PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL MANTENIMIENTO DE INFRAESTRUCTURA DE FIREWALLS

Septiembre- 2021

nasertic

Navarra de Servicios y Tecnologías, S.A.

| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |
| info@nasertic.es | www.nasertic.es |
| Tel: 848 420 500 | Fax: 848 426 751 |

INDICE

1. Objeto y ámbito

El objeto de la presente contratación es la oferta de los servicios de mantenimiento necesarios para la infraestructura de cortafuegos, en adelante Firewalls, tanto propia como la gestionada por Nasertic. Esta infraestructura constará de Firewalls de marca CheckPoint como Palo Alto en diferentes modelos.

2. Criterios de prescripción de condiciones particulares

A continuación, se relacionan las prescripciones técnicas particulares que obligatoriamente habrán de cumplir los equipos objeto del mantenimiento.

Las siguientes prescripciones técnicas tendrán carácter obligatorio.

Aquellas ofertas que no cumplan las especificaciones obligatorias indicadas en este apartado de prescripciones técnicas particulares serán objeto de exclusión del procedimiento de licitación.

Igualmente será motivo de exclusión la falta de justificación adecuada del cumplimiento de los requerimientos obligatorios solicitados.

3. Descripción general de necesidades

Debido a las crecientes necesidades de servicio y del incremento de equipos a mantener, se dispone a tener la capacidad para poder solucionar la operativa diaria, así como para la resolución de las incidencias que puedan surgir. Debido a la naturaleza dispar de la infraestructura a mantener en cuanto a fabricantes, se precisa un mantenimiento por cada uno de los fabricantes de firewalls soportados por Nasertic, en concreto CheckPoint y Palo Alto.

Durante la prestación del servicio a lo largo de la vida del contrato, se podrá producir la renovación de los equipos actuales ante la obsolescencia tecnológica, productos descatalogados o por la renovación de equipos por parte de Nasertic, siendo sustituidos por equipos de gamas similares, en los que se deberá cubrir el mantenimiento como si fuesen los

actuales.

LOTE 1: CheckPoint.

Dentro de la infraestructura de firewalls de la marca Checkpoint gestionada por Nasertic se necesitan cubrir los siguientes puntos.:

1. Mantenimiento con el fabricante de los equipos. Todos los mantenimientos deberán renovarse y estar vigentes durante la vigencia del contrato de forma automática.
2. Realización de los upgrade de versiones de los sistemas ante: vulnerabilidades críticas, recomendación del fabricante o al menos una actualización de versión anual de todos los sistemas. Se deberá mantener una versión homogénea de toda la infraestructura en la medida de lo posible.
3. Disponer de una bolsa de al menos 50 horas anuales para la resolución de dudas, configuraciones complejas y servicios de auditoría y mejora continua del funcionamiento de los equipos. Esta bolsa de horas podrá ser utilizada indistintamente por cada uno de los equipos.
4. Anualmente se realizará una auditoría en la que se realizarán acciones de:
    - Comprobación de la integridad del sistema, pruebas de conmutación (en los que estén en clúster), comprobación de reglas (eliminación obsoletas, priorización, optimización de las mismas), carga de tráfico en interfaces, copias de seguridad, etc..
    - Actualizar documentación del sistema. Interfaces, esquemas de conexión, etc.
    - Conexiones concurrentes
5. Servicios Gestionados para la asistencia en situaciones de emergencia durante el horario fuera de oficinas, es decir desde las 15:00 h a las 08:00 del día siguiente entre semana laboral y las 24 en fines de semana y festivos locales. Esta asistencia será para la solución de incidentes críticos de pérdida o degradación grave del servicio o ante solicitudes de creación de reglas de emergencia para poder dar servicios puntuales.

LOTE 2: Palo Alto

Para el mantenimiento de los Firewalls de Palo Alto se necesitan cubrir los siguientes puntos:

1. Monitorización del estado del dispositivo, cubriendo aspectos como estado de las máquinas, fallos del clúster, y estados generales de CPU, memoria, etc.
2. Operación remota de la plataforma: En caso de que sea necesario y así se solicite se podrá gestionar de forma remota la plataforma cubriendo las siguientes tareas de gestión: Modificación de reglas, Modificación de perfiles de acceso, Aplicación de soluciones ante incidencias, Aplicación de actualizaciones y parches.

