

CENTRO DE CÁLCULO DE ÁLAVA, S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS (PPT)

**PRESTACIÓN DE LOS SERVICIOS DE “CENTRO DE OPERACIONES DE
SEGURIDAD (SOC) PARA DIPUTACIÓN FORAL DE ÁLAVA Y SECTOR
PÚBLICO FORAL ”**

EXP. 26010



1. INTRODUCCION	3
2. ENTIDADES DENTRO DEL ALCANCE ¡ERROR! DEFINIDO.	MARCADOR NO
3. OBJETO	3
4. CONDICIONES DE EJECUCIÓN DEL SERVICIO	8
4.1. Composición del equipo	8
4.2. Calidad y seguimiento del servicio	9
4.3. Acuerdos de Nivel de Servicio (ANS)	10
4.4. Lugar de trabajo y equipamiento.	12
5. FORMATO, ESTRUCTURA Y CONTENIDO DE LA OFERTA	12
6. INFORMACIÓN ADICIONAL.	14

1. INTRODUCCION

El CCASA, como principal prestador de servicios TIC de la Diputación Foral de Álava (en adelante DFA) y del sector público foral, realiza labores de instalación, configuración, y mantenimiento de los sistemas de información durante su ciclo de vida.

La propia evolución funcional de los sistemas de información (en adelante SSII), las actividades de configuración ad-hoc en la instalación y la publicación de vulnerabilidades de protocolos, productos, etc. hace que los sistemas de información pierdan la seguridad con la que fueron concebidos.

Este cúmulo de debilidades son aprovechadas por organizaciones cibercriminales para acceder a información confidencial, alterar datos de las organizaciones o cifrar información con objeto de obtener réditos económicos como compensación ante el cese de las actividades o exfiltración de información de las organizaciones atacadas. Evidentemente, estas actividades suponen un menoscabo en las funcionalidades disponibles en los sistemas de información que los usuarios internos y externos utilizan, y con ello la imagen y credibilidad de las organizaciones se ve perjudicada.

Por estos motivos, es necesaria la implantación de herramientas de seguridad que detecten y bloqueen ataques externos a las organizaciones. En la actualidad, los ataques a las organizaciones son complejos y prolongados en el tiempo, intentando eludir las medidas de seguridad de las herramientas instaladas. Por ello, se necesita un seguimiento constante de las actividades existentes en todos elementos que conforma el equipamiento informático, tanto de la superficie expuesta a ser usada por la ciudadanía, así como de los equipos internos de la red corporativa.

El seguimiento de las actividades durante las 24 horas de los 7 días de la semana requiere la interacción de sistemas recolectores y analizadores de eventos acaecidos, así como de personal experto que revise las alertas ante actividad sospechosa.

Por este motivo, y de forma resumida, la DFA y el sector público foral requieren de:

1. Centro de Operaciones de Seguridad (SOC): análisis, detección y reacción ante ataques.
2. Threat Hunting y detección de brechas de seguridad
3. Asesoramiento de un Equipo de Respuesta ante Incidentes (CSIRT) en el caso de que DFA o algún ente perteneciente al sector público foral sufra un incidente de seguridad crítico.

2. OBJETO Y ALCANCE

El objeto es dotar a la DFA y al sector público foral de la capacidad de detección (proactiva y reactiva), análisis y resolución de actividades sospechosas contra los SSII gestionados por el Centro de Cálculo de Álava. Además, en caso de que la DFA o alguno de los entes del sector público foral sufriera un ciberincidente crítico en los SSII gestionado por CCASA, se requiere disponer de un equipo de respuesta ante incidentes (CSIRT) que asesore y colabore con el personal involucrado en la resolución.

El alcance del trabajo se refiere a los SSII de la DFA y del sector público foral que esté gestionado por CCASA.

La duración de la prestación de este servicio es desde el 15 de noviembre de 2026 hasta el 31 de diciembre de 2029. En el caso de que la empresa adjudicataria de este contrato coincidiera con la que actualmente está prestando el servicio, el servicio comenzaría tras la finalización del contrato actual. En este caso, el pago del primer mes será la parte proporcional del pago mensual derivado de la oferta de la adjudicataria a los días existentes entre la finalización del contrato actual y el último día del mes.

A continuación, se detallan los requisitos de los servicios demandados de:

- Centro de Operaciones de Seguridad (SOC).
- Threat Hunting y detección de brechas de seguridad (Seguridad preventiva)
- Asesoramiento de un Equipo de Respuesta ante Incidentes (CSIRT/DFIR).

