Congreso de los Diputados

PROCEDIMIENTO ABIERTO PARA LA ADJUDICACIÓN DEL CONTRATO PARA LA PRESTACIÓN DE SERVICIOS INTEGRALES DE CIBERSEGURIDAD GESTIONADA EN RÉGIMEN DE 24x7

PLIEGO DE PRESCRIPCIONES TÉCNICAS

ÍNDICE

1. OBJETO DEL CONTRATO

El objeto de este procedimiento es la contratación de servicios integrales de ciberseguridad gestionada en régimen 24x7, comprendiendo el hardware y/o software necesarios para la prestación del servicio, la operación, configuración, administración y soporte de todos los dispositivos y software asociados, la gestión ante incidentes de seguridad, y la tecnología asociada, así como la asistencia para la implantación de un sistema de gestión de la seguridad de la información para el cumplimiento normativo relativo al Esquema Nacional de Seguridad (ENS), al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales y a cualquier otra norma aplicable.

La finalidad del contrato es garantizar la seguridad de todos los activos de información del Congreso de los Diputados y de los sistemas que les dan soporte con arreglo a los niveles de seguridad derivados a partir de la categorización de seguridad del Sistema Informático de la Cámara y conforme a los acuerdos de nivel de servicio que se definan para cada caso y establecer un marco para la mejora continua de todos los procesos relacionados con la gestión de la seguridad de la información. El Congreso de los Diputados es plenamente consciente de la relevancia de la protección de seguridad de la información para el correcto desempeño de sus funciones y como fundamento esencial para la prestación de servicios TIC fiables y de calidad.

2. CONSIDERACIONES PRELIMINARES

Como regla general, el licitador proporcionará en su oferta una explicación pormenorizada del cumplimiento de los requisitos mínimos y detalles relativos a los parámetros a valorar, no siendo suficiente, en ningún caso, la mera repetición mimética de las especificaciones establecidas en este pliego.

El Congreso de los Diputados proporcionará a los licitadores, previa firma de un acuerdo de confidencialidad, un documento detallado con todos los sistemas preexistentes, su arquitectura y los niveles de criticidad a los efectos de su integración con la tecnología ofertada.

La solución ofertada será llave en mano, por lo que, con carácter previo al inicio de la prestación del servicio, el contratista deberá proveer, instalar y configurar todos los elementos necesarios para su correcto funcionamiento, incluyendo el hardware y software necesario como prerrequisito para el software ofertado—(sistemas operativos, middleware, almacenamiento, memoria, etc.) indistintamente del lugar en el que vaya a ser desplegado, así como los cables de alimentación eléctrica y conexión de red y todos los elementos necesarios para la instalación física de todo el equipamiento,

proporcionando el Congreso de los Diputados el espacio necesario dentro de bastidores de 19 pulgadas para los elementos que deban albergarse en sus instalaciones.

Se establece un plazo máximo de tres meses para el aprovisionamiento de la infraestructura, instalación y configuración, previo al inicio de la prestación del servicio.

3. CUESTIONES GENERALES

Los licitadores especificarán de manera detallada la arquitectura de seguridad propuesta a partir de la configuración existente en el Congreso de los Diputados junto con todos aquellos elementos de tecnología incluidos en su oferta, y su engarce dentro del *NIST Cybersecurity Framework Core*. También deberán presentar un plan de implantación de la tecnología y servicios ofertados con detalles de las actividades, dependencias y recursos humanos y materiales.

Como regla general, se permitirá que la funcionalidad establecida en los requisitos mínimos para cada uno de los sistemas pueda ser implementada mediante múltiples elementos, e incluso que puedan existir elementos compartidos entre múltiples sistemas, siempre y cuando la configuración resultante, para cada caso, sea equivalente a la de cada sistema implementado de forma unitaria, sobre todo en lo relativo a los requisitos mínimos de rendimiento.

Es obligatorio que toda la tecnología ofertada, incluyendo hardware, software y suscripciones de cualquier tipo, disponga de mantenimiento y soporte en régimen 24x7 y actualizaciones durante toda la vigencia del contrato, comprometiéndose el adjudicatario a conservar todos los elementos dentro de los parámetros necesarios para asegurar el soporte por parte de los respectivos fabricantes y con el máximo nivel de actualización posible conforme con las restricciones que impongan los requisitos de integración con los restantes elementos de la arquitectura de seguridad. Si se produjesen situaciones en las que los fabricantes anunciaran el paso a situación de fin de soporte (*end of support*) o fin de vida (*end of life*) de cualquier elemento durante la duración del contrato, el adjudicatario procederá a su renovación por otros con características iguales o superiores a los ofertados antes de la llegada de las fechas de tales situaciones.

