ANEXO III

PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN, PUESTA EN MARCHA Y SOPORTE DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA EL PARLAMENTO DE NAVARRA

Antecedentes y necesidades:

El Parlamento de Navarra cuenta en la actualidad con un sistema de seguridad perimetral basada en un firewall de código abierto basado en máquinas virtuales. Este firewall realiza las funciones de:

- Enrutador entre las diferentes redes.
- Protección ante accesos indeseados entre equipos y redes.
- Proporcionar los accesos a personal desde redes externas al Parlamento de Navarra para diferentes perfiles y con diferente granularidad.
- Proporcionar los accesos a internet por diferentes medios según el servicio a utilizar.
- Controlar los accesos a los servicios Web públicos del Parlamento de Navarra.

La solución actual ha llegado a su fin de soporte, haciéndose necesaria una renovación tecnológica que ayude a protegerse ante las nuevas amenazas que van surgiendo cada día. A su vez, los nuevos retos en movilidad, acceso telemático, necesidades crecientes en teletrabajo y la protección de los equipos en entornos externos al Parlamento, hacen necesaria una renovación tecnológica que ayude a simplificar la gestión de la seguridad, pero sobre todo que ayude a mejorar la seguridad integral de la infraestructura TIC del Parlamento de Navarra, en el más amplio sentido.

Por ello, se estima necesario la adquisición, instalación y puesta en marcha de un clúster de firewalls de nueva generación o NGFW (Next Generation FireWall) con capacidades de análisis y filtrado de capa 7 (según el estándar OSI) que ayude a mejorar la seguridad de las infraestructuras y la información de Parlamento de Navarra.

Propuesta

Por las necesidades de renovación tecnológica descritas anteriormente, el Parlamento de Navarra solicita un clúster de Firewalls, 2 equipos físicos en configuración de alta disponibilidad HA, perimetrales de alto rendimiento que cumplan con las características definidas en los diferentes apartados de este pliego. Estas serán las características mínimas que deberá cumplir la solución adoptada.

La solución planteada se tratará como un proyecto “llave en mano”, es decir, una solución completa tanto de software como de hardware que incluyen el diseño, la operatividad, el desarrollo y la implementación que mejor se adapte a las necesidades, garantizando en todo momento la puesta en funcionamiento de la misma. Por ello, la solución planteada no solo deberá

contemplar los equipos físicos necesarios, sino que se requieren todas las licencias y suscripciones necesarias, cableados y adaptadores, etc., y en general cualquier elemento o licencia no incluida en el pliego que sea necesaria para la puesta en marcha con los requerimientos solicitados.

Todos los equipos, así como las funcionalidades (licencias y suscripciones), deberán tener una vigencia de al menos 5 años. Asimismo, se deberá garantizar que el tiempo de vida de los equipos ofertados no sea inferior a 7 años.

Adicionalmente se requerirán los servicios descritos posteriormente para todo el ámbito temporal descrito en este pliego.

1. CARACTERÍSTICAS DE LOS EQUIPOS A SUMISTRAR

CARACTERÍSTICAS HARDWARE Y CAPACIDADES MÍNIMAS

Cada firewall ofertado, en total deberán ser 2 en arquitectura de alta disponibilidad (HA Activo/Pasivo), deberá proporcionar al menos las siguientes características hardware:

- 8 puertos 10/100/1000.
- 4 puertos 1G/2.5G/5G con PoE.
- 6 puertos 1G SFP.
- 4 puertos 1G/10G SFP/SFP+.
- Ocupación de 1 Rack Units por equipo.
- Disco duro SSD de 120GB para almacenar sistema, configuración y logs.
- Puerto dedicado para gestión “fuera de banda”.
- Puerto de consola RJ45.
- Puerto dedicado a funciones propias del HA de 10 GB (sincronización de configuración, de sesiones, etc.) sin necesidad de utilizar puertos de servicio para esta tarea.
- Recursos hardware (CPU, RAM y HD) dedicados e independientes para el plano de control y para el de servicio, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa.
- Fuentes de alimentación redundadas Hot-swap.
- Flujo de aire front to back.
- Prestaciones o capacidad del firewall con la identificación de aplicaciones habilitada (es decir, trabajando a nivel 7 para todo el tráfico) medidos con transacciones de 64 KB HTTP: 8,9 Gbps.
- Prestaciones o capacidad con todos los servicios de seguridad habilitados, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, File Blocking, etc.) como frente a amenazas desconocidas (Sandboxing) y Logging habilitado medidos en transacciones APPMix: 3.2 Gbps.
- Nuevas sesiones por segundo: 100.000.
- Número de sesiones totales: 945.000.
- Incluidos 1 sistema virtual y ampliable hasta 6 con licencia adicional.