La empresa licitadora garantizará el cumplimiento de aquellas obligaciones legales establecidas en el ENS (Real Decreto 3/2010 de 8 enero) en lo referido a la adopción de medidas de seguridad de la prestación de servicios ofertados. **Será requisito mínimo para la ejecución del contrato disponer de Certificación de nivel MEDIO ENS de los servicios de SOC ofertados.**

CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El Centro de Operaciones de Seguridad (en adelante, SOC) prestará servicios de monitorización de eventos de seguridad y respuesta ante incidentes. Estos servicios se prestarán en modalidad 24x7x365 y la información relacionada con la prestación del servicio de este contrato se encontrará ubicada en DataCenters en alta disponibilidad ubicados en la Unión Europea. Además, el idioma de atención del SOC a DFA-CCASA será al menos en castellano.

La prestación del servicio de SOC se basará principalmente sobre la información existente en las soluciones de seguridad disponibles en la DFA. Por ello, el presente contrato no contempla la compra de ninguna solución adicional a las especificadas en el “Información adicional I – Descripción técnica”. Si la empresa licitadora entiende necesaria la utilización de herramientas adicionales, los costes derivados de la utilización de éstas no serán imputables a CCASA; debiendo asegurarse de que, una vez finalizado el contrato, la información relacionada con el servicio de SOC ofertado que estuviera en estas herramientas adicionales ha de ponerse a disposición de CCASA en formatos explotables.

La información referida a los logs de los SSII gestionado por CCASA en ningún momento será redireccionada a otros SSII ajenos a DFA-CCASA.

Las funciones y actividades del SOC serán:

- Monitorización y correlación de eventos en tiempo real (*Req001*)
- Identificación de nuevas fuentes (*Req002*) de la infraestructura de DFA-CCASA que la oferente o CCASA considere relevante para la prestación del servicio y colaboración en la configuración en la herramienta SIEM.

- Identificación, detección y categorización de incidentes (*Req003*). Con la información monitorizada, la empresa licitadora deberá, en base a las alertas, identificar y analizar los posibles incidentes, determinar su alcance y posible escalado. Antes del escalado a CCASA se requerirá de:
 - Detección de falsos positivos o Clasificación y tipología del incidente
 - Análisis de situación e impacto
 - Propuesta de medidas correctivas y/o remediación
 - Documentación del caso.
- Gestión de incidentes y actividades sospechosas en tiempo real (*Req004*), que implica:
 - el registro y escalado del mismo si procede tras la evaluación previa. El escalado será según lo acordado con CCASA al inicio del servicio en el Procedimiento de gestión y escalado de incidentes.
 - Búsqueda, análisis e investigación detallada (identificando impacto, activos, identificativos de usuario asociados, etc.) en los ciberincidentes que requieran de esta actividad.
 - Actuación según lo establecido en los “Planes de respuesta ante incidentes” y la criticidad, impacto y tipología del incidente. Los “Planes de respuesta ante incidentes” definidos al inicio del servicio serán documentados y actualizados por la empresa licitadora según las necesidades detectadas. Este plan de respuesta ante incidentes incluirá los diferentes tipos, incluidos los críticos. Este procedimiento se aprobará en los dos primeros meses de servicio y a lo largo del primer año, se hará un simulacro del plan ante incidentes críticos.
 - Tras la resolución de incidente, se plantearán las lecciones aprendidas/retrospectivas para su estudio y, si procede, se realizará el diseño de procedimientos e incorporación de estos en los procesos de mejora.
 - Los “Planes de respuesta ante incidentes” podrán ser manuales y podrán delegarse en la empresa adjudicataria. Además, CCASA tiene prevista la implantación de una herramienta SOAR (especificada en “Información adicional I – Descripción técnica”) que automatice estas respuestas manuales.
- Integración feeds de inteligencia (*Req005*) propios a las herramientas de seguridad descritas en el “Información adicional I – Descripción técnica”, así como aquellos procedentes de otras fuentes públicas o privadas, que mediante la pertinente adecuación al contexto de DFA-CCASA sean de aplicación para el servicio ofertado.
- Monitorización y análisis de múltiples fuentes de información (públicas y privadas) (*Req006*) e investigaciones de la empresa licitadora para mejorar la detección y visibilidad de amenazas externas o internas que pudieran afectar a los SSII de DFA-CCASA.
- Diseño y colaboración en la implementación de nuevos casos de uso (*Req007*) para la detección de posibles acciones malintencionadas contra los SSII de DFA-CCASA.