Dada la naturaleza evolutiva de las amenazas a la seguridad de la información y del propio Sistema Informático del Congreso de los Diputados, el adjudicatario se compromete a colaborar, durante la duración del contrato, en todas las integraciones y reconfiguraciones necesarias del sistema ofertado para incorporar todos aquellos elementos y tecnologías en relación con la seguridad de la información que el Congreso de los Diputados estime necesario agregar a sus sistemas a lo largo del tiempo. El personal del

Centro de Tecnologías de la Información y de las Comunicaciones (en adelante CTIC) que designe el Congreso de los Diputados dispondrá de acceso para visualizar la configuración de todos los sistemas y dispositivos desplegados en las instalaciones de la Cámara en el marco del contrato.

4. SISTEMA DE PROTECCIÓN PERIMETRAL DE RED

Se deberá ofertar un sistema de cortafuegos perimetrales de red de nueva generación (*next generation firewall*) compuesto por dos capas separadas (externa e interna) con diferente fabricante y tecnología de protección cada una de ellas. El cortafuegos exterior funcionará como frontera entre las redes externas al Congreso y las redes DMZ y el cortafuegos interno servirá como frontera entre las redes DMZ e internas.

Los requisitos mínimos comunes de cada una de las capas será la siguiente:

- Configuración redundante con dos nodos independientes con respaldo mutuo de tipo activo/pasivo y sincronización de estado y configuración entre ellos.
- Caja con formato para montaje en bastidor de 19 pulgadas con los raíles y guías pasacables correspondientes.
- Fuentes de alimentación eléctrica redundante.
- Soporte para IPv4 e IPv6 así como configuración dual stack.
- Soporte para 802.1Q y jumbo frames.
- Soporte para relé de DHCP.
- Perfilado granular de tráfico de red (*traffic shaping*) y políticas de calidad de servicio.
- Soporte para translación de direcciones y puertos (funcionalidad NAT/NAPT) con soporte específico para protocolos que incluyan (o manejen) direcciones IP dentro de sus operaciones.
- Inspección del tráfico de conexiones cifradas SSL/TLS.
- Funcionalidad de establecimiento de políticas de filtrado, con un amplio conjunto de criterios, de manera granular con base en aplicaciones (tanto categorías como de forma individualizada), usuarios, grupos y puertos, con identificación de las aplicaciones de forma independiente al puerto, la encapsulación utilizada y, en su caso, de la distinción de múltiples operaciones en un mismo tipo de aplicación. Para el caso de usuarios y grupos, deberá soportar tanto Active Directory como disponer de una base de datos de usuarios local.
- Funcionalidad de detección y prevención de intrusiones y filtrado de malware en general, con actualizaciones periódicas.
- Soporte para mitigación de ataques de denegación de servicio (*denial of service*).
- Soporte para monitorización mediante protocolo SNMP.
- Generación de registros detallados de actividad, con posibilidad de procesamiento mediante sistemas externos.

La capa exterior dispondrá de los siguientes requisitos mínimos adicionales:

- Rendimiento de 5 Gbps en filtrado de tráfico con inspección de estado (*stateful inspection*) y 2 Gbps en inspección profunda contra amenazas (prevención de intrusiones, malware, etc.), incluyendo el tráfico cifrado TLS/SSL.
- Gestión de la conectividad a la red Internet mediante el uso de múltiples enlaces con diferentes operadores, con posibilidad de perfilado del tráfico en función de ancho de banda y latencia y tratamiento de enlaces caídos.
- Soporte para políticas de filtrado basadas en geolocalización de direcciones IP.
- Funcionalidad de redes privadas virtuales (*virtual private networks* -- VPN) con configuraciones *site to site* y usuario móvil (con sistemas operativos Windows, Android, iOS y MacOS) y soporte de protocolos IPSec y SSL.
- 8 interfaces de red Ethernet 1000 BASE-T y 2 interfaces 10GBASE-T sin contar aquellos dedicados a la alta disponibilidad entre los dos nodos.

