PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SERVICIO DE MANTENIMIENTO DE CORTAFUEGOS Y SERVICIOS DE SEGURIDAD DE LA UNIVERSIDAD DE LA RIOJA

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SERVICIO DE MANTENIMIENTO DE CORTAFUEGOS Y SERVICIOS DE SEGURIDAD DE LA UNIVERSIDAD DE LA RIOJA.

Índice

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE SERVICIO DE MANTENIMIENTO DE CORTAFUEGOS Y SERVICIOS DE SEGURIDAD DE LA UNIVERSIDAD DE LA RIOJA.

1. OBJETO DEL CONTRATO

El objeto del presente pliego es regular las condiciones del servicio de mantenimiento de cortafuegos y servicios de seguridad de la Universidad de la Rioja, concretadas en la auditoría, mantenimiento preventivo y soporte de su infraestructura de seguridad.

Asimismo atenderá las necesidades de formación de los técnicos de la Universidad, ayudándoles a gestionar eficientemente la infraestructura y posibilitando el conocimiento de nuevas tecnologías de seguridad que puedan resultar de interés en la implantación de futuras mejoras técnicas.

2. SERVICIOS INCLUIDOS

- Soporte y mantenimiento de las plataformas Checkpoint.
- Auditoría de seguridad.
- Pruebas de intrusión.
- Gestión remota de cortafuegos.
- Formación.

3. SOPORTE Y MANTENIMIENTO DE LAS PLATAFORMAS CHECKPOINT

3.1. PRESTACIONES INCLUIDAS

La Universidad de La Rioja dispone de una arquitectura de red segura basada en tres cortafuegos del fabricante Checkpoint (Firewall NGX R65) y una estación de gestión. Cada uno de estos cortafuegos se compone de dos nodos físicos configurados en alta disponibilidad. En el anexo I se especifica las licencias de este fabricante de las que dispone la Universidad de La Rioja.

Respecto a las citadas licencias, el servicio incluirá:

- Actualización de las licencias de software a las últimas versiones que vayan surgiendo.

- Soporte telefónico y por correo electrónico para la resolución de incidencias o problemas en la instalación, actualización o uso del software.

- Soporte telefónico y por correo electrónico a los técnicos de la Universidad para la resolución de incidencias en la interconexión por VPN de los sistemas de la Universidad con usuarios remotos o sistemas de terceros.

- Resolución de dudas sobrelicenciamiento del software e interoperabilidad con otros productos del fabricante.

- No se fijará ningún límite en el número máximo de incidencias que puedan ser reportadas ni en el número de horas dedicadas a una incidencia.

- Soporte de backend por parte del fabricante, incluyendo la corrección de bugs mediante parchea, acceso a la base de datos de conocimiento del producto, descarga de nuevas versiones y de paquetes de actualización de parches.

- Acceso a toda la documentación de los productos adquiridos y foros del fabricante.

3.1. HORARIOS

El servicio de ofrecerá en jornadas laborables de ámbito nacional, de lunes a viernes, de 8:00 a 18:00 horas.

3.2. TIEMPOS DE RESPUESTA

El técnico de la Universidad que abra una incidencia fijará el nivel de prioridad de la misma. El adjudicatario deberá cumplir los siguientes tiempos de respuesta mínimos para la atención de las incidencias en función de su nivel de prioridad:

- Incidencias de prioridad alta: 30 minutos.
- Incidencias de prioridad normal: 4 horas.
- Incidencias de prioridad baja: día siguiente laborable.

El tiempo de respuesta se consideran dentro del horario indicado en el apartado 3.1.

3.3. ACTUALIZACIONES DE VERSIONES

Al menos una vez al año se realizará una actualización de las versiones de la estación de gestión y de los tres clusters de cortafuegos.

Se instalará la última versión y parches disponibles del software o bien la que se acuerde con el personal de la UR.

Esta actualización se realizará in-situ en las dependencias de la UR, intentando buscar los horarios en los que menos se perjudique el funcionamiento de los servicios de red pero siempre en jornadas laborales.

Se evitará concentrar la migración de todos los dispositivos en la misma jornada para tratar de minimizar posibles problemas inherentes a la nueva versión. Una aproximación sería,

migrar una jornada la estación de gestión, la semana siguiente uno de los cortafuegos, y en una última jornada los 2 cortafuegos restantes.

Pevio a la actualización, se hará un proceso de estudio de las diferencias entre las versiones y los posibles problemas o puntos a tener en cuenta en la migración o que afecten al despliegue de la nueva versión en la infraestructura UR. Antes de acometarla se presentará un informe a la UR con las conclusiones de este proceso de estudio.

3.4. EQUIPO TÉCNICO DE SOPORTE

Se empleará un equipo técnico de soporte compuesto entre 2 y 5 técnicos que responderá a las incidencias. El adjudicatario se compromete a que, salvo situaciones extraordinarias y excepcionales, serán estos técnicos y no otros los que atenderán las incidencias de seguridad.

