Expediente nº: 2021022

Objeto de la contratación: Suministro e Implantación de tecnologías SIEM y EDR para el Basque Cybersecurity Centre

Documento: Pliego de prescripciones técnicas particulares

Contenido

1. CONTEXTO 3
2. OBJETO DE LA CONTRATACIÓN 3
2.1. Suministro de la solución 3
2.2. Servicios profesionales 4
3. ESPECIFICACIONES TÉCNICAS 4
3.1. Consideraciones 4
3.2. Requisitos técnicos de la solución 4
3.2.1. Diseño de la solución 4
3.2.2. Características técnicas de la solución EDR 6
3.2.3. Características técnicas de la solución SIEM 7
3.3. Requisitos de los servicios profesionales 9
3.3.1. Organización y equipo de trabajo 9
3.3.2. Implantación de la solución 9
3.3.3. Mantenimiento 11
4. PLANIFICACIÓN Y ORGANIZACIÓN 12
4.1. Equipo de trabajo 12
4.2. Gestión del servicio 12
4.3. Seguimiento del servicio 12
4.4. Horario y lugar de prestación del servicio 13
4.5. Acuerdo de Nivel de Servicio 13
4.5.1. SLA para incidencias 13
4.5.2. SLA para peticiones de servicio 14
4.5.3. Penalidades 14
4.6. Plan de transición 15
5. PLAZOS DE EJECUCIÓN 15

1. CONTEXTO

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca dentro de la Agencia Vasca De Desarrollo Empresarial - Enpresen Garapenerako Euskal Agentzia (en adelante SPRI), ente público de derecho privado dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco.

El BCSC, como unidad de SPRI, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad abarca proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de Comité Permanente del BCSC.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. OBJETO DE LA CONTRATACIÓN

El objeto de esta contratación es el suministro e implantación de un Sistema de Gestión de Eventos e Información de Seguridad (SIEM, del inglés Security Information and Event Management) y una plataforma EDR (Endpoint Detection and Response) para el Basque Cybersecurity Centre.

La solución propuesta debe consistir en una solución integral que incluya todos los elementos necesarios para el cumplimiento de los requisitos y especificaciones descritas a lo largo del presente pliego.

A continuación, se detalla el alcance del contrato cuyo contenido se complementa con los requerimientos descritos en el apartado 3.

2.1. Suministro de la solución

La empresa adjudicataria deberá suministrar todo el equipamiento tanto hardware como software, incluyendo licencias, que sea necesario para la implantación y el correcto funcionamiento de un sistema de gestión de eventos e información de seguridad y una plataforma EDR para el BCSC.

La solución suministrada deberá cumplir con los requisitos establecidos en el presente pliego de condiciones técnicas.

2.2. Servicios profesionales

El adjudicatario deberá aportar y describir los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto. Así mismo, deberá prestar al menos los siguientes servicios, cuyos requerimientos se establecen en el apartado 3 del presente pliego de prescripciones técnicas.

- Ajuste de la solución final, del plan de trabajo y de la metodología establecida tras su revisión por parte del BCSC, hasta su validación.
- En caso de ser necesario, instalación del equipamiento hardware en la Sala Técnica del BCSC de acuerdo con la arquitectura de la solución propuesta y validada.
- Provisión del software y las licencias necesarias para las diferentes funcionalidades y tecnologías propuestas.
- Despliegue de los agentes EDR.
- Configuración básica de la solución.
- Integración de todas fuentes necesarias para realizar una gestión integral de la infraestructura del BCSC.
- Optimización del sistema.
- Elaboración y ejecución de un plan de pruebas que certifique la adecuada puesta en marcha de la solución.
- Formación y documentación de la solución desplegada.
- Garantía y soporte de fabricante de acuerdo con los requisitos descritos en el presente pliego de prescripciones técnicas.
- Servicio de mantenimiento, operación y soporte técnico avanzado de la solución desplegada.

3. ESPECIFICACIONES TÉCNICAS

3.1. Consideraciones

La infraestructura TIC del BCSC está compuesta por diversos sistemas y elementos conectados que se distribuyen entre las dependencias del BCSC y un tenant dedicado en el entorno de BATERA (EJIE). Todos estos componentes generan información muy relevante para la seguridad de la infraestructura si se dispone de un sistema que permita su explotación. Este hecho, sumado a la creciente complejidad y especialización de las amenazas de seguridad actuales, hacen prácticamente imprescindible disponer de una herramienta SIEM que permita centralizar los logs de los diferentes elementos y realizar el análisis de estos de cara a la detección de incidentes de seguridad y a la investigación de los mismos.