La capa interior dispondrá de los siguientes requisitos mínimos adicionales:

- Rendimiento de 20 Gbps en filtrado de tráfico con inspección de estado (*stateful inspection*) y 9 Gbps en inspección profunda contra amenazas (prevención de intrusiones, malware, etc.), incluyendo el tráfico cifrado TLS/SSL.
- 10 interfaces de red 10GBASE-T y 2 interfaces 40G QSFP, con su conector de fibra correspondiente, sin contar aquellos dedicados a la alta disponibilidad entre los dos nodos. Para los interfaces de fibra, se deberán ofertar los módulos de interconexión para conmutadores Extreme Networks X690.
- Filtrado de URL con soporte para categorización con base en múltiples criterios.

Se valorará:

- Rendimiento efectivo de filtrado de tráfico e inspección profunda contra amenazas con todas las políticas de protección activadas. A tal efecto, el licitador aportará tests de evaluación de entidades independientes de los dispositivos ofertados o de otros de tecnología similar.
- Alcance y completitud de los mecanismos de inspección.
- *Cypher suites* soportadas en la inspección SSL.

- Soporte para funcionalidad de tipo CASB (*cloud access security broker*).
- Mitigación ante amenazas persistentes avanzadas.
- Mitigación ante ataques con técnicas de evasión avanzadas.
- Soporte para protección ante ataques basados en DNS.
- Soporte para proxy HTTP explícito.
- Certificaciones de seguridad (Common Criteria, catálogo del CCN, etc.).
- Soporte para balance de carga entre servidores (*server load balancing*).

5. SISTEMA DE CONTROLADORES DE ENTREGA DE APLICACIONES Y PROTECCIÓN DE APLICACIONES WEB

Se deberá ofertar un sistema con funcionalidades de controlador de entrega de aplicaciones (*application delivery controller*) y de firewall de aplicaciones web (*web application firewall*).

Los requisitos mínimos del sistema ofertado serán los siguientes:

- Soporte para múltiples servicios y un mínimo de 3 zonas de seguridad.
- Arquitectura redundante con dos elementos independientes configurados para operar en alta disponibilidad en modo activo/pasivo (para cada una de las zonas de seguridad).
- Mecanismos para garantizar la independencia de cada una de las zonas de seguridad.
- Consola de gestión y administración con interfaz gráfico y panel de control que contemple los aspectos esenciales del sistema.
- Funcionalidad para la protección de los mecanismos de sesión.
- Capacidad para repartir la carga de proceso de aplicaciones entre distintos servidores backend, incluyendo mecanismos de distribución con múltiples criterios, así como la detección y gestión de servidores backend caídos.
- Soporte para funcionamiento en modo de proxy inverso y capacidad para terminar túneles SSL/TLS, con soporte para TLS 1.3.
- Soporte para redirección, encaminamiento y reescritura de URL y de contenido HTML.
- Funcionalidades de single sign-on y control de autorización con soporte para protocolo LDAP y RADIUS.
- Funcionalidad para protección de aplicaciones y servicios web (multidominio) mediante reglas con control granular, comprendiendo al menos el *OWASP Top Ten*, así como soporte de validación para contenidos XML.
- Funcionalidad para compresión y caché de contenidos.

- Funcionalidad de perfilado de la protección de las aplicaciones mediante módulo de aprendizaje automatizado, así como disponibilidad de asistentes y plantillas de configuración.
- Soporte para funcionalidad para mitigación de ataques de denegación del servicio (*denial of service*).
- Funcionalidad de registro detallado de la actividad del sistema, incluyendo generación de informes parametrizables e integración con sistemas de recogida y gestión de eventos.
- Soporte para normalización de protocolos.
- Soporte para IPv4 e IPv6.
- Certificación de funcionamiento con entornos Oracle y Microsoft.
- Rendimiento mínimo en protocolo HTTP de 5 Gbps, con soporte para 200K conexiones por segundo y 500K peticiones HTTP por segundo (para cada uno de los elementos).
- Rendimiento mínimo en SSL de 4 Gbps, 4000 transacciones SSL/TLS por segundo con certificados de 2048 bits (para cada uno de los elementos).

