar que lo llevará a cabo. Destaca también la descripción metodológica aplicada, basada en *TaHiTI (Targeted Hunting integrating Threat Intelligence)*, respaldada por la herramienta *MaGMA for threat hunting*.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- En el servicio de búsqueda proactiva de amenazas, no se recoge la relación de casos de búsqueda propuestos para el servicio, clasificados en base a la tipología de la búsqueda implementada.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

3,2 puntos

3.1.4.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **SOBRESALIENTE**, ya que recoge de forma muy detallada la organización de los recursos para cada servicio ofertando además recursos específicos adicionales para integrar las funcionalidades de IA en los distintos servicios, las actividades y procedimientos propuestos para la monitorización de seguridad, con especial foco en las actividades de administración y operación de plataformas, monitorización de eventos, o propuesta de tipología de casos de uso de monitorización a implementar. Destaca también la propuesta de procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad dentro del servicio de detección de incidentes, criterios de priorización y mecanismos de reducción de falsos positivos. En cuanto al servicio de *hunting*, la metodología, herramientas y propuesta de casos de búsqueda a definir se considera muy completa y orientada a la identificación y reducción de los tiempos en los incidentes de seguridad detectados.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- La organización del equipo de trabajo, tanto para las labores de monitorización y administración y operación de las diferentes plataformas como para la detección de ciberincidentes y la búsqueda proactiva de amenazas, es muy detallada y clara, añadiendo como mejora a la oferta de equipo ofrecido, perfiles adicionales orientados a la incorporación de la IA en todos los procesos, un arquitecto IA para las actividades de arquitectura, integraciones, administración y operación, y un analista IA para los procesos de monitorización y detección.
- En cuanto al servicio de monitorización, enumera dos herramientas que aportan valor añadido al servicio: un elemento para recolección de logs y descubrimiento e inventariado de activos (CMDB de Ciberseguridad), y una plataforma orientada a utilizar la IA de forma transversal para mejorar las tareas de monitorización y detección, a la vez que añade mecanismos de confidencialidad en el propio uso de la IA. Se explica de forma precisa las actividades de administración y operación a realizar en las plataformas SIEM y NDR, las funciones de los arquitectos de seguridad definidos en el pliego, la tipología de casos de uso de monitorización propuestos, a fin de maximizar la detección y las fuentes de eventos más comunes a integrar en primera instancia.
- Respecto al servicio de detección, describe con precisión, de forma muy clara y completa la organización de recursos y las actividades que realizará cada uno de los niveles (N1 – N3) y sus interrelaciones (especificando que tanto el N2 como el N3 pertenecen al equipo de análisis y respuesta que será valorado en el criterio 7.6). Se presentan gráficos que facilitan su comprensión.
- Respecto a los procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad, están muy desarrollados y se fundamentan en criterios de priorización de criticidad, gracias a que el triaje vendrá pre-filtrado por las herramientas avanzadas propuestas, que utilizan mecanismos de *Machine Learning* y IA para reducir los falsos positivos y alertar cuando se supera un umbral de riesgo determinado.
- En cuanto a la búsqueda proactiva de amenazas, define de manera extensa los casos de búsqueda que propone. La metodología propuesta está orientada a reducir los tiempos medios de detección, respuesta y contención de incidentes, así como a minimizar la superficie de exposición a ataques tanto internos como externos. La tipología de casos de búsqueda a definir tiene diferentes aproximaciones, basándose en inteligencia de amenazas (IOC's, TTP's), basándose en hipótesis de analistas, o en análisis de valores atípicos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

4 puntos

3.1.4.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA**; describe los procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad, y las fuentes de inteligencia de amenazas utilizadas para el enriquecimiento de los procesos de monitorización y detección. No aporta ninguna propuesta de valor relativa a los

procedimientos de integración de fuentes, implementación y administración de las plataformas SIEM, SOAR y NDR, organización y relaciones dentro del equipo de trabajo y recursos dedicados, o propuesta de casos de búsqueda proactiva de amenazas organizada por tipología.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación con el servicio de monitorización, aporta valor añadido al ofertar tres fuentes de inteligencia de amenazas que enriquecen la monitorización y detección de eventos de seguridad. Anuncian que en su SOC las plataformas de amenazas se encuentran completamente integradas, de modo que toda la información consultada en las distintas fuentes está disponible de manera automática para los analistas en cada evento generado. Esto hace que los tiempos de investigación y resolución de incidentes se vean reducidos de manera drástica.
- Para el servicio de detección propone una metodología de gestión proactiva de incidentes de seguridad que estructura el servicio en fases claras que van desde la identificación y evaluación hasta la notificación y respuesta.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Respecto al servicio de monitorización, falta desarrollo con respecto a la integración de las fuentes de eventos, la generación de IOC's y cómo incluirlos en la MISP de Madrid Digital. No aporta valor respecto a la implementación, administración y operación de las herramientas que llevará el servicio, salvo las plataformas de amenazas definidas previamente.
- En relación con el servicio de detección, falta detalle en la organización de recursos y en la documentación, informes y uso de los ANS propuestos. Tampoco aporta valor en cómo realizará el triaje de alertas de seguridad (según la guía nacional de notificación y gestión de ciberincidentes).
- En cuanto al servicio de búsqueda proactiva de amenazas, la propuesta no es clara llegando a confundirse con el proceso de definición de caso de uso de monitorización. No define tipologías de búsquedas a implementar, casos de búsqueda propuestos o equipo de trabajo.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.	0,8 puntos
--	-------------------

3.1.4.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **ADECUADA** destacando la metodología de detección de ciberincidentes propuesta; sin embargo, no desarrolla con suficiente concreción las actividades de generales de monitorización y administración de los sistemas definidos, ni las actividades asociadas al desarrollo y mantenimiento de casos de uso de monitorización y de búsqueda de amenazas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Metodología propuesta de detección de ciberincidentes, detallando el equipo de trabajo, fases y actividades a desarrollar en cada una de ellas, así como documentación, informes y cuadros de mando a elaborar de seguimiento de la actividad.
- Metodología propuesta para el servicio de búsqueda proactiva de amenazas (*Threat Hunting*) basado en *Cyber Kill Chain* combinado con *MITRE ATT&CK*, y descripción de la operación del servicio en fases y actividades.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Procedimientos a seguir y actividades relacionadas con la monitorización, administración de los sistemas principales soporte del servicio de detección (SIEM, SOAR, NDR, sondas IDS), e incorporación de nuevas fuentes de eventos de seguridad. Tampoco se detalla la relación entre los equipos de trabajo dedicados en exclusividad para el contrato y las actividades a desarrollar por el proveedor de cloud/fabricante de cada plataforma.
- Actividades relacionadas con la creación y administración de los casos de uso de monitorización a implementar.
- Propuesta de casos de búsqueda de amenazas a implementar en el servicio de *hunting*.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

0,8 puntos

3.1.4.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **ADECUADA** destacando de la misma la definición de objetivos del servicio y la metodología de detección de ciberincidentes propuesta; sin embargo, no desarrolla con suficiente concreción las actividades generales de monitorización y administración de los sistemas definidos, ni las actividades asociadas al desarrollo y mantenimiento de casos de uso de monitorización o de búsqueda de amenazas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se describen correctamente los objetivos del servicio de detección de incidentes, la organización de los analistas de seguridad en niveles de especialización y la metodología seguida para el tratamiento de cada alerta y la detección incidentes de seguridad, a través de las herramientas de monitorización propuestas para el servicio (SIEM, NDR) y fuentes de eventos contempladas inicialmente para el proyecto (EDR, correo, etc.), y la información obtenida de los servicios de vigilancia digital y análisis de vulnerabilidades.
- Destaca la propuesta de documentación del servicio, de incorporación de información de contexto para enriquecimiento de las alertas, y de seguimiento de todas las alertas e incidentes a través de una plataforma centralizada, específica para tal fin, que centraliza toda la actividad.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Procedimientos operativos relacionados con la monitorización y administración de los sistemas principales soporte del servicio de detección (SIEM, NDR, sondas IDS), procedimientos de notificación y escalado de incidentes relacionados con las plataformas y fuentes de eventos integradas, y relación de los equipos de trabajo dedicados en exclusividad para el contrato y equipos terceros de proveedores de soluciones.
- Procedimientos operativos para la creación y administración de los casos de uso de monitorización implementados.
- Propuesta inicial de casos de búsqueda de amenazas a implementar en el servicio de *hunting*.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

0,8 puntos

3.1.4.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **ADECUADA** destacando de la misma la enumeración que realiza sobre las tareas a realizar en el servicio de monitorización y el planteamiento general del servicio de *hunting* propuesto, basado en hipótesis de comportamiento en lugar de alertas; sin embargo, no desarrolla con suficiente detalle los equipos de trabajo en cada servicio y relaciones entre ellos, los procedimientos operativos y actividades generales para la ejecución de las actividades de monitorización, detección de ciberincidentes y búsqueda proactiva de amenazas, la propuesta concreta de casos de uso de *hunting* a implementar.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se enumeran las principales actividades a realizar en el servicio de monitorización de eventos de seguridad, la administración y operación de las plataformas SIEM/SOAR, sondas IDS y NDR, el proceso de integración de fuentes, y las tipologías de alertas a generar, alertas de salud de la plataforma y alertas resultado de la ingesta y correlación de eventos.
- El servicio de búsqueda proactiva de amenazas propuesto, basado en la generación de hipótesis centradas en comportamiento empleando como fuentes principales el SIEM, EDR y SOAR. Se explica de forma somera metodología y plan de campañas propuesto.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Procedimientos operativos concretos para la ejecución de las actividades relacionadas con el servicio de monitorización requerido, separados en procedimientos de monitorización e integración de fuentes, administración y operación de plataformas SIEM, SOAR, NDR, y procedimientos para notificación y escalado de incidentes de monitorización. Tampoco se describe cómo se organizarán todos los recursos involucrados.

- Procedimientos operativos concretos para la detección de ciberincidentes a partir de la monitorización continua de los eventos y alertas de seguridad generados por los distintos servicios y plataformas, así como actividades de triaje, investigación escalado y documentación del servicio que se llevarán a cabo. Tampoco se detalla la organización propuesta de los recursos.
- Organización de los recursos del servicio de *hunting*, propuesta de casos de uso/búsquedas a implementar, y procedimientos operativos de identificación y escalado de incidentes detectados. Se echa en falta también mención específica de la plataforma NDR como fuente de investigación del servicio.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

0,8 puntos

3.1.4.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **ADECUADA** destacando de la misma la descripción detallada de las actividades de administración y operación de los sistemas SIEM/NDR ofertados y el planteamiento del servicio de *hunting* propuesto; sin embargo, no desarrolla con suficiente detalle la organización de los recursos, los procedimientos propuestos para la monitorización de alertas y la detección de incidentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se describe sucintamente la propuesta de administración y operación de las herramientas SIEM y NDR propuestas para el servicio, detallando las diferentes actividades contempladas.
- Metodología utilizada para el servicio de búsqueda de amenazas, basada en el marco *TaHiTI* (*Targeted Hunting integrating Threat Intelligence*), que facilita un método estructurado de búsqueda de amenazas, integrando la información de inteligencia de amenazas en el flujo de trabajo, y detalle de las diferentes fases de *hunting* a desarrollar.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Organización de los recursos y procedimientos asociados al servicio de monitorización: actividades para la integración de fuentes, creación y administración de los casos de uso de monitorización, generación de IOC's., etc.
- Organización de los recursos y procedimientos operativos relacionados con la detección de ciberincidentes como son actividades de triaje, investigación de alertas, protocolos de escalado, y documentación del servicio. Tampoco se detalla la relación entre los equipos de monitorización y de administración de las plataformas SIEM/SOAR y NDR.
- Propuesta de casos de búsqueda concretos a generar para el servicio de *hunting*.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

0,8 puntos

3.1.4.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **BUENA** debido a que detalla todas las actividades a desarrollar relacionadas con el servicio de monitorización de eventos, ofreciendo un recurso de apoyo para la elaboración de los casos de uso de monitorización (*profiling*). También destaca la propuesta de organización y actividades del servicio de detección de incidentes de seguridad; sin embargo, no concreta aspectos básicos como la organización del equipo de trabajo y su participación en cada uno de los servicios, la documentación a elaborar resultado de los servicios de monitorización y detección, o los casos de búsqueda concretos a desarrollar en el servicio de búsqueda proactiva de amenazas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de monitorización se oferta la incorporación de un analista de *profiling* de apoyo, para la definición de casos de uso de monitorización.
- Se definen las principales fases y actividades del servicio de detección con un sistema de triaje y una propuesta de automatización de acciones, orientada a mejorar la eficiencia del proceso de tratamiento de alertas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se facilita información suficiente sobre la organización de los recursos y sus relaciones con otros equipos de trabajo, para los diferentes servicios. Por ejemplo, no queda claro qué recursos realizarán las actividades de gestión y administración de las plataformas SIEM/SOAR y NDR. Tampoco se detalla información que permita valorar la documentación de seguimiento y resultado de cada servicio, informes a elaborar o ANS de cada servicio.
- Si bien se describe adecuadamente la metodología aplicada para el servicio de *Threat Hunting*, basada en *TaHiTi*, *MaGMA for Threat Hunting* y *MITRE ATT&CK*, no se aporta información suficiente sobre la relación de casos de uso de *hunting* propuesta a aplicar para cada una de las plataformas propuestas (SIEM, SOAR, NDR y EDR), ni la periodicidad de su ejecución,

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.4 – Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas. Hasta 4 puntos.

