PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL SERVICIO DE ADMINISTRACIÓN Y MONITORIZACIÓN DE LA SEGURIDAD DE RED DE LA ADMINISTRACIÓN DE LA COMUNIDAD DE CASTILLA Y LEÓN

1. OBJETO

El objeto del presente contrato es la gestión de la seguridad de red, que comprende, la administración y operación de los cortafuegos, el servicio de monitorización de seguridad de red (en adelante, NSM) y la gestión de los incidentes de seguridad detectados por los cortafuegos, el servicio de NSM y otras fuentes de información adicionales.

2. CONDICIONES GENERALES

A efectos de este concurso se define el horario laboral de lunes a viernes no festivos de 8:00 a 19:00 excluyendo las festividades de ámbito nacional y de la Comunidad Autónoma de Castilla y León.

Las tareas del presente concurso se realizarán como mínimo de forma presencial de 9:00 a 14:00 en las instalaciones que la ACCyL determine en Valladolid, siendo valorable la ampliación de dicho tiempo presencial con un máximo de 8 horas diarias dentro del horario de apertura de dichas instalaciones.

Toda la arquitectura de acceso a Internet está redundada en dos emplazamientos físicos independientes en la ciudad de Valladolid. El adjudicatario deberá disponer de los medios materiales (hardware y software) y humanos necesarios para la prestación de los servicios solicitados. Asimismo deberá presentar una propuesta de arquitectura de los elementos que considere necesarios para la prestación de los servicios requeridos en el presente pliego.

La ACCyL proporcionará un número de teléfono fijo y una cuenta de correo electrónico para la interlocución con el exterior durante el horario laboral.

3. ADMINISTRACIÓN DE CORTAFUEGOS

La administración de cortafuegos consistirá en las tareas de operación y monitorización de los cortafuegos propiedad de la ACCYL. Los cortafuegos objeto de estas tareas son, a día de hoy:

Fabricante	Modelo
Fortinet	2 Fortigate 3810 A
Stonesoft	2 Stonegate 3201-P
Juniper	2 SSG 320
Cisco	26 ASA 5505 39 PIX 501

Para la gestión de los equipos del fabricante Stonesoft se dispone de una consola de gestión Stonegate Management Center (en adelante, SMC) y para la gestión de los equipos Cisco de la herramienta Cisco Security Manager (en adelante, CSM).

Para la definición del servicio se clasificarán los cortafuegos como críticos o no críticos. En la arquitectura actual se consideran cortafuegos críticos los clústeres de Fortinet y Stonesoft. El resto de cortafuegos Juniper o Cisco son considerados como no críticos a los efectos del presente concurso.

Las recepción de las peticiones de operación en los cortafuegos así como la notificación y asignación de incidencias en los mismos serán tramitadas a través de la plataforma de ticketing del Centro de Operación de Redes y Servicios de la Administración de la Comunidad de Castilla y León (en adelante CORS), actualmente EasyVista.

Se valorará la experiencia del licitador en la prestación de servicios similares, así como que el personal participante en el proyecto esté certificado por los fabricantes Fortinet y/o Stonesoft.

La plataforma puede cambiar a lo largo de la vida del contrato. En este caso la ACCyL proporcionará la formación necesaria para realizar las operaciones objeto de este servicio.

3.1 Operación de cortafuegos

La tarea de operación de los cortafuegos consistirá en las siguientes subtareas:

a. Crear, modificar y eliminar reglas en los mismos.

b. Resolución de problemas relacionados con aplicaciones que requieran de permisos en los cortafuegos.

c. Creación, implementación y verificación de la política de copias de seguridad de la configuración de los cortafuegos, con los requisitos de seguridad adecuados.

d. Actualización de versiones de software/firmware.

Se valorará la inclusión de herramientas de gestión especializadas en políticas de cortafuegos que faciliten la detección de reglas no utilizadas y la optimización de las políticas aplicables a cada uno de los fabricantes de la plataforma actual.

Se valorará cualquier otra aportación que permita la mejora de la operación de los cortafuegos.

3.2 Monitorización de cortafuegos

La tarea de monitorización de los cortafuegos tendrá como objetivo mejorar la disponibilidad de la solución.

Esta tarea se realizará en horario 24x7, siendo el adjudicatario responsable de disponer de los medios y personal adecuado para su realización.

El adjudicatario prestará los servicios 24x7 mediante alguna de estas opciones:

- Túneles VPN SSL o VPN IPSec contra equipos de la ACCyL presentes en Internet.