Se valorará:

- Amplitud y granularidad de las funcionalidades de seguridad y mecanismos para mitigación de falsos positivos.
- Rendimiento HTTP y SSL/TLS por encima de los mínimos requeridos.
- Soporte para particionamiento en múltiples sistemas virtuales.
- Mecanismos para la detección y protección ante ataques automatizados mediante programas maliciosos (bots).
- *Cypher suites* soportadas.
- Certificaciones de seguridad (Common Criteria, catálogo del CCN, etc.).
- Capacidad de funcionamiento en alta disponibilidad en modo activo/activo.

6. SISTEMA DE MONITORIZACIÓN Y GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD

Se deberá implantar un sistema de gestión de eventos de información de seguridad (*Security Information and Event Management*), que referiremos en adelante como SIEM, que permita la monitorización y la correlación de eventos de seguridad, integrando las fuentes de datos que generen todos los dispositivos y sistemas de red ofertados así como los sistemas preexistentes en el Congreso de los Diputados, con el objeto de detectar anomalías de seguridad y generar alertas que permitan la adecuada clasificación del nivel de amenaza de cualquiera de los incidentes de seguridad detectados. El sistema deberá soportar la creación de *tickets* en el sistema de *helpdesk*

OTRS implementado en el Congreso de los Diputados para aquellas actividades que deban ser atendidas por el personal de este.

El licitador detallará la arquitectura de componentes del sistema SIEM propuesto, incluyendo todos los elementos de recolección, agregación y procesamiento de eventos, así como la ubicación de los mismos (en las instalaciones del Congreso, en las SOC del propio licitador u otras al efecto).

El licitador indicará las métricas de licenciamiento que sean aplicables al sistema SIEM ofertado, justificando adecuadamente su dimensionamiento para las fuentes de datos de los sistemas que formen parte de su oferta, así como de las fuentes de los sistemas preexistentes en el Congreso de los Diputados, durante toda la duración del contrato.

Se valorarán las automatizaciones y correlaciones a implantar en el SIEM, por lo que, para su correcta valoración, se deberán detallar los casos de uso a implantar en la propuesta. También se valorará la inclusión de elementos que faciliten la integración con las herramientas del ecosistema del Centro Criptológico Nacional y el envío de tráfico de red de forma selectiva a las mismas.

El SIEM incorporará la posibilidad de consulta por parte del personal del CTIC del Congreso de los Diputados.

El adjudicatario proporcionará, como mínimo cada tres meses, los registros de actividad completos de los sistemas ofertados en formato interoperable.

Se valorará:

- Características y amplitud del licenciamiento ofertado para el sistema SIEM y su adecuación al entorno operativo del Congreso de los Diputados.
- Soporte para automatizaciones basadas en aprendizaje automatizado (*machine learning*).
- Soporte para automatizaciones basadas en análisis de comportamiento de entidades y usuarios (*user and entity behavior analytics*).
- Integraciones con las herramientas del ecosistema del CCN, incluyendo el envío de tráfico selectivo a las mismas.
- Casos de uso propuestos para la correlación de eventos en los casos de configuración por parte de expertos.
- Casos de uso propuestos para la automatización de respuestas ante incidentes.
- Certificaciones de seguridad (Common Criteria, catálogo del CCN, etc.).

7. SERVICIO DE GESTIÓN Y CONFIGURACIÓN DE SEGURIDAD Y RESPUESTA ANTE INCIDENTES

Este servicio comprenderá la instalación y configuración de todos los elementos ofertados, así como de las integraciones de seguridad propuestas entre los sistemas ofertados junto con todos aquellos elementos preexistentes en el Congreso. También comprenderá la gestión proactiva de todas las actualizaciones de hardware y software aplicables a los mismos, de acuerdo con las especificaciones de los respectivos fabricantes, así como todas las reconfiguraciones necesarias para adecuarse a la evolución del Sistema Informático del Congreso de los Diputados a lo largo del tiempo.

Asimismo, el servicio comprenderá la operación y gestión de todos los sistemas ofertados, de acuerdo con los requisitos especificados por el Congreso de los Diputados y las medidas de seguridad aplicables según el Sistema de Gestión de la Seguridad de la Información, con excepción de los siguientes:

- Sistema de gestión de identidades.
- Sistema de soporte remoto a usuarios y acceso privilegiado.