Los casos de uso pueden ser demandados por CCASA o proactivamente facilitados por la empresa oferente con el objeto de mejorar la seguridad de los SSII de DFA-CCASA. Se valorará en los criterios numéricos el número de propuestas de mejora mínimas (adaptados a las particularidades de DFA-CCASA) comprometidos anualmente.

- Colaboración con CCASA en la integración de IOCs (*Req008*) en base a feeds de inteligencia propios del servicio de SOC o de terceras entidades.
- Colaboración con CCASA en la comunicación y gestión de los incidentes recibidos por el Sistema de Alerta Temprana (SAT-INET) del CCN-CERT.
- Colaboración con CCASA en la gestión de incidentes reportados por la herramienta XDR.
- Definición y asesoramiento a CCASA en la implementación del conjunto de cuadros de mando de las métricas e indicadores (*Req009*) que reflejen el nivel de seguridad de DFA-CCASA:
 - Alarmas e incidentes gestionados.
 - Identificación de incidentes por categorías, criticidad...
 - Ratios de falsos positivos
 - Otros indicadores de seguridad
 - Cumplimiento de los niveles de servicios acordados
 - Etc.
- Generación de informes del servicio contratado (*Req010*). cuyo formato y contenido se acordarán con CCASA al inicio del servicio contratado y se adaptará a las necesidades a lo largo de la prestación del servicio.
- Actualización, junto con CCASA, de la plataforma SIEM y SOAR (*Req011*) para la inclusión de elementos (nuevas fuentes, reglas, respuestas automatizadas, etc.) que mejoren la prestación del servicio ofertado.

Todas estas funciones estarán regladas mediante los Acuerdos de Nivel de Servicio (en adelante ANS) especificados en el “Información adicional II – Acuerdos de Nivel de Servicio” y su incumplimiento supondrá el incumplimiento del contrato con las penalidades que de ello puedan derivar.

THREAT HUNTING Y DETECCIÓN DE BRECHAS DE SEGURIDAD

La acción preventiva ante posibles ciberincidentes es tan relevante como la reactiva. Por este motivo, DFA-CCASA considera necesaria una actividad proactiva de:

- Threat Hunting, es decir, la búsqueda proactiva de ciberamenazas que permanecen ocultas en la red corporativa y no han sido detectadas por las herramientas de protección.

- Análisis de vulnerabilidades de sistemas de información (o parte de ellos) expuestos en Internet
- Análisis de vulnerabilidades de los SSII internos que la DFA-CCASA dispone.

La concreción de estas actividades preventivas se detalla a continuación:

- El origen de las actividades de Threat hunting puede ser proactiva por parte de la empresa licitadora (en base a su conocimiento y su información de inteligencia del momento) o a demanda de DFA-CCASA en relación con casuísticas específicas (*Req012*).
- El Threat hunting podrá surgir de planteamiento de hipótesis de investigación (ante nuevos vectores de ataque o noticias que sugieran posibilidad de ataque) o de TTPs (Tactics, techniques and procedures) (*Req013*).
- Partiendo del Threat hunting la empresa licitadora proporcionará recomendaciones (*Req014*) para el ajuste de las medidas de seguridad, de alertas personalizadas o nuevos casos de uso en los SSII especificados en el “Información adicional I – Descripción técnica”.
- Ante la detección de una amenaza o incidente, se facilitará información ejecutiva (*Req015*) y detallada del conocimiento existente en cada momento.
- En base a las herramientas disponibles en DFA-CCASA, especificadas en el “Información adicional I – Descripción técnica”, CCASA podrá delegar su uso parcial en la empresa licitadora al objeto de facilitar el Threat hunting, así como la ejecución de actividades de remediación acordadas en los “Planes de respuesta ante incidentes”.
- Revisión de las configuraciones de los elementos de seguridad (*Req016*) establecidos en la arquitectura tecnológica de DFA-CCASA.
- Escaneo de vulnerabilidades automatizado (*Req017*) de los sistemas de información (expuestos en Internet e internos) de DFA-CCASA. La frecuencia de esta actividad será cuando menos mensual en los sistemas expuestos a Internet y trimestral para los sistemas internos.
- Recomendación de acciones/contramedidas (*Req018*) derivadas de los escaneos de vulnerabilidades automatizados, casos de uso, etc. que reduzcan la probabilidad de explotación de las vulnerabilidades de seguridad detectadas.
- Se reportará mensualmente (*Req019*) el conjunto de actividades preventivas realizadas y trimestralmente se revisará el estado de implementación de las propuestas realizadas.

ASESORAMIENTO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES (CSIRT/DFIR).