Se ha de garantizar que el firewall ofertado no sufrirá degradación conforme se vayan habilitando perfiles de seguridad relacionados con la protección, es decir, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc.) como

frente a amenazas desconocidas (Sandboxing), de forma que sea predecible el impacto en el rendimiento de la solución en la activación progresiva de estas funciones de seguridad, independientemente del número de ellas.

La arquitectura hardware de la plataforma deberá permitir la aplicación paralela de diferentes módulos de seguridad, asegurando una sola inspección por cada paquete. No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, DNS, URL Filtering…).

CARACTERÍSTICAS DE GESTIÓN Y ADMINISTRACIÓN

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión y administración de la propia plataforma, entendiéndose como funcionalidades mínimas a cumplir:

- Procesadores y memoria dedicados para los planos control y datos, para asegurar el acceso a la gestión en caso de saturación del plano de datos.
- Gestión completa del firewall desde el propio dispositivo sin necesidad de appliance externos, es decir, se podrá realizar políticas de seguridad, obtención de informes, etc., desde el propio firewall.
- Gestión de políticas, objetos, interfaces, etc., desde la propia interfaz del firewall, sin necesidad de instalar otros componentes.
- Gestión y administración por medio de interfaz web y a través de línea de comandos, debiendo existir la posibilidad de utilizar API XML para configuración de ciertas funcionalidades.
- Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.
- Posibilidad de aplicar cambios en configuración pendientes, visualizar dichos cambios antes de aplicarlos, así como validarlos antes de aplicarlos en configuración. Se debe también tener la posibilidad de almacenar diferentes versiones de configuraciones, así como descartar cambios en configuración realizados.
- Envío de logs vía SYSLOG, FTP, SCP y TFTP para retención y posterior tratamiento, con posibilidad de envío de logs selectivos según niveles de severidad y también según atributos como, por ejemplo, los tipos de amenaza.
- Soporte SNMP incluyendo la posibilidad de obtener estadísticas relativas a los procesos de recolección de logs y del estado de salud de las funciones de alta disponibilidad
- Debe existir la posibilidad, aunque no fuera objeto de este contrato, de disponer una consola de gestión única para firewalls físicos, virtuales, o en cloud, para reducir los costes de operación y la curva de aprendizaje.

CARACTERÍSTICAS DE RED BÁSICAS

Cada firewall ofertado deberá tener las siguientes características técnicas de red básicas, entendiéndose como funcionalidades mínimas a cumplir:

- Los interfaces del firewall deben soportar los siguientes modos de funcionamiento:
    - Modo TAP para monitorizar tráfico de forma pasiva a través de puertos mirror.
    - Modo transparente para inspección de tráfico en el flujo de datos y despliegues “in-line”.
    - Modo layer 2 o switching.
    - Modo layer 3 o routing.
- Debe ofrecer la posibilidad de utilizar varios interfaces trabajando en diferente modo, al mismo tiempo y en la misma instancia, para poder abarcar despliegues híbridos.
- Soporte de IEEE 802.1Q y agregación de interfaces mediante 802.1AD soportando al menos 8 interfaces en agregación.
- Soporte de protocolos dinámicos de routing RIP, OSPF y BGP4 así como routing estático.
- Soporte de DHCP, NAT y PAT.
- Capacidad de detección de fallos bidireccional entre Firewall y Router para aplicar a protocolos de routing dinámicos o rutas estáticas.
- Capacidad de realizar policy base routing en base a IP o red de origen, o también basado en usuarios/grupos o por tipo de aplicación.
- Capacidad de soportar arquitecturas de alta disponibilidad de tipo activo/pasivo o activo/activo.
- Capacidad de realizar VPN “Site to Site” o “SSL VPN”.

CARACTERÍSTICAS DE GESTIÓN DE USUARIOS

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión e identificación de usuarios, entendiéndose como funcionalidades mínimas a cumplir:

- Posibilidad de aplicar políticas basadas en usuarios y grupos en vez de únicamente por IP.
- Integración con sistemas de directorios para obtención de usuarios y grupos, incluyendo Microsoft Active Directory.
- Posibilidad de integración con sistemas multiusuario como Citrix o Microsoft Terminal Server para la identificación unívoca de los usuarios para el tráfico generado desde estos sistemas.