Para los dos sistemas anteriormente mencionados, su gestión será asumida por el Congreso de los Diputados, para la cual el adjudicatario impartirá un programa de formación para cada uno de los sistemas ofertados, asumiendo también el soporte de primer nivel para los productos que integren tales soluciones, así como el escalado a otros niveles de los incidentes relacionados con los mismos.

El licitador dispondrá de un centro de operaciones de seguridad (*security operations center*, en adelante SOC) con todas las capacidades necesarias para la prestación del servicio. El SOC deberá disponer de personal especializado en las tecnologías ofertadas y en la gestión de la seguridad de la información y de incidentes de seguridad.

La prestación del servicio se realizará en régimen de 24x7x365 y, de forma principal, desde centros ubicados en la Unión Europea y en lengua castellana, cumpliendo todas las normativas aplicables que se encuentren en vigor.

El servicio contemplará la clasificación y priorización de las alertas generadas por el SIEM y otros sistemas conexos, el tratamiento de los incidentes de seguridad que no hayan sido contenidos mediante las configuraciones prestablecidas en el sistema, y la implantación de un modelo de mejora continua de acuerdo con la evolución de las amenazas y vulnerabilidades que pudieran ir surgiendo durante la duración del contrato.

El SOC dispondrá de un portal de acceso para la gestión de incidentes y de peticiones de servicio, así como de los diferentes informes recapitulativos. También dispondrá de un mecanismo de atención telefónica para aquellos incidentes y peticiones que se consideren de mayor urgencia y/o gravedad. En todo caso, el servicio contemplará una persona ubicada, en régimen de 8x5, en las instalaciones del Congreso de los Diputados cuyo propósito será la de la coordinación del servicio entre el SOC y el CTIC, y agilizar las peticiones de servicio y de respuesta ante incidentes durante el horario laborable.

Con periodicidad mensual, se elaborarán informes recapitulativos de los incidentes de seguridad, clasificados por tipologías y nivel de gravedad.

Dentro de este servicio se contemplará la gestión de vulnerabilidades, tanto de la infraestructura (comprendiendo tanto los fallos del software como de la configuración) como de todas aquellas aplicaciones accesibles desde la red Internet. La gestión comprenderá el análisis periódico bimestral mediante herramientas automatizadas y, en su caso, por personal experto, del estado de seguridad tanto de la infraestructura como de las aplicaciones mencionadas, y la elaboración de los informes correspondientes relativos a las vulnerabilidades encontradas y las propuestas para la corrección de estas.

El SOC asumirá también la coordinación para la activación de mecanismos de seguridad no incluidos en este contrato, que sean prestados por terceras partes para el Congreso de los Diputados, como puede ser el caso, por ejemplo, de los servicios de protección de ataques de denegación de servicio proporcionados por los proveedores de acceso a Internet.

También se contemplará la disponibilidad de un servicio de vigilancia digital que rastree en redes sociales, internet profunda, foros, etc. posibles amenazas dirigidas contra el Congreso de los Diputados tales como la coordinación de ataques de denegación de servicio, la exposición de credenciales de usuario, la revelación de vulnerabilidades en sistemas y aplicaciones, así como otras de naturaleza similar, debiendo contemplar un mínimo de 200 identidades digitales.

Finalmente, el servicio contemplará la asistencia para recogida *in situ* de evidencias forenses relativas a incidentes de seguridad y su custodia y preservación a efectos legales y/o procesales por un mínimo de dos jornadas anuales.

Los niveles de criticidad del servicio serán los siguientes:

- Nivel 1: Fallo general en el sistema con afectación a más de un 40% de los usuarios, así como subsistemas que no puedan asumir una interrupción del servicio superior a dos horas.
- Nivel 2: Fallo en subsistemas críticos con afectación a más de un 25% de los usuarios, así como subsistemas que no puedan asumir una interrupción del servicio superior a las cuatro horas.

- Nivel 3: Fallo en subsistemas no críticos o en todos aquellos que no puedan asumir una interrupción del servicio superior a 8 horas.

Los servicios de gestión y configuración de seguridad y respuesta ante incidentes deberán disponer, como mínimo, de los siguientes acuerdos de nivel de servicio:

- Severidad 1: Que afecten a servicios con nivel 1 de criticidad.
    - Tiempo de respuesta máximo de ½ hora.
    - Tiempo de resolución máximo de 2 horas.
- Severidad 2: Que afecten a servicios con nivel de criticidad 2 o bien a servicios con impacto en el nivel de redundancia de servicios con nivel de criticidad 1.
    - Tiempo de respuesta máximo de ½ hora.
    - Tiempo de resolución máximo de 4 horas.
- Severidad 3: Que afecten a servicios con nivel de criticidad 3 o bien a servicios con impacto en el nivel de redundancia de servicios con nivel de criticidad 2.
    - Tiempo de respuesta máximo de ½ hora.
    - Tiempo de resolución máximo de 8 horas.