Por otro lado, las plataformas EDR permiten una monitorización continua de las actividades de los endpoints (dispositivos de usuario y servidores), identificando patrones de comportamiento anómalos que puedan constituir una amenaza e, incluso, permitiendo responder ante ellas para detenerla. Esta información aporta por sí misma un gran valor, y si se correla con los logs generados por el resto de los elementos que componen la infraestructura permiten tener una visión global de lo que pueda estar ocurriendo. De este modo, incluyendo también la ingesta de los eventos generados por la plataforma EDR, se conseguirá enriquecer los logs del SIEM y esto, a su vez, contribuirá a una mayor capacidad de detección, ya que cuanto mejor sea la calidad de los logs de un SIEM mayor será su capacidad de detección.

3.2. Requisitos técnicos de la solución

3.2.1. Diseño de la solución

La solución propuesta por el licitador deberá incluir todos aquellos elementos, tanto hardware

(equipamiento, transceivers, latiguillos, etc.) como software (firmware, licencias, etc.), necesarios para dotar al BCSC de un sistema de gestión de eventos e información de seguridad (SIEM) y una plataforma de detección y respuesta en equipos finales (EDR).

Para dimensionar la solución se han definido unos requisitos técnicos basándose tanto en las necesidades actuales de los sistemas como en su evolución esperada, de forma que no sólo satisfagan las necesidades actuales, sino que permitan las mejoras necesarias y doten de escalabilidad futura.

A continuación, se detallan los aspectos mínimos que deberán considerarse para realizar el diseño de solución propuesta. El incumplimiento de alguno de los requisitos implicará el descarte de la empresa licitadora en el expediente.

La plataforma EDR recibirá información de los agentes desplegados en todos los equipos de usuarios y servidores que componen el equipamiento del BCSC. Más concretamente se instalarán agentes en los siguientes equipos:

- Dispositivos finales de usuario (Windows 10)
- Servidores (Windows y Linux) ubicados en el BCSC
- Servidores (Windows y Linux) ubicados en el tenant del BCSC en BATERA

El SIEM recibirá información de las redes internas del BCSC. Éstas incluirán los servidores, así como el resto de los elementos y sistemas que conforman su infraestructura. Más concretamente recibirá información de las siguientes fuentes:

- Firewalls
- Switches
- Soluciones de Seguridad
- Infraestructura hiperconvergente
- Soluciones de autenticación
- Servidores (Windows y Linux) ubicados en el BCSC
- Servidores (Windows y Linux) ubicados en el tenant del BCSC en BATERA
- Plataforma EDR

Las soluciones SIEM y EDR serán on-premise. Actualmente en el BCSC disponemos de una infraestructura hiperconvergente con hipervisores Nutanix. La solución propuesta por la empresa licitadora podrá hacer uso de esta infraestructura siempre que el consumo asociado de recursos no supere 32 vCPU ni 128 GB de RAM ni 15 TB de disco. En caso de contrario, la oferta deberá incluir el coste de ampliar la infraestructura de virtualización añadiendo nuevos nodos a la misma o el suministro de un servidor dedicado. En el primer caso, los nodos incluidos deberán ser de las mismas características que los actuales. En estos casos, cualquier coste asociado deberá estar incluido en el precio de la licitación.

La empresa licitadora deberá detallar en su propuesta, tanto para el EDR como el SIEM, si las soluciones se desplegarán sobre nuestra infraestructura de Nutanix (1) o sobre una nueva infraestructura (2).

(1) En el caso de que se despliegue sobre la infraestructura Nutanix existente se presentará la matriz de compatibilidad o certificado del fabricante que garantice que el software, EDR y SIEM, está soportado sobre una infraestructura hiperconvergente de Nutanix con hipervisores AHV de Nutanix y que está totalmente cubierta por el contrato de mantenimiento del fabricante sin limitaciones ni condicionantes.

(2) En el caso de que se despliegue sobre una nueva infraestructura, la propuesta detallará

las características tanto del hardware como del software suministrado. Todos los costes derivados del despliegue de esta nueva infraestructura deberán estar incluidos en el presupuesto. Así mismo, se incluirá la matriz de compatibilidad o certificado de los fabricantes que garantice que el SW, EDR y SIEM, están soportados sobre la infraestructura propuesta.

En ambos casos, tanto para la solución EDR como SIEM, se detallarán los recursos necesarios (CPU, RAM y disco) necesarios para su implementación. Así mismo, se detallarán explícitamente los periodos de retención soportados con la infraestructura y licenciamiento incluidos en la propuesta.

3.2.2. Características técnicas de la solución EDR

La solución EDR propuesta deberá permitir hacer una monitorización continua de las actividades de los endpoint (dispositivos de usuario y servidores), identificando patrones de comportamientos anómalos que puedan constituir una amenaza e, incluso, permitiendo responder ante ella para detenerla.

El equipamiento propuesto por el licitador deberá cumplir, al menos, con las características detalladas en la siguiente tabla. La propuesta deberá incluir todo el software, las licencias, módulos hardware o componentes necesarios para ello.