- VPN dedicada proporcionada por la ACCyL a una única dependencia del adjudicatario

El Servicio de Red Corporativa pondrá a disposición de uso del adjudicatario la herramienta de monitorización Nagios así como las posibilidades de notificación por correo electrónico y SMS. Cualquier desarrollo o adaptación de dicho sistema a los sistemas de monitorización del adjudicatario para ofrecer el servicio de 24x7 correrá a cargo del mismo. Se valorará en el sobre 3 de la oferta el tiempo de integración del sistema de monitorización de la ACCYL con el del adjudicatario (SLA 2.A).

3.3 Gestión de incidencias de cortafuegos

Se definen los siguientes tipos de incidencias según la criticidad de los equipos establecida anteriormente:

a. Tipo I (leve): Deterioro del funcionamiento del equipo que no afecta a servicios críticos o cuyo impacto es limitado.

b. Tipo II (grave): Deterioro del funcionamiento del equipo que afecta a servicios críticos, de gran impacto o interrupción total del servicio.

El adjudicatario deberá responder a las incidencias en el tiempo máximo ofertado para el SLA 1. Se valorará en el sobre 3 de la oferta la reducción en los tiempos de respuesta con los límites establecidos en el PPT.

El adjudicatario será el encargado del tratamiento de la incidencia, incluyendo su seguimiento, la interlocución con terceros y cualquier otra actividad relacionada hasta el cierre de la misma.

El Servicio de Red Corporativa facilitará al adjudicatario el acceso al soporte experto que la ACCyL tenga para estos equipos. El adjudicatario será el encargado de gestionar las incidencias y las posibles sustituciones de equipos con los soportes correspondientes.

Por su propio carácter, la gestión de incidencias graves y críticas se realizará en horario 24x7, siendo el adjudicatario responsable de disponer de los medios y personal adecuado para su realización, de cara al cumplimiento de los SLAs. Para cada una de las incidencias del 24x7 fuera del horario laboral deberá redactarse un informe con todas las actuaciones realizadas.

4. SERVICIO DE MONITORIZACIÓN DE LA SEGURIDAD DE LA RED

La monitorización de la seguridad de red se realizará, al menos, en los segmentos de red mostrados en la tabla siguiente. Todos ellos son Gigabit Ehternet en cobre. La información de tráfico en Mbits/s incluye el tráfico bidireccional medido en una semana concreta.

SEGMENTO	TRÁFICO MEDIO (Mbits/s)	TRÁFICO MÁXIMO (Mbits/s)
DMZ 1	66,84	222,97
DMZ 2	18,53	115,28
DMZ 3	0,20	26,56

DMZ 4	1,00	10,00
Segmento interno 1	77,68	228,49
Segmento interno 2	87,29	364,12

Se utilizarán elementos de monitorización como taps, agregadores de puertos/enlaces, bróker de paquetes o similares para la inspección de los segmentos de red anteriores. Se valorará la escalabilidad, disponibilidad y versatilidad de estos elementos.

Se utilizará un sistema de detección de intrusos de red basado en firmas (en adelante, NIDS) para la generación de alertas de intrusión. Se valorará lo siguiente:

a. La posibilidad de que el NIDS sea capaz de bloquear ataques actuando como un Sistema de Prevención de Intrusos (IPS). En este último caso se requerirá que los elementos de monitorización permitan una configuración “fail-open”.

b. La posibilidad de utilización de diferentes motores de NIDS y de conjuntos de firmas de diferentes fabricantes.

c. La posibilidad de integración con un sistema de detección de intrusos de host (HIDS).

El adjudicatario deberá ajustar las políticas en cada segmento para mejorar la detección y la eliminación de falsos positivos, así como actualizar las firmas de forma periódica según las recomendaciones del fabricante.

Se valorarán las prestaciones (almacenamiento, latencias, velocidad de almacenamiento, memoria, segmentos, tráfico, escalabilidad, disponibilidad, etc.) de la plataforma completa que se vaya a usar para prestar el servicio. Se considerará su certificación de seguridad por entidades independientes de reconocida solvencia según normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

Se valorará la recolección de la siguiente información adicional para la investigación de posibles incidentes de seguridad:

a. La captura de toda la información de sesiones (flujos) en los segmentos monitorizados. La información básica a recoger serán las direcciones IP y puertos origen y destino, un sello temporal (del momento en el que se inició la sesión) y la cantidad de tráfico intercambiada entre las partes.

b. La captura de todo el tráfico que circula por los segmentos monitorizados y su almacenamiento en disco duro de forma temporal para su análisis posterior.

c. La generación de registros de actividad de protocolos a nivel de aplicación como DNS, HTTP, FTP, SMTP, etc. así como un lenguaje de script específico que permita realizar otras tareas de análisis bajo demanda.

d. La integración con bases de datos públicas de inteligencia (“Collective Intelligence Framework”) o con registros públicos de hashes de malware.