Asimismo, la gestión del servicio deberá garantizar una disponibilidad anual mínima del 99,75 % del conjunto de los sistemas de protección perimetral de red, controladores de entrega de aplicaciones y protección de aplicaciones web, y protección ante malware para servidores y *endpoints*.

Se valorará:

- Integraciones de seguridad entre los distintos elementos que compongan la solución ofertada, así como los preexistentes en el Congreso de los Diputados, entendiéndose como tales aquellas que mejoren la inteligencia sobre amenazas a partir de unos elementos a partir de la información sintetizada por otros y/o que generen respuestas automáticas ante incidentes en unos elementos a partir de la información de detección de otros.
- Características y capacidades del centro de operaciones y del personal asignado para atención al Congreso de los Diputados, así como propuesta para la coordinación entre el SOC y el personal del CTIC del Congreso de los Diputados.
- Acuerdos de colaboración y coordinación con otros centros de respuesta ante incidentes y entidades de naturaleza similar.

- Características del servicio de gestión de vulnerabilidades.
- Fuentes de inteligencia y número de identidades digitales cubiertas (sobre el mínimo requerido) del servicio de vigilancia digital.
- Certificaciones de seguridad, de gestión de TI y de calidad de las que disponga el SOC de forma adicional a las especificadas como requisito mínimo.
- Soporte para analítica y orquestación de políticas de seguridad.
- Capacidades para la redundancia del SOC mediante la prestación del servicio desde distintas localizaciones físicas, así como prestación del soporte *around the clock*.
- Disponibilidad de un cuadro de mando integral del funcionamiento del servicio.

8. SISTEMA DE PROTECCIÓN ANTE MALWARE PARA SERVIDORES Y ENDPOINTS

Se proporcionará un sistema para la protección ante malware y ataques de naturaleza similar que soporte *endpoints* basados en ordenadores personales con Microsoft Windows 7 y 10 así como servidores basados en Microsoft Windows Server y Linux en un entorno de virtualización con VMWare VSphere. El esquema de protección comprenderá el bloqueo y eliminación del malware con origen en soportes de almacenamiento (fijos y removibles), memoria y medios de red, con detección basada tanto en firmas como en comportamiento y otros indicadores, tratando de forma específica la problemática del *ransomware*. Permitirá la configuración de políticas personalizables por grupos de dispositivos y combinará el uso de modelos negativos (firmas y otros mecanismos) y positivos (listas blancas) para la detección, permitiendo configurar estas últimas con los desarrollos propios del Congreso de los Diputados. Asimismo, dispondrá de capacidades de detección y respuesta (*endpoint detection and response*) para la neutralización de *malware* no previamente conocido.

Se proporcionarán licencias para un mínimo de 1600 puestos de trabajo con Microsoft Windows y 50 servidores en entorno virtual con VMware. Se considerará incluido durante la duración del contrato un incremento anual del 2 por ciento sobre las licencias indicadas, sin que suponga modificación del contrato ni incremento del precio ofertado para el servicio.

El sistema dispondrá de una consola centralizada para la gestión de los elementos que lo integren, comprendiendo la instalación, configuración, actualización y supresión de todos los componentes software, la recolección de eventos y alertas de actividad, la elaboración de informes personalizados a partir de tales eventos y alertas.

También deberá disponer de un sistema de *sandboxing* para la evaluación de contenidos descargados por la red para los que los restantes sistemas de detección no puedan proporcionar un veredicto sobre su seguridad.

El licitador proporcionará un detalle exacto de los intercambios de información de este sistema con sistemas externos al Congreso y acreditará las medidas para la protección de la información extraída de los sistemas del Congreso de los Diputados, con especial énfasis en los datos de carácter personal y para la eliminación de cualquier dato no relevante a los efectos de la recopilación de la inteligencia de amenazas.