A pesar del establecimiento de actividades de monitorización continua, análisis preventivo, etc. DFA-CCASA requieren de un apoyo de un equipo que asesore a estas organizaciones en la gestión y resolución de ciberincidentes críticos (alto impacto en los SSII de DFA-CCASA). Es por ello que la empresa licitadora deberá facilitar para esta casuística los siguientes servicios:

- Análisis forense (DFIR) de los eventos (*Req020*), para determinar orígenes del ataque, medios utilizados, IOC, TTPs y objetivos.
- Soporte especializado en la definición de las medidas de contención a aplicar, planes para la recuperación de los sistemas y preservación de evidencias (*Req021*).
- Servicios de gestión y coordinación técnica, organizativa, y de negocio de los diferentes grupos de trabajo (*Req022*) que puedan estar involucrados, con el objetivo de reducir al mínimo posible los tiempos de recuperación de los sistemas y servicios.
- Servicios de asesoría y asistencia legal (*Req023*) como apoyo en la ejecución de medidas legales en caso de incidentes graves de seguridad o acciones derivadas de obligaciones normativas y/o regulatorias.
- Documentación e informe del incidente (*Req024*) desde su identificación, impacto, a las medidas para su resolución y ajustes propuestos sobre el global del servicio

Esta parte del servicio contratado podrá ser activada en cualquier momento (24x7x365) y la empresa licitadora pondrá a disposición de DFA-CCASA el personal colaborador en un tiempo máximo de 4 horas. A lo largo de su intervención, podrá requerirse su presencia física en las instalaciones de DFA-CCASA.

En el caso de que los servicios CSIRT no sean utilizados en periodos de 12 meses, se sustituirá esta parte del servicio por un simulacro de ciberincidente crítico (*Req025*). Es decir, en caso de no utilizarse los servicios CSIRT/DFIR en el primer año de vigencia del contrato, se hará un simulacro. De igual manera, en los años siguientes de vigencia del contrato. La empresa licitadora planteará un hipotético ciberincidente y, previo acuerdo del alcance con la dirección del proyecto en CCASA, se realizará el simulacro. Durante el simulacro se revisará la operatividad de los procedimientos de Gestión de Ciberincidentes vigentes al supuesto planteando, obteniéndose planes de acción y actualizaciones de las documentaciones.

3. CONDICIONES DE EJECUCIÓN DEL SERVICIO

La empresa licitadora deberá realizar una propuesta detallada del Modelo de servicio propuesto, indicando los procesos de coordinación en las 3 líneas de prestación (SOC, seguridad preventiva y asesoramiento CSIRT/DFIR).

Este modelo de servicio se considerará de mínimos y en las fases iniciales se adaptará y acordará con DFA-CCASA para su puesta en vigor.

En la propuesta técnica se tendrán en cuenta los siguientes apartados.

3.1. Composición del equipo

La empresa licitadora deberá describir en su propuesta la organización prevista para la prestación de los diferentes servicios de seguridad solicitados, perfiles, rol o función, jerarquías, niveles especialización, así como otras herramientas y recursos propios (colaboración o pertenencia a determinadas asociaciones, fuentes de información, certificaciones...), que aporten valor al servicio prestado.

A la hora de identificar los perfiles adscritos en la propuesta técnica en ningún caso deberá revelarse información que deba ser objeto de valoración conforme a criterios de valoración automática (por ejemplo, sexo de las personas adscritas), **siendo ello causa de exclusión del proceso de licitación (en caso de que la documentación incluida en el sobre B contenga cualquier información o referencia a criterios de valoración automática, la empresa licitadora quedará automáticamente excluida de la licitación).**

3.2. Calidad y seguimiento del servicio

La empresa licitadora deberá especificar el modelo de seguimiento del servicio contratado (*Req026*), con al menos una reunión mensual en la que se reportará la actividad/seguimiento en sus 3 líneas de prestación (SOC, seguridad preventiva y asesoramiento CSIRT/DFIR).

La empresa licitadora deberá detallar en su oferta la relación de informes/cuadros de seguimiento (*Req027*) que permitan realizar el seguimiento de la calidad del servicio contratado, indicando formatos, posibles contenidos, posibilidades de personalización... Así mismo, se mostrarán ejemplos de cada uno de ellos. Estos informes/cuadros de mando serán utilizados durante la prestación del servicio para su seguimiento.

Los informes de seguimiento tendrán en cuenta los requerimientos comprometidos sobre los acuerdos de nivel de servicio.