- Capacidad de analizar mensajes de syslog con información de login y logout para identificación de usuarios.
- Posibilidad de inyectar usuarios mediante aplicaciones de terceros a través de API XML.
- Capacidad de poder identificar usuarios mediante portal de autenticación propio haciendo uso de protocolos como Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.

CAPACIDADES GENERALES DE SEGURIDAD

Los equipos ofertados deben cumplir con los siguientes requerimientos mínimos en cuanto a funcionalidades relativas a seguridad:

- Posibilidad de agrupar interfaces del propio firewall en conjuntos independientes formando zonas, de forma que las políticas de seguridad se definan por zonas, pudiendo incluir en las mismas políticas varias zonas origen para el análisis de tráfico y procesado de reglas de seguridad, así como la posibilidad de crear múltiples reglas de seguridad entre zonas origen y destino o incluir cualquier zona origen o destino de tráfico en dichas reglas. Posibilidad de disponer de hasta 50 zonas de seguridad.
- Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 3600 identificadas, así como la identificación de subfunciones dentro de una aplicación como por ejemplo “compartir escritorio de webex”, “chat dentro de webex”, “transferencia de ficheros en webex”, etc.
- Posibilidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.
- Posibilidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.
- Posibilidad de identificar aplicaciones propietarias que usen los protocolos HTTP y TCP.
- Posibilidad de identificar aplicaciones que vayan bajo túneles encriptados SSL.
- Capacidad de descifrar tráfico SSH y detectar aplicaciones no legítimas sobre este protocolo.
- Posibilidad de crear reglas de calidad de servicio según las aplicaciones que se usen en el tráfico, y los usuarios o grupos de usuarios que lo generen.
- Posibilidad de aplicar diferentes perfiles de seguridad (IPS, Antivirus, Antispyware, Sandboxing, etc.) para diferentes aplicaciones que funcionen por el mismo puerto.
- Posibilidad de aplicar políticas de NAT de forma independiente a las políticas de seguridad ante vulnerabilidades y de protección de la red interna.

- Posibilidad de habilitar todas las funciones de seguridad que ofrezca el equipo, sin penalización en rendimiento dependiendo del número de ellas habilitadas.
- Capacidad de requerir autenticación de múltiple factor en el acceso a cualquier servicio del datacenter para verificar la identidad real del usuario, independientemente de la aplicación utilizada. Deberá permitir la integración de forma nativa con soluciones como Okta, Ping Identity, Duo v2, RSA SecureID Access, y en general con cualquier otra vía Radius o SAML.
- Posibilidad de descifrar tráfico cifrado y enviarlo en claro a otras soluciones para realización de sus funciones, y recibirlo nuevamente después para su envío a destino previa aplicación de las políticas de seguridad que correspondan en el firewall.
- Utilización de motores propios de inspección para los servicios de seguridad (Antivirus, IPS, URL Filtering, Antimalware, etc.) y no de terceros.
- NGFW con motores basados en Machine Learning o Inteligencia Artificial con soporte en la nube para proporcionar protección en tiempo real de amenazas desconocidas, URL maliciosas, y protección de DNS.
- Integrar machine learning (ML) o Inteligencia Artificial IA, en el núcleo del firewall a fin de proporcionar una prevención de ataques sin firma internos para los ataques basados en archivos, mientras identifica y detiene de inmediato los intentos de phishing nunca antes vistos.
- Posibilidad de importar reglas de Snort y Suricata como firmas de IPS del Firewall, ya sea a través del Firewall o a través de la consola de gestión.

PROTECCIÓN ANTE ATAQUES DENEGACIÓN SERVICIO.

El administrador será capaz de configurar las políticas de denegación de servicio que son empleadas para asociar configuraciones DoS con tráfico que llega a una interfaz basada en los servicios definidos, y en las direcciones o rangos IP de origen y destino.

- Los firewalls ofertados deben contar con medidas de protección ante ataques de Denegación de Servicios de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las direcciones ip origen y destino a inspeccionar o el usuario o grupo de usuarios interno de la red que puede estar originando el ataque.
- Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

MOTOR DE ROUTING AVANZADO

Los firewalls deben disponer de un motor avanzado de routing, que simplifica las operaciones con configuraciones basados en estándar similar al utilizado por otros fabricantes de routers.

Se deben permitir la configuración de perfiles para cada protocolo y el filtrado granular de cada perfil para multiples routers lógicos y sistemas virtuales.

Se debe permitir la redistribución de rutas con perfiles de redistribución.