Características Técnicas de la solución EDR
La solución EDR propuesta deberá haber participado en las tres rondas de evaluación de ATT&CK Evaluations de MITRE Engenuity y tener una visibilidad superior al 80% en la última evaluación del 2020. Así mismo, la solución propuesta deberá haber participado en los test de protección de esta tercera ronda y haber bloqueado satisfactoriamente al menos un 70% de los test ejecutados. La información está disponible en el siguiente enlace: https://attackevals.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak_fin7,apt29,apt3 De este modo, el BCSC puede asegurarse de que la solución EDR que resulte adjudicataria ofrece unas características tecnológicas suficientes y que su trayectoria ha sido suficientemente contrastada.
Solución dimensionada y licenciada para al menos 100 endpoints.
Plataforma EDR en formato OnPremise.
Arquitectura escalable que permita el crecimiento según se necesite.
Consola, con datos en tiempo real, con soporte de cuadros de mando, capacidades de búsqueda y de generación de informes.
Capacidad del agente EDR para trabajar tanto online como offline, de manera que la lógica de prevención, detección y respuesta del agente sea realizada localmente en el propio agente y su capacidad de detección no dependa de la conectividad con la consola central ni con Internet.
Capacidad de detección basada en comportamiento.
Telemetría de comportamiento de los endpoints (ficheros, procesos, registro, conexiones, etc).
Capacidad de búsqueda retroactiva en dicha telemetría.
Capacidad de detección de malware avanzado, PUP (potential unwanted programs), ataques sin archivos, troyanos de nueva generación indetectables por los antivirus, amenazas zero-day, amenazas avanzadas.
Posibilidad de ejecutar acciones de respuesta desde la plataforma EDR para contención en caso de detectarse una amenaza.
Funciones de EDR automatizadas.
Capacidad de inclusión de inteligencia (feeds de inteligencia, IOCs,…)
Posibilidad de generación de reglas personalizadas para detectar nuevas actividades sospechosas en tiempo real, así como implementar detecciones personalizadas.
La plataforma deberá soportar capacidades avanzadas de Threat Hunting para la búsqueda proactiva de amenazas, mediante correlación de históricos y análisis de telemetría e identificación de anomalías. **La empresa licitadora deberá especificar detalladamente dichas capacidades.** Ej. Búsqueda de archivos y procesos, búsqueda de conexiones de red, detección de amenazas avanzadas y comportamientos anómalos, análisis de actividad sospechosa, etc.
Capacidad de investigación forense basado en timeline, destacando los elementos sospechosos que han generado cada alerta.

Capacidad para generar información forense relacionada con cada equipo de tal forma que pueda ser explotada posteriormente.
Capacidad de extracción de artefactos forenses de los endpoints.
Capacidad de agrupación de alertas en incidentes de seguridad.
La plataforma EDR deberá integrarse con el SIEM ofertado.
Capacidad de integración vía API con diferentes herramientas de seguridad y automatización.
API capaz de desempeñar todas las acciones previamente descritas
La empresa licitadora debe garantizar que la herramienta EDR ofertada sea compatible con las soluciones de seguridad actualmente desplegadas como son la solución de antivirus Panda y Microsoft Defender. No se podrá reutilizar la infraestructura de antivirus existente actualmente, incluyendo el agente. En caso de que la solución propuesta pueda utilizarse para sustituir la solución antivirus actual deberá indicarse explícitamente en la oferta.
Soporte para múltiples S.O., como mínimo: ▪ Windows server: 2016 y posteriores ▪ Windows Cliente: Windows 10 y posteriores ▪ Linux: RHEL 7 y posteriores, Centos 7 y posteriores, Ubuntu 18.0 y posteriores
La empresa licitadora deberá especificar detalladamente la información recopilada por el agente EDR.
En lo relativo a la retención de datos, la solución recopilará y almacenará toda la telemetría necesaria (no solo la relativa a eventos sospechosos) para poder hacer investigaciones durante 90 días y posibilidad de recuperación de la información más relevante que será almacenada durante 12 meses como mínimo.

Las características detalladas a continuación no son requisitos obligatorios, pero sí se valorarán positivamente. Para que estas funcionalidades de valor añadido sean valoradas la oferta deberá incluir todos los costes asociados a las licencias, módulos hardware o componentes software que puedan ser necesarios para su completo funcionamiento.

Características Técnicas de VALOR AÑADIDO de la solución EDR
Detección de versiones de aplicaciones vulnerables en los endpoints.
El licitador deberá especificar todas las compatibilidades con S.O. soportadas, incluyendo aquellas relativas a sistemas operativos móviles, para su valoración.
Periodos de retención mayores a los indicados en los requisitos técnicos de obligado cumplimiento. **Indicar periodo de retención máximo con la infraestructura y modo de licenciamiento incluidos en la oferta**.