El adjudicatario deberá correr con los todos los gastos necesarios para su implementación y mantenimiento, incluyendo licencias, suscripciones y cualquier otro gasto necesario para la correcta prestación de este servicio hasta la finalización del presente contrato. Esta plataforma completa (hardware, licencias, etc.) pasará a titularidad de la ACCyL una vez terminado el contrato.

Se valorará la inclusión de herramientas de análisis forense de red y cualquier otra aportación que permita la mejora del servicio.

5. SERVICIO DE ANÁLISIS Y ESCALADO DE INCIDENTES DE SEGURIDAD

El objetivo final de la prestación de este servicio es permitir una gestión efectiva y homogénea de los potenciales incidentes de seguridad, durante todo su ciclo de vida.

A partir de la información proporcionada por el servicio de monitorización de la seguridad de red el adjudicatario deberá registrar el incidente, analizarlo y escalarlo conforme al procedimiento de gestión de incidentes indicado por la ACCyL.

Dicho servicio consistirá en:

a. La detección de incidentes de seguridad generados a partir del servicio de monitorización de la seguridad de red o por la infraestructura del Servicio de Red Corporativa.

b. El análisis de cualquier incidente de seguridad que le sea reportado por los medios que establezca el Servicio de Red Corporativa, con independencia de haber sido detectado por el propio adjudicatario, de cara a determinar su posible alcance y/o escalarlo a los grupos de actuación oportunos.

c. Comunicación, tratamiento y registro de todos estos incidentes de seguridad. La ACCyL proporcionará las herramientas necesarias para la gestión de incidentes.

Las ofertas que presenten los licitadores, incluirán una descripción de la solución propuesta para llevar a cabo la prestación de este servicio.

Se valorará la experiencia del licitador en la prestación de servicios similares.

Se valorará cualquier otra aportación que permita la mejora de este servicio.

6. CALIDAD DEL SERVICIO

El acuerdo de nivel de servicio (SLA – Service Level Agreement) que regirá el presente contrato seguirá las siguientes directrices:

a. En el presente pliego se exponen los parámetros de control que forman parte del SLA con el umbral mínimo al que los licitadores se comprometen por el hecho de presentar oferta.

b. Las mejoras de estos parámetros que los licitadores presenten en los sobres 3 de sus ofertas, puntuarán positivamente en la valoración técnica de las mismas.

c. Sólo serán valorados los compromisos explícitos de mejora, y no los estadísticos de servicio utilizando la tabla del PCAP o similar.

d. Tras la adjudicación del contrato, en el periodo de implantación, se concretará el detalle operativo del SLA, de forma que se pueda llevar a cabo un control efectivo de los parámetros de forma periódica por parte de la ACCyL.

e. La medición de los diferentes SLAs se realizará con periodicidad trimestral.

SLA	Denominación	Parámetro	Especificación y método de medida	Compromiso mínimo	Para puntuación máxima
SLA 1	Tiempo de respuesta de incidencia de equipos críticos	1.A	Tiempo de respuesta a incidencias de tipo I: Se define como tiempo transcurrido desde que la ACCyL comunica al adjudicatario la apertura de la incidencia de tipo I o es detectada por el adjudicatario hasta que éste asigna una persona para el tratamiento de la incidencia.	4 horas laborables	2 horas laborables
		1.B	Tiempo de respuesta a incidencias de tipo II: Se define como tiempo transcurrido desde que la ACCyL comunica al adjudicatario la apertura de la incidencia de tipo II o es detectada por el adjudicatario hasta que éste asigna una persona para el tratamiento de la incidencia.	1 hora natural	15 minutos naturales
SLA 2	Plazos de integración de soluciones	2.A	Integración del sistema de monitorización.	4 semanas naturales	1 semana natural

7. CONFIDENCIALIDAD

7.1. Propiedad y confidencialidad de la información

Todos los informes, estudios y documentos elaborados durante la implantación, puesta en marcha y funcionamiento del servicio, serán propiedad de la ACCyL, reservándose esta Administración todas las facultades inherentes a este derecho, pudiendo reproducirlos, publicarlos o divulgarlos parcialmente o en su totalidad, en la medida que tenga conveniente, sin que pueda oponerse por ello la empresa adjudicataria alegando derechos de autor.