Se debe permitir grupos de peers BGP y peers BGP que hereden configuraciones.

Se debe dar soporte a rutas estáticas BGP, MP-BGP, OSPFv2, OSPFv3, RIPv2, IPv4 multicast routing, BFD, redistribución, filtrado de rutas en el RUB, access lists, prefix lists y route maps.

PROTECCIÓN ANTE VULNERABILIDADES

Los firewalls ofertados deben contar con la posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente, debiendo cumplir con las siguientes funcionalidades:

- Se debe poder aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de Internet sin incurrir en latencia superior a 1 milisegundo para no penalizar la sensación del usuario, efectuando el análisis en una única pasada para todo tipo de amenazas.
- En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas.
- Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades especificando si son vulnerabilidades que aplican a los clientes, los servidores o a ambos indistintamente.
- Las vulnerabilidades deben estar categorizadas por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.
- Se debe permitir usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.
- Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.

FILTRADO DE URL

Los equipos ofertados deben tener la posibilidad de filtrar la navegación http o https según la URL que se desea visitar basándose en diferentes criterios:

- Posibilidad de definir manualmente listas estáticas de URL o de IP permitidas y no permitidas para la navegación, con posibilidad de definir para las no permitidas la acción a realizar (bloquear, permitir pero advertir, generar solamente un log, etc.).
- Permitir la navegación basándose en categorías de URL, siendo dichas categorías actualizadas periódicamente a través de un servicio en la nube que permita al menos categorías de URL como “malware”, “phishing”, “command-and-control”, “hacking”, etc.
- Posibilidad de incluir listas dinámicas, de forma que los equipos puedan ser configurados para que de forma periódica consulten fuentes de inteligencia propios o

de terceros con IoCs maliciosos, y permita automatizar la denegación del tráfico hacia/desde estos IoCs en la política del firewall. Se valorará positivamente que el fabricante ofrezca listas de IP maliciosas que se actualicen y mantengan automáticamente.

- Posibilidad de detectar el robo y envío de credenciales corporativas (usuarios y password de la red corporativa) hacia las webs que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales en función de las categorías de web visitadas.
- Se deberá dotar al firewall de modelos de Machine Learning (ML) o de Inteligencia artificial (IA) para poder detectar Inline, en el propio firewall de páginas de phishing, así como de scripts Javascript maliciosos.
- Se deberá disponer de mecanismos de Machine Learning o de Inteligencia Artificial (IA) basada en la nube para categorizar páginas web que no estén categorizadas por el sistema del filtrado de URL general.
- Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

DETECCIÓN DE EQUIPOS COMPROMETIDOS EN LA RED

Los firewalls ofrecidos deben tener la capacidad mediante firmas de detectar posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante log este tipo de tráfico.

Entre las acciones posibles, se debe tener la capacidad de habilitar mecanismos de DNS sinkholing que permitan interceptar las peticiones de resolución de dominios realizadas desde servidores propios DNS internos a la red o hacia servidores DNS externos de forma que se identifique los equipos internos comprometidos por algún tipo de malware.

ANTIVIRUS

Los firewalls propuestos deben tener la capacidad de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet a red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

Se debe poder aplicar políticas que permitan aplicar el motor de antivirus sobre protocolos como ftp, http, imap, pop3, smb o smtp, definiendo para cada uno de estos protocolos la acción a realizar (permitir los ficheros, descartar los ficheros, desconectar la sesión o registrar mediante logs) ante la detección del fichero malicioso por el motor de antivirus, adicionalmente, se debe poder tener la posibilidad de enviar el fichero que se inspecciona a un servicio en Internet que permita el análisis de dicho contenido y emita un veredicto en caso de que el fichero sea malicioso que permita realizar a los firewalls las acciones oportunas.

Los firewalls deben permitir la aplicación de políticas de antivirus de forma granular, permitiendo por ejemplo la aplicación de dichas políticas a ciertos usuarios de determinados grupos o a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

El módulo de Antimalware deberá de disponer de un motor de análisis estático basado en algoritmos de Machine Learning (ML) o de Inteligencia Artificial (IA) que permitan identificar muestras maliciosas desconocidas en tiempo real sin necesidad de tener que esperar al veredicto del módulo de Sandboxing.