El cumplimiento de los requisitos, tanto los obligatorios como los de valor añadido, se justificará mediante la utilización de la tabla correspondiente, según se indica en el pliego de cláusulas administrativas.

3.2.3. Características técnicas de la solución SIEM

La solución propuesta deberá permitir la recolección, análisis y correlación de eventos e información de seguridad. Así mismo posibilitará el almacenamiento y la gestión combinada de los mismos, generando alertas en tiempo real y permitiendo configuraciones específicas de la herramienta en base a las necesidades del BCSC.

El equipamiento propuesto por la empresa licitadora deberá cumplir con las características detalladas en la siguiente tabla. La propuesta deberá incluir todas las licencias, módulos hardware o componentes necesarios para ello.

Características Técnicas de la solución SIEM
La solución SIEM propuesta deberá estar reconocida por Gartner como Leader en el último Magic Quadrant for Security Information and Event Management (publicado el 29 de junio del 2021). De este modo, el BCSC puede asegurarse de que la solución SIEM que resulte adjudicataria ofrece unas características tecnológicas de primer nivel y que su fabricante ofrece una trayectoria empresarial especializada en soluciones SIEM.
Solución dimensionada para soportar una ingesta de 30GBytes diarios y 500 eventos por segundo en momentos normales, pudiendo soportar picos puntuales de ingesta de mayor magnitud.
Solución SIEM en formato OnPremise.

Arquitectura escalable que permita el crecimiento según se necesite.
Gestión centralizada de todos los eventos a través de una consola de gestión única y basada en Web sin necesidad de Java ni de Flash.
En lo relativo a la retención de datos, la solución ofrecerá un mínimo de 3 meses online sobre los que pueda trabajar la herramienta. Además, se retendrá un histórico mínimo de 12 meses. Los datos históricos, en caso de necesidad, deben poder ser cargados/importados en la herramienta para una operación "online".
Correlación de eventos en tiempo real.
Correlación histórica sobre los datos que tenga online. Esta correlación histórica le debe permitir analizar IOC o casos de uso nuevos sobre eventos pasados.
La solución debe ofrecer casos de uso predefinidos mantenidos y documentados por el fabricante. **La empresa licitadora deberá indicar en su oferta el número de caso de uso predefinidos por el fabricante incluyendo una breve descripción de estos**.
La solución debe ofrecer informes predefinidos mantenidos y documentados por el fabricante.
Durante el tiempo de vida del contrato el fabricante proporcionará actualizaciones periódicas que incluirán nuevas reglas de correlación, casos de uso, informes y alertas predefinidos y documentados por fabricante.
La solución debe soportar reglas que permitan detectar anomalías en tiempo real como puede ser el cambio repentino de un valor o un suceso (incremento repentino de tráfico o de logins fallidos, por ejemplo).
La solución debe soportar reglas que permitan detectar anomalías estacionales como puede ser el cambio de un valor o un suceso respecto al que tenía en una fecha previa.
La solución debe ser capaz de agrupar incidentes relacionados en un único incidente, aunque los eventos estén separados en el tiempo por horas o días.
La solución debe proporcionar una API que permita automatizar tareas de configuración, administración y consulta.
La solución propuesta deberá integrarse con la plataforma EDR ofertada.
La solución debe ser personalizable, permitiendo crear, como mínimo, vistas, gráficos, filtros y cuadros de mando personalizados.
La solución debe permitir realizar consultas avanzadas en lenguajes similares a los utilizados para bases de datos.
La solución debe permitir incorporar feeds de inteligencia con datos sobre amenazas de seguridad que utilice posteriormente en sus correlaciones y búsquedas de eventos de seguridad.
La solución debe clasificar los incidentes o alertas de seguridad detectados en base a la matriz MITRE ATT&CK.
La herramienta debe permitir la recolección de logs utilizando entre otros los siguientes protocolos (Syslog, TLS Syslog, Syslog multilínea, SNMPv3, SMB, SCP/SFTP, WMI, MSRPC, API)
La solución debe detectar y reconocer automáticamente las fuentes syslog más comunes.
La solución debe permitir integrar, sin necesidad de desarrollos a medida, las siguientes fuentes (al menos el 70% de ellas): - Firewalls: FortiGate Security Gateway (Fortinet) y Palo Alto PA Series - Antivirus: Panda y Microsoft Defender - EDR: El propuesto en el pliego - Microsoft Office 365 - VPN: Palo Alto - Autenticación: LDAP, Active Directory, FreeIPA, RADIUS, TACACS (Clearpass) - DHCP Server (Linux y Windows) - DNS (Microsoft) - Microsoft Windows Event Security Log - Infraestructura de virtualización Acropolis de Nutanix - Servidores: Linux/Unix y Windows - ClearPass Policy Manager (Aruba Networks) - Catalyst Switches (Cisco) - CheckPoint Sandblast **La empresa licitadora deberá detallar cuales son las fuentes integrables sin necesidad de desarrollos a medida.**
La solución debe permitir incorporar fuentes personalizadas o no soportadas por defecto.
La herramienta debe disponer de una librería de extensiones descargables de un "market place" validado por el fabricante, donde el propio fabricante, partners y terceros puedan contribuir con sus desarrollos y casos de uso
Integración con herramientas de ticketing a través de protocolos estándar (especificar cuales).