Se valorará:

- Amplitud del espectro de protección ante *malware*.
- Mecanismos de protección de red y control de dispositivos.
- Integraciones de seguridad con otros elementos de la arquitectura de seguridad propuesta.
- Capacidades de integración con las plataformas de hipervisor disponibles en el Congreso de los Diputados.
- Rendimiento del entorno de s*andboxing*.
- Instalación *on premises* del entorno de *sandboxing*.
- Soporte específico para servidores con Microsoft Exchange Server.
- Capacidades para la personalización del entorno de *sandboxing*.
- Certificaciones de seguridad (Common Criteria, catálogo del CCN, etc.).

9. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se proveerán los servicios necesarios para la implantación de un sistema de gestión de la seguridad de la información (en adelante SGSI), que tendrá en cuenta todos los activos de información y actividades existentes en la organización y del análisis del riesgo de estos.

Se proveerán un mínimo de 300 horas anuales de consultoría que comprenderán las siguientes materias:

- Cumplimiento normativo del Esquema Nacional de Seguridad, del Reglamento General de Protección de Datos, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales y de cualquier otra normativa aplicable.
- Soporte a la implementación y desarrollo de medidas de seguridad y de continuidad de negocio.
- Realización de análisis de riesgos y de evaluaciones de impacto.
- La oferta deberá incluir una descripción detallada de la metodología para el análisis y gestión de riesgos propuesta para este sistema.
- El sistema de gestión deberá estar sustentado por una herramienta software GRC (Gobernanza, Riesgo y Cumplimiento) que soportará la modelización y evaluación del riesgo, el seguimiento del cumplimiento normativo y la gobernanza, y que permita seguir de forma progresiva la evolución del estado de la seguridad de acuerdo con la implantación sucesiva de las medidas de seguridad y de las actividades de mejora continua. El licitador podrá ofertar soluciones

basadas *on premises* o en la nube. El personal del CTIC del Congreso de los Diputados designado dispondrá de pleno acceso a los contenidos de la herramienta.

El licitador especificará los perfiles del personal propuesto para la prestación de los servicios, así como las certificaciones, formación y experiencia de la que dispongan en materia de gestión de la seguridad de la información.

A la finalización del contrato, se deberá entregar al Congreso de los Diputados toda la información relativa a los análisis de riesgos en formato electrónico compatible con la herramienta PILAR.

Se valorará:

- Horas de consultoría por encima de los mínimos requeridos.
- Certificaciones y experiencia en gestión de la seguridad de la información del personal propuesto para la prestación de estos servicios.
- Metodología de análisis y gestión de riesgos propuesta.
- Nivel de funcionalidad de la herramienta de GRC propuesta y soporte para presentación de cuadros de mando integrales con todos los indicadores significativos.

10. FORMACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Se proveerán servicios de formación y de evaluación para mejorar la concienciación en ciberseguridad por parte del personal de la Cámara.

Se propondrá un programa formativo para la concienciación en seguridad de la información y protección de datos personales y la capacitación en competencias básicas de ciberseguridad. El programa comprenderá clases presenciales y mediante *e-learning*, dispondrá de materias teóricas, supuestos prácticos y otros aspectos relacionados, con especial énfasis en cuestiones de ingeniería social. Asimismo, se complementará el programa con la realización de pruebas periódicas simuladas que permitan determinar de forma continua el grado de asimilación de los conocimientos del programa. El Congreso de los Diputados podrá solicitar la impartición de nuevas sesiones si las incorporaciones de nuevos diputados y nuevo personal de la Cámara así lo requirieran, en un número no superior de una por año.

Se valorará:

- Programa de formación propuesto.
- Calidad de los aspectos formativos de la concienciación y de los mecanismos de incentivos para el aprendizaje y otros aspectos conexos, así como los mecanismos para la evaluación del grado de

asimilación por parte del personal y de las acciones correctivas que, en su caso, se implementarían.
- Propuesta para la formación continua del personal a largo plazo.

11. SISTEMA DE GESTIÓN DE IDENTIDADES

Se deberá proveer una solución de gestión de identidades que permita el provisionamiento y gestión de los usuarios del sistema, así como los permisos que correspondan a cada uno de ellos de acuerdo con una serie de roles acorde con los privilegios asociados a cada una de las unidades organizativas que componen el Congreso de los Diputados. Formará parte del servicio su instalación y configuración básica de los flujos de aprovisionamiento de usuarios y asignación de privilegios en función de la estructura de la organización.