2,4 puntos

3.1.5 CRITERIO 7.5 – Servicio de orquestación, automatización y respuesta - SOAR. Hasta 3 puntos.

3.1.5.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **SOBRESALIENTE** ya que propone solución SOAR, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con el NDR y con los sistemas de Madrid Digital, amplia librería de casos de uso predefinidos y propuesta de operación, mantenimiento, administración remota y monitorización de la solución SOAR.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa e integrada con el SIEM propuesto, licenciada por suscripción y como mejora ofrece acceso ilimitado de analistas concurrentes. Se describen y relacionan los procesos SOAR.
- Respecto a la integración con herramientas o feeds de inteligencia soporta feeds de IP's y URL's dominios y ofrece capacidades de IA para crear *playbooks* relacionados a partir de lenguaje natural. También se indica la integración con conectores para todas las fuentes de eventos indicadas, incluido las integraciones con EDR. Se describe la integración con el NDR. Se añade para mejor comprensión ejemplo detallado de integración con FW y modelo conceptual de capacidades de integración con fuentes cloud.
- Se recoge también la integración con ITSM-FARO (producto BMC) de forma nativa y se describe que la integración con LUCIA se realizará vía API.
- Se ofertan gran número de *playbooks* ya definidos y adaptables predefinidos, que son modificables en el IDE (entorno de desarrollo integrado) tanto por programación como gráficamente, incorporando capacidades de IA generativa. Evolutio incluye sin coste el perfil de especialista SecDevOps para gestionar el ciclo de vida de los *playbooks*.
- Presenta propuesta de operación, administración remota y mantenimiento de la solución de forma singular a la del SIEM.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

3 puntos

3.1.5.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **NOTABLE** ya que propone solución SOAR, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con los sistemas de Madrid Digital, y amplia librería de casos de uso predefinidos; sin embargo, no se detalla de forma diferencial como se opera, mantiene y administra la plataforma, y la integración con la solución NDR no se especifica.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa e integrada con el SIEM propuesto, licenciada por suscripción y como mejora ofrece acceso ilimitado de analistas concurrentes, que se valora muy positivamente.
- Ofrece capacidades de IA y respecto a la integración con herramientas o feeds de inteligencia se incide en el soporte de feeds de reputación de direcciones IP y URL's de dominios e IOC's. También dispone de capacidades de conexión e integración con todas las fuentes de eventos indicadas, precisando también que se integra con el EDR. Se recoge y detalla la capacidad de integración con el NDR.
- La solución SOAR propuesta se integrará con las herramientas de *ticketing* de MD (ITSM-FARO) y del Centro Criptológico Nacional CCN-CERT (herramienta LUCIA) vía API.
- Se menciona la existencia de gran número de *playbooks* ya definidos y adaptables, documentados en la plataforma del fabricante y en Github.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detallan ningunas de las actividades de operación, mantenimiento, administración remota y monitorización de la solución SOAR de forma singular.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

2,4 puntos

3.1.5.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **BUENA** ya que propone solución SOAR, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con los sistemas de Madrid Digital, y amplia librería de casos de uso predefinidos; sin embargo, los procesos de orquestación, automatización y respuesta se presentan de forma general, no se detalla de forma diferencial como se opera, mantiene y administra la plataforma, y la integración con la solución NDR no se especifica.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa e integrada con el SIEM propuesto, licenciada por suscripción y como mejora ofrece acceso ilimitado de analistas concurrentes.
- Ofrece capacidades de IA y respecto a la integración con herramientas o feeds de inteligencia se incide en el soporte de feeds de reputación de direcciones IP y URL's de dominios e IOC's. También dispone de capacidades de conexión e integración con todas las fuentes de eventos indicadas a través de conectores syslog, CEF y API REST. Se recoge la capacidad de integración con el NDR sin detalle.
- La solución SOAR propuesta se integrará con las herramientas de *ticketing* de MD (ITSM-FARO) y del Centro Criptológico Nacional CCN-CERT (herramienta LUCIA) ambos vía API y

mediante correos. Se indica que será posible establecer sincronización bidireccional de incidentes.

- Se menciona la existencia de gran número de *playbooks* ya definidos y adaptables.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Los procesos SOAR de orquestación, automatización y respuesta no se describen en detalle ni se presentan gráficos y ejemplos que permitan valorar su funcionamiento.
- No se detallan ningunas de las actividades de operación, mantenimiento, administración remota y monitorización de la solución SOAR de forma singular.
- La integración con el NDR no se define ni detalla a nivel de proceso con flujos, actividades y resultados, ni se indica posibles beneficios y/o ventajas.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

1,8 puntos

3.1.5.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **BUENA** ya que propone solución SOAR basada en tecnología Open Source, integrada de forma nativa con el SIEM, integración con feeds de inteligencia mejorada, capacidades de automatización con IA, capacidades de integración con los sistemas de Madrid Digital, y amplia librería de casos de uso predefinidos; sin embargo, los procesos de orquestación, automatización y respuesta se presentan de forma general, no se detalla de forma diferencial como se opera, mantiene y administra la plataforma, y la integración con la solución NDR no se especifica.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa e integrada con el SIEM propuesto, licenciada para 4 “seats”, 4 analistas concurrentes. Se apoya en plataforma OpenSource con la posibilidad de utilizar API’s abiertas, *OpenAPI*.
- Respecto a la integración con herramientas o feeds de inteligencia, propone a disposición integración con fuentes comerciales reconocidas y con plataforma MISP. También ofrece capacidades de conexión e integración con todas las fuentes de eventos indicadas, incluido EDR.
- La solución SOAR propuesta se integra con las herramientas de *ticketing* de MD (ITSM- FARO) y del Centro Criptológico Nacional CCN-CERT (herramienta LUCIA) vía API. Se indica que será posible establecer sincronización bidireccional de incidentes.
- En referencia a casos de uso predefinidos, se proporcionan muchos *playbooks* construidos y documentados, destacando la capacidad de desarrollar nuevos *playbooks* personalizados para agregar nuevas funcionalidades a *playbooks* existentes o para integrar nuevas herramientas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Los procesos SOAR de orquestación, automatización y respuesta no se describen en detalle ni se presentan gráficos y ejemplos que permitan valorar su funcionamiento.
- No se detallan ningunas de las actividades de operación, mantenimiento, administración remota y monitorización de la solución SOAR de forma singular.
- La integración con el NDR no se define ni detalla a nivel de proceso con flujos, actividades y resultados, ni se indica posibles beneficios y/o ventajas.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.	1,8 puntos
---	-------------------

3.1.5.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **SOBRESALIENTE** ya que propone una solución SOAR completa y detallada de forma excepcional, integrada de forma nativa con el SIEM, enfocada no sólo al área de respuesta a incidentes, sino también al de prevención, con capacidades de automatización mejoradas con IA, capacidades de integración con los sistemas de Madrid Digital, amplia librería de casos de uso predefinidos, aportando explicación diferencial de cómo se opera, mantiene y administra la plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa del SIEM, licenciada por suscripción en base al número de analistas para la administración y operación de todas las actividades de análisis y respuesta a incidentes (4 analistas concurrentes). Además de esta solución se oferta una complementaria, orientada a la prevención. Estas dos visiones integradas permiten una coordinación automática entre las tareas de prevención y de respuesta, reducen la necesidad de intervención manual, permiten la aplicación dinámica de políticas de seguridad en base a vulnerabilidades, una gestión basada en riesgos, y una reducción de los tiempos de respuesta, creando un ciclo de mejora continua de las capacidades de prevención y respuesta.
- Se integra con las herramientas de inteligencia de amenazas de la plataforma ofertada de prevención soportando todos los protocolos de intercambio de fuentes de eventos y de inteligencia exigidos. Ofrece un amplio catálogo de aplicaciones integrables con el producto, entre los que se encuentran las soluciones para NDR y vulnerabilidades ofertadas, y herramientas de seguridad habituales como FW, IPS, EDR, correo, etc. Se recoge también la integración con LUCIA e ITSM-FARO.
- Facilita registro de todas las acciones llevadas a cabo por los usuarios, integrándose con la herramienta propuesta para gestión de ciber crisis, facilitando así el histórico de acciones realizadas y la toma de decisiones.
- Dispone de más de 200 *playbooks* predefinidos y facilita un editor visual para crear y modificar nuevos casos, y se detalla exhaustivamente las capacidades aplicadas de aprendizaje

automático e inteligencia artificial, complementadas con capacidades IA y LLM ofrecidas por soluciones complementarias ofertadas en la propuesta. Facilita también un espacio seguro para la investigación de incidentes.

- Se describe de forma diferencial como se opera y administra la plataforma SOAR. Actualizaciones y mejoras de herramientas sincronizadas con las del SIEM, asegurando que las nuevas funcionalidades y parches de seguridad sean implementados de manera consistente y sin interrupciones en la operación.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

3 puntos

3.1.5.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera que **NO APORTA VALOR** dado que no desarrolla en profundidad arquitectura de la solución propuesta, más allá de indicar que se trata de una solución nativa integrada con el SIEM ofertado. Tampoco facilita información suficiente en aspectos como las capacidades de integración con otras plataformas del pliego y equipos de seguridad, librerías de casos de uso predefinidos, o el plan de operación, mantenimiento, administración y monitorización de la plataforma.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

0 puntos

3.1.5.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **ADECUADA** debido a que oferta una solución perfectamente integrada con la solución de SIEM y un apartado completo de propuesta de desarrollo y entrega de *playbooks* de automatización; sin embargo, no concreta la integración de la solución con el resto de plataformas y equipos sobre los que previsiblemente actuará, ni detalles de operación y mantenimiento de plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución nativa integrada con la solución SIEM propuesta, dimensionada para permitir el acceso de 4 usuarios concurrentes, y un modelo de entrega de *playbooks* en modalidad servicio, a través de una unidad experta específica, que desarrollará las automatizaciones en función de su complejidad (baja, media, avanzada) y tiempos de respuesta acordes. Se ofrecen *playbooks* ya desarrollados por el licitador, basados en mejores prácticas, multi-tecnología y con enfoque extremo a extremo.
- La plataforma integra feeds de inteligencia de amenazas facilitadas por el propio fabricante del SIEM/SOAR y ofrece capacidades de aprendizaje automático, creación de modelos

personalizados, respuestas predefinidas y asistente AI con recomendaciones inteligentes para la toma de decisiones

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- La oferta no detalla la solución de integración de la herramienta con el resto de plataformas ofertadas, incluido el NDR, y equipos de seguridad habituales sobre los que actuar.
- Si bien se recoge la capacidad de integración con la herramienta de *ticketing* LUCIA, no se menciona la herramienta corporativa ITSM-FARO
- No se detallan actividades de operación, mantenimiento, administración y monitorización de la plataforma propuesta de forma singular.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

0,6 puntos

3.1.5.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de la **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **NOTABLE** debido a que presenta una solución muy sólida de SOAR nativo del SIEM propuesto, sin límite de usuarios concurrentes, complementada con una plataforma opensource que aporta capacidades adicionales de análisis entre otras, una propuesta de fuentes de inteligencia de amenazas muy completa, y un detalle exhaustivo de fuentes de eventos, equipos de seguridad y herramientas consideradas para introducir automatizaciones; sin embargo, no concreta las actividades de operación, mantenimiento, administración y monitorización de las dos plataformas propuestas, ni describe la integración con el NDR