Las características detalladas a continuación no son requisitos obligatorios, pero sí se valorarán positivamente. Para que estas funcionalidades de valor añadido sean valoradas la oferta deberá

incluir todos los costes asociados a las licencias, módulos hardware o componentes software que puedan ser necesarios para su completo funcionamiento.

Características Técnicas de VALOR AÑADIDO de la solución SIEM
Periodos de retención mayores a los indicados en los requisitos técnicos de obligado cumplimiento. **Indicar periodo de retención máximo con la infraestructura y modo de licenciamiento incluidos en la oferta**.
Módulo específico basado en Machine Learning para el análisis de comportamiento de usuarios (UBA). Este módulo debe formar parte de la solución de SIEM, gestionándose y viendo los resultados desde la consola única del SIEM. Este módulo debe permitir alertar ante desviaciones de comportamiento habitual de los usuarios. Este módulo debe permitir evaluar el riesgo de las actividades de un usuario y alertar ante actividades de riesgo. **Indicar el nombre del módulo o licencia que proporciona la funcionalidad (debe estar incluida en el precio).**
Módulo basado en Inteligencia Artificial que permita realizar análisis automatizados de los incidentes, reduciendo el tiempo dedicado por los analistas. Este módulo debe formar parte de la solución de SIEM, gestionándose y viendo los resultados a través de la consola única del SIEM. **Indicar el nombre del módulo o licencia que proporciona la funcionalidad (debe estar incluida en el precio).**

El cumplimiento de los requisitos, tanto los obligatorios y como los de valor añadido, se justificará mediante la utilización de la tabla correspondiente, según se indica en el pliego de cláusulas administrativas.

3.3. Requisitos de los servicios profesionales

3.3.1. Organización y equipo de trabajo

El adjudicatario deberá aportar y describir los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

En la propuesta se detallarán los currículums de cada una de las personas que vayan a participar en el proyecto, tanto en la fase de implantación como en el mantenimiento. El equipo de trabajo propuesto deberá contemplar al menos los roles de *Responsable del Servicio*, *Operación* y *Soporte Técnico Avanzado*. Las responsabilidades y características de dichos roles se detallan en el apartado 4.1 del presente documento.

La empresa adjudicataria deberá comunicar por escrito la designación de una persona de su organización, encargada de ejercer las facultades de responsable del proyecto en lo referente al proyecto contratado, siendo el interlocutor y responsabilizándose frente al BCSC de las personas que prestan el servicio.

El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y consecuentemente valorado.

3.3.2. Implantación de la solución

La empresa licitadora deberá incluir en su oferta un cronograma y la descripción de las tareas que se llevarán a cabo en cada una de las siguientes fases:

Planificación

Tras la formalización del contrato la empresa adjudicataria entregará un **plan de implantación** consistente en una propuesta inicial detallando la solución final, el plan de trabajo y la metodología establecida para la ejecución del proyecto para su validación por parte del BCSC. Dicho plan detallará también el modo en el que se propone abordar el despliegue de la solución propuesta.

Despliegue de la solución

En caso de ser necesaria la instalación de algún componente hardware, el despliegue de la solución consistirá en el traslado, suministro, instalación, configuración y puesta en marcha de la solución técnica propuesta y validada.

La instalación de este se realizará en la sala técnica del BCSC en el Parque Tecnológico de

Álava sobre bastidor en formato rack de 19'' ya existente. El adjudicatario deberá aportar todos los elementos hardware, software, accesorios, cableados y materiales que sean necesarios para la implantación de la solución propuesta, que deberán ser necesariamente nuevos. Así mismo deberá destinar al proyecto el personal técnico adecuado para la realización de los trabajos.

El reciclaje de los embalajes, así como la retirada del equipamiento actual correrá por cuenta del adjudicatario y deberá estar incluido en la propuesta.

En caso de no ser necesaria la instalación de ningún componente hardware, la fase de despliegue consistirá en la instalación de todo el software necesario para la implantación de la solución propuesta.

Configuración y puesta en marcha

El adjudicatario llevará a cabo todas las tareas necesarias para que la solución técnica quede completamente operativa, incluyendo la configuración y puesta en marcha de la solución incluida en el contrato. El BCSC deberá validar y aprobar la configuración final antes de su implementación.