La solución que se oferte deberá integrarse con el software actual del Sistema Informático del Congreso de los Diputados y con el que se incluya en los diferentes apartados de este pliego, para un colectivo de unos 2000 usuarios. Dicha solución deberá proporcionar las funcionalidades siguientes:

- Gestión de control de accesos: La solución proporcionará facilidades de gestión de perfiles o roles que establezcan los privilegios de un usuario, aplicación o servicio para la autorización de acceso a los recursos del sistema (aplicaciones, servicios en la web, ficheros) y la gestión de la asignación de estos perfiles a identidades (usuarios, aplicaciones, servicios, o grupos de los anteriores).
- Gestión de usuarios: El sistema debe permitir la gestión centralizada de usuarios y del ciclo de vida de su identidad: creación, modificación, asignación de perfiles, roles y privilegios de acceso. Asimismo, se proporcionarán los mecanismos para la sincronización o provisión de los cambios necesarios de cuentas, clave, privilegios u otra información, en los sistemas actuales (Base de datos de personal, Active Directory, Microsoft Exchange, Oracle Internet Directory).
- Auditoría: El sistema ofertado proporcionará acceso a información sobre cambios de las identidades y sobre los accesos a los recursos y generar informes.
- La gestión de este sistema corresponderá al personal del Congreso de los Diputados, por lo que se ofertará formación para administradores del sistema para un mínimo de dos personas.

Se valorará:

- Modelo de licenciamiento.
- Capacidad del sistema para definir reglas y flujos de trabajo para implantación de esta gestión.
- Soporte para integración mediante servicios REST.

- Soporte para federación de identidades.
- Soporte para la creación de cuadros de mando personalizados.

12. SISTEMA DE SOPORTE REMOTO A USUARIOS Y CONTROL DE CUENTAS PRIVILEGIADAS

Se deberá proveer una herramienta de soporte remoto a usuarios, con soporte para sistemas operativos Windows, Linux, MacOS, iOS y Android, con funcionalidad para visualizar la pantalla del dispositivo remoto y permitir la toma de control de la interacción con el mismo en aquellos sistemas operativos que así lo soporten. La herramienta deberá permitir proporcionar tal soporte tanto de forma atendida como desatendida y proporcionará al usuario pleno control sobre las sesiones de soporte remoto, pudiendo interrumpirlas en cualquier momento. La herramienta dispondrá de un mecanismo para establecer permisos y controles de acceso para los administradores, una auditoría completa sobre la actividad del sistema y permitirá la grabación, en su caso, de las sesiones de soporte remoto. Deberá disponer de funcionalidades de colaboración entre los técnicos de soporte, permitiendo la interacción sobre una misma sesión de soporte, el traspaso de sesiones entre técnicos de soporte y la mensajería mediante un chat. Las sesiones de soporte remoto se establecerán mediante protocolos de red seguros y con soporte para el cifrado de la comunicación, y no necesitarán de ningún tipo de VPN para proporcionar la conectividad.

También se deberá ofertar una solución para la gestión de cuentas privilegiadas, permitiendo su control y el establecimiento de sesiones de administración sin necesidad de revelar sus contraseñas y permitiendo una auditoría completa de la actividad de los administradores designados. Asimismo, permitirá establecer políticas basadas en el contexto para autorizar el acceso. Debe soportar sistemas Unix/Linux, Windows e interfaces de administración basados en HTTP/HTTPS.

Se deberá proporcionar licenciamiento para un mínimo de 7 técnicos de soporte concurrentes/15 técnicos de soporte nominales.

La gestión de este sistema corresponderá al personal del Congreso de los Diputados, por lo que se ofertará formación para administradores del sistema para un mínimo de dos personas.

Se valorará:

- Arquitectura con appliance (virtual o físico) en las instalaciones del Congreso de los Diputados.
- Nivel de redundancia de la solución ofertada.
- Licenciamiento para técnicos de soporte sobre el mínimo requerido.
- Integración entre la herramienta de soporte remoto y la de gestión de cuentas privilegiadas.

- Grabación de las sesiones de soporte remoto y acceso privilegiado de manera centralizada.
- Integraciones con sistemas ITSM y CRM y soporte para API para integración con otros sistemas.
- Interoperabilidad con Intel vPro.