PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE UN SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM) MEDIANTE PROCEDIMIENTO ABIERTO

EXPEDIENTE: 2021.39

30/04/2021 (Versión 0)

ÍNDICE

1 ANTECEDENTES 3

2 OBJETO 3

3 DESCRIPCIÓN DEL SUMINISTRO 4

4 REQUERIMIENTOS TECNICOS MINIMOS DE LA SOLUCION OFERTADA 4

5 INSTALACIÓN, INTEGRACIÓN Y PUESTA EN MARCHA 8

6 SERVICIOS DE SOPORTE TÉCNICO DURANTE EL PERIODO DE GARANTÍA 8

7 DURACIÓN Y LUGAR DE EJECUCIÓN 8

8 OTROS REQUISITOS DEL SERVICIO 8

9 MEDIOS HUMANOS PARA LA PRESTACIÓN DEL SERVICIO 9

9.1 CONDICIONES GENERALES 9

9.2 CONDICIONES PARTICULARES 10

10 SEGUIMIENTO Y ACREDITACIÓN EN MATERIA LABORAL, SEGURIDAD SOCIAL Y DE SEGURIDAD Y SALUD EN EL TRABAJO 10

11 PENALIZACIONES 11

12 DOCUMENTACIÓN A PRESENTAR POR LOS LICITADORES 11

12.1 SOBRE A.- DOCUMENTACIÓN ACREDITATIVA DEL CUMPLIMIENTO DE LOS REQUISITOS PREVIOS Y OFERTA EVALUABLE AUTOMÁTICAMENTE A TRAVÉS DE FÓRMULAS. 12

1 ANTECEDENTES

EITB MEDIA dispone en sus instalaciones de multitud de elementos informáticos conectados y protegidos por un complejo sistema de seguridad informática y entre todos ellos generan una cantidad ingente de información relevante a su seguridad.

Mediante su recopilación centralizada se pretende conocer la situación de seguridad de múltiples ubicaciones desde una perspectiva unificada y correlacionada para la detección de tendencias y patrones no habituales.

Aunque se trata de una necesidad identificada hace bastante tiempo y cuya implantación es un requisito de muchas políticas de seguridad con las que trabajamos, la activación masiva del teletrabajo por motivo de la COVID-19 que ha experimentado EITB MEDIA, ha llevado al Departamento impulsor a considerar imprescindible su puesta en marcha para poder manejar el incremento de los riesgos asociados a la ciberseguridad (en el teletrabajo).

Este hecho hace aconsejable iniciar este procedimiento a fin de:

- ✓ Recopilar en un único punto toda la información generada por los elementos conectados.

- ✓ Conocer tras su análisis la situación de seguridad de múltiples ubicaciones de forma unificada y correlacionada con el fin de auditar y detectar tendencias y patrones para alertar y actuar de la forma más efectiva cuando sea necesario.

Durante meses el Departamento impulsor ha venido realizando los estudios y evaluaciones necesarias para determinar los requerimientos del mencionado sistema y que han dado lugar al lanzamiento de la presente contratación.

El producto/sistema que resulte adjudicatario deberá estar incluido en el Catálogo del CCN-CERT de Productos de ciberseguridad de las Tecnologías de la Información y la Comunicación recomendados por CCN-CERT en la guía **CCN-STIC-818**: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/527-ccn-stic-818-herramientas-de-seguridad-en-el-ens/file.html, en concreto en la sección referida a módulos de Monitorización y Análisis de Logs, en el ANEXO A. RELACIÓN DE HERRAMIENTAS ORIENTATIVAS, en la página 24, con lo cual su adquisición se encuentra dentro de las recomendaciones del Esquema Nacional de Seguridad, ENS.

Es por todo lo anterior por lo que inicia la contratación del suministro de la naturaleza y extensión que a continuación se describe.

2 OBJETO

El objeto del contrato al que se refiere el presente pliego lo constituye el suministro, instalación y puesta en marcha de un Sistema de Gestión de Eventos e Información de Seguridad para EITB MEDIA, S.A.U. (en lo sucesivo, EITB MEDIA o EC, indistintamente).

La ejecución de este contrato deberá ser efectuado con arreglo a los requerimientos y condiciones que se estipulan en este Pliego de Prescripciones Técnicas Particulares (en adelante, **PPTP**), así como en el correspondiente Pliego de Cláusulas Administrativas

Particulares (en adelante, **PCAP**), relativas a la presente contratación, de los que se derivan los derechos y obligaciones de las partes contratantes.