Al menos un técnico de los que compongan este equipo deberá cumplir con la certificación CCSE.

Al menos un técnico de los que compongan este equipo deberá cumplir con la certificación CISA.

Al menos un técnico de los que compongan este equipo deberá cumplir con la certificación CISSP.

Si durante la ejecución del contrato la empresa adjudicataria necesitase reemplazar a alguno de los técnicos, deberá hacerlo por otro con las mismas certificaciones y capacidad técnica, debiendo comunicarlo y acreditarlo a la Universidad, para su aceptación.

4. AUDITORÍA DE SEGURIDAD

4.1. PRESTACIONES INCLUIDAS

El adjudicatario realizará una auditoría de seguridad, en el transcurso de los tres primeros meses de ejecución del contrato, que incluirá al menos:

- Auditoría de seguridad de la configuración de los cortafuegos:

    - Auditoría de la configuración global de los cortafuegos.
    - Auditoría de la configuración de VPNs.
    - Auditoría de reglas de seguridad.

- Auditoría de arquitectura de seguridad física y lógica, infraestructura de seguridad y medidas implementadas.

Esta auditoría podrá realizarse bien en las instalaciones de la Universidad o en las dependencias del adjudicatario.

La Universidad facilitará toda la información de configuración y documentación que se necesite para su realización.

Como resultado de esta auditoría se entregará un informe que contenga al menos:

- Detalle de los aspectos auditados.
- Conclusiones de la auditoría, indicando puntos fuertes y débiles.
- Propuestas de mejora.

4.2. EQUIPO DE AUDITORÍA DE SEGURIDAD

Deberá ser el mismo que el equipo técnico de soporte.

4.3. JORNADAS DE AUDITORÍA

El adjudicatario dedicará, al menos, cuatro jornadas de sus técnicos a realizar labores de auditorías de seguridad.

5. PRUEBAS DE INTRUSIÓN

5.1. PRESTACIONES INCLUIDAS

El adjudicatario realizará una prueba de intrusión de “caja blanca” contra servidores y/o aplicaciones de la Universidad, en el transcurso de los nueve primeros meses de ejecución del contrato, y tras haber realizado la auditoría de seguridad.

El test de intrusión se realizará sobre los servidores ubicados en la red DMZ de la Universidad.

Las pruebas de intrusión se realizarán desde internet simulando ser un atacante en el exterior del campus.

Se realizarán dos tipos de pruebas de intrusión:

a) Pruebas de la seguridad de la red y servicios

   Identificar vulnerabilidades encontradas en los servidores expuestos a internet y en los servicios de red que éstos ofrecen cara a l público (DNS, SMTP, POP, IMAP, HTTP, ...)
   Localizar errores de configuración o de implantación de estos servidores y servicios que puedan provocar un problema de seguridad.

b) Pruebas de la seguridad de las aplicaciones web

Identificar vulnerabilidades en las aplicaciones que se ejecutan en entorno web y que corren en los servidores de la Universidad.

El objetivo no es profundizar exhaustivamente en la explotación de las vulnerabilidades para conocer su alcance en profundidad, solamente se pretende detectarlas, identificarlas y asignarles un nivel de criticidad aproximado.

A la hora de hacer las pruebas de intrusión de aplicaciones web se tomarán como base, la documentación de los proyectos Top Ten y Testing Guide de OWASP. Haciendo al menos las siguientes pruebas de intrusión:

- Pruebas en la validación de entrada de datos. Inyecciones.
- Pruebas de autenticación.
- Pruebas de gestión de sesiones.
- Pruebas de autorización.
- Pruebas de denegación de servicio.

La empresa adjudicataria acordará con el Responsable del Contrato cuáles serán los servidores o aplicaciones auditadas y el nivel de profundidad hasta el que se realizará.

Las pruebas de intrusión se realizarán después de haberse finalizado la auditoría de seguridad, de forma que habrá un conocimiento previo de la arquitectura de seguridad.

La Universidad de La Rioja proporcionará previamente información detallada de aquellos servidores/aplicaciones contra los que se vayan a realizar las pruebas de intrusión. Por tanto, dado que se dispondrá de toda la información, se evitarán, en la medida de lo posible, las pruebas automáticas, centrándose principalmente en tests de intrusión manuales.

El adjudicatario presentará un documento con la metodología que se seguirá durante las pruebas de intrusión.

Como resultado de las pruebas de intrusión, el adjudicatario entregará un informe que contendrá, al menos:

- Alcance de las pruebas de intrusión.
- Detalle de los sistemas, aplicaciones o servicios auditados.
- Enumeración de vulnerabilidades encontradas, asignándoles un nivel de criticidad aproximado y un nivel de dificultad para explotar la vulnerabilidad.
- Conclusiones del test de intrusión, indicando puntos fuertes y puntos débiles.
- Propuestas de mejora o corrección de problemas.