TECNOLOGÍA DE SANDBOXING

Los firewalls propuestos deben tener la capacidad de disponer de un servicio en la nube capaz de analizar ficheros de tipo desconocido o enlaces URL recibidos en correos electrónicos, de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

El servicio en la nube será capaz de analizar los siguientes tipos de ficheros: paquetes de aplicaciones Android, ficheros flash, applets java, ficheros de Microsoft office, ficheros ejecutables con formato PE incluyendo dll, ficheros pdf y enlaces HTTP y HTTPS incluidos en correos electrónicos recibidos por SMTP y POP3.

El análisis realizado por este servicio en la nube en caso de que la muestra enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad deberá generar las firmas apropiadas en un plazo máximo de 5 minutos que se utilizarán para actualizar los motores propios de antivirus y filtrado URL de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas por dichos firewalls.

Además, el firewall también se aprovechará, en el mismo plazo de tiempo, de la inteligencia generada para cualquier muestra analizada en dicho servicio incluso procedente de otros clientes u otras fuentes externas.

Será valorable la compartición de esta inteligencia con alguna solución de puesto de trabajo para que, en ese plazo máximo de 5 minutos, también lo desconocido sea convertido en conocido en el contexto de protección en el puesto.

Los firewalls deben tener la capacidad de enviar también al servicio de sandboxing en la nube no solamente aquellos ficheros de tipo sospechoso sino aquellos que hayan sido bloqueados por su propio sistema de firmas, con objeto de poder analizar variantes de malware e incorporar esas variantes al sistema de firmas de los propios motores del equipo. Además, se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, este servicio en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que las muestras enviadas a esta nube permanecerían dentro de sus fronteras.

Además, este servicio en la nube habrá de estar basado en un hipervisor específicamente diseñado por el fabricante y contará con la posibilidad de detonación en hardware físico para aquellas muestras altamente evasivas en entornos de sandbox virtuales.

Capacidad para detectar y bloquear variantes maliciosas de los ejecutables y los scripts de PowerShell en tiempo real mediante el aprendizaje automático (ML) en el propio firewall.

SEGURIDAD EN DNS

Los firewalls propuestos habrán de contar con la posibilidad de activar un servicio de seguridad DNS en tiempo real basado en nube para permitir escalado ilimitado en la detección de millones de dominios maliciosos, predecir y bloquear de forma inmediata dominios maliciosos procedentes de malware que utilizan DGA (Domain Generation Algorithm) para comando y control, detectar robo o fuga de datos utilizando DNS Tunneling y en general incorporar cualquier innovación de seguridad a este respecto sin necesitar hardware o software adicional. Este servicio no deberá tener ningún impacto en el rendimiento de la plataforma.

Protección DNS con la capacidad de gestionar categorías DNS, Fast Flux DNS, Ultra-Slow DNS Tunneling, Dictionary DGA, Dangling DNS, y dominios maliciosos de reciente creación, sin usar herramientas externas adicionales.

VPN. ACCESO REMOTO

El servicio VPN permitirá facilitar el acceso remoto de usuarios, proveedores, empleados y demás colaboradores a los recursos informáticos que para cada caso se requiera y con el nivel de seguridad que se precise para cada perfil de acceso.

Se podrán definir, por lo tanto, diferentes perfiles de usuario sobre los que se aplicarán diferentes políticas de acceso: solo acceso web, acceso a aplicaciones específicas, a equipos, etc.

Se diferencian en esta funcionalidad dos tipos de conexiones remotas:

1. Conexiones punto a punto (Site2Site, L2L): La solución posibilitará el establecimiento de conexiones punto a punto mediante protocolos estándar de conexiones remotas privadas IPSEC.
2. Conexiones remotas de usuario (User2Site): El servicio de conexión remota de usuarios cumplirá, al menos, las características que se detallan a continuación:

Conexiones SSL VPN en modo web y modo túnel, es decir, ya sea con o sin agente en el equipo cliente:

- Sin agente (modo web): para clientes remotos que sólo necesiten un navegador y no requiera la instalación de ningún agente, con el fin de acceder vía web a: HTTP/ HTTPS, etc.
- Con agente (modo túnel): para equipos remotos que ejecuten una variedad de aplicaciones de cliente y servidor

Versatilidad frente a sistemas operativos: será compatible con GNU/Linux, Microsoft Windows, MacOSX, iOS y Android.

Integración con cualquier tipo de repositorio corporativo de usuarios (Microsoft Active Directory, LDAP, Radius, etc.)

La solución permitirá configuraciones en modo Full Tunnel, así como en modo split tunneling (sólo se cursará por el túnel el tráfico que se requiera). Se deberá poder realizar exclusiones o inclusiones basados en dominios, procesos, DNS o aplicaciones de streaming.

