PLIEGO DE PRESCRIPCIONES TÉCNICAS SERVICIO DE SOPORTE, PREVENCIÓN DE AMENAZAS Y MANTENIMIENTO DE LA PLATAFORMA DE CORTAFUEGOS DE ENRESA	Clave: 000-ES-SD-0001 Páginas: 4

N.º Expediente: CO-SD-22-002

ÍNDICE

1. OBJETO DEL PLIEGO TÉCNICO

Este pliego establece las prescripciones técnicas requeridas para la prestación del servicio de soporte, prevención de amenazas y mantenimiento de la plataforma de cortafuegos de Enresa.

2. ALCANCE DEL SERVICIO Y TAREAS A REALIZAR

Enresa dispone de una plataforma de cortafuegos o firewall como parte de su arquitectura técnica de seguridad para la gestión y protección de los sistemas de información de la organización, compuesta por dos dispositivos del fabricante Palo Alto Networks, modelo PA-3020, configurados en alta disponibilidad, con suscripción de seguridad relativa a prevención de amenazas.

El servicio debe cubrir las siguientes actividades, para un periodo de 22 meses:

- Renovación del soporte Premium por fabricante, que incluirá la disponibilidad de las diferentes actualizaciones de software o parches de seguridad del equipamiento, así como la resolución de incidencias o consultas.
- Renovación de la suscripción de seguridad de prevención de amenazas, para el equipamiento en alta disponibilidad.
- Servicio de mantenimiento integral que, en integración con el soporte del fabricante, proporcione servicios de Service Desk para la gestión de incidencias, de mantenimiento preventivo, para la revisión cada once meses o auditoria de estado de los equipos, y de mantenimiento evolutivo, para la instalación efectiva de nuevas versiones o actualizaciones.

2.1. RENOVACIÓN DEL SOPORTE PREMIUM

El contratista proporcionará a Enresa, la renovación del servicio de soporte premium, que incluirá los siguientes requisitos:

- Soporte Premium de la plataforma de cortafuegos ofrecido por el fabricante Palo Alto Networks. En este tipo de soporte, el fabricante tiene los mejores recursos técnicos que estarán disponibles para apoyar a Enresa en la implementación de seguridad. Esta asistencia técnica en remoto y presencial se proporciona en un horario de 24x7.

- Este nivel de soporte incluye el acceso a Security Assurance para ayudar con expertos de seguridad cuando se produzca un incidente.

- Servicio de actualizaciones de software o parches de seguridad para permitir que los cortafuegos cuenten con las últimas funcionalidades que mejoran el servicio que proporcionan.

- Servicio de interlocución para gestión de consultas, lo que facilita un canal directo con el fabricante agilizándolas.

2.2. RENOVACIÓN DE LA SUSCRIPCIÓN DE SEGURIDAD DE PREVENCIÓN DE AMENAZAS

El contratista proporcionará a Enresa, la renovación de la suscripción de seguridad de prevención de amenazas (Threat Prevention), que incluirá los siguientes requisitos y capacidades:

- La suscripción será ofrecida directamente por el fabricante Palo Alto Networks para poder beneficiarnos de su amplia red de dispositivos instalados que recogen información alrededor del mundo y mediante un sistema de inteligencia artificial actúa de forma proactiva ante las amenazas.
- Deberá proveer inspección y clasificación del tráfico, analizando paquetes por separado y en grupo, lo que posibilita la comprobación pormenorizada de todo lo que circula por la red de Enresa.
- Dispondrá de capacidades de detección y bloqueo de amenazas en todos y cada uno de los puertos del equipamiento.
- Dado que las actuales técnicas de intrusión utilizan los canales encriptados, incluirá la posibilidad de descifrar selectivamente mediante políticas e inspeccionar el tráfico de estos canales mejorando su eficacia.
- Incorporará análisis heurístico para detección de paquetes y patrones de tráfico anómalos, como por ejemplo análisis de puertos, barridos de hosts y ataques de denegación de servicio.
- Incluirá funcionalidades de configuración de firmas de vulnerabilidades y prevención de intrusiones personalizadas e importación de reglas de formatos de código abierto.
- Una táctica aprovechada en una red para evadir la detección de dispositivos de seguridad es la ofuscación y ocultación de las comunicaciones HTTP de forma que un posible incidente de seguridad en el ordenador de un usuario permite la interpretación de los datos. La suscripción de prevención de amenazas contará con capacidades de protección contra estas tácticas.
- La suscripción deberá permitir la integración con otras suscripciones de seguridad que puedan adquirirse durante la duración del contrato.

2.3. SERVICIO DE MANTENIMIENTO INTEGRAL

En combinación con el servicio de soporte premium del fabricante, enunciado en el apartado 2.1, el contratista proporcionará un servicio de mantenimiento integral, que incluirá los siguientes requisitos:

- Service Desk: El contratista proporcionará un servicio de contacto y ayuda, para la gestión de incidencias y consultas sobre la plataforma, así como la interlocución con el fabricante en caso de necesidad. El servicio se prestará en modalidad 24x7 los 365 días del año, con un tiempo de respuesta determinado en función de la severidad, tal y como se determina en el Acuerdo de Nivel de Servicio (ANS) establecido en los Anexo al Pliego Tipo de Cláusulas Administrativas.
- Mantenimiento preventivo: Con el objeto de garantizar el correcto funcionamiento del equipamiento y sus capacidades funcionales, el contratista realizará como mínimo una revisión técnica cada once meses del del estado del equipamiento y su configuración. Como resultado de la revisión, el contratista elaborará un informe, donde desarrollará como mínimo el siguiente índice:

- Objetivo y alcance de la revisión.
- Análisis de versiones de software.
- Análisis de estado.
- Análisis de amenazas y estadísticas.
- Conclusiones.

- Mantenimiento evolutivo y correctivo: El contratista proporcionará, a demanda de Enresa y tras una notificación por parte del fabricante de una evolución del equipamiento, un servicio de mantenimiento evolutivo, ofreciendo soporte remoto y presencial, mediante técnicos especialistas en la instalación de nuevas versiones de software o actualización de versiones correctivas que resuelvan un fallo o incidencia en la infraestructura.

3. MODELO DE RELACIÓN DEL SERVICIO

Por parte de Enresa, el responsable del contrato será la persona de referencia para la gestión y coordinación de las actividades derivadas de la ejecución del servicio.

El contratista designará un gestor del contrato que será la persona de referencia encargada de la supervisión y cumplimiento de los Acuerdos de Nivel de Servicio, así como de coordinar y garantizar el cumplimiento de los requisitos técnicos asignando los medios adecuados para la correcta prestación del servicio.

Para el seguimiento de estos acuerdos de nivel de servicio se realizará un informe bimensual con los indicadores y su cumplimiento.

Enresa podrá solicitar la convocatoria de una reunión, presencial o telemática, cuando lo crea conveniente y con los asistentes necesarios para el buen funcionamiento de la misma.