Para la ejecución del servicio demandado, CCASA establecerá una persona responsable de servicio encargada de:

- Realizar el seguimiento y evaluación del progreso de puesta en marcha y ejecución del servicio
- Verificación de que el personal asignado por la empresa adjudicataria dispone de medios y capacitación necesarios para una prestación adecuada del servicio.
- Analizar y validar, si procede, los cambios, recomendaciones de ajuste y en general propuestas de mejora del servicio por la empresa adjudicataria. Revisar la evolución sobre la implantación de las propuestas aprobadas.
- Verificar el cumplimiento de los acuerdos de nivel de servicio (ANS) adoptados, y determinar la necesidad de aplicación de las penalizaciones correspondientes en caso de incumplimiento.
- Realizar seguimiento a la proyección económica del contrato y facturación del servicio.

La persona responsable del contrato en CCASA tendrá en la empresa adjudicataria una única persona interlocutora para la prestación de este servicio, quien asegurará la correcta prestación en los términos acordados.

Durante el proceso de seguimiento del servicio, la empresa adjudicataria podrá realizar propuestas de mejora que redunden en una mejora en la calidad y eficiencia del servicio de seguridad prestado (cambios en políticas, nuevas reglas, mecanismos correctivos...) cuya adopción deberá ser autorizada por CCASA, pero que en ningún caso podrán suponer modificación de los servicios, mejoras no establecidas en el pliego de condiciones particulares, ni cambios en los precios

3.3. Acuerdos de Nivel de Servicio (ANS)

La prestación de los servicios objeto del pliego conllevará el cumplimiento de una serie de niveles de servicio. El incumplimiento de las propuestas ofertadas conllevará la ejecución de las acciones habilitadas por la legislación vigente.

En la propuesta, el licitador deberá especificar los valores (respetando o mejorando aquellos para los que se aporta valor en la siguiente tabla) a los que se compromete con relación, al menos, a los siguientes indicadores:

INDICADOR	DESCRIPCIÓN	VALOR OBJETIVO
<i>Eficacia en notificación de nivel CRÍTICO en menos de 1 horas</i>	Es el porcentaje de incidentes que se categorizan de nivel CRÍTICO en los cuales el tiempo transcurrido entre la detección y notificación a CCASA es inferior a 1 horas	>95%
<i>Eficacia en el diagnóstico de incidentes</i>	% de incidentes correctamente categorizados	>95%
<i>Eficacia en la notificación</i>	% de falsos positivos	<5%
<i>Detección temprana de amenazas ocultas</i>	Número de threat hunting realizados al mes	>=1

Nota: Los niveles de tipología de incidente CRÍTICO se especifican en el “Información adicional I – Descripción técnica”.

La información relativa a estos indicadores deberá aportarse únicamente en el **Sobre A** (*criterios evaluables automáticamente*), sin que, **en ningún caso, pueda informarse al respecto en la propuesta técnica, Sobre B** (en caso de que la documentación incluida en el sobre B contenga cualquier información o referencia a criterios de valoración automática, la empresa licitadora quedará automáticamente excluida de la licitación).

El control de los ANS comprometidos en ningún caso se demorará más allá de los dos meses iniciales de prestación del servicio.

Durante el seguimiento del servicio, se analizará el cumplimiento de los valores objetivo comprometidos. En caso de incumplimiento de los valores propuestos en la oferta se llevarán a cabo la ejecución de las acciones habilitadas por la legislación vigente y/o penalizaciones especificadas.

3.4. Acogida del servicio

La empresa licitadora coincidirá al menos durante 1 mes con la empresa que actualmente presta el servicio. Durante este solapamiento de contratos la adjudicataria de esta licitación deberá recoger el conocimiento y procedimientos existentes para que el servicio continúe.

Por lo tanto, la empresa licitadora cumplirá al menos las siguientes condiciones para la acogida del servicio:

- Análisis de todas las configuraciones (IOCs, reglas, etc.) realizadas en las herramientas que pone a disposición CCASA y que han sido utilizadas por la empresa saliente en la prestación del servicio.
- Análisis de toda documentación técnica y administrativa necesaria para el traspaso del servicio
- Interlocución con la empresa saliente para recabar el conocimiento necesario que garantice la continuidad del servicio.
- Presentación de un plan de mejora a acometer durante el proyecto 2026-2029 de la organización, documentación, etc. con la que se prestó el servicio durante 2024-2026.

Estas tareas no serán de aplicación en el caso de que la empresa adjudicataria coincida con la que actualmente presta el servicio

3.5. Devolución del servicio

La empresa licitadora deberá garantizar que CCASA (u otra empresa contratada por CCASA) pueda continuar con la explotación de los servicios ofertados en este pliego una vez finalizado el contrato sin que se produzca interrupción en el servicio como consecuencia del cambio.