La empresa licitadora deberá incluir en su oferta una **descripción detallada de las tareas** que realizará durante la fase de implantación.

Plan de pruebas

El adjudicatario elaborará un **plan de pruebas** que permita confirmar que la solución es completamente operativa y certificar la adecuada puesta en marcha de la solución, así como la prestación de todas las funcionalidades solicitadas.

El plan de pruebas será ejecutado por el adjudicatario y, opcionalmente, por personal del BCSC. Los resultados obtenidos serán validados por parte del BCSC y condicionarán el cierre del proyecto. En el caso de que los resultados del plan de pruebas evidencien que la solución implantada no cumple con los requisitos establecidos, el adjudicatario deberá realizar todos los cambios y/o correcciones necesarias hasta lograr el cumplimiento de la totalidad de los requisitos establecidos sin que esto suponga un incremento en los costes del proyecto.

Traspaso del conocimiento

El adjudicatario deberá incluir en su propuesta un plan de formación en la solución implantada. El objetivo de dicha formación no será obtener un conocimiento generalista del equipamiento, sino traspasar al personal del BCSC el conocimiento y las particularidades de la infraestructura tecnológica implantada.

A continuación, se indican algunos de los aspectos mínimos que se desean tratar en la sesión de traspaso del conocimiento del proyecto:

- Familiarización con los distintos componentes de la infraestructura con el objetivo de conocer la arquitectura y las configuraciones realizadas.
- Administración de las consolas de gestión de la solución implantada.
- Monitorización de la nueva plataforma.
- Procedimientos de explotación de la solución implantada.

Documentación

Tras la implantación de la solución el adjudicatario deberá entregar en un plazo no superior a 7 días la documentación completa de la misma incluyendo en ella toda la información relevante y necesaria para su posterior administración y gestión por parte del BCSC.

Entre la documentación a aportar, no debe faltar la siguiente:

- En caso de haber realizado instalación de algún componente hardware: Inventario del equipamiento instalado, con número de serie, modelo y marca de los equipos.

- Documentación de la configuración de la plataforma a nivel de arquitectura y conectividad.
- Configuraciones realizadas en todos los equipos: IP's, configuración del software, parametrización, contraseñas y demás.
- Guía de comandos útiles y/o de uso habitual.
- Guía de resolución de problemas comunes.
- Pruebas de validación realizadas y los resultados obtenidos.
- Documentación del fabricante y garantía, incluyendo manuales.

3.3.3. Mantenimiento

Servicio de operación y soporte técnico avanzado

El servicio de operación y soporte técnico avanzado tendrá una duración de **1 año** a contar desde la fecha de aceptación de la solución implantada (hito formal asociado al cierre de la fase anterior de Implantación de la solución).

El servicio contemplará la **operación de la solución propuesta**. Se realizarán todas las tareas solicitadas por el BCSC en este ámbito, así como todas aquellas que el adjudicatario considere necesarias para realizar la monitorización de los eventos de seguridad y la gestión de las soluciones objeto del contrato.

Así mismo, el adjudicatario deberá mantener actualizada la documentación existente y generar los nuevos documentos que se consideren necesarios para mantener debidamente documentadas las plataformas objeto del servicio.

La operación será realizada de forma peticionada por el BCSC o consensuada entre ambas partes cuando el adjudicatario lo proponga de forma proactiva. Todas las tareas realizadas, tanto las solicitadas por parte del BCSC como aquellas propuestas proactivamente por el adjudicatario, deberán quedar debidamente documentadas y registradas en las herramientas de gestión ITSM del BCSC.

Adicionalmente, el licitador deberá incluir en su propuesta la prestación de un **servicio de soporte técnico avanzado**, cuyo objetivo principal será el mantenimiento y optimización de la instalación inicial, así como la implantación de los nuevos casos de uso que surjan. El soporte técnico experto se prestará en formato de bolsa de horas. **Se recuerda que el número de horas incluidas en la bolsa es un dato de carácter objetivo a incluir en el Sobre B y NO se debe INCLUIR dentro de la Propuesta Técnica del Sobre C ya que en caso contrario se procederá a la exclusión de la propuesta presentada**.

Garantía, mantenimiento de fabricante y licencias

La propuesta deberá incluir todo el hardware, software y las licencias necesarias para las diferentes funcionalidades propuestas durante los **2 primeros años**.

Todos los componentes, tanto hardware como software, incluidos en la propuesta deberán disponer de un contrato de mantenimiento con el fabricante durante los 2 primeros años. La oferta presentada por la empresa licitadora deberá detallar el alcance de dicho soporte.

La oferta de la empresa licitadora detallará la modalidad de licenciamiento y soporte a contratar tanto con el fabricante de la solución EDR como SIEM. La propuesta deberá detallar las características y el alcance de dichos contratos.