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se presenta una solución SOAR nativa del SIEM sin límite de usuarios concurrentes, autoescalable, que asigna los recursos necesarios según se necesite, complementada con una solución opensource ampliamente utilizada como herramienta de gestión de ciberincidentes, que facilita capacidades adicionales automatización, enriquecimiento y análisis.
- Facilita detalle exhaustivo de las fuentes de alertas, equipos de seguridad, y herramientas consideradas para ofrecer un servicio integral de monitorización y respuesta a incidentes, incluyendo los sistemas de Madrid Digital ITSM-FARO, LUCIA y MISP.
- Amplia disponibilidad de *playbooks* integrados en la solución, que facilitan la personalización y creación de nuevos flujos de trabajo a través de herramientas gráficas visuales. Se describen también *workbooks* específicos para monitoreo del tiempo de ejecución de cada *playbook* y metodología de implementación de casos de uso y procesos automatizables, detallando actividades.
- Propuesta muy completa de integración de la plataforma con herramientas y feeds de inteligencia de amenazas y de enriquecimiento de contexto de incidentes. Destaca también las

capacidades de inteligencia artificial integradas en la solución, que permiten consultas en lenguaje natural sobre reputación, URL's, dominios, vulnerabilidades, actores maliciosos, etc.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detallan actividades de operación, mantenimiento, administración y monitorización de las dos plataformas propuestas, ni de integración con el NDR.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

2,4 puntos

3.1.5.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **BUENA** debido a que oferta una solución nativa a la solución de SIEM y, por tanto, perfectamente integrada, sin límite de usuarios concurrentes, con un amplio catálogo de *playbooks* y reglas de automatización ya predefinidos, e incorporación de capacidades de inteligencia artificial para búsquedas en lenguaje natural; sin embargo, no concreta la propuesta de integraciones con el resto de plataformas y equipos de seguridad, ni se detallan actividades de operación, mantenimiento, administración de la plataforma de forma singular.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Solución SOAR nativa de la solución SIEM propuesta, sin límite de usuarios concurrentes, y fácilmente escalable.
- Proceso de definición de automatizaciones completo, contemplando desde la identificación de los casos de uso a automatizar, el desarrollo del automatismo o las fases de pruebas y despliegue. Se dispone de reglas de automatización y *playbooks* predefinidos por el fabricante y desarrollados específicamente por el licitador.
- Se ofrece la posibilidad de incorporar herramientas de IA generativa para reforzar las capacidades de detección e identificación de actividad maliciosa, permitiendo búsquedas en lenguaje natural.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Mecanismos de integración con el resto de plataformas ni con las fuentes de eventos previstas contempladas (NDR, LUCIA, FARO, correo, DA, FW, etc.), a excepción de la herramienta de vulnerabilidades propuesta.
- No se detallan actividades de operación, mantenimiento, administración y monitorización de la solución.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

1,8 puntos

3.1.5.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **ADECUADA** debido a que se recogen las principales características de la solución propuesta y los sistemas iniciales con los que se integrará para la orquestación, automatización y respuesta; sin embargo, no concreta otros elementos de seguridad susceptibles de automatizar o en nube, *playbooks* de automatización, o actividades relacionadas con la operación y mantenimiento, administración, monitorización singular de la plataforma.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se oferta solución nativa completamente integrada con la solución SIEM, optimizando así los flujos de trabajo de seguridad, y facilitando una gestión centralizada y una visión completa del ciclo de vida de los incidentes, desde la detección hasta la respuesta automatizada.
- Se detallan los sistemas iniciales que se integrarán en la solución de SOAR propuesta, del SOC del licitador como son su sistema interno de *ticketing*, plataforma MISP o herramientas específicas de análisis, y específicas de Madrid Digital como son el sistema de *ticketing* FARO, la plataforma LUCIA, la plataforma REYES, el correo, y la solución NDR ofertada.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Interacción de la solución con elementos, sistemas en nube y otros elementos de seguridad, fundamentales en la definición de automatizaciones (cortafuegos, EDR, directorio activo, etc.).
- Se menciona la puesta a disposición de *playbooks* predefinidos por el licitador, pero no se detalla cantidad, tipología ni propuesta concreta de conjunto mínimo inicial a configurar.
- Actividades de operación y mantenimiento, administración y monitorización de la solución de forma singular.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

0,6 puntos

3.1.5.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U – CIPHERBIT, S.L.U.** a este criterio se considera **NOTABLE** ya que propone solución SOAR descrita en detalle, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con soluciones NDR y con los sistemas de Madrid Digital, y amplía librería de casos de uso predefinidos; sin embargo, al ser la solución SOAR parte del SIEM el licitador se limita a indicar que las actividades de operación, mantenimiento y

administración remota son la mismas del SIEM sin aportar casuística diferencial, ni se describe la integración con el NDR.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Oferta una solución SOAR nativa e integrada con el SIEM propuesto, licenciada por suscripción y como mejora ofrece acceso ilimitado de analistas concurrentes. Se describen los procesos SOAR de orquestación, automatización y respuesta.
- Respecto a la integración con herramientas o feeds de inteligencia soporta reputación de IP's y URL's/dominios, y proporciona soporte completo para la integración de amplio número de IOC's a través de su API REST. Ofrece capacidades de IA generativa integrada también con el SIEM. También se indica la integración con conectores para todas las fuentes de eventos indicadas, y también con la herramienta de gestión de vulnerabilidades ofertada.
- Se recoge también la integración con ITSM-FARO (producto BMC) de forma nativa y se describe que la integración con LUCIA se realizará vía API.
- Amplia librería de casos de uso ya desarrollados con integraciones y flujos de trabajo preconfigurados, se indican ejemplos de muchos de ellos.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No se detallan ningunas de las actividades de operación, mantenimiento, administración remota y monitorización de la solución SOAR de forma singular, ni se describe la integración con el NDR.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.5 – Servicio de orquestación, automatización y respuesta – SOAR. Hasta 3 puntos.

2,4 puntos

3.1.6 CRITERIO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis. Hasta 4 puntos.

3.1.6.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **ADECUADA**, ya que describe sin profundizar la metodología y procedimientos de los servicios de análisis forense y gestión de ciber crisis; sin embargo, no aporta suficiente información sobre la propuesta del servicio de análisis y respuesta a incidentes, la organización de los recursos en base a niveles de criticidad y capacidades técnicas requeridas, y la integración de todos los canales de notificación y protocolos de activación de equipos adicionales.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Respecto al análisis forense, desarrolla a alto nivel la metodología y enfoque de actuación describiendo las fases por las que pasará el análisis. Incluye una propuesta de elaboración de informe final.

- En cuanto a la gestión de ciber crisis, describe sin profundidad las distintas tareas mínimas de las que constará el servicio, entre las que se encuentran: la evaluación de incidentes de seguridad graves, la definición de medidas de contención y eliminación, la definición y desarrollo de medidas de recuperación, el soporte en la gestión de la comunicación durante la crisis, el soporte a las actividades de comunicación corporativa y la elaboración del informe final de ciber crisis.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo a lo indicado para este criterio, en los siguientes aspectos:

- Poco detalle en el procedimiento y metodología del servicio de análisis y respuesta a incidentes, limitándose a describir las actividades solicitadas en el pliego.
- Falta profundidad en la organización de los recursos, identificando, únicamente para el caso del servicio de análisis y respuesta a incidentes, los analistas que integrarán el servicio. Tampoco detalla los protocolos de activación de equipos adicionales
- No describe cómo se realiza la integración de todos los canales de notificación.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis. Hasta 4 puntos.

0,8 puntos

3.1.6.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **NOTABLE**; ya que recoge de forma idónea y completa la metodología y procedimientos explicativos de cada uno de los servicios, incluyendo esquemas ilustrativos complementarios y claros, así como la propuesta de integración de herramientas de *ticketing* con el SOAR. Sin embargo, falta detalle en la organización de los recursos en base a servicios, niveles de criticidad y capacidades técnicas, y los planes de recuperación y protocolos de activación de equipos adicionales.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Respecto al servicio de análisis y respuesta a incidentes, la metodología, los procedimientos y los procesos se describen de forma detallada, con todas las fases de identificación, análisis y respuesta claramente descritas y amplio catálogo de informes y entregables.
- En cuanto al análisis forense, describe igualmente una metodología estructurada y detallada, dividida en seis etapas que van desde la preparación y evaluación a la presentación de resultados y lecciones aprendidas. Incluye una descripción de las principales herramientas a utilizar.
- En relación con la gestión de ciber crisis, detalla el procedimiento a seguir incorporando un diagrama ilustrativo claro y completo. Incluye la descripción del comité de crisis y del grupo de intervención rápida, equipo compuesto por expertos en dar respuesta a incidentes de ciber seguridad. Este equipo, si fuera necesario, se desplazará físicamente a las dependencias de Madrid Digital afectadas para establecer entornos de contención y organizar la recuperación ante la declaración de un incidente.

- Se describe la integración de la herramienta SOAR con los distintos canales de notificación de incidentes mediante API propias, permitiendo la sincronización bidireccional de incidentes, con gestión unificada desde una única consola.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo a lo indicado para este criterio, en los siguientes aspectos:

- Organización de los recursos en base a niveles de criticidad y capacidades técnicas, no suficientemente detallado, ni protocolos de activación de equipos adicionales.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis. Hasta 4 puntos.

3,2 puntos

3.1.6.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **ADECUADA**; ya que describe pormenorizadamente las herramientas empleadas en el servicio de análisis forense, los distintos tipos de análisis que podrán realizarse y las medidas de contención propuestas. Se menciona también la integración de los principales canales de notificación en los servicios descritos; sin embargo, no detalla cómo va a realizarse esta integración. Respecto a los servicios de análisis y respuesta y análisis forense se proponen metodologías y procedimientos poco orientados a los requerimientos del pliego. Por último, define sin profundidad la propuesta de organización de los recursos del proveedor y los protocolos de activación de equipos adicionales.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Propuesta de elaboración de informes suficientemente detallada para cada uno de los servicios. Menciona que utilizará *playbooks* automatizados, elaborados mediante diagramas de flujo en formato BPM. Para la gestión de ciber crisis, incluye la definición de los principales KPI para medir la calidad del servicio.
- En cuanto al análisis forense, la descripción de las herramientas es muy correcta y ajustada a los distintos escenarios (por ejemplo, herramientas para la adquisición de evidencias, análisis de *malware*, análisis del registro de Windows, etc.). Se hace foco también en la descripción de los distintos tipos de análisis a realizar y medidas de contención.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta de claridad en la metodología, procedimientos y capacidades propuestas para cada uno de los servicios. La descripción de tareas parece mezclada entre los distintos servicios.
- No describe en profundidad la propuesta de integración de los diferentes canales de comunicación: CCN-Lucia, ITSM-FARO, áreas técnicas de Madrid Digital y organismos externos con el equipo prestador del servicio.
- Propuesta de organización de los recursos del proveedor y protocolos de activación de equipos adicionales poco claros.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

0,8 puntos

3.1.6.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **BUENA** debido a que describe la metodología y los procedimientos asociados a cada uno de los servicios, la integración de los principales canales de notificación a utilizar por los distintos servicios, y la propuesta de organización de los recursos del proveedor y los protocolos de activación de equipos adicionales; sin embargo, no profundiza en ninguno de estos aspectos valorables, quedándose en la mayoría de casos en un listado de características y funcionalidades a alto nivel.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Respecto al servicio de análisis y respuesta a incidentes, indica que emplea las mejores prácticas de respuesta ante incidentes, como las recomendadas en la guía *Guide to Integrating Forensic Techniques into Incident Response Special Publication 800-86* del NIST estadounidense o en la guía *CCN-STIC 817 de Gestión de Ciberincidentes del CCN-CERT*.
- Detalla de manera satisfactoria cada fase en el análisis forense, incluyendo el almacenamiento de evidencias para el que propone plazos en función de la criticidad del incidente. De igual modo, indica que dispone de hardware forense (clonadora, bloqueadores de escritura, etc.) y de software especializado que permite la adquisición con garantías legales de dispositivos de los principales sistemas operativos, así como de terminales móviles y procedimientos para la adquisición de logs en la nube.
- Describe la integración de las herramientas de *ticketing* con las herramientas SIEM/SOAR propuestas: bien a través de un modo sencillo como el correo electrónico, bien a través de REST API.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Respecto a la metodología y procedimientos del servicio de análisis y respuesta a incidentes, no propone nuevas automatizaciones para la herramienta SOAR. Tampoco desarrolla estrategias de contención ni incluye una propuesta de lecciones aprendidas. Respecto a la gestión de cibercrisis, detalla las actividades de las que se encargará al que denomina Gestor del Incidente sin profundizar en el desarrollo del servicio en sí.
- Falta descripción detallada de la propuesta de organización del equipo de trabajo y los procedimientos de activación de los servicios adicionales.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