Deberá poder disponer de hasta 1500 túneles a través del cliente VPN.

Deberá soportar conexiones IPv6.

Deberá tener funcionalidad “host checker”, pudiendo generar perfiles con los siguientes atributos:

- Dominio.
- Sistema operativo.
- Verificar la existencia/activación de Antimalware, Backup de disco, Cifrado de disco. Parcheo de vulnerabilidades, firewall, DLP.
- Otros atributos como: claves de registro, ficheros, procesos activos, certificados, etc.

AIOPS

Los firewalls proporcionados deberán proveer de una solución en nube del fabricante que permita lo siguiente:

- Evaluar la configuración del cortafuegos e identificar áreas de mejora.
- Proporcionar un fácil acceso a los datos de telemetría históricos y de tiempo de ejecución de los cortafuegos.

- Detectar problemas del sistema (independientemente del método de detección), como, por ejemplo, posibles fallos en ventiladores, fuentes de alimentación, interfaces, uso de CPU y RAM.
- Reducir el tiempo de resolución a través de flujos de trabajo de alerta/notificación.
- Proporcionar paneles dinámicos y visualizaciones para suscripciones de seguridad como DNS o Sandbox.

INFORMES

Los firewalls proporcionados deben tener la capacidad de generar informes tanto predefinidos como personalizados utilizando los logs generados por los propios equipos sin necesidad de equipos externos adicionales, limitándose dicha funcionalidad exclusivamente por la cantidad de logs que dichos firewalls sean capaces de almacenar en su propio almacenamiento permanente.

Se debe disponer de la capacidad de generar informes de actividad por usuario, incluyendo aplicaciones utilizadas, sitios web visitados.

Se debe poder generar los informes de forma automática, así como agrupar varios informes en un único documento con formato PDF.

Entre los informes disponibles, se debe disponer de informes sobre los anchos de banda consumidos por las diferentes aplicaciones, informes sobre los orígenes y destinos geográficos de las amenazas detectadas, e informes sobre el análisis de comportamiento de tráfico observado que permita detectar equipos comprometidos participantes de botnets.

Los firewalls proporcionados deben permitir la capacidad de programar el momento en el cual se desea la generación del informe correspondiente y su envío a través de correo electrónico, así como el intervalo de fechas entre las cuales se desea la información de dicho report, dentro de las limitaciones de almacenamiento de los propios equipos.

PROCESAMIENTO DE LOGS

Los firewalls ofertados deberán tener la posibilidad de almacenar los logs localmente con la única restricción de la capacidad de almacenamiento local del propio dispositivo o bien enviar los logs a una plataforma de gestión y procesamiento especializada con objeto de mantener dichos logs a largo plazo.

El sistema de procesamiento de logs deberá cumplir también con las siguientes características:

- Disponer de un cuadro de mando personalizable por usuario que accede al sistema con al menos la siguiente información: Aplicaciones más usadas, Aplicaciones de alto riesgo, Información general del sistema, Estado de los Interfaces, Logs relativos a las amenazas más observadas, Logs de filtrados URL o Recursos del sistema.

- Cuadro de mando de aplicaciones generado a partir de los logs, personalizable por usuario que permita disponer de información como los usuarios que más generan tráfico, las reglas de seguridad que más se usan, vulnerabilidades que más se han detectado y bloqueado, equipos que navegan hacia dominios maliciosos, virus detectados, información enviada a los servicios de sandboxing o host comprometidos en la red interna.
- Capacidad de uso de motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs recibidos se pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con indicación de tiempos, usuarios, direcciones IP y vulnerabilidades o amenazas detectadas.
- Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.

GESTION LINEAS WAN

Los firewalls ofertados deberán tener la posibilidad de gestionar diferentes redes WAN. Esta gestión deberá poder ofrecer soluciones como:

- Asignación estática por reglas.
- Configuración de redes WAN con balanceo en función de cargas, latencias y reglas QoS.
- Protección ante caídas y recuperación automática.
- Configuración por VLAN e interfaces de entrada.

OTRAS FUNCIONALIDADES

Los firewalls ofertados deberán disponer de funcionalidades adicionales a las descritas anteriormente, entre las que se encuentran:

Se ofrecerá una herramienta de Migración de configuración y políticas de seguridad del fabricante de cortafuegos en uso, a la tecnología adquirida, de manera que se eviten errores de configuración y se acelere el proceso de la misma. Esta herramienta no tendrá ningún coste.