5.2. EQUIPO TÉCNICO

El licitador destinará un equipo técnico para las pruebas de intrusión compuesto de 2 a 5 técnicos. El adjudicatario se compromete a que, salvo situaciones extraordinarias y excepcionales, serán estos técnicos y no otros los que realizarán las pruebas de intrusión.

Si durante la ejecución del contrato la empresa adjudicataria necesitase reemplazar a alguno de los técnicos, deberá hacerlo por otro con las mismas certificaciones y capacidad técnica, debiendo comunicarlo y acreditarlo a la Universidad, para su aceptación.

5.3. JORNADAS DE PRUEBAS DE INTRUSIÓN

El adjudicatario dedicará, al menos, 12 jornadas de sus técnicos a realizar labores de pruebas de intrusión.

6. GESTIÓN REMOTA DE CORTAFUEGOS

6.1. PRESTACIONES INCLUIDAS

Se deberá proveer de un servicio de configuración remota de los cortafuegos corporativos. Este servicio incluirá la conexión remota a los sistemas de la Universidad para gestión de las políticas de seguridad.

Este servicio podrá ser solicitado de forma esporádica por la Universidad de La Rioja, y se utilizará en los casos en que los técnicos de la Universidad no tengan la posibilidad de realizar estas modificaciones.

El responsable del contrato acordará el método de trabajo junto con el adjudicatario, estableciendo canales de comunicación, así como la forma de documentar los cambios realizados.

6.2. HORARIO DE PRESTACIÓN DEL SERVICIO

El servicio se ofrecerá en jornadas laborables de ámbito nacional, de lunes a viernes, en horario de 8:00 a 18:00 horas.

6.3. TIEMPO DE RESPUESTA

El tiempo máximo de respuesta será de tres horas.

6.4. EQUIPO TÉCNICO DE GESTIÓN REMOTA

Será el mismo que realice los servicios de soporte y auditoría.

6. FORMACIÓN

6.1. PRESTACIONES INCLUIDAS

El adjudicartario organizará, a su cargo, la impartición de cursos de formación destinados a la actualización de conocimientos de los técnicos de la Universidad de La Rioja, en materia de seguridad.

El contenido de los cursos estará relacionado con los productos de seguridad objeto de este concurso, con otros productos de seguridad que utilice la Universidad, temas de seguridad en general, o con nuevas tecnologías, productos, metodologías o normativas relacionadas con la seguridad de la información. Los contenidos se acordarán previamente con el responsable del contrato.

No se considerarán cursos de formación las presentaciones de nuevos productos, que puedan considerarse como presentaciones comerciales o de preventa.

Los cursos se impartirán en las instalaciones de la Universidad, aportando ésta los medios materiales y tecnológicos básicos para su realización (sala, ordenadores, proyectores, conexión a red, etc.).

El adjudicatario entregará la documentación para los cursos en formato electrónico e impreso.

6.2. JORNADAS DE FORMACIÓN

Se impartirán un mínimo de siete jornadas de formación durante el plazo de ejecución inicial del contrato.

7. NÚMERO DE SERVIDORES/APLICACIONES

A efectos de la formulación de las ofertas de los licitadores, el número estimado de servidores y aplicaciones es el siguiente:

- Número de aplicaciones web para pruebas de intrusión: 16.
    - Complejidad de dichas aplicaciones:
        - Baja: 10
        - Media: 6
        - Alta: Ninguna.
- Número de servidores instalados en la red DMZ: 9

Anexo 1. Datos contrato checkpoint

Account ID: 0006011663

Account Name: UR2005-08

1	CPMP-VFE-U-3DES-MODULE-NGX CPVP-VPS-1-NGX CPMP-PPK-1-NGX CK-2561AF97B29D	2561AF97B29D
2	CPMP-VFF-U-3DES-NGX CPVP-VPS-1-NGX CPMP-PPK-1-NGX CK-AD08B6A2C55E	AD08B6A2C55E
3	CPMP-HVPG-XL-NGX CPVP-VPS-1-NGX CK-751FB632A306	751FB632A306
4	CPMP-VPG-XL-NGX CPVP-VPS-1-NGX CK-A5672966EB5D	A5672966EB5D
5	CPXP-CI-VPX-250-NGX CK-647C8567F24A	647C8567F24A
6	CPXP-CI-HVPX-250-NGX CK-50ADB7C4D760	50ADB7C4D760
7	CPVP-VSR-5000-NGX CK-839A320012E8	839A320012E8
8	CPVP-VSR-5000-NGX CK-F6534C37967D	F6534C37967D
9	CPUTM-EDGE-XG16-ADSL-A-EU	00:08:DA:58:04:1F
10	CPCES-CO-STANDARD-ADD	75A6G79
11	CPCES-CO-STANDARD	9OA6UH8