2,4 puntos

3.1.6.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **NOTABLE**; describe de forma clara y completa la metodología, procedimientos, capacidades y herramientas tanto del servicio de análisis y respuesta como el de gestión de cibercrisis, define la propuesta de organización de los recursos del proveedor y los protocolos de activación de equipos adicionales e informa de la integración de los principales canales de notificación; sin embargo, en cuanto al análisis forense, no profundiza en las características de este servicio, limitándose a describir la metodología a utilizar y las herramientas.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Respecto al servicio de análisis y respuesta a incidentes, destaca el asistente inteligente que apoya a los analistas de operaciones de seguridad. Dicho asistente ofrece sugerencias para ayudar a investigar, contener, erradicar y recuperarse de un incidente de seguridad. Funciona conectando la información de los eventos de seguridad con las herramientas del SOC y los *playbooks* (automatizaciones) definidas. También propone un ejemplo detallado y completo de automatización sobre múltiples accesos remotos VPN fallidos. De igual modo, respecto a los *playbooks*, propone un ejemplo práctico relacionado con ransomware.
- Respecto a la integración de la solución con las herramientas de *ticketing*, describe cómo realizar el proceso a través de los conectores.
- En relación al análisis forense, indica el uso de herramientas de amplio reconocimiento en el mercado que garantiza que el proceso sea riguroso, metodológico y que la evidencia recolectada sea válida y utilizable, especializándose en el análisis técnico detallado de la evidencia, así como en la gestión de casos y la correlación de datos a un nivel más amplio, facilitando la colaboración y la comunicación efectiva durante la investigación.
- En cuanto a la gestión de cibercrisis, incluye una herramienta de gestión de Cibercrisis Escalado y Activación del Equipo de Gestión de Crisis, gracias a la cual se puede crear de forma automática un entorno de colaboración para el equipo de crisis, generando salas de *war room* virtuales donde se llevan a cabo las reuniones y se intercambia información crítica.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- En cuanto al análisis forense, falta profundidad en la distinción de los distintos tipos de análisis, equipo de trabajo, almacenamiento de la información forense durante la duración del contrato, la remisión de IOC's, la cadena de custodia y el proceso de desplazamiento de técnicos a las instalaciones de Madrid Digital en caso de que fuera necesario.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

3,2 puntos

3.1.6.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA**; describe a alto nivel la metodología y procedimientos a seguir de cada uno de los servicios; sin embargo, no profundiza en las capacidades, herramientas, organización de los recursos, protocolos de activación e integración de los principales canales de notificación.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- En relación al servicio de análisis y respuesta a incidentes, describe los tipos de incidentes más habituales y la información que se maneja en cada uno de ellos.
- Respecto al análisis forense, indica que hará uso de una plataforma de análisis de amenazas de malware (*sandbox*) para generar informes de análisis detallados sobre el sistema, la red, y comportamientos de manipulación de código y comunicaciones.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Respecto a la metodología y procedimientos, falta una descripción detallada del servicio de análisis y respuesta atendiendo a criterios como, planes de respuesta ante incidentes específicos y estrategias de contención de ataques. Respecto al análisis forense, falta profundidad en la descripción del almacenamiento de la información forense, remisión de IOC's y elaboración de procedimientos de preservación de evidencias y cadena de custodia. En cuanto a la gestión de ciber crisis, falta concreción en la identificación de datos necesarios para la puesta en marcha de los servicios.
- No describe la integración de los canales de recepción de notificaciones.
- No detalla la organización del equipo de trabajo para cada uno de los servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis. Hasta 4 puntos.

0,8 puntos

3.1.6.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **ADECUADA** dado que define de manera completa las actividades a realizar para gestionar el servicio de análisis y respuesta, algo que también lo hace para el servicio de ciber crisis; sin embargo, no profundizan en detallar el servicio de análisis forense, ni en la organización del servicio así como los métodos de activación de los servicios a demanda, ni en detallar cómo será la integración de la herramienta con los canales de notificación de las alertas/incidentes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de análisis y respuesta se explican las actividades a realizar para gestionar una alerta y los posteriores pasos en caso de derivar en un incidente.

- En cuanto al servicio de gestión de cibercrisis, ofrecen su servicio de gestión de crisis, formado por un equipo de expertos para actuar en estas situaciones, además detallan las actividades a realizar durante el ciclo de vida de una crisis, agrupadas en las fases que lo componen.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Con respecto al servicio de análisis forense se indica el ciclo de vida del análisis, junto con algunas actividades a realizar, pero no se detalla nada al respecto sobre tipos de informes han emitir según el incidente, que procedimientos se seguirán para preservar evidencias, recolectar datos, etc.
- La propuesta de organización del servicio no se detalla en profundidad, se limita a indicar lo solicitado y no se definen procedimientos de activación de los servicios adicionales.
- Aunque indican que la herramienta de SOAR se integrará con las herramientas del CCN sobre el resto de canales de entrada de alertas (correo, herramientas de *ticketing*, etc.) sólo se indica que se integrará en el flujo operativo no detalla cómo ni si lo hará en la herramienta.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

0.8 puntos

3.1.6.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera que **BUENA** dado que detalla las actividades a realizar para gestionar el servicio de análisis y respuesta, también detalla el servicio de análisis forense y cómo gestionar una cibercrisis; sin embargo, no establecen la organización de los recursos para el servicio ni los procedimientos de activación de los servicios adicionales, como tampoco indican cómo se integrarán los canales de notificación de incidentes de Madrid Digital con las herramientas del servicio.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de análisis y respuesta se describe la metodología que se usará, además de detallar las etapas a seguir junto con las actividades que la componen. También se indican posibles herramientas y tecnologías de las que hará uso el servicio para la investigación del incidente. Una vez finalizada la investigación se culminará con un informe detallado de ésta.
- Con respecto al servicio de análisis forense se indica que se seguirá una metodología de la cuál describen las fases más importantes siendo la última fase la generación de un informe detallado con la información necesaria para asegurar su validez ante la autoridad judicial.
- En cuanto al servicio de gestión de cibercrisis, se detallan los componentes de los diversos comités y qué responsabilidades tiene cada uno y actividades a realizar.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- No detallan como estará organizado el servicio de análisis y respuesta, solo que se hará como se solicita en el pliego y no especifican como se activarán los servicios adicionales.
- Aunque indican que recogerán y notificarán las alertas de todos los canales, FARO, correo, LUCIA, no especifican si esos canales estarán integrados con la herramienta SOAR ofertada.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

2,4 puntos

3.1.6.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **ADECUADA** dado que propone la metodología a seguir y detalla las actividades a realizar para gestionar el servicio de análisis y respuesta, también detalla cómo se integrarán las distintas herramientas de notificación de Madrid Digital con los servicios; sin embargo no desarrolla el servicio de análisis forense ni la organización de los recursos y procedimientos de activación de servicios adicionales para el servicio de análisis y respuesta.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de análisis y respuesta se indican la metodología a seguir junto con las actividades a realizar, considerando las opciones de remediación automáticas o manuales, según la casuística del incidente.
- Se indica que la herramienta de SOAR ofertada se integrará con los distintos canales de notificación de incidentes y se describe cómo.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Con respecto al servicio de análisis forense se indica que se realizará en caso de ser necesario por un equipo experto, pero no se detalla que procedimientos se seguirán para ello, como se obtendrán y preservarán los datos recogidos, los tipos de informes a elaborar o la validez jurídica de los mismos.
- En cuanto al servicio de gestión de cibercrisis, aunque se indica que tienen personal cualificado para realizar este servicio, no se detalla cómo se prestará más allá de indicar que harán lo que se ha solicitado en el pliego, se cuenta de manera generalista.
- No se define como será la organización del servicio de análisis y respuesta, indicando por quien estará formado, ni definen los procedimientos y canales de activación, en caso de ser necesario, de los servicios adicionales.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

0,8 puntos

3.1.6.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **ADECUADA** dado que se detalla de manera completa las actividades a realizar para gestionar el servicio de análisis y respuesta y el servicio de cibercrisis; sin embargo, no profundizan en las actividades del servicio de análisis forense ni en cómo se integrarán las herramientas de notificación de Madrid Digital con la herramienta propuesta de SOAR, ni se definen los procedimientos de activación de los servicios adicionales.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de análisis y respuesta se indica la metodología a seguir junto con las fases y puntos clave para obtener la información necesaria para valorar el incidente y realizar las acciones necesarias para contenerlo. Además, indica la integración de este servicio con el de monitorización a través de herramientas para tener un seguimiento unificado. También se indica que se usaran capacidades de *Machine Learning* e Inteligencia Artificial para optimizar el servicio.
- En cuanto al servicio de gestión de cibercrisis, se indica que se seguirán las normas vigentes en cibercrisis, también se detallan las fases en las que se divide dicha gestión junto con las actividades a realizar en cada fase, obteniendo al finalizar los informes correspondientes de resumen del incidente y lecciones aprendidas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Con respecto al servicio de análisis forense, aunque se indica la normativa por la que se rigen, así como posibles tipos de análisis a realizar, según lo solicitado en el pliego, no detallan actividades a realizar ni actuaciones según sea el tipo de incidente o pasos necesarios para obtener informes válidos jurídicamente, etc.
- Aunque indican que la herramienta de SOAR se conectará con las distintas herramientas de notificación de Madrid Digital y CCN no se concreta como se realizará dicha integración.
- Se indica el equipo de trabajo que formará parte del servicio, tal y como se solicita en el pliego, sin mayor detalle. Tampoco se definen los procedimientos y/o canales de activación en caso de ser necesaria la activación de servicios adicionales.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

0,8 puntos

3.1.6.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **NOTABLE** dado que detalla correctamente las actividades a realizar para gestionar el servicio de análisis y respuesta, el servicio de análisis forense y se establece la organización de los recursos para el servicio de análisis y respuesta y los procedimientos de activación de los servicios adicionales; sin embargo, el servicio de gestión de cibercrisis se recoge superficialmente.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Para el servicio de análisis y respuesta se aporta una metodología a seguir y se detallan las actividades a realizar ante un incidente, análisis, recopilación de datos, posterior informe con los datos del incidente (causa raíz, acciones realizadas, calificación, propuesta de mejora y lecciones aprendidas).
- Con respecto al servicio de análisis forense se indica la metodología a seguir junto con los principios que la forman. También detallan y explican los pasos necesarios en la realización del análisis, así como posibles tipos de investigaciones a realizar según sea el incidente, tipos de informes que se pueden ofrecer y otros detalles sobre actuaciones necesarias para que, en caso de ser necesario, el análisis sea completo y válido jurídicamente.
- Se define en detalle cómo será la organización del servicio de análisis y respuesta, indicando por quien estará formado, cómo dar cobertura 24x7x365 al servicio, y los procedimientos y canales de activación, en caso de ser necesario, del soporte 24x7x365.
- En cuanto al servicio de gestión de cibercrisis, se indica que se seguirá una metodología desarrollada por la UTE relacionando varias fases.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes puntos:

- Falta detalle y explicación del contenido de las fases del servicio de gestión de cibercrisis que permita determinar todo su alcance.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 7.6 – Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis. Hasta 4 puntos.