Tanto las licencias como el mantenimiento con el fabricante se contratarán por un periodo de dos años completos desde el comienzo. No se admitirán planteamientos basados en la contratación sucesiva por periodos inferiores (por ejemplo, no se admitirá una contratación de 1 año + 1 año).

La no inclusión en la propuesta de cualquier concepto de licencia asociado tanto al hardware

como al software de la solución y que sea necesario para el completo funcionamiento de esta, podrá dar lugar a la descalificación de la propuesta.

4. PLANIFICACIÓN Y ORGANIZACIÓN

4.1. Equipo de trabajo

La propuesta deberá incluir el detalle del equipo de trabajo propuesto que al menos deberá contemplar los siguientes roles:

- **Responsable del Servicio**

  La empresa adjudicataria deberá comunicar por escrito la designación de una persona de su organización, encargada de ejercer las facultades de Responsable del Servicio en lo referente al servicio contratado, siendo el interlocutor y responsabilizándose frente al BCSC de las personas que prestan el servicio.

- **Operación**

  Personal dedicado a la monitorización de los eventos de seguridad, a la gestión de las soluciones objeto del contrato y al escalado de aspectos que no puedan ser resueltos por el primer nivel.

- **Soporte Técnico Avanzado**

  Especialistas en cada una de las tecnologías objeto del contrato para el escalado de aspectos que no puedan ser resueltos en primera instancia por el personal de operación. Así mismo, realizarán el mantenimiento y optimización de la instalación inicial y la implantación de los nuevos casos de uso que puedan surgir.

  Las personas designadas al soporte técnico avanzado deberán contar con al menos 3 años de experiencia demostrable en las tecnologías objeto del contrato.

Para cada una de las personas que componga el equipo de trabajo se deberá indicar en que roles participa, así como, su dedicación y centro de trabajo desde donde prestará el servicio.

El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y consecuentemente valorado.

Las características del equipo de trabajo se justificarán mediante la utilización de la tabla correspondiente, según se indica en el pliego de cláusulas administrativas.

4.2. Gestión del servicio

El BCSC dispone de su propia herramienta de gestión ITSM. La gestión del servicio objeto del contrato se realizará exclusivamente con dicha herramienta. La empresa adjudicataria deberá asumir y adecuarse a ésta, para ello se le proporcionará un usuario de acceso a la misma con el que podrá desarrollar su trabajo. No obstante, dicha utilización podrá llevarse a cabo mediante integraciones con las herramientas ITSM de la empresa adjudicataria.

Cualquier acción realizada en el marco del proyecto por el adjudicatario, independientemente de su naturaleza, deberá quedar debidamente documentada y registrada en la herramienta ITSM del BCSC. Así mismo, los indicadores del servicio, incluyendo aquellos empleados en el cálculo del cumplimiento del Acuerdo de Nivel de Servicio establecido, se obtendrán de esta herramienta.

Del mismo modo, la apertura de cualquier incidencia o petición de servicio por parte del BCSC se realizará exclusivamente desde nuestra herramienta.

4.3. Seguimiento del servicio

El adjudicatario realizará un seguimiento continuado del estado de las incidencias y peticiones de servicio con objeto de identificar posibles incumplimientos en el nivel de servicio establecido. Cualquier desviación importante en este sentido deberá ser inmediatamente notificada a la

persona designada por el BCSC para su tratamiento con el responsable del servicio. Del mismo modo, si el BCSC identificase desviaciones importantes en el nivel de cumplimiento del SLA este hecho se pondrá en conocimiento del responsable del servicio para su análisis.

Adicionalmente, el adjudicatario realizará un informe de seguimiento mensual donde se detallarán las incidencias y peticiones de servicios del periodo. El objetivo de dicho informe será asegurar la calidad final del servicio realizado y su contenido detallado se acordará entre la empresa adjudicataria y la persona designada por el BCSC.

4.4. Horario y lugar de prestación del servicio

El servicio objeto del presente contrato se prestará de forma habitual en las dependencias del adjudicatario, sin perjuicio de que haya ciertas situaciones en las que el BCSC pueda requerir la presencia de uno o varios de los miembros del equipo de trabajo en sus dependencias. Estas situaciones pueden venir derivadas de la criticidad de los trabajos a realizar o de una necesitad puntual del BCSC.

De manera específica las siguientes actividades se realizarán de forma presencial en las oficinas del BCSC y requerirán la participación del responsable del servicio y del soporte avanzado: implantación de la solución, reuniones de seguimiento mensuales, simulacros para verificar los planes de contingencia, intervenciones que por su alcance o impacto el BCSC considere conveniente realizar in-situ y otras situaciones análogas.