3 DESCRIPCIÓN DEL SUMINISTRO

La EC dispone del hardware, tanto a nivel de proceso, memoria y red como de almacenamiento, adecuados (procesador Intel Xeon 20 cores, 128GB RAM, 24TB discos SSD, 4 NIC) para alojar en sus instalaciones el producto que resulte elegido y sobre el que la solución deberá funcionar de forma sencilla y con rendimientos adecuados.

La adjudicataria deberá proporcionar el software y las licencias del producto necesarias que aseguren las siguientes prestaciones:

1) Recopilar los logs de los sistemas corporativos de la EC.
2) Establecer unos permisos de acceso a los logs con independencia de los permisos existentes en el sistema que los ha generado.
3) Evitar que puedan ser alterados o eliminados.
4) Permitir la realización de búsquedas en dichos logs.
5) Comprobar lo que ha ido ocurriendo como una secuencia de registros.
6) Generar, si así procediera, alarmas cuando se identifiquen sucesos fuera de lo común o no autorizados gracias a la correlación de eventos, observando lo que ocurre en varios sistemas como un todo y no con la visión parcial que de cada sistema pueda disponer.

Por tanto, de acuerdo con los descrito, la adjudicataria deberá realizar las siguientes prestaciones/trabajos :

- ✓ Integración con la infraestructura de la EC.
- ✓ Puesta a punto.
- ✓ Puesta en producción.
- ✓ Documentación.
- ✓ Mantenimiento mínimo de 1 año, en modalidad 8x5.

Los requerimientos numéricos del contrato y por tanto de las licencias objeto de suministro e instalación deberán ser las siguientes:

- ✓ Capacidad de gestionar una ingesta de eventos de al menos 100GB día.

4 REQUERIMIENTOS TECNICOS MINIMOS DE LA SOLUCION OFERTADA

La solución ofertada deberá dar debido cumplimiento a los siguientes requerimientos técnicos mínimos:

a. Reconocimiento por analistas/mercado

- ✓ Todas las funcionalidades requeridas en el presente pliego, deberán estar plenamente soportadas por el fabricante, y llevar un mínimo de 3 meses publicadas en el momento de publicar el pliego, con la intención de evitar inestabilidades de versiones beta o no suficientemente probadas en instalaciones reales.

b. Condiciones de Ingesta

- ✓ Deberá implementar un Schema On Read para la ingesta.
- ✓ Los datos que se ingesten deberán estar normalizados en un formado estándar NO PROPIETARIO.
- ✓ El mapeo de los datos deberá ser sencillo, con posibilidad de usar RegEx.
- ✓ Deberá dar opción de ingesta mediante agente ligero.
- ✓ Deberá recolectar y analizar todos los datos de todas las fuentes de ingesta disponibles y usarla para enriquecer casos de uso de Seguridad.
- ✓ Deberá permitir la ingesta de información generada por cualquier sistema de seguridad así como por instancias alojadas en cualquier *Cloud Service Provider*.
- ✓ Deberá permitir ingestar diariamente un mínimo de 100GB de logs sin limitación al número de EPS (eventos por segundo).

c. Detección Out of the Box

- ✓ Las reglas de detección deben ser facilitadas para su personalización de forma completa y no parcial.
- ✓ Deberá *usar Machine Learning* para incrementar las capacidades de detección de amenazas y no sólo la utilización de reglas.
- ✓ Deberá incorporar decenas de algoritmos de *Machine Learning* permitiendo su modificación.

d. Investigaciones

- ✓ La solución deberá contener un sistema de Gestión de Incidentes completo con integraciones bidireccionales con sistemas de ticketing.
- ✓ La solución deberá permitir añadir información de manera manual a los eventos.
- ✓ Deberá permitir el uso de los Frameworks de MITRE Att&ck y Kill-Chain (sin coste adicional).
- ✓ Integración con al menos 20 *feeds* de inteligencia de amenazas gratuitos y comerciales (sin necesidad de desarrollo adicional).
- ✓ **Monitorización de actividad del usuario** (UAM) que nos permita detectar y responder rápidamente a amenazas avanzadas y amenazas internas.
- ✓ **Soporte nativo para formatos basados en estándares** como Expresión de información de amenazas estructuradas (**STIX**, **CybOX**) e Indicadores abiertos de compromiso (**OpenIOC**), así como soporte para múltiples mecanismos de transporte como TCP/UDP e Intercambio automatizado confiable de información de indicadores (**TAXII**).

- ✓ Integración con centros de identidad y activos que incorporan contexto de usuario y activo de las bases de datos de administración de configuración (**CMDB**) y las herramientas de Lightweight Directory Access Protocol (**LDAP**).

- ✓ Gestión de Seguridad en Tiempo Real. Recogida en Tiempo Real de las fuentes de forma nativa (routers, switches, directorio, apps, …).

- ✓ Deberá tener la capacidad de asignar puntuaciones de riesgo personalizadas de manera automática a cualquier correlación para informar o alertar en función de la postura de riesgo específica de la organización, todo ello también personalizable.

- ✓ Deberá proporcionar búsquedas de correlación preconstruidas, incluyendo en las mismas datos en tiempo real y datos históricos, que cubran las correlaciones más solicitadas en ciberseguridad.

- ✓ Creación rápida y flexible de búsquedas de correlación, alertas, informes y paneles para equipos de seguridad, propietarios de líneas comerciales, ejecutivos y auditores.

e. Capacidades

- ✓ Deberá facilitar cientos de paneles e informes configurados OOB y personalizables para su uso.

- ✓ Deberá ser capaz de generar alertas en tiempo real y permitir la programación de ejecución de informes y búsquedas.

- ✓ Deberá permitir un escalado dinámico que permita el crecimiento de la plataforma hasta el orden del los PB de volumen de ingesta.

- ✓ Deberá posibilitar ingesta y explotación de información en tiempo real y datos almacenados con más antigüedad.

- ✓ Deberá dar cobertura a la detección de Amenazas avanzadas (Análisis de riesgos, Inteligencia para las amenazas, Inteligencia en protocolos, Actividad inusual) de forma nativa.

- ✓ Deberá permitir la creación de roles de acceso que limite tanto las capacidades de los usuarios como el catálogo de datos a consultar.

- ✓ Deberá integrarse con soluciones LDAP y MFA.

- ✓ Deberá cubrir OOB más de 450 casos de uso.

f. Marketplace

- ✓ Deberá tener una plataforma de aplicaciones abierta, donde terceros puedan desarrollar estas aplicaciones y ponerlas a disposición.

- ✓ La solución SIEM debe dar acceso a miles de aplicaciones extra sin coste adicional.

g. Estrategia

- ✓ La Herramienta deberá ser escalable a funcionalidades de ITOA

h. Soporte de logs nativo

- ✓ Soportará logs de multitud de fuentes, incluyendo entre otras

AIX
Apache/Tomcat
Brocade FabricOS
CheckPoint
CISCO FirePower IPS/IDS
CISCO ISE
CISCO Nexus
CISCO Switches and Firewalls
CISCO Wireless Controllers (WISM)
CITRIX Netscalers
Carbon Black Protection
CrowdStrike
CyberArk Vault
EMC VMWare (ESXi)
F5 Networks IPM
FireEye (NX, HX, CM)
Forescout
Guardium
IIS
IOS (CISCO)
ISC BIND
InfoBlox NIOS (DHCP/DNS)
Juniper Firewalls (MX Series)
LDAP (Generic)
Linux (auditd, iptables, smtp, SSH)
McAfee EPO (Antivirus, HIPS)
Medicare Security Database Events
Microsoft O365
NGINX
OpenDNS
Panda Security
Palo Alto Firewall (PA Series)
PostFix Mail
RACF (Mainframe)
RSA Authentication Manager
Sysmon
Tenable (Vulnerability Management)
Tipping Point IPS/IDS
Tripwire (FIM)
Windows Server and Workstation Logs

5 INSTALACIÓN, INTEGRACIÓN Y PUESTA EN MARCHA

Conforme a lo descrito en la cláusula 3 el suministro objeto de la presente contratación llevará aparejado la realización de los trabajos de instalación y puesta en marcha.

Estos trabajos deberán ser prestados por la adjudicataria de acuerdo a los siguientes parámetros técnicos:

- El suministro, instalación y configuración de elementos de forma que queden plenamente integrados y en producción en el entorno de ciberseguridad de la EC.

- El suministro, instalación y configuración deberá ser completado en un plazo máximo de UN (1) semana a contar desde el día siguiente de la formalización del contrato.

Por su parte la EC dispone de equipamiento de red y hará los ajustes físicos necesarios para conectar los equipos a las subredes apropiadas.

6 SERVICIOS DE SOPORTE TÉCNICO DURANTE EL PERIODO DE GARANTÍA

Los equipamientos y trabajos a realizar al amparo de la presente contratación deberán contar con una garantía de, al menos UN (1) año a contar desde la instalación, puesta en marcha y visto bueno de la EC.

Asimismo, todos los sistemas suministrados deberán incluir un servicio de mantenimiento de, al menos, un (1) año a contar desde la instalación, puesta en marcha y visto bueno y en modalidad 8x5.

En cuanto a los tiempos de respuesta para posibles incidencias que puedan ocurrir, la adjudicataria deberá atender cualquier incidencia comunicada por la EC con una disponibilidad de 24/7 en un plazo máximo de respuesta de ciento veinte (120) minutos a contar desde remisión del correspondiente con el fin de poder valorar la gravedad de la avería. El intervalo de actualización será diario, con un tiempo objetivo de resolución de hasta una semana laboral.

7 DURACIÓN Y LUGAR DE EJECUCIÓN

El contrato tendrá una vigencia igual a la duración del periodo de garantía del equipamiento suministrado.

No obstante lo anterior el suministro, instalación y configuración deberá ser completado en un plazo máximo de UNA (1) semana a contar desde el día siguiente de la formalización del contrato

8 OTROS REQUISITOS DEL SERVICIO

Para la correcta prestación del servicio objeto de la presente contratación las licitadoras deberán acreditar su condición NECESARIA de distribuidor autorizado de las licencias objeto de la presente contratación, así como, de los servicios de soporte en los términos solicitados en este pliego y el PCAP.

9 MEDIOS HUMANOS PARA LA PRESTACIÓN DEL SERVICIO

9.1 Condiciones generales

El personal adscrito a la prestación del servicio dependerá exclusivamente de la entidad que resulte adjudicataria (contratista), única que ostentará los derechos y obligaciones inherentes a su condición de empleadora.

A tales efectos, la empresa contratista asumirá las siguientes obligaciones:

1. Corresponderá exclusivamente a la entidad que resulte adjudicataria (contratista) la selección del personal que, reuniendo los requisitos de titulación y experiencia exigidos en la clausula siguiente del presente pliego formará parte del equipo de trabajo adscrito a la ejecución del contrato, sin perjuicio de la verificación por parte de la Entidad Contratante del cumplimiento de aquellos requisitos.

2. La entidad que resulte adjudicataria (contratista) procurará que exista estabilidad en el equipo de trabajo, y que las variaciones en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio (cuando existan razones que justifiquen esta exigencia), informando en todo momento a la Entidad Contratante.

3. La entidad que resulte adjudicataria (contratista) asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a toda empresa.

   En particular asumirá la negociación y pago de los salarios, la concesión de permisos, licencias y vacaciones, las sustituciones del personal en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y se deriven de la relación contractual entre las partes empleada y empleadora.

4. La entidad que resulte adjudicataria (contratista) deberá designar al menos una persona coordinadora o responsable, perteneciente a su plantilla de personal, que tendrá entre sus obligaciones las siguientes:

   a. Actuar como interlocutora de la entidad adjudicataria (contratista) frente a la Entidad Contratante, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo adscrito al contrato, de un lado, y la Entidad Contratante, de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.

   b. Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir al mismo las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratado.

   c. Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.

d. Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente la contratista con la Entidad Contratante, a efectos de no alterar el buen funcionamiento del servicio.

e. Informar a la Entidad Contratante acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato.

f. Garantizar que mientras las personas puestas a disposición del servicio objeto de la presente contratación se encuentren en alguna una de los Centros de la Entidad Contratante estos cumplan con las normas de seguridad de la Entidad Contratante y cuenten con los correspondientes distintivos que los identifique como personal de la entidad que resulte adjudicataria del servicio.

Si a consecuencia del incumplimiento por la entidad que resulte adjudicataria (contratista) de las obligaciones asumidas en virtud de esta cláusula, la Entidad Contratante fuera condenada al pago de cantidades con carácter solidario con la empresa contratista, se repercutirá en ésta la suma satisfecha, a cuyos efectos las entidades contratantes se reservan el ejercicio de cualesquiera acciones, administrativas o judiciales, que sean adecuadas y convenientes hasta la total recuperación de las cantidades pagadas.

9.2 Condiciones particulares

La adjudicataria deberá poner a disposición de la presente contratación un equipo profesional adecuado para la prestación del servicio.

Dicho equipo deberá contar con la certificación del fabricante de la solución ofertada para prestar servicios de soporte.

10 SEGUIMIENTO Y ACREDITACIÓN EN MATERIA LABORAL, SEGURIDAD SOCIAL Y DE SEGURIDAD Y SALUD EN EL TRABAJO

Para el seguimiento y acreditación de las obligaciones en materia laboral, seguridad social y de seguridad y salud en el trabajo prevista en la presente contratación la EC proporcionará a la contratista el acceso a la plataforma "*Koordinatu*".

Esta plataforma ha sido habilitada para el intercambio *on-line* de la documentación correspondiente al cumplimiento de las obligaciones en materia laboral, seguridad social y de seguridad y salud en el trabajo inherentes en la ejecución del contrato.

A tal efecto, una vez habilitado el acceso a "Koordinatu", la contratista tendrá la obligación de transferir, en el plazo indicado por la propia plataforma, la documentación solicitada y en especial la relativa a:

- Listado de trabajadores adscritos a la prestación del servicio.
- Certificados varios de la Seguridad Social (ITA, TC1, TC2, etc.)
- Certificados varios relativos al cumplimento de obligaciones en materia de prevención, seguridad en el trabajo (Identificación de riesgos, formación específica, certificados aptitud, etc.)
- Certificados de varios.

Si la entidad que resulte adjudicataria (y por tanto contratista), subcontrata parte de la ejecución del servicio contratado, deberá exigir a las entidades subcontratadas los justificantes de las obligaciones anteriores y entregarlos en los mismos términos en la plataforma "*Koordinatu*".

11 PENALIZACIONES

Además de las previstas en el Pliego de Cláusulas Administrativas Particulares, el Grupo EiTB se reserva la facultad de aplicar penalizaciones en aquellos casos en que la empresa que resulte adjudicataria incurra en alguno de los siguientes supuestos:

- Incumplimiento de los tiempos de respuesta

  Penalización: Hasta **500 euros** de penalización por cada incumplimiento en función de la gravedad.

- Otros supuestos a ser penalizados:

  - No prestar el contrato en las condiciones pactadas en el Pliego o en la oferta Adjudicataria.
  - Falta de diligencia en la prestación del contrato, incurriendo de forma injustificable, en más tiempo del necesario.
  - Negarse o demorarse a facilitar la información, que relativa al contrato, sea demandada por el responsable de la EC. El plazo máximo para la entrega de la documentación solicitada será de 15 días a partir de la comunicación formal.
  - La desobediencia inexcusable a las órdenes que la EC facilite por escrito a la empresa que resulte Adjudicataria para corregir deficiencias correctamente señaladas por aquel.
  - La modificación del contrato sin causa justificada y sin notificación previa.
  - Incumplimiento de los plazos comprometidos en el contrato.
  - Otros incumplimientos de normas generales y específicas previstas en el pliego.

  Penalización: Hasta **500 euros** de penalización por cada incumplimiento en función de la gravedad.

Las penalidades, que en su caso, pudieran llegar a imponerse lo harán por acuerdo del órgano de contratación, adoptado a propuesta del responsable del contrato de la EC, que serán inmediatamente ejecutivas, y se harán efectivas mediante deducción de las cantidades que, en concepto de pago total o parcial, deban abonarse al contratista o sobre la garantía que, en su caso, se hubiese constituido, cuando no puedan deducirse de las mencionadas cantidades.

DOS (2) incumplimientos facultarán a la EC a la resolución del contrato. La cuantía global por estas penalizaciones en ningún caso podrá superar el 10 por 100 del presupuesto del contrato. Superado este importe, la EC se reserva la facultad de resolver el contrato con la correspondiente incautación de la garantía definitiva.

12 DOCUMENTACIÓN A PRESENTAR POR LOS LICITADORES

Las entidades licitadoras deberán entregar sus propuestas de acuerdo con lo dispuesto en la cláusula 24 de las cláusulas específicas del PCAP.

12.1 SOBRE A.- DOCUMENTACIÓN ACREDITATIVA DEL CUMPLIMIENTO DE LOS REQUISITOS PREVIOS Y OFERTA EVALUABLE AUTOMÁTICAMENTE A TRAVÉS DE FÓRMULAS.

Las entidades presentarán sus ofertas ajustándose al modelo de tabla indicado en el **ANEXO III.1** del Pliego de Cláusulas Administrativas Particulares: FÓRMULAS MATEMÁTICAS.