3,2 puntos

3.2 CRITERIO NÚMERO 8: PLANES OPERATIVOS. HASTA 10 PUNTOS.

3.2.1 CRITERIO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

3.2.1.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **SOBRESALIENTE** ya que realiza una propuesta clara y completa, indicando el despliegue de las plataformas implicadas en cada servicio, incluyendo un cronograma detallado, siendo relevante la explicación de las fases y actividades del SIEM, SOAR y NDR. También especifica la organización del equipo de trabajo del SOC

incluyendo los servicios de soporte 24x7, aportando y explicando el plan requerido para el mantenimiento y operación de los servicios de ciberseguridad ya desplegados.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se especifica un plan general bien organizado y explicado con claridad, aportando esquemas de los diferentes procesos, e identificando la información, datos necesaria para la puesta en marcha de cada servicio. Detalla el despliegue de las plataformas utilizadas, explicando para cada una las fases y actividades a realizar.
- Incluye un cronograma en el que se incluyen los hitos de la fase de implantación para cada uno de los servicios, cumpliendo todos los plazos requeridos, incluso poniendo disponible la CMDDB antes de lo solicitado. También se indica el equipo humano asociado a la implantación de cada servicio.
- Se detalla despliegue de las plataformas para las soluciones de SIEM/SOAR y NDR, acompañado de gráficos que facilitan su entendimiento.
- Se especifica el equipo de trabajo para cada servicio, no solo cumpliendo con lo requerido sino aportando más perfiles que permitan realizar de forma óptima el trabajo.
- Sobre el mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital, se indican las diferentes fases para llevarlo a cabo, así como el calendario y los perfiles asociados a estas actividades.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

6 puntos

3.2.1.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE S.A.U.** a este criterio se considera **SOBRESALIENTE** ya que realiza una propuesta estructurada, en la que se plantea una metodología con diferentes fases para la implantación de los servicios, con identificación de información necesaria, planificación y duración de cada actividad dentro de las fases, se hace hincapié en el despliegue de las soluciones SIEM, SOAR y NDR, se indica la organización del SOC incluyendo los servicios 24x7 y se aporta la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se especifica un plan general de implantación bien estructurado con una metodología dividida en varias etapas, desglosando las actividades de cada fase, así como los entregables asociados, y asociando el equipo o perfil encargado de llevar a cabo su ejecución. También se recoge la información necesaria y se plantea cómo realizar la gestión de los riesgos asociados al plan de implantación.
- Se proporciona un diagrama de Gantt para la implantación de los servicios, indicando la planificación y duración de cada actividad dentro de las diferentes fases del plan de implantación. Se incluye una matriz RACI relacionando los principales perfiles del proyecto y las actividades de cada etapa.

- Se detallan las actividades relacionadas con el despliegue de las plataformas para las soluciones de SIEM, SOAR y NDR.
- Se incluye la composición del equipo de trabajo, indicando los perfiles asociados a cada servicio del SOC, e incluyendo los servicios que se prestan con disponibilidad 24x7. También se indican las actividades relacionadas con el flujo de gestión de alertas y las interrelaciones entre los diferentes niveles de perfiles del servicio de monitorización y detección de ciberincidentes.
- Sobre la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital, indica calendario, fases y personal dedicado.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

6 puntos

3.2.1.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **ADECUADA** ya que desarrolla un plan de proyecto a alto nivel idóneo, con identificación de las actividades principales a ejecutar para la puesta en marcha de cada servicio; sin embargo, falta el plan de detalle de actividades asociadas a la puesta en marcha del NDR, falta detalle en la planificación de actividades y seguimiento de la organización del SOC y en la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plan de proyecto de alto nivel identificando las principales actividades asociadas a la puesta en marcha de cada servicio. Plan de migración del SIEM/SOAR. Planificación mediante diagrama Gantt de proyecto.
- Matrices de tareas por fases, recogiendo la implantación tanto de herramientas como de soluciones propuestas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Plan de fases y actividades asociadas a la puesta en marcha de la solución NDR.
- Detalle en la planificación y calendario de ejecución de cada una de las actividades identificadas, así como en la organización del SOC, incluyendo los servicios 24x7, sistemas de *ticketing*, con detalle de actividades y recursos operativos dedicados a cada uno de los servicios.
- Mayor desarrollo en la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital, ya que carece de actividades, perfiles y calendario.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

1,2 puntos

3.2.1.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **NOTABLE** ya que propone un plan de proyecto completo, claro y bien estructurado, con todas las fases y actividades asociadas a la implantación de todos los nuevos servicios e identificando la información necesaria, destaca el plan de implantación de la solución SIEM, SOAR y NDR y el mantenimiento y operación de los servicios actuales, todo planificado asegurando su coexistencia; sin embargo, no profundiza en la implantación de la organización del SOC y los servicios de soporte 24x7.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plan de proyecto general organizado en cinco fases, orientadas a la preparación inicial, análisis y diseño de la solución, despliegue de la solución, integración de fuentes y validación, optimización y formación.
- Describe de forma completa, idónea y clara, para cada fase, los objetivos de todas las actividades asociadas, identificando el equipo humano para cada una de ellas y definiendo un calendario de actuación en consonancia al solicitado por pliego.
- Detalla, con especial consistencia, todas las fases relacionadas con la instalación del sistema SIEM/SOAR y NDR, su calendario y el equipo humano asociado.
- Detalla una estrategia de mantenimiento y coexistencia de los servicios de ciberseguridad ya desplegados clara y completa; dividida por fases de las que destacan la transición gradual y supervisada, el mantenimiento preventivo, la coordinación entre los servicios y la evaluación continua del impacto.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en relación con:

- La implantación de la organización del SOC y los servicios de soporte 24x7, pues no especifica las interrelaciones entre los equipos dedicados y equipos no dedicados del adjudicatario y los sistemas de *ticketing*/seguimiento propuestos para el plan de implantación.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

4,8 puntos

3.2.1.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **SOBRESALIENTE** ya que propone un plan de proyecto completo, muy bien estructurado y claro, con todas las fases y actividades asociadas a la implantación de todos los servicios del SOC, identificando previamente la información necesaria, se aporta planes de detalle específicos de puesta en marcha SIEM, SOAR y NDR, y propuesta planificada de organización del SOC, considerando la operación y mantenimiento de los servicios actuales .

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Plan de proyecto general orientado a servicios y subdividido a su vez en fases claras y sencillas, entre las que se incluyen: una fase inicial de arranque, una de adquisición y transformación de

los servicios, despliegue e implantación, identificando la información necesaria para cada una de ellas.

- Describe de forma clara y completa, para cada fase, los objetivos de todas las actividades asociadas, implementando un plan minucioso para cada uno de los subservicios dentro de los servicios principales (prevención, detección, etc.) incluyendo el equipo humano dedicado y el calendario de actuación.
- Detalla, con especial consistencia, todas las fases relacionadas con la instalación del sistema SIEM, SOAR y NDR, su calendario y el equipo humano asociado.
- Detalla la propuesta de organización del SOC y los servicios de soporte 24x7, dentro de cada una de las fases del plan, destacando las integraciones definidas en cada una de dichas fases.
- Dentro de cada fase, detalla la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados, destacando una auditoria previa del estado de los sistemas para identificar claramente si existe algún riesgo asociado actualmente al servicio cuya respuesta/mitigación deba ser priorizada.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

6 puntos

3.2.1.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA** ya que propone un plan de proyecto específico de cada uno de los servicios, identificando las actividades asociadas a la puesta en marcha de cada uno de ellos y el calendario propuesto, además tiene en cuenta la operación y mantenimiento de los servicios actuales; sin embargo, falta un plan general a alto nivel con distinción clara entre cada uno de los servicios, falta detalle en el despliegue de la plataforma SIEM, SOAR y NDR, y no se ha especificado la implantación de la organización del SOC y los servicios 24x7.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Estructura del plan por fases, incluyendo una planificación específica mediante diagrama de Gantt de cada uno de los servicios, identificando las principales actividades asociadas a su puesta en marcha.
- Definición clara de la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No se presenta plan general a alto nivel identificando los datos necesarios para la puesta en marcha de todos los servicios (datos críticos, infraestructuras y sistemas a supervisar, capacidades de seguridad, procedimientos de la seguridad).
- No existe plan de específico detallado de despliegue de las plataformas SIEM, SOAR y NDR.

- Organización del SOC, incluyendo los servicios 24x7, detallando los recursos operativos dedicados a cada uno de los servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

1,2 puntos

3.2.1.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **BUENA** debido a que propone un plan de puesta en marcha para cada uno de los servicios y herramientas (SIEM, SOAR y NDR), identificando las actividades asociadas junto con el calendario, además identifica los datos necesarios para la puesta en marcha de cada servicio; sin embargo, no concreta el mantenimiento y la operación de los servicios actuales ni las actividades necesarias para organizar el nuevo SOC y el soporte 24x7.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se identifica los datos necesarios a tener en cuenta para la puesta en marcha de los servicios, detallando que información es necesaria por cada servicio solicitado.
- Detalla la puesta en marcha del servicio mediante un plan claro y estructurado que especifica las distintas etapas necesarias para conseguir que los servicios se desplieguen con el mínimo riesgo, dicho plan abarca todos los aspectos relevantes, desde la planificación inicial hasta la evaluación final, junto con una gestión de riesgos.
- Propone un cronograma detallado de las actividades a realizar en cada fase necesaria para desplegar las herramientas solicitadas, SIEM, SOAR y NDR, junto con el equipo que realizará cada una de las tareas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No detallan la organización del SOC, sus actividades y recursos dedicados a ellas, sólo se indican los servicios y personal asignado a cada uno de ellos. Tampoco se detallan las actividades que necesitarán los servicios 24x7, sólo que servicios lo tendrán.
- La propuesta de mantenimiento y operación de los servicios ya desplegados es escueta, no detallan que equipo se hará cargo de ellas ni cómo. Sólo se indica que lo harán y durante el tiempo estipulado hasta la implantación de los nuevos servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

3,6 puntos

3.2.1.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. – NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **BUENA** ya que realiza una propuesta de implantación con una metodología en varias fases diferenciadas, especifica una propuesta de despliegue para el SIEM, SOAR y NDR e indica la organización de los perfiles del SOC incluyendo los servicios 24x7; sin embargo, la propuesta de puesta en marcha es genérica, no está especificada para cada servicio de forma independiente y hay pocos detalles sobre la propuesta de mantenimiento y operación de los servicios de ciberseguridad desplegados en Madrid Digital.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se especifica un plan de implantación general con diferentes fases, indicando las actividades en cada de las subfases de las fases principales. Se incluye un calendario de actividades que indica el despliegue de soluciones y el despliegue de servicios. También se incluye un diagrama con la participación de los miembros del equipo en cada fase de plan de implantación.
- Se hace hincapié en los detalles del despliegue de las plataformas para las soluciones de SIEM, SOAR y NDR. Se propone la migración de MVP (*minimum viable product*) para un despliegue ágil de las nuevas soluciones y migración de los casos de uso. Respecto a la migración de fuentes, se proponen varias opciones de cómo se podría realizar y se propone la priorización de fuentes de información.
- Se recoge la propuesta organización y composición del equipo de trabajo de los diferentes servicios del SOC incluyendo el soporte en horario 24x7.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- La propuesta de puesta en marcha está planteada de forma genérica, sin especificar con suficiente detalle el plan para cada uno de los servicios de modo independiente.
- Sobre la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital, no se aporta información ni detalle como las fases para llevarlo a cabo, calendario y perfiles asociados a estas actividades.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.	3,6 puntos
---	-------------------

3.2.1.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **NOTABLE** debido a que identifican los datos necesarios para la puesta en marcha, así como detallan un plan completo de migración y puesta en marcha para cada uno de los servicios y herramientas (SIEM, SOAR y NDR), junto con las actividades a realizar durante el tiempo de mantenimiento y la operación de los servicios actuales hasta

su migración; sin embargo no detallan las actividades necesarias para implantar y organizar el nuevo SOC.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se identifica los aspectos y datos necesarios a tener en cuenta para la puesta en marcha de los servicios, clasificándolos por ámbito y detallando las actividades a realizar junto con los entregables/hitos para cada ámbito.
- Propone un plan de puesta en marcha de cada uno de los servicios detallando las actividades necesarias para ello junto con un cronograma, además propone una gestión del riesgo para evitar o mitigar los riesgos asociados a dicha implantación.
- Propone un plan detallado de las actividades a realizar en cada fase necesaria para desplegar las herramientas solicitadas, SIEM/SOAR y NDR, junto con un cronograma.
- La propuesta de mantenimiento y operación de los servicios ya desplegados, una vez se ha hecho la transferencia de conocimiento del proveedor anterior, es completa y detalla las actividades a realizar.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No detallan las actividades ni recursos asociados a cada actividad que formaran parte de la organización del nuevo SOC, sólo se enumeran los servicios solicitados y personal asignado a cada uno de ellos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

4,8 puntos

3.2.1.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. – CHG- MERIDIAN SPAIN, S.L.U.** a este criterio se considera **SOBRESALIENTE** ya que realiza una propuesta muy completa sobre la implantación, identificando información necesaria y explicando con mucho detalle las fases y actividades asociadas a la implantación de todos los servicios solicitados, incluso a nivel de subservicios, destacando los planes de puesta en marcha SIEM, SOAR y NDR, y la propuesta de organización del nuevo SOC. Se incluye también la operación de los servicios de ciberseguridad ya desplegados hasta su migración

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se especifica un plan general muy completo y detallado, estructurado acorde a los diferentes servicios que se prestan, con identificación de información necesaria.
- Describe con gran nivel de detalle, los objetivos, fases y entregables contempladas en el periodo de implantación para todos y cada uno de los servicios, incluso a nivel de subservicios dentro de los servicios principales. Se incluye el calendario de actuación para cada servicio y se hace hincapié en que se la migración asegure la continuidad del servicio sin interrupciones.
- Detalla, con especial consistencia, todas las fases relacionadas con la instalación del sistema SIEM, SOAR y NDR, incluyendo el calendario asociado.