Los adjudicatarios no podrán hacer ningún uso o divulgación de los informes, estudios y documentos elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa por escrito de la ACCyL. Todos estos trabajos se entenderán como confidenciales, debiendo los adjudicatarios asegurara de la forma más razonable posible esta característica.

Toda la documentación que se genere como consecuencia de la instalación y configuración del equipamiento objeto de este pliego, deberán entregarse tanto impresa como en soporte informático, en los formatos especificados, o los formatos estándar que la ACCyL indique en su momento para cualquier otro tipo de fichero.

Las empresas adjudicatarias se comprometen a no desvelar ni utilizar para otros fines o proyectos, la información de cualquier tipo, sobre la ACCyL, obtenida como consecuencia de la ejecución del servicio contratado.

Los adjudicatarios tomarán las debidas medidas técnicas y organizativas para asegurar la confidencialidad de toda la información que obre en su poder relativa al presente pliego.

7.2. Protección de datos

En la medida en que la prestación y el cumplimiento del presente contrato impliquen el acceso del adjudicatario a datos de carácter personal incorporados a los Ficheros de los que sea titular la ACCyL, el tratamiento de dichos datos por parte del adjudicatario deberá realizarse en la forma y condiciones siguientes:

a. El adjudicatario, sea persona física o jurídica, y el personal a su servicio que tenga acceso o realice cualquier tratamiento con los datos de carácter personal, tendrá la consideración de "encargado del tratamiento" y el acceso a la información de carácter personal necesario para l realización de los trabajos no supondrá "comunicación de datos", a efectos de lo dispuesto en la Ley Orgánica 15/1999, de 12 de diciembre, de Protección de Datos de Carácter Personal, cuando se cumpla lo previsto en el artículo 12.2 y 12.3 de dicha Ley, y en todo caso, las previsiones del artículo 12.2 deberán constar por escrito.

b. Los datos del fichero serán propiedad exclusiva de la ACCyL, extendiéndose esta titularidad a cuantas elaboraciones realice el adjudicatario con ocasión del cumplimiento del contrato.

c. A los efectos de la prestación de servicios por parte del adjudicatario a la ACCyL, el primero tendrá la condición de encargado del tratamiento y se sujetará al deber de confidencialidad y seguridad de los datos personales a los que tenga acceso conforme a lo previsto en la normativa que resulte aplicable, obligándose específicamente a lo siguiente:

- Utilizar y aplicar los datos personales a los exclusivos fines del cumplimiento del objeto del contrato

- En todo caso se obliga a aplicar las medidas de seguridad del nivel que correspondan en función de los datos a tratar de conformidad con lo previsto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

- Mantener la más absoluta confidencialidad sobre los datos personales a los que tenga acceso para la prestación de servicios así como sobre los que resulten de su tratamiento cualquiera que sea el soporte en el que se hubieren cometido.

- No comunicar o ceder los datos del fichero a otra persona, ni siquiera para su conservación, debiendo destruir los datos personales a los que haya tenido acceso, así como los resultados derivados de su tratamiento, al igual que cualquier soporte o documentos en los que conste algún dato de carácter personal objeto del tratamiento, salvo que la ACCyL requiera que le sean devueltos.

- Guardar secreto profesional de todos los datos de carácter personal que conozca o a los que tenga acceso en ejecución del contrato. Igualmente se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno. Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario.

- Comunicar y hacer cumplir a sus empleados las obligaciones establecidas en los apartados anteriores y, en particular, las relativas al deber de secreto y medidas de seguridad.

- En el caso de que el adjudicatario destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones establecidas en el contrato, será considerado responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente, previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El adjudicatario se comprometerá a comunicar a la ACCyL de forma inmediata, cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la puesta en conocimiento de terceros de información confidencial obtenida durante la ejecución del contrato.

Asimismo, a la finalización del contrato el adjudicatario quedará obligado a la entrega a la ACCyL, o destrucción en caso de ser solicitada, de cualquier información obtenida o generada como consecuencia de la prestación del servicio objeto del presente contrato.

De acuerdo al RD 1720/2007, de 21 de diciembre, en su Disposición Adicional Única se estable que todos los productos de software destinados al tratamiento automatizado de datos personales, deberán incluir en su descripción técnica el nivel de seguridad, básico, medio, alto que permitan alcanzar de acuerdo a lo establecido en el Título VIII del Reglamento de desarrollo de la LOPD (RD 1720/2007, de 21 de diciembre).