Por lo tanto, la empresa licitadora cumplirá al menos las siguientes condiciones para la devolución del servicio:

- Todas las configuraciones (IOCs, reglas, etc.) realizadas en las herramientas que pone a disposición CCASA de la empresa licitadora quedarán a disposición de CCASA, de forma que sea posible su explotación por parte de CCASA o a quien encomiende el servicio CCASA.
- Deberá realizar la entrega de toda documentación técnica y administrativa necesaria para el traspaso del servicio
- Deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas necesarias para garantizar la continuidad del servicio por CCASA.
- Garantizar el borrado de información relacionada con el servicio prestado a CCASA en los sistemas propios de la empresa licitadora, certificando mediante documento escrito la ejecución de dichos trabajos.

El periodo mínimo para preparar la devolución del servicio será de 1 mes. El periodo de devolución supone que CCASA (o la empresa en que encomiende el futuro servicio de SOC) empezará a recibir la información necesaria para el traspaso del servicio en la fecha en que se comprometa la empresa licitadora del presente pliego.

En caso de que la empresa adjudicataria no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, se llevarán a cabo la ejecución de las acciones habilitadas por la legislación vigente.

La empresa licitadora deberá describir en su propuesta técnica el alcance y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato (*Req029*).

3.6. Lugar de trabajo y equipamiento.

La prestación del servicio demandado se realizará principalmente en las instalaciones de la empresa adjudicataria. Las reuniones de lanzamiento del servicio o seguimiento de este que por eficacia y eficiencia se consideren necesarias su realización en presencial, se realizarán en las instalaciones de CCASA.

Así mismo, en el caso de ser necesaria la colaboración del equipo CSIRT/DFIR para la resolución de ciberincidentes críticos, CCASA podrá requerir la presencialidad de parte o la globalidad del equipo.

La empresa adjudicataria aportará toda la infraestructura necesaria para la prestación del servicio, incluida la herramienta de ticketing necesaria para el escalado de casos al CCASA. Así mismo, CCASA podrá solicitar la integración de la herramienta de ticketing de la empresa adjudicataria con la herramienta de ticketing de CCASA, sin que esto suponga ningún gasto adicional a CCASA.

4. FORMATO, ESTRUCTURA Y CONTENIDO DE LA OFERTA TÉCNICA

La oferta Técnica se presentará con letra preferiblemente tipo Arial, tamaño mínimo 10 e interlineado mínimo de 1,15. El tamaño de la oferta en ningún caso excederá de las 40 páginas, excluyendo los anexos. **No serán objeto de valoración el contenido de las páginas que excedan de los límites señalados anteriormente.**

Es obligatorio que la oferta técnica presentada siga el índice descrito en este punto, y aporten dentro del capítulo correspondiente la documentación necesaria que permita realizar la valoración de la propuesta técnica de forma correcta.

El índice de la oferta presentada será:

1. Introducción y resumen ejecutivo de la propuesta
2. Servicios prestados por el Centro de Operaciones de Seguridad (SOC)

Descripción detallada del alcance, características y nivel de servicio de los servicios prestados por el SOC, garantizando el cumplimiento de los servicios mínimos solicitados en el pliego:

- Servicios de Monitorización y Respuesta mediante las herramientas de monitorización especificadas en el “ANEXO 1 – Descripción técnica”: monitorización de eventos de seguridad, detección y categorización de incidentes, priorización, notificación y escalado, tratamiento de incidentes críticos, propuestas de inclusión de feeds/IOCs/ adaptados a DFA-CCASA, etc.
- Propuesta la organización prevista, jerarquías de servicio, niveles especialización, así como otras herramientas propias que contribuyan a las capacidades finales del servicio. Se incluirá la relación de metodologías y procedimientos operativos vinculados a la prestación del servicio y organización del mismo.

- Descripción de otros servicios/recursos propuestos como parte del servicio que redunden en la mejora de la eficiencia sobre el servicio de seguridad ofertado, sin coste adicional para CCASA.
- Creación de informes y cuadros de mando de seguimiento de esta línea del servicio.
- Etc.

3. Servicios prestados de Threat Hunting y detección de brechas de seguridad

Descripción detallada del alcance del servicio de ofertado incluyendo:

- Actividad proactiva de detección de amenazas sobre las herramientas disponibles en el “Información adicional I – Descripción técnica”, los diferentes niveles de servicio ofertados, procedimiento y metodologías a aplicar, reporte de las actividades realizadas, etc.
- Escaneo automatizado de vulnerabilidades, especificando la metodología de ejecución y gestión de la información obtenida, nivel de asesoramiento en la implantación de contramedidas, etc.
- Creación de informes y cuadros de mando de seguimiento de esta línea del servicio.