El Responsable del Servicio, así como aquellos componentes del equipo de trabajo cuyo rol sea de Soporte Técnico Avanzado, deberán prestar el servicio desde una oficina técnica, situada a una distancia no superior a 150 Kms de las oficinas en las que se encuentra el BCSC (Parque Tecnológico de Miñano – 015010 Vitoria-Gasteiz - Araba), ubicación lo suficientemente cercana al BCSC para garantizar, ante cualquier eventualidad que pueda surgir, una presencia en las dependencias del BCSC en un plazo adecuado y en cualquier caso, no superior a una hora y media.

El servicio de soporte técnico avanzado se prestará en el siguiente horario:

- Jornada partida (octubre a mayo):
    - Lunes a jueves: de 8:00 a 18:00
    - Viernes: de 8:00 a 15:00
- Jornada intensiva (junio a septiembre):
    - Lunes a viernes: de 8:00 a 15:00

El servicio de operación se prestará en horario continuado 24x7.

4.5. Acuerdo de Nivel de Servicio

La empresa licitadora deberá proponer un modelo de acuerdo de nivel de servicio que garantice la prestación de los servicios contratados dentro de unos límites aceptables, comprometiéndose al menos a garantizar que los servicios serán prestados de acuerdo con los niveles mínimos que se detallan a continuación:

4.5.1. SLA para incidencias

Prioridad	Descripción	Tiempo de respuesta	Tiempo de resolución
Crítica	Pérdida de un servicio crítico	< 1 hora	< 3 horas laborables
Alta	Pérdida de un servicio que no tiene consideración de crítico	< 2 hora	< 6 horas laborables
Media	Degradación de un servicio que impide trabajar adecuadamente	< 3 horas	< 12 horas laborables

Baja	Sin pérdida de servicio	< 6 horas	< 24 horas laborables

4.5.2. SLA para peticiones de servicio

Prioridad	Descripción	Tiempo de respuesta	Tiempo de resolución
Crítica	Peticiones urgentes o cuya no aplicación impide la puesta en marcha de una funcionalidad prioritaria	< 2 horas	< 8 horas laborables
Alta	Petición cuya no aplicación impide la puesta en marcha de una nueva funcionalidad	< 3 horas	< 16 horas laborables
Media	Petición que permite el funcionamiento habitual del servicio	< 4 horas	< 24 horas laborables
Baja	Petición cuyo aplazamiento no afecta al funcionamiento habitual del servicio	< 8 horas	< 48 horas laborables

4.5.3. Penalidades

En caso de incumplimiento, la penalización a aplicar será acumulativa tomando como base para el cálculo de los porcentajes una duodécima parte del precio de adjudicación. El primer incumplimiento de las incidencias de prioridad media y baja no conllevará penalización y se registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.

El modelo de penalización será el siguiente:

- Tickets de Prioridad Crítica:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 80%: Penalización 3%.
  - Cumplimiento < 80%: Penalización 5%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Crítica del mes.
- Tickets de Prioridad Alta:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 75%: Penalización 3%.
  - Cumplimiento < 75%: Penalización 5%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Alta del mes.

- Tickets de Prioridad Media:
  - Cumplimiento >= 90%: Sin penalización.
  - 90% > Cumplimiento >= 75%: Penalización 1%.
  - Cumplimiento <75%: Penalización 3%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Media del mes.
- Tickets de Prioridad Baja:
  - Cumplimiento >= 80%: Sin penalización.
  - 80% > Cumplimiento >= 70%: Penalización 1%.
  - Cumplimiento <70%: Penalización 3%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Baja del mes.

Se entenderá por ticket cualquier incidencia o petición de servicio. A pesar de que las fórmulas aplicables son las mismas, los indicadores correspondientes a las incidencias y peticiones se calcularán por separado.

4.6. Plan de transición

El licitador deberá detallar en su oferta de forma clara y concisa su propuesta tanto de plan de transición de entrada al servicio como de salida al finalizar el contrato. Ninguna de estas fases de transición del servicio podrá suponer coste adicional alguno para el BCSC.

Los planes de transición propuestos deberán contemplar los siguientes requisitos:

- Se establece un período de devolución del servicio a realizar en el último mes de vigencia del contrato, para la eventualidad de que a la finalización se produjera un cambio de adjudicatario.
- La transición de entrada a este expediente, en su caso, deberá llevarse a cabo en las dos semanas iniciales de prestación efectiva del servicio.

5. PLAZOS DE EJECUCIÓN

El plazo máximo para la ejecución del suministro e implantación de la solución será de 3 meses a partir de la fecha de formalización del contrato.

El periodo de operación y soporte técnico avanzado será de 12 meses a partir de la fecha de finalización de la fase de implantación de la solución.

La contratación de las licencias y el mantenimiento con los fabricantes, tanto hardware como software, se realizarán por un periodo de 2 años.