Capacidad de mostrar un portal cautivo con todos los sistemas de autenticación cuando se accede a determinadas URL que se encuentran detrás del firewall. Esta funcionalidad se podrá programar para una, varias o todas las aplicaciones.

Herramientas embebidas en el firewall para migrar políticas basadas en IP y puertos a políticas basadas en aplicación.

Herramienta embebida en el firewall para identificar reglas sin uso en función del tiempo, al menos los últimos 30 días y últimos 90 días.

El firewall deberá mostrar el número de hits de cada regla, así como cuando fue la primera y última vez que hizo hit.

El firewall deberá mostrar sobre la misma vista de reglas de seguridad el número de aplicaciones que se ha identificado por cada regla definida, así como los días transcurridos sin identificar una nueva aplicación.

El firewall deberá mostrar sobre la misma vista de reglas de seguridad la fecha y hora de creación y modificación de cada una de las reglas.

Herramientas que evalúen la aplicación de mejores prácticas de seguridad.

Posibilidad de definir aplicaciones y/o vulnerabilidades propias mediante diferentes parámetros como los puertos tcp o udp que se usan en dicha aplicación y combinaciones de patrones dentro de las cabeceras de los paquetes o en los propios payloads de dichos paquetes que se deben cumplir para que se reconozca la aplicación y/o vulnerabilidad.

Los firewalls ofertados deben tener la posibilidad de descifrar tráfico SSL y SSH de forma granular, de forma que se puedan establecer políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las direcciones ip origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, siendo posible excluir categorías de sitios de internet a descifrar.

Posibilidad de descifrar tráfico que pasa a través del firewall destinado a sitios web que utilicen certificados de curva elíptica (ECC), entre ellos: X25519 y X448

Posibilidad de activar a través de licencia adicional el envío de tráfico descifrado hacia una interfaz del firewall específico para análisis.

Captura de tráfico. Los firewalls propuestos deben tener la capacidad de realizar capturas del tráfico que atraviesa sus interfaces en formato pcap, de forma que se puedan establecer criterios de la captura, como capturar el tráfico originado por un cierto origen ip o destino, cierto puerto o también capturar tráfico de una aplicación en concreto independientemente del origen o destino del tráfico o incluso aplicar filtros de captura de tráfico exclusivamente cuando se detecte un virus o un ataque en los motores de protección.

El fabricante deberá disponer de un servicio de inteligencia de amenazas que en algún momento permita ampliar la plataforma ofreciendo visibilidad y contexto de las amenazas identificando autores, familias de malware, campañas, sectores objetivo, comportamientos maliciosos, exploits, etc.

Todas las funcionalidades se podrán activar de forma concurrente en todos los Sistema de Seguridad tanto virtuales como físicos.

En caso de que alguna característica ofrezca diferentes datos de rendimiento en los datasheets oficiales para diferentes escenarios, se considerará siempre el de peor valor en el entendimiento de que se puede requerir su uso en esas condiciones.

Deberá tener la capacidad de integrarse con soluciones ofrecidas por el mismo fabricante e incluidas en la propuesta, que permitan procesar inteligencia de amenazas procedentes de

feeds propios y de terceros, recogiendo, agregando y normalizando esos IOC para hacerlos disponibles para su consumo en el propio firewall.

Deberá incluir la capacidad de poder enviar descifrado, todo o parte del tráfico cifrado que pase a través del firewall y que cumpla con la política de seguridad configurada en el firewall, a una cadena de soluciones de seguridad de terceros, constituyendo una cadena privada de análisis de seguridad para aplicación de otras funciones proporcionada por dichas soluciones.

Protección de la inversión y mayor ciclo de vida de los equipos mediante el uso de FPGA programables en lugar de ASIC estáticos. Las FPGA permiten añadir nuevas funcionalidades de seguridad con una simple reprogramación, sin necesidad de tener que cambiar de equipo obligados por el rediseño con nuevos ASIC, o tener que enviar el tráfico a la CPU de propósito general con la consiguiente degradación de rendimiento.

2. CARACTERÍSITICAS DE LOS SERVICIOS REQUERIDOS EN ESTE PLIEGO.

Adicionalmente al suministro de los equipos con sus licencias que cumplan con los requerimientos anteriores, en el presente pliego se solicitan una serie de servicios que se deberán prestar por parte de la empresa licitadora de cara a la mejor puesta en marcha y aprovechamiento del equipamiento suministrado.