3. Aplicación de Medidas extraordinarias contra amenazas: Se contemplan la aplicación de medidas contra amenazas generalizadas y críticas como por ejemplo la creación de reglas específicas para la protección contra Malware de alto impacto (Ransomware, troyanos, etc.)
4. Envío y generación de informes. Se generarán informes periódicos, al menos cada 6 meses, del estado de la plataforma con las recomendaciones de mejora. Este informe debe tener una finalidad preventiva y proactiva ante la solución de futuras incidencias.

4. Descripciones técnicas de la infraestructura de cortafuegos gestionada por Nasertic.

A continuación, se presenta el detalle técnico de la infraestructura actual presente en Nasertic, presentando los modelos exactos, así como los identificadores necesarios para identificar correctamente los equipos para su mantenimiento.

En caso de que un equipo esté sin mantenimiento activo por cualquier causa, este deberá incluirse a la mayor brevedad posible.

Lote 1: Equipos CheckPoint:

Los equipos checkpoint actuales, como los futuros en caso de renovación, deberán estar gestionados desde la cuenta de Nasertic dentro del usercenter de CheckPoint.

Account ID	Product Name	SKU
8042286	5100 Next Generation Threat Prevention Appliance	CPAP-SG5100-NGTP
	5100 Next Generation Threat Prevention Appliance for High Availability	CPAP-SG5100-NGTP-HA
	Next Generation Security Management Software for 10 gateways	CPSM-NGSM10
8100151	1490 Security Appliance with Threat Prevention Security suite, Wired	CPAP-SG1490-NGTP
	1490 Security Appliance with Threat Prevention Security suite, Wired	CPAP-SG1490-NGTP
8381876	1570 Base Appliance with SandBlast	CPAP-SG1570-SNBT

Lote 2: Equipos Palo Alto:

Los equipos Palo actuales, como los futuros en caso de renovación, deberán estar

gestionados por la cuenta de Nasertic.

Modelo	Número de Serie	Licencia
PAN-PA-220	012801053783	Threat Prevention
PAN-PA-220	012801091340	PAN-DB URL Filtering Premium Partner Support WildFire License

5. Control de calidad del servicio - SLA

En este apartado se describirá con mayor detalle cuales deberán ser los niveles del servicio prestado en función del canal utilizado y del nivel de criticidad de la alerta. Estos acuerdos se aplicarán por igual a los dos lotes del servicio.

A nivel general, el servicio deberá contar en todo momento con el apoyo del fabricante del dispositivo tanto para consultas técnicas, la apertura de casos como sobre todo la resolución de incidencias críticas.

Ante una alerta, ésta se podrá reportar las 24 horas cualquier día del año (24x7). En función del canal y de la criticidad de esta incidencia deberá haber unos tiempos de respuesta ante la recepción y procesado de las alertas. Estos tiempos se reflejan en la siguiente tabla:

RECEPCIÓN Y PROCESADO DE LAS ALERTAS		
Tipo	SLA	Cobertura
Respuesta telefónica	95% en 5 minutos	24 x 7
Abandono de llamadas	< 5 %	24 x 7
Respuesta a herramientas de monitorización	95% en 10 minutos	24 x 7
Respuesta a alertas por email	95% en 30 minutos	24 x 7

Todo el servicio independientemente del lote deberá proveer de unos tiempos de respuesta acorde a la naturaleza del problema y su impacto.

Los tiempos de respuesta ante el incidente se muestran en la siguiente tabla:

INCIDENCIA	RIESGO/IMPACTO	DESCRIPCIÓN	TIEMPO MÁXIMO DE RESPUESTA	PENALIZACIÓN /MES
CRÍTICA	Caída del equipo completo o de un servicio crítico	El servicio está interrumpido, el impacto es muy alto o el sistema está inutilizable	95% <= 30 minutos	2.000€
ALTA	Sólo un servicio no crítico afectado	Un servicio no crítico se ve afectado.	95% <= 1 hora	500€
MEDIA	Riesgo en el servicio	La incidencia produce problemas puntuales, o intermitentes, sin poner en riesgo el servicio	95% <= 2 horas	200€
BAJA	Bajo rendimiento	La incidencia no produce ningún tipo de problema a los usuarios/servicios en su operativa normal	95% <= 4 horas	100€
CONSULTA	Asistencia general/consulta	Consultas sobre cómo hacer, cómo configurar, o resolución de incidencias sin ningún impacto en los usuarios/servicios	95% <= 24 horas	100€