- Especifica una propuesta de organización del SOC, incluyendo interacciones entre servicios. Sobre los servicios de soporte 24x7, se citan sus responsabilidades, vinculaciones con otros servicios y herramientas a utilizar.
- Con relación a la propuesta de mantenimiento y operación de los servicios ya desplegados, se especifica cómo realizar la migración de las plataformas actuales a las nuevas. Se hace referencia a un plan de asunción de servicios y plan operativo de toma de control, donde se refleja la planificación del proceso de transición y los entregables asociados.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

6 puntos

3.2.1.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **BUENA** debido a que identifica los datos e información necesaria para la puesta en marcha de los servicios, propone un plan detallado de puesta en marcha para los servicios y herramientas que lo soportan (SIEM, SOAR y NDR) y herramienta de vulnerabilidades, e indican cómo mantendrán el servicio actual; sin embargo, no detalla el plan de puesta en marcha del total de los servicios, faltando también la propuesta de implantación de la organización del nuevo SOC y de los servicios 24x7.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se identifican los aspectos y datos necesarios para la puesta en marcha de los servicios.
- Propone un plan detallado de las actividades a realizar en cada fase necesaria para desplegar el SIEM, SOAR con tiempos estimados y con una arquitectura propuesta. Para el despliegue e implantación del NDR se establece un cronograma con las actividades a realizar y configuraciones necesarias. Se presenta también el despliegue de la herramienta de análisis de vulnerabilidades.
- Proponen mantener el servicio con los actuales recursos y dedicar nuevos a la implantación de los nuevos servicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta plan de puesta en marcha de algunos de los servicios, a excepción de los que soporta el despliegue del SIEM, SOAR, NDR y herramienta de análisis de vulnerabilidades, que sí aparecen descritos.
- No se detalla la propuesta de organización del nuevo SOC, de los servicios de soporte 24x7 y de las interrelaciones de los equipos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.1 – Plan de implantación de los servicios. Hasta 6 puntos.

3,6 puntos

3.2.2 CRITERIO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

3.2.2.1 EVOLUTIO CLOUD ENABLER S.A.U.

La propuesta de **EVOLUTIO CLOUD ENABLER S.A.U.** a este criterio se considera **SOBRESALIENTE**, debido al planteamiento de una metodología clara de operación de los servicios y a los detalles sobre el modelo de relación propuesto, aportando procedimientos operativos consistentes. Además, se especifican KPI's y KRI's junto con una herramienta para mejorarlos. El plan de devolución del servicio está bien estructurado y se profundiza en el proceso de borrado de datos.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se explican en detalle las diferentes fases de la metodología y se establecen sus objetivos, apoyándose en el framework FIRST.
- Los procedimientos operativos se proponen de forma agregada, contemplando todos los servicios solicitados, considerando las peculiaridades de cada uno.
- El modelo de relación está bien planteado, siguiendo un esquema jerárquico en el que se establecen comités a diferentes niveles, sobre los que se concretan asistentes, periodicidad y objetivos para cada comité.
- Se proporciona una buena batería de KPI's y KRI's para realizar el seguimiento, divididos para cada uno de los servicios. Además, se propone una herramienta para mejorar los KPI's y KRI's. Se especifica método de control para seguimiento de los ANS, proporcionando un perfil adicional especializado en gestión de servicios y con conocimientos en la metodología ITIL.
- El plan de devolución del servicio se plantea de una forma completa, detallando la metodología, fases y plazos. Se proponen sesiones de *shadowing* y transferencia de conocimiento al proveedor entrante, además de un comité de seguimiento de la devolución liderado por el *Transition Manager* para facilitar el proceso. También se detalla el proceso de borrado de datos de las plataformas.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

4 puntos

3.2.2.2 ORANGE ESPAGNE S.A.U.

La propuesta de **ORANGE ESPAGNE, S.A.U.** a este criterio se considera **SOBRESALIENTE**, debido a que se propone un plan claro de operación de los servicios con procedimientos operativos aplicables a todos los servicios, se establece un modelo de relación bien estructurado y detallado, se plantean KPI's que se representan en un cuadro de mandos y se indican las herramientas a utilizar y finalmente, se estructura y desarrolla el plan de devolución de los servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se plantea un plan de operación de los servicios basado en una combinación de varios estándares metodológicos. Se indican las actividades para la prestación de los servicios y los

grupos o perfiles encargados de su ejecución. Se incluye una matriz RACI relacionando los principales perfiles del proyecto y las actividades de cada etapa del plan de operación.

- Los procedimientos operativos se presentan estructurados en fases y aplicables para cada servicio.
- Se especifica el modelo de relación con los diferentes niveles de interlocución. Para cada comité se detallan los objetivos, actividades a llevar cabo, frecuencia de reunión y asistentes. También se indica el contenido mínimo del informe de seguimiento.
- Se incluye la construcción y puesta en marcha de cuadros de mando para reflejar diferentes indicadores. Se proponen KPI's para el seguimiento de los servicios y ANS. Además, se indican herramientas concretas para la realización de cuadros de mando.
- El plan de devolución de los servicios se segrega en diferentes fases, planteando que se haga una transferencia de forma gradual y se minimice la disminución de la calidad de los servicios prestados durante la transición. El plan detalla las obligaciones y tareas a realizar por cada una de las partes involucradas. Se aporta un plan para gestionar los riesgos asociados al plan de devolución.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

4 puntos

3.2.2.3 PROSEGUR CIBERSEGURIDAD S.L.

La propuesta de **PROSEGUR CIBERSEGURIDAD S.L.** a este criterio se considera **NOTABLE**, debido a que describe una metodología completa para el plan de operación, así como para el de devolución de los servicios, la propuesta de procesos contempla procedimientos generales y específicos relacionados, y el modelo de relación está bien detallado; sin embargo, no describe con suficiente detalle los recursos técnicos y humanos de los procedimientos operativos.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Metodología del plan de operación detallada y completa, basada en servicios, en las buenas prácticas determinadas por ITIL, en la mejora continua y en el cumplimiento de las premisas determinadas por el Esquema Nacional de Seguridad. Se incluye amplia descripción de procedimientos generales y específicos de los servicios requeridos.
- Modelo de relación estructurado en capas estratégica, táctica y operativa indicando las relaciones y vías de comunicación entre el personal del licitador y Madrid Digital
- Propone numerosas métricas (KPI's y KRI's) para el control de cada uno de los servicios.
- Plan de devolución detallado y completo identificando documentación y equipo dedicado a la devolución.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta detalle en la identificación de los recursos técnicos y humanos de los procedimientos operativos.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

3,2 puntos

3.2.2.4 S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.

La propuesta de **S2 GRUPO SOLUCIONES DE SEGURIDAD S.L.U.** a este criterio se considera **NOTABLE**, debido a que describe la metodología propuesta y el modelo de relación, realiza una propuesta completa de métricas (KPI's, KRI's y KGI's) para el control de los servicios y aporta un plan de devolución de servicio completo; sin embargo, no describe con suficiente detalle todos los procesos operativos, indicando recursos humanos y técnicos dependientes.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Metodología en la que destaca, además del uso de *MITRE ATT&CK*, *SOC Critical Path* que permite guiar la estrategia de defensa del SOC, proponiendo un modelo de alto nivel de organización del SOC y de gestión de ciberincidente basado en las mejores prácticas de la industria y en la mejora continua.
- Modelo de relación bien estructurado en 3 niveles con identificación de responsabilidades y entregables.
- La propuesta de KPI's, KRI's y de KGI's permiten un adecuado seguimiento del servicio, indicando que estarán disponibles en el portal de ciberseguridad y en los cuadros de mando resumen de gobierno del servicio.
- Presenta un plan de devolución que contempla documentación de arquitectura técnica y de operación, CMDB, inventarios y herramientas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta detalle en la descripción los procedimientos operativos de los servicios, en concreto de los recursos técnicos y humanos asociados.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

3,2 puntos

3.2.2.5 SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.

La propuesta de **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.** a este criterio se considera **NOTABLE**, debido a que especifica un plan de operación del servicio y un plan de devolución del servicio completos y claros, detallando recursos técnicos, humanos y los sistemas de seguimiento y control; sin embargo, no presenta una propuesta de métricas KPI's, KRI's para el control de los servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- A nivel organizativo, define áreas de servicio claras y estructuradas que responden a los requisitos establecidos para este criterio.

- Apuesta por un modelo de relación a nivel operativo sin comités, basado en facilitar la comunicación ágil y la interacción directa, así como promover los puntos de contacto entre los equipos de explotación y prestación del servicio.
- En cuanto a los sistemas de seguimiento y control, detalla los cuadros de mando que implementará para este cometido, poniendo énfasis en la gestión de riesgos de seguridad basada en los marcos de referencia de la ISO 27002 e ISO 27032.
- Respecto al plan de devolución, describe cada una de las fases del plan, destacando la fase de transferencia de conocimiento y el *shadowing* inverso.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Falta 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.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

3,2 puntos

3.2.2.6 SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.

La propuesta de **SOTHIS SERVICIOS TECNOLÓGICOS S.L.U.** a este criterio se considera **ADECUADA**, describiendo de manera detallada el plan de devolución de los servicios; sin embargo, no describe las actividades de los procedimientos operativos del servicio, incluyendo los recursos técnicos y humanos, no se describe el modelo de relación, y no presenta propuesta de métricas de seguimiento del servicio.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Inclusión de plan de proyecto con diagrama Gantt y calendario tanto para el plan de operación como para el de devolución con las fases y fechas propuestas.
- Plan de transición y retorno detallado y completo, incluyendo una propuesta de traspaso tanto del SIEM, del hardware relacionado con el NDR y sondas IDS como de los servicios en modalidad SaaS.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- Detalle en la propuesta de procedimientos operativos del servicio.
- Concreción sobre aspectos del sistema de seguimiento y control, modelo de relación.
- Relación de métricas, propuesta de sistemas de seguimiento y control.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

0,8 puntos

3.2.2.7 TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.

La propuesta de **TELEFONICA SOLUCIONES DE INFORMATICA Y COMUNICACIONES DE ESPAÑA S.A.U.** a este criterio se considera **BUENA** debido a que define una metodología para la operación de los servicios completa, ofrece unos mecanismos de seguimiento y control del servicio y un plan exhaustivo de devolución del servicio; sin embargo, no concreta los procedimientos operativos a seguir en cada uno de los servicios solicitados ni realizan propuestas de métricas para facilitar el control y seguimiento de los servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Definen una metodología basada en una gestión detallada de los distintos procesos implicados en la operación del servicio y en la interrelación entre ellos. Para cada proceso define las acciones a realizar.
- Detallan un sistema de seguimiento y control del servicio para Madrid Digital mediante reuniones, informes, y una gestión de la calidad de manera continua. También define un modelo de gestión de incidencias y peticiones entre los recursos del adjudicatario y Madrid Digital.
- Definen un plan detallado de devolución del servicio basado en fases, actividades y entregables obtenidos en cada una de ellas.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No detallan paso a paso los procedimientos operativos a seguir para la prestación de los servicios.
- No realiza una propuesta de métricas, ni de KPI's, KRI's para medir los distintos servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.	2,4 puntos
---	-------------------

3.2.2.8 UTE NTT DATA SPAIN, S.L.U. - NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.

La propuesta de **UTE NTT DATA SPAIN, S.L.U. – NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.U.** a este criterio se considera **SOBRESALIENTE**, debido a que especifica un modelo de gestión para la operación de los servicios y los procedimientos operativos necesarios, se explica el modelo de relación, se aportan herramientas tanto para el seguimiento de los KPI como para el cumplimiento de ANS y se aporta un plan para la devolución del servicio.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se explica un enfoque metodológico para la gestión de los servicios durante todo el ciclo de vida, dividido en varias fases. Además, se incluyen procesos de mejora continua.
- Los procedimientos operativos se detallan de forma agrupada, considerando para cada uno de los diferentes servicios los aspectos a tener en cuenta.
- Se incluye un modelo de relación y gobierno de los servicios, donde se incluyen varias medidas de contingencia que permiten controlar las posibles variaciones en las necesidades de los

servicios o posibles imprevistos que puedan surgir. También se identifican comités y se especifica el equipo de trabajo para cada servicio, indicado la cualificación de cada perfil.

- Se realiza una propuesta de KPI's y se establecen ANS. Además, se incluye un cuadro de mandos para facilitar el control de los servicios y se aportan herramientas específicas tanto para la elaboración del cuadro de mando como para la gestión del cumplimiento de los ANS.
- Se elabora un plan de devolución con varias fases, realizando una cesión gradual de la gestión de los servicios. Se proponen reuniones para realizar un seguimiento del proceso y se entregan informes actualizados.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

4 puntos

3.2.2.9 UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.

La propuesta de **UTE ACCENTURE SLU - SPECIALIST COMPUTER CENTRES, S.L. - PÉREZ-LLORCA ABOGADOS, S.L.P.** a este criterio se considera **NOTABLE** debido a que define una metodología para la operación de los servicios completa, establecen mecanismos de seguimiento y control del servicio que permiten, junto con los indicadores definidos, garantizar que los servicios se prestan sin inconvenientes, también definen un plan completo de devolución de los servicios; sin embargo, no concreta los procedimientos a seguir en cada uno de los servicios solicitados.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Proponen una metodología propia que explican detalladamente para gestionar el servicio basada en 4 pilares fundamentales para conseguir un servicio de calidad.
- El modelo propuesto de seguimiento y control establece un sistema de gobernanza basado en diversos comités, de los cuales detallan las funciones principales, los participantes y la periodicidad. También se definen una gestión de la demanda entre el adjudicatario y Madrid Digital, basada en la ejecución de tareas definidas de acuerdo a los ANS establecidos y en la relación entre los recursos.
- Proponen un plan de calidad con una metodología propia que permite evaluar y controlar los servicios. También proponen una serie de métricas por servicio, las cuales detallan e indican su periodicidad, para medirlos.
- Detallan de manera completa un plan de devolución del servicio, describiendo para cada etapa las actividades y entregables obtenidos en cada una de ellas, incluyendo la aceptación por parte de Madrid Digital de la devolución de los servicios.

La propuesta no incluye suficiente información que permita identificar la aportación de valor, de acuerdo con lo indicado para este criterio, en los siguientes aspectos:

- No detallan paso a paso los procedimientos operativos a seguir para la prestación de los servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

3,2 puntos

3.2.2.10 UTE INETUM ESPAÑA, S.A. - CHG-MERIDIAN SPAIN, S.L.U.

La propuesta de **UTE INETUM ESPAÑA, S.A. – CHG-MERIDIAN SPAIN, S.L.U.** a este criterio se considera **SOBRESALIENTE**, debido a que especifica con gran nivel de detalle la operación del servicio y la devolución, de forma completa y bien estructurada, aportando KPI y medición de ANS.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Se especifica con gran nivel de detalle el modelo operativo separadamente para cada servicio, incluso a nivel de subservicio dentro de cada servicio principal. Se indica el equipo de trabajo para cada servicio, cumpliendo con lo requerido y aportando perfiles extra para aumentar la calidad de los servicios prestados.
- El modelo organizativo define tres planos: estratégico, táctico y operativo. Para cada comité se establecen los puntos a tratar, frecuencia de reunión y entregables. Adicionalmente, se incluyen comités de coordinación e innovación.
- Además de los ANS incluidos en el pliego se aporta una lista adicional que los complementa. Se indica también un listado de KPI que permiten hacer un seguimiento de los servicios y se indica la elaboración de un cuadro de mando que permita identificar la eficiencia de los procesos y la priorización de las acciones de mejora.
- El modelo de relación propuesto sigue un esquema jerárquico, estableciendo comités a diferentes niveles. Se concreta los asistentes, periodicidad y objetivos de cada comité.
- Se elabora un plan de devolución del servicio claro, donde se plantea que la devolución se realice de manera gradual para evitar afectación en la calidad del servicio. Se especifican las diferentes fases del plan, incluyendo un cronograma con las actividades y reuniones asociadas a cada fase. Se propone hacer *shadowing* (directo e inverso) y hay un periodo post-implantación.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

4 puntos

3.2.2.11 UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.

La propuesta de **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.** a este criterio se considera **SOBRESALIENTE** debido a que define una metodología para la operación de los servicios bastante completa con propuesta agregada de procedimientos operativos, ofrecen buenos y detallados mecanismos de seguimiento y control del servicio que permiten, junto con los indicadores definidos, garantizar que los servicios se prestan sin inconvenientes, también se define un plan completo de devolución de los servicios.

Los aspectos más positivos y destacables de la propuesta son los siguientes:

- Definen una metodología basada en estándares donde se detalla el modelo de gestión a seguir para la operación de los servicios, cómo será la operación de los equipos participantes y la

interrelación entre ellos en los distintos servicios. Además, de los procesos y pilares en los que se basa dicha gestión.

- Procedimientos operativos descritos considerando las necesidades de cada servicio.
- Detallan un sistema de seguimiento y control del servicio para Madrid Digital mediante distintos modelos de reporte con sus entregables. También establecen un modelo de relación entre los recursos del adjudicatario y Madrid Digital mediante diversos comités de los cuales se detallan los objetivos y participantes en ellos.
- Hace una propuesta de métricas para medir los distintos servicios junto con una propuesta de una gestión de riesgos continua durante toda la prestación del servicio que permitirá medir y revisar los posibles riesgos que puedan surgir para mitigarlos lo antes posible.
- Definen un plan detallado de devolución del servicio que contiene varias fases, las cuales detallan junto con las actividades a realizar y entregables obtenidos en ellas; incluyendo la aceptación por parte de Madrid Digital de la devolución de los servicios.

Según la valoración realizada, la puntuación de la oferta es de:

CRITERIO NÚMERO 8.2 – Plan de operación y devolución de los servicios. Hasta 4 puntos.

4 puntos

4. Resumen de la valoración de los criterios cualitativos. Hasta 45 puntos

A continuación, se recoge el resumen de la valoración final de las propuestas:

CRITERIO N°	DESCRIPCIÓN CRITERIO	EVOLUTIO	ORANGE	PROSEGUR	S2 GRUPO
7	Solución técnica propuesta para los servicios requeridos				
7.1	Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios.	6 puntos	3,6 puntos	4,8 puntos	3,6 puntos
7.2	Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad SIEM.	10 puntos	10 puntos	8 puntos	6 puntos
7.3	Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR.	6,4 puntos	6,4 puntos	4,8 puntos	8 puntos
7.4	Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas.	3,2 puntos	3,2 puntos	0,8 puntos	3,2 puntos
7.5	Servicio de orquestación, automatización y respuesta – SOAR.	3 puntos	2,4 puntos	1,8 puntos	1,8 puntos
7.6	Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis	0,8 puntos	3,2 puntos	0,8 puntos	2,4 puntos
8	Planes operativos				
8.1	Plan de implantación de los servicios.	6 puntos	6 puntos	1,2 puntos	4,8 puntos
8.2	Plan de operación y devolución de los servicios.	4 puntos	4 puntos	3,2 puntos	3,2 puntos
		39,4 puntos	38,8 puntos	25,4 puntos	33 puntos

CRITERIO N°	DESCRIPCIÓN CRITERIO	SIRT	SOTHIS	TELEFÓNICA	UTE NTT DATA - NTT SPAIN
7	Solución técnica propuesta para los servicios requeridos				
7.1	Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios.	6 puntos	1,2 puntos	4,8 puntos	4,8 puntos
7.2	Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad SIEM.	10 puntos	2 puntos	2 puntos	8 puntos
7.3	Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR.	6,4 puntos	4,8 puntos	6,4 puntos	8 puntos
7.4	Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas.	4 puntos	0,8 puntos	0,8 puntos	0,8 puntos
7.5	Servicio de orquestación, automatización y respuesta – SOAR.	3 puntos	0 puntos	0,6 puntos	2,4 puntos
7.6	Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis	3,2 puntos	0,8 puntos	0,8 puntos	2,4 puntos
8	Planes operativos				

CRITERIO N°	DESCRIPCIÓN CRITERIO	SIRT	SOTHIS	TELEFÓNICA	UTE NTT DATA - NTT SPAIN
8.1	Plan de implantación de los servicios.	6 puntos	1,2 puntos	3,6 puntos	3,6 puntos
8.2	Plan de operación y devolución de los servicios.	3,2 puntos	0,8 puntos	2,4 puntos	4 puntos
		41,8 puntos	11,6 puntos	21,4 puntos	34 puntos

CRITERIO N°	DESCRIPCIÓN CRITERIO	UTE ACCENTURE - SCC - PEREZ-LLORCA	UTE INETUM - CHG	UTE SIA - CIPHERBIT
7	Solución técnica propuesta para los servicios requeridos			
7.1	Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios.	3,6 puntos	1,2 puntos	4,8 puntos
7.2	Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad SIEM.	8 puntos	6 puntos	10 puntos
7.3	Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR.	6,4 puntos	4,8 puntos	8 puntos
7.4	Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas.	0,8 puntos	0,8 puntos	2,4 puntos
7.5	Servicio de orquestación, automatización y respuesta – SOAR.	1,8 puntos	0,6 puntos	2,4 puntos
7.6	Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis	0,8 puntos	0,8 puntos	3,2 puntos
8	Planes operativos			
8.1	Plan de implantación de los servicios.	4,8 puntos	6 puntos	3,6 puntos
8.2	Plan de operación y devolución de los servicios.	3,2 puntos	4 puntos	4 puntos
		29,4 puntos	24,2 puntos	38,4 puntos

La oferta técnica ofertada por **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L (SIRT)**, responde a los requisitos técnicos recogidos en el Pliego de Prescripciones Técnicas y es la **mejor oferta presentada con 41,8 puntos**. Como resumen de la valoración hay que destacar:

- Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios: plantea una solución detallada para cada uno de los servicios, poniendo el foco en la integración y automatización de estos servicios a través de la plataforma de IA que expone. Desarrolla con gran nivel de profundidad el uso de las distintas herramientas y equipos de trabajo.
- Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM: detalla exhaustivamente la arquitectura de la solución SIEM, dimensionamiento, escalado, solución completa de comunicaciones y conectividad, fuentes de

inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas, y librerías de casos de uso de monitorización disponibles ya predefinidos y mapeados con la matriz *MITRE ATT&CK*. Adicionalmente describe en detalle el modelo de operación, mantenimiento, administración y monitorización.

- Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR: describe de forma idónea y completa la plataforma NDR propuesta, incluyendo un esquema de arquitectura muy claro que facilita su comprensión. La solución está bien posicionada en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red, es escalable y permite la automatización. Se describen perfectamente las medidas de disponibilidad y continuidad y las capacidades de integración de la solución con otras plataformas y servicios. En el apartado de casos de uso de monitorización, se aporta una tabla muy completa con ejemplos de casos.
- Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas: recoge de forma muy detallada la organización de los recursos para cada servicio ofertando además recursos específicos adicionales para integrar las funcionalidades de IA en los distintos servicios, las actividades y procedimientos propuestos para la monitorización de seguridad, con especial foco en las actividades de administración y operación de plataformas, monitorización de eventos, o propuesta de tipología de casos de uso de monitorización a implementar. Destaca también la propuesta de procedimientos de identificación, tratamiento y escalado de incidentes y amenazas de seguridad dentro del servicio de detección de incidentes, criterios de priorización y mecanismos de reducción de falsos positivos. En cuanto al servicio de búsqueda proactiva de amenazas (*hunting*), la metodología, herramientas y propuesta de casos de búsqueda a definir se considera muy completa y orientada a la identificación y reducción de los tiempos en los incidentes de seguridad detectados.
- Servicio de orquestación, automatización y respuesta – SOAR: propone una solución SOAR completa y detallada de forma excepcional, integrada de forma nativa con el SIEM, enfocada no sólo al área de respuesta a incidentes, sino también al de prevención, con capacidades de automatización mejoradas con IA, capacidades de integración con los sistemas de Madrid Digital, amplía librería de casos de uso predefinidos, aportando explicación diferencial de cómo se opera, mantiene y administra la plataforma.
- Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis: describe de forma clara y completa la metodología, procedimientos, capacidades y herramientas tanto del servicio de análisis y respuesta como el de gestión de ciber crisis, define la propuesta de organización de los recursos del proveedor y los protocolos de activación de equipos adicionales e informa de la integración de los principales canales de notificación. En cuanto al análisis forense se aporta la metodología a utilizar y las herramientas.
- Plan de implantación de los servicios: propone un plan de proyecto completo, muy bien estructurado y claro, con todas las fases y actividades asociadas a la implantación de todos los servicios del SOC, identificando previamente la información necesaria, se aporta planes de detalle específicos de puesta en marcha SIEM, SOAR y NDR, y propuesta planificada de organización del SOC, considerando la operación y mantenimiento de los servicios actuales.

- Plan de operación y devolución de los servicios: especifica un plan de operación del servicio y un plan de devolución del servicio completos y claros, detallando recursos técnicos, humanos y los sistemas de seguimiento y control.

Junto con la mejor oferta de la empresa **SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L (SIRT)**, es de destacar las propuestas de **EVOLUTIO CLOUD ENABLER S.A.U.**, **ORANGE ESPAGNE S.A.U.** y **UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.**, todas ellas responden a los requisitos del Pliego de Prescripciones Técnicas, con propuestas de valor por encima de los 38 puntos. Como resumen de sus valoraciones se destaca:

EVOLUTIO CLOUD ENABLER S.A.U.:

- Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios: debido al aporte de valor de su solución en la identificación de amenazas y vigilancia digital, en la que se ofrece una solución de inteligencia de amenazas que incorpora fuentes muy bien posicionadas comercialmente y con gran aporte de valor. La solución ofrece funcionalidades adicionales, como una base de datos ya elaborada de vulnerabilidades asociadas a CPE's conocidos, o funcionalidades como poder identificar cambios no autorizados en el inventario de activos generado. La solución propuesta para el análisis de vulnerabilidades de sistemas y redes ofrece elementos extra a los requisitos solicitados en el pliego, como una suscripción adicional gratuita o capacidades de análisis de aplicaciones web y directorio activo. Por último, la propuesta de ciberejercicios detalla metodología, actividades y herramientas.
- Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM: debido a que detalla exhaustivamente la arquitectura de la solución SIEM, capacidades de conectividad y comunicaciones entre elementos *on-premise* y entre CPD's y nubes, dimensionamiento con capacidad de correlación mejorada con 12 meses de datos online, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de Madrid Digital, detallando librerías de casos de uso de monitorización disponibles ya predefinidos y mapeados con la matriz *MITRE ATT&CK*. Incorpora amplia propuesta de operación, mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.
- Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR: describe de forma idónea y completa la plataforma propuesta NDR. La herramienta está bien posicionada dentro del último cuadrante de Forrester de soluciones de análisis y visibilidad de red, es escalable y permite la automatización. Detalla las medidas de disponibilidad, continuidad y las capacidades de integración.
- Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas: destaca de su oferta los procedimientos y actividades de operación SIEM, NDR y sondas, los procedimientos propuestos para la integración de fuentes de eventos y los recursos específicos para el desarrollo de casos de uso de monitorización; los procedimientos asociados al servicio de detección de identificación, tratamiento y escalado de incidentes y amenazas de seguridad, y para el servicio de búsqueda proactiva de amenazas, la tipología y detalle de informes propuesta y herramientas propuestas.

- Servicio de orquestación, automatización y respuesta – SOAR: propone una solución SOAR, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con el NDR y con los sistemas de Madrid Digital, amplia librería de casos de uso predefinidos y propuesta de operación, mantenimiento, administración remota y monitorización de la solución SOAR.
- Servicio de análisis y respuesta a incidentes, análisis forense y gestión de cibercrisis: describe la metodología y procedimientos de los servicios de análisis forense y gestión de cibercrisis.
- Plan de implantación de los servicios: realiza una propuesta clara y completa, indicando el despliegue de las plataformas implicadas en cada servicio, incluyendo un cronograma detallado, siendo relevante la explicación de las fases y actividades del SIEM, SOAR y NDR. También especifica la organización del equipo de trabajo del SOC incluyendo los servicios de soporte 24x7, aportando y explicando el plan requerido para el mantenimiento y operación de los servicios de ciberseguridad ya desplegados.
- Plan de operación y devolución de los servicios: plantea una metodología clara de operación de los servicios y detalla el modelo de relación propuesto, aportando procedimientos operativos consistentes. Además, se especifican KPI's y KRI's junto con una herramienta para mejorarlos. El plan de devolución del servicio está bien estructurado y se profundiza en el proceso de borrado de datos

ORANGE ESPAGNE S.A.U.:

- Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios: gran aporte de valor de la solución propuesta para la identificación de amenazas y vigilancia digital, con descripción muy detallada de los tipos de activos a monitorizar y una metodología de obtención de información bien estructurada. Se detalla la metodología de gestión del servicio de análisis de vulnerabilidades de sistemas y redes, y se propone una herramienta específica con la que trabajar. Igualmente, se detalla la metodología y herramientas a utilizar para la realización del análisis de vulnerabilidades de aplicaciones. La propuesta de ciberejercicios refleja los tipos de ciberejercicios a realizar y un calendario con la planificación propuesta.
- Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM: detalla exhaustivamente la arquitectura de la solución SIEM, capacidades de conectividad y comunicaciones de forma completa, dimensionamiento, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y con sistemas de *ticketing* requeridos, aportando completa librerías de casos de uso de monitorización predefinidos y mapeados con la matriz *MITRE ATT&CK*. Incorpora amplia propuesta de operación y mantenimiento de la plataforma, administración remota y monitorización de los diferentes componentes.
- Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR: describe de forma idónea y completa la plataforma propuesta NDR, siendo una de las soluciones líder en el último cuadrante de Forrester de soluciones de análisis y visibilidad de red. La solución permite automatización, se detalla en profundidad la propuesta de operación y

mantenimiento, y se recogen de forma clara las medidas de disponibilidad, escalabilidad, rendimiento, funcionalidad y cumplimiento normativo de la solución.

- Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas: desarrolla de forma detallada y muy completa los procedimientos de administración y operación de las distintas plataformas, el servicio ofrecido de modelado de amenazas a partir del cual se definirán los casos de uso de monitorización a desarrollar, y los procedimientos de monitorización de eventos y alertas, y de identificación, tratamiento y escalado de incidentes y amenazas de seguridad reportadas por cada uno de los servicios. Destaca también la propuesta metodológica del servicio de *hunting*, así como los entregables del servicio previstos.
- Servicio de orquestación, automatización y respuesta – SOAR: propone solución SOAR, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con los sistemas de Madrid Digital, y amplia librería de casos de uso predefinidos.
- Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis: recoge de forma idónea y completa la metodología y procedimientos explicativos de cada uno de los servicios, incluyendo esquemas ilustrativos complementarios y claros, así como la propuesta de integración de herramientas de *ticketing* con el SOAR.
- Plan de implantación de los servicios: realiza una propuesta estructurada, en la que se plantea una metodología con diferentes fases para la implantación de los servicios, con identificación de información necesaria, planificación y duración de cada actividad dentro de las fases, se hace hincapié en el despliegue de las soluciones SIEM, SOAR y NDR, se indica la organización del SOC incluyendo los servicios 24x7; y se aporta la propuesta de mantenimiento y operación de los servicios de ciberseguridad ya desplegados en Madrid Digital.
- Plan de operación y devolución de los servicios: propone un plan claro de operación de los servicios con procedimientos operativos aplicables a todos los servicios, se establece un modelo de relación bien estructurado y detallado, se plantean KPI's que se representan en un cuadro de mandos y se indican las herramientas a utilizar y finalmente, se estructura y desarrolla el plan de devolución de los servicios.

UTE SISTEMAS INFORMATICOS ABIERTOS, S.A.U. - CIPHERBIT, S.L.U.:

- Servicios de prevención: identificación de amenazas y vigilancia digital, análisis de vulnerabilidades de seguridad de redes y sistemas y de aplicaciones, y ciberejercicios: describe de forma completa la metodología y herramientas a utilizar en los ciberejercicios y en el análisis de vulnerabilidades de seguridad de aplicaciones, así como las herramientas a utilizar en el escaneo de vulnerabilidades y las fuentes a consultar en el servicio de identificación de amenazas y vigilancia digital.
- Servicio de monitorización y detección: plataforma de gestión de eventos e información de seguridad – SIEM: detalla la arquitectura de la solución SIEM, infraestructura de conectividad *on-premise* y en nube, dimensionamiento con capacidad de correlación mejorada, escalado, fuentes de inteligencia utilizadas para enriquecimiento de la información, capacidades de integración con fuentes de eventos y sistemas de *ticketing*, amplia librerías de casos de uso de

monitorización ya predefinidos y mapeados con la matriz *MITRE ATT&CK*, aportando descripción detallada de las capacidades de operación, administración y monitorización.

- Servicio de monitorización y detección: servicio de análisis avanzado de tráfico de red – NDR: describe de forma muy completa la plataforma presentada NDR, incluyendo un esquema detallado de la arquitectura, así como un listado de los equipos empleados con sus correspondientes capacidades y redundancias, que, unidas a la propuesta de la monitorización constante, confieren a la solución un alto grado de disponibilidad y escalabilidad. La solución dispone entre otras características, de diversos mecanismos de automatización, que, junto a sus capacidades de integración con otros sistemas de seguridad, la posicionan en un buen lugar el ultimo cuadrante Forrester de soluciones de análisis y visibilidad de red. Por último, la propuesta presenta distintas librerías de casos de uso.
- Servicio de monitorización y detección: monitorización, detección y búsqueda proactiva de amenazas: detalla todas las actividades a desarrollar relacionadas con el servicio de monitorización de eventos, ofreciendo un recurso de apoyo para la elaboración de los casos de uso de monitorización (profiling). También destaca la propuesta de organización y actividades del servicio de detección de incidentes de seguridad.
- Servicio de orquestación, automatización y respuesta – SOAR: propone solución SOAR descrita en detalle, integrada de forma nativa con el SIEM, sin límites en el número de usuarios-analistas concurrentes, con capacidades de automatización mejoradas con IA, capacidades de integración con soluciones NDR y con los sistemas de Madrid Digital, y amplia librería de casos de uso predefinidos.
- Servicio de análisis y respuesta a incidentes, análisis forense y gestión de ciber crisis: detalla correctamente las actividades a realizar para gestionar el servicio de análisis y respuesta, el servicio de análisis forense y se establece la organización de los recursos para el servicio de análisis y respuesta y los procedimientos de activación de los servicios adicionales.
- Plan de implantación de los servicios: identifica los datos e información necesaria para la puesta en marcha de los servicios, propone un plan detallado de puesta en marcha para los servicios y herramientas que lo soportan (SIEM, SOAR y NDR) y herramienta de vulnerabilidades, e indican cómo mantendrán el servicio actual.
- Plan de operación y devolución de los servicios: define una metodología para la operación de los servicios bastante completa con propuesta agregada de procedimientos operativos, ofrece buenos y detallados mecanismos de seguimiento y control del servicio que permiten, junto con los indicadores definidos, garantizar que los servicios se prestan sin inconvenientes, también se define un plan completo de devolución de los servicios.

La Subdirectora General de Ciberseguridad, Protección de Datos y Privacidad

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2024.10.07 10:55

Fdo. Esther Muñoz Fuentes