4. Servicios prestados de asesoramiento del equipo de respuesta ante incidentes (CSIRT/DFIR)

Descripción detallada del alcance del servicio de ofertado incluyendo:

- procedimiento y metodologías a aplicar
- niveles de servicio ofertados
- relación de perfiles expertos (de diferentes disciplinas: legal, experto seguridad, RRHH a consideración del licitador) que considere necesario para la prestación de los servicios especializados de respuesta ante incidentes críticos

5. Plan de implantación

La empresa licitadora deberá presentar una propuesta detallada sobre el Plan de implantación para la puesta en marcha del servicio, identificando:

- las diferentes actuaciones y fases de trabajo, el inicio operativo de la explotación de los servicios desde el SOC, y modo de integración con la operativa actual de CCASA.
- Identificación de actuaciones responsabilidad de CCASA para su integración en el plan de implantación.

6. Plan para seguimiento y control de calidad del servicio

Se especificará la propuesta del Plan de seguimiento y control de calidad con las metodologías, procedimientos, documentación, indicadores, etc. propuestos para el seguimiento, mejora y optimización de los servicios prestados:

- Propuesta de métricas e indicadores de servicio para control de calidad sobre el servicio prestado.
- Propuesta de indicadores de Nivel de Servicio adicionales a los especificados. **No se indicarán los valores objetivo de compromiso de los ANSs especificados porque estos se reflejarán en el sobre A.**
- Metodologías para la medición y seguimiento.
- Introducción de medidas correctivas para optimización del servicio.
- Etc.

7. Plan de acogida del servicio

Se describirá el alcance de tareas de adopción de documentación existente en el contrato previo, así como el modelo de transformación a la nueva forma de prestación del servicio.

8. Plan de devolución del servicio

Se describirá el alcance de tareas, transferencia de documentación, procedimientos y plazos necesarios para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos, ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas.

9. Ejemplos de Informes y cuadros de mando

Se detallará la propuesta de informes y cuadros de mando incluidos con la prestación del servicio, indicando formatos, posibles contenidos, posibilidades de personalización y mostrando ejemplos de cada uno de ellos para su valoración.

10. Relación de requisitos (Reqxxx) y páginas/párrafo donde aparece su explicación según formato de Anexo 4 (Información adicional IV)

5. INFORMACIÓN ADICIONAL.

Anexo 1: Descripción técnica

Anexo 2: Fórmulas de cálculo de los indicadores de los ANSs establecidos

Anexo 3: Compromiso de confidencialidad sobre información técnica.

Anexo 4: Relación entre requisitos y ubicación de su explicación

Información adicional : Descripción técnica

El contenido de este anexo no se publica por la confidencialidad de la información contenida.

Las empresas interesadas en presentar sus ofertas deberán dirigirse a la dirección licitacion_CCASA@araba.eus con Asunto "Expediente 26010 - Solicitud de información técnica adicional", aportando:

1. Datos de la empresa solicitante
2. Información adicional III - Compromiso de confidencialidad sobre información técnica, firmado electrónicamente con **certificado digital** incluido dentro de la Lista de confianza de prestadores cualificados de servicios electrónicos de confianza **(TSL) del Ministerio de Industria y Turismo**.
3. Datos de la persona solicitante

Una vez finalizado el plazo de presentación, esta información deberá de ser destruida.

CCASA se reserva el derecho de proceder a la entrega de dicha documentación de forma presencial, si lo considerara oportuno.

La información contenida en este documento no será facilitada a empresas que por su tipología y en opinión de CCASA no tengan interés legítimo en participar en el proceso.

Información adicional II: Fórmulas de cálculo de los indicadores de ANS establecidos

INDICADOR 1: EFICACIA EN NOTIFICACIÓN DE INCIDENTES DE NIVEL CRITICO EN MENOS DE 1 HORA

Descripción: Es el porcentaje de incidentes que se categorizan de nivel CRITICO en los cuales el tiempo transcurrido entre la detección y notificación a CCASA es inferior a 1 hora. El tiempo de notificación es la diferencia entre el momento de activación de la alerta en el SIEM de CCASA y el momento de envío de la notificación a CCASA.

$$\text{IND1} = \text{NumNotCRITICOen1} / \text{TotNotCRITICO}$$

Siendo:

- NumNotCRITICOen1 = Número de notificaciones de incidentes de nivel CRITICO que se han realizado en menos de 1 hora.
- TotNotCRITICO = Número total de notificaciones de incidentes de nivel CRITICO.