Los servicios requeridos, que se describen con mayor precisión más adelante, son los siguientes:

- Servicios de Puesta en marcha de la plataforma:
    - Plan de proyecto.
    - Instalación física y configuración básica.
    - Migración/optimización de las reglas, servicios y configuraciones actuales. (Anexo V).
    - Configuración de VPN: punto a punto, equipos en remoto con el objetivo de securizar los endpoints.
    - Documentación de la solución.
- Servicios de Formación.
- Servicios de Soporte.
    - Soporte con el fabricante de los equipos.
    - Consultas sobre el sistema instalado.
    - Intervenciones remotas para la resolución de incidencias.
    - Aplicación de medidas extraordinarias contra amenazas críticas.
    - Realización de los upgrade de versiones de los sistemas (al menos una anual).
    - Monitorización del sistema

SERVICIOS DE PUESTA EN MARCHA DE LA PLATAFORMA.

Todos los precios ofertados deberán incluir todos los gastos de entrega y transporte de los equipos en el lugar designado por Parlamento de Navarra. A su vez el desembalaje, la instalación física y la configuración requerida, la documentación técnica de los trabajos realizados, así como las pruebas de verificación necesarias que aseguren el correcto funcionamiento de la instalación.

La empresa adjudicataria deberá realizar las tareas de configuración para la puesta en marcha de los firewalls suministrados siguiendo las guías de mejores prácticas o “best practices” recomendadas por el fabricante del producto.

Será responsabilidad del adjudicatario las tareas necesarias para que los actuales servicios queden perfectamente operativos en los nuevos equipos suministrados.

Una vez realizada la instalación y la configuración del equipamiento se realizarán las pruebas pertinentes para comprobar la respuesta del sistema ante caídas, recuperación, etc. Unido a estas pruebas finales, se realizará un informe del estado y de cumplimiento de las best practices recomendadas y de que no haya problemas de seguridad. Estas validaciones deberán ser similares a un commisioning imparcial de la instalación.

La instalación deberá ser resiliente ante fallos, caídas puntuales, problemas de cableado, etc, minimizando en la medida de lo posible los puntos únicos de fallo en la solución propuesta. Se deberán identificar estos puntos únicos de fallo en caso de que los hubiera y ser comunicados al personal de Parlamento de Navarra.

Plan de Proyecto

El licitador deberá elaborar un plan de proyecto detallado que se valorará según criterios de valoración que se indican más adelante y que incluya:

- Calendario de implantación, migración y puesta en marcha de servicios. Deberá indicar claramente y con detalle en qué consisten los procesos de la implantación, las fases, la convivencia o no de la nueva solución con la actual y el impacto que tendrá la implantación y los posibles tiempos de parada.
- Personal destinado al proyecto. Deberá indicar claramente las personas que van a intervenir en el proyecto con sus respectivos roles.
- Detalle técnico de cómo se van a implementar tanto las funcionalidades actuales como las mejoras que se pretenden abordar, detallando las principales configuraciones a poner en marcha con la nueva solución y las mejoras introducidas en cada una de ellas respecto de la solución actual.
- Descripción del sistema final implantado, principales funcionalidades, fortalezas de la nueva instalación, así como los puntos débiles o de mejora que se detecten.

De ser necesario un corte de servicios en la puesta en marcha del nuevo sistema, éste deberá ser mínimo, garantizando la conectividad y continuidad de las comunicaciones y servicios de parlamento. En caso de necesitar algún corte de servicios estos habrán de planificarse de acuerdo con el personal técnico designado por Parlamento de Navarra, generalmente en viernes por la tarde o fin de semana, y deberán indicarse en el plan de proyecto.

Instalación física y configuración básica.

Se considera el servicio de instalación física y configuración básica al servido de entrega, desempaquetado e instalación física en los huecos de rack que Parlamento de Navarra destine a ello.

La instalación física se considera “llave en mano” por lo que cualquier elemento necesario para la instalación como soportes, tornillería, cableado, guías de cable latiguillos, SFP, etc., tanto

del firewall como de la electrónica de red de Parlamento de Navarra se considerarán incluidos en la propuesta, no siendo en ningún caso motivo de la ampliación del coste del contrato.

En función de la configuración proporcionada por la empresa licitadora se deberá a proceder al conexionado con los elementos centrales de Parlamento de Navarra, switchs core, redes WAN, y redes de Gestión y HA, con todos los medios necesarios, latiguillos de cobre, fibra, SFP quedando la instalación perfectamente conectada, etiquetada y el cableado debidamente peinado.

Una vez procedido a la instalación se procederá a realizar la primera configuración básica, que permitirá el acceso de gestión al dispositivo sin interrupción de la actