PLIEGO DE PRESCRIPCIONES TÉCNICAS

Nº EXPEDIENTE: CF050-24-004

Renovación y optimización de la Infraestructura de Seguridad Perimetral y Puesto de Trabajo existente

ÍNDICE

1. ANTECEDENTES

Las necesidades de servicio en la red de VEIASA ha evolucionado se requieren nuevas funcionalidades a proporcionar, tanto desde el punto de vista técnico como de negocio:

- La seguridad como pilar fundamental, debido a la creciente concienciación sobre el grave impacto de los ciberataques
- Rápida aceleración y adaptabilidad desde los entornos cloud y la adopción de software como servicio (SaaS).
- Adoptar la automatización y la consolidación como técnicas para reducir los costes operativos y cubrir las necesidades dinámicas de SecOps/DevSecOps.
- Aumentar la capacidad de rendimiento bajo demanda (escalabilidad) para absorber tanto crecimientos vegetativos propios de la red, como nuevos retos basados en la aparición de nuevos servicios y necesidades.

Para absorber este nuevo tipo de demandas en las cuales la seguridad se consume como si fuese un servicio totalmente trasversal a los sistemas, se requiere evolucionar la solución de seguridad existente, integrando el equipamiento actual en producción.

2. OBJETO

1. Renovación de soportes y licencias de los actuales sistemas de Firewalls centrales y sistemas de Sandboxing por un periodo de 12 meses
2. Migracion al tenant de VEIASA en la nube del fabricante de los actuales sistemas de gestión y reporting centralizado por un periodo de 12 meses
3. Renovación de licencias, durante 12 meses, de todo el software de protección de sistemas de usuario final (Endpoint) de este fabricante, que actualmente utiliza VEIASA para detectar y bloquear amenazas a nivel de dispositivo en equipamiento TIC no corporativo, a saber ,Colaboradores Externos, Cadena de Suministro, equipamiento no plataformado de usuarios y dispositivos BYOD

4. DURACIÓN

El contrato tendrá una duración de 12 meses a contar desde la fecha indicada en el pedido.

5. REQUISITOS DEL SERVICIO

5.1: Renovación y optimización de la Infraestructura de Seguridad Perimetral existente

El objeto del presente pliego es la renovación de licenciamiento y soporte de la infraestructura actualmente desplegada en ITVs y SSCC de VEIASA, relacionadas con Firewalls y clientes de Endpoint para proveedores externos, para los 12 meses siguientes a la adjudicación del contrato.

Desde un punto de vista de optimización de costes tanto economicaos como de infraestructura de TI on-prem de VEIASA se pretende migrar la Consola de gestion en el tenant de VEIASA de la nuble del fabricante

Las soluciones designadas son de vital importancia para hacer posible la conformidad de los sistemas de información de VEIASA con respecto al Real Decreto 311/2022, de 3 de mayo, por

el que se regula el Esquema Nacional de Seguridad, en lo que respecta a los sistemas de categoría media. En general, todas las adquisiciones cumplen con los principios básicos (Art.5 del ENS) y en especial con el requisito mínimo g) Adquisición de productos de seguridad y contratación de servicios de seguridad (Art.12.6 del ENS).

5.1.1 Renovación de soportes y licencias de los equipos de seguridad perimetral

En la actualidad VEIASA tiene en todas sus delegaciones un cluster de cortafuegos para garantizar la máxima protección en los usuarios, sistemas y servicios de la compañía. Se requiere renovar durante un año las licencias y soportes asociados a los equipos

Para la realización de las ofertas se podrá solicitar al contacto publicado en el perfil del contratante de la JdA el detalle del equipamiento a renovar (modelo, SKU, número de serie, MAC asociada al equipo). El resumen del alcance sería el siguiente:

- *Estaciones ITV con menor tráfico*

Para las estaciones con menor tráfico se requiere la renovación durante un tres de los soportes y licencias de 80 equipos Check Point modelo SG-1570. El soporte y licencias serán del siguiente nivel:

- Soporte: soporte directo con el fabricante tipo 24x7
- Licencias:
  - Prevención de amenazas de nueva generación: Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, identificación y control de aplicaciones y de contenido, filtrado web (bloqueando acceso a páginas inapropiadas y/o peligrosas), reconocimiento y gestión de identidades, sistemas de protección de intrusión (IPS), seguridad DNS, antibot, antispam, antimalware y zero phising

- *Estaciones ITV con mayor tráfico*

Para las estaciones con mayor tráfico se requiere la renovación durante un año de los soportes y licencias de 62 equipos Check Point modelo SG-1600. El soporte y licencias serán del siguiente nivel:

- Soporte: soporte directo con el fabricante tipo 24x7
- Licencias:
  - Prevención de amenazas de nueva generación: Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, identificación y control de aplicaciones y de contenido, filtrado web (bloqueando acceso a páginas inapropiadas y/o peligrosas), reconocimiento y gestión de identidades, sistemas de protección de intrusión (IPS), seguridad DNS, antibot, antispam, antimalware y zero phising

- *Sede de Servicios Centrales*

Para los Servicios Centrales de VEAISA se requiere la renovación durante un año de los soportes y licencias de 2 equipos Check Point modelo SG-16200. El soporte y licencias serán del siguiente nivel:

- Soporte: soporte directo con el fabricante tipo 24x7
- Licencias:
  - Prevención de amenazas de nueva generación: Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, identificación y control de aplicaciones y de contenido, filtrado web (bloqueando acceso a páginas inapropiadas y/o peligrosas), reconocimiento

y gestión de identidades, sistemas de protección de intrusión (IPS), seguridad DNS, antibot, antispam, antimalware y zero phising
- Prevención y mitigación de amenazas de día cero: capacidad de realizar diagnósticos de ficheros y extracción de contenido malicioso en emuladores Sandbox.

5.1.2 Renovación de las licencias y soporte para la protección del puesto de trabajo

Se requiere renovar las licencias y soportes de la solución de seguridad que utiliza VEIASA para detectar y bloquear amenazas a nivel de dispositivo en equipamiento TIC no corporativo, a saber Colaboradores Externos, Cadena de Suministro, equipamiento no plataformado de usuarios y dispositivos BYOD. La solución de EPP (Endpoint Protection Platform) que Veiasa tiene desplegada en sus dispositivos Windows, Linux, MacOS así como las tablets que se pretenden desplegar en las estaciones ITV para el control de las mediciones es Harmony Endpoint Complete del fabricante Check Point.

Entre las funcionalidades de esta solución se encuentran:

- Consola de gestión unificada con la consola de los firewalls con objeto de optimizar y centralizar la plataforma de seguridad
- Antivirus para archivos, correo y web. Permitiendo la detección y desinfección de cualquier tipo de amenaza, detectando malware por comportamiento. En cuanto a la protección web se detectarán los intentos de acceso a páginas web que contengan elementos maliciosos, bloqueándolos.
- Firewall personal gestionado forma centralizada desde la consola. Debe permitir:
    - Bloquear las conexiones entrantes y/o salientes de las aplicaciones que se deseen.
    - Prevención de intrusiones.
    - Crear reglas de firewall para permitir/denegar el tráfico en sentido entrante/saliente de las maquinas, protocolos y puertos que se determinen.
- Bloqueo de todos o alguno de los dispositivos de los equipos de usuario (unidades de almacenamiento extraíbles, dispositivos de captura de imágenes, unidades de CD/DVD, módems USB, Bluetooth, etc.), impidiendo la entrada de malware y fugas de información. La solución permitirá la definición de diferentes acciones para cada tipo de dispositivo (bloqueo, acceso, lectura/escritura)
- Bloqueo de acceso a páginas web no deseadas. Deberá ser posible configurar esta protección basada en categorías, aunque se podrán también añadir listas blancas y negras de sitios y dominios permitidos.
- La solución proporciona protección sin comprometer la experiencia del usuario y el rendimiento del dispositivo
- La solución se integra con herramientas SIEM (para enviar syslog / rsyslog).
- El software se integra y complementa futuras soluciones EdR corporativas de Junta de Andalucía.

La cantidad de licencias a renovar son 650 y dispondrá soporte directo con el fabricante tipo 24x7

5.1.3 Consola SaaS para administración de los Firewalls, log y reporting

Se proporcionará una plataforma SaaS para la gestión, configuración y administración tanto de los equipos como de los logs, eventos y alertas de seguridad generados por la planta actual de firewalls de VEIASA.

Esta plataforma SaaS permitirá a los administradores de VEAISA optimizar su trabajo ya que no requiere mantenimiento (instalación o actualizaciones), las nuevas funcionalidades se importan automáticamente y permite la expansión bajo demanda sin preocuparse por el espacio de almacenamiento físico limitado.

La consola será compatible con la consola on premise que existe en el CPD y poseerá las mismas funcionalidades, garantizando una migración de plataforma sencilla y con la misma forma de administrar para los técnicos de VEIASA optimizando el coste y el proceso de aprendizaje.

La consola de gestión actual es Next Generation Security Management Software para 150 gateways del fabricante Check Point.

Tendrá la capacidad de realizar informes personalizables que den visibilidad completa de las amenazas detectadas, riesgos de seguridad, tipología de tráfico cursado en la red, etc

Dispondrá de una herramienta de gestión y correlación para automatizar la agregación y la correlación de los datos de registro, y los patrones de ataque potenciales, facilitando a los técnicos de VEIASA la revisión de logs para que puedan identificar rápidamente las amenzas de seguridad reales.

Dispondrá de módulo de compliance para gestión del cumplimiento normativo y de buenas prácticas. La adjudicataria debe proporcionar informes de cumplimiento de, al menos, las siguientes normativas: ISO 27001, ISO 27002. La política de seguridad se monitorizará de forma continua y automática, indicando el grado de cumplimiento en cada una de sus normas y la acción a tomar para configurarla adecuadamente.

La consola tendrá la posibilidad de gestionarse desde un único panel de control junto al resto de soluciones incluidas en el expediente.

La consola SaaS dispondrá de licencias necesarias para gestionar como mínimo 144 y contará con soporte directo con el fabricante tipo 24x7.

6. GARANTÍA

En la oferta se deberá contemplar el servicio de soporte 24x7 y el derecho a actualización de versiones incluido por el fabricante durante la vigencia del contrato, esto es, durante 12 meses.
La empresa adjudicataria deberá suministrar los documentos necesarios que justifique dicha garantía.

7. PLAZO DE ENTREGA

El plazo máximo para la renovación de las licencias será el indicado en el pedido enviado por la Unidad de Compras de VEIASA.

8. LUGAR DE ENTREGA

Las licencias se enviaran por medios electrónicos a la dirección que se indique una vez formalizado el pedido.

9. ASISTENCIA TÉCNICA Y CONTROL DE CALIDAD

La empresa adjudicataria deberá establecer un control de calidad certificando que los contratos son renovados teniendo en cuenta las descripciones indicadas en el apartado 5. La renovación deberá producirse en el plazo máximo de la fecha indicada en el pedido y se certificará mediante documento oficial del fabricante que constate que esta renovación se ha llevado a cabo. Esta confirmación oficial podrá facilitarse por correo electrónico, sin perjuicio del envío del documento original a las Oficinas Centrales de VEIASA, lo que no supondrá en ningún caso coste alguno para VEIASA.

Así mismo VEIASA dispondrá de 30 días adicionales tras la mencionada confirmación para verificar que las licencias asociadas en los supuestos detallados en el apartado 5 están efectivamente renovadas. Durante este período, el adjudicatario deberá interceder con el fabricante para aclarar cualquier cuestión relacionada con la renovación. Si durante ese plazo, VEIASA advirtiera algún error o incidencia en la gestión de la renovación objeto de esta licitación lo pondrá en conocimiento de la adjudicataria, que vendrá obligada a solucionarlo en el plazo máximo de 7 días naturales, debiendo comunicar la resolución del error o incidencia a VEIASA, disponiendo ésta de otros 30 días naturales para dar su conformidad.

CASTRO PEREZ JOSE JUAN - 36092741Z

Firmado digitalmente por CASTRO PEREZ JOSE JUAN - 36092741Z
Fecha: 2024.02.02 11:23:54 +01'00'

28764181J DAVID PELAYO (C:A41398645)

Firmado digitalmente por 28764181J DAVID PELAYO (C:A41398645)
Fecha: 2024.02.06 10:27:47 +01'00'

Propuesta de redacción elaborada por:
Jose Juan Castro Perez
Tecnico de Unidad de Mantenimiento de SSII