Este indicador será utilizado para las condiciones de penalizaciones.

INDICADOR 2: EFICACIA EN EL DIAGNÓSTICO DE INCIDENTES

Descripción: Es el porcentaje de incidentes que se categorizan (BAJA, MEDIA, CRÍTICA) inicialmente de forma correcta.

$$\text{IND4} = (\text{TInc} - \text{TincErr}) / \text{TInc}$$

Siendo:

- TInc = Total de incidentes notificados en el mes
- TincErr = Total de incidentes notificados en el mes cuya catalogación inicial ha sido posteriormente modificada.

Frecuencia de medición: mensual

INDICADOR 3: EFICACIA EN LA NOTIFICACIÓN

Descripción: Es el porcentaje de incidentes notificados a CCASA que tras su tratamiento se determinen que realmente no eran incidentes de seguridad.

$$\text{IND5} = \text{TIncFal} / \text{TInc}$$

Siendo:

- TIncFal = Es el total de incidentes notificados en el mes al CCASA cuya conclusión final se determina como no-incidente
- TInc = Total de incidentes notificados en el mes al CCASA

Frecuencia de medición: mensual

INDICADOR 4: DETECCIÓN TEMPRANA DE AMENAZAS OCULTAS



Arabako Kalkulu Gunea, A.B.
Centro de Cálculo de Álava, S.A.

Descripción: Es el número de estudios de threat hunting realizados en un mes que derivan en un informe de estado y propuesta de acción.

IND5= NumThreat

Siendo:

- NumThreat = Numero de estudios de threat hunting realizado en un mes

Frecuencia de medición: mensual

Información adicional III: Compromiso de confidencialidad sobre información técnica

D./Dña..... con DNI nº
en nombre propio y/o en representación de la empresa
..... con domicilio en Tfno.: y
C.I.F. Nº, lo que acredito mediante escritura de poder otorgada en
.....ante el notario con el número
..... de su protocolo.

DECLARA:

Que tiene interés en solicitar información completa de la “Descripción técnica” necesaria para preparar y presentar la oferta para participar en el procedimiento de licitación para la adjudicación de la “*CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA DIPUTACIÓN FORAL DE ÁLAVA Y SECTOR PÚBLICO FORAL*” (Exp.: 26010)

Que bajo su entera responsabilidad declara que utilizará dicha información a los únicos y exclusivos efectos de preparar la oferta para participar en el procedimiento de licitación.

Que bajo su entera responsabilidad declara que la referida documentación será destruida una vez haya sido adjudicado el contrato que tiene por objeto la ejecución del servicio.

Que la persona jurídica a la que representa asumirá de manera individual, irrevocable y principal la responsabilidad directa e indirecta por los eventuales efectos negativos o adversos que pudieran recaer sobre o que pudiera sufrir el Centro de Cálculo de Álava, S.A. y que tuvieran su causa o se produjeran como consecuencia de la utilización de dicha información para un fin distinto a la preparación de la oferta para participar en dicho procedimiento de licitación, o como consecuencia de la falta de destrucción de dicha información.

Que a tal efecto se compromete a mantener indemne a el Centro de Cálculo de Álava, S.A. de tales consecuencias, efectos o perjuicios tanto económicos como jurídicos.

Lugar, fecha y firma del representante

Información adicional IV: Relación entre requisitos y ubicación de su explicación

REQUISITO	PÁGINA	PÁRRAFO/S	OBSERVACIÓN
<i>Req001</i>			
<i>Req002</i>			
<i>Req003</i>			
<i>Req004</i>			
<i>Req005</i>			
<i>Req006</i>			
<i>Req007</i>			
<i>Req008</i>			
<i>Req009</i>			
<i>Req010</i>			
<i>Req011</i>			
<i>Req012</i>			
<i>Req013</i>			
<i>Req014</i>			
<i>Req015</i>			
<i>Req016</i>			
<i>Req017</i>			
<i>Req018</i>			
<i>Req019</i>			
<i>Req020</i>			
<i>Req021</i>			
<i>Req022</i>			



Arabako Kalkulu Gunea, A.B.
Centro de Cálculo de Álava, S.A.

<i>Req023</i>			
<i>Req024</i>			
<i>Req025</i>			
<i>Req026</i>			
<i>Req027</i>			
<i>Req028</i>			
<i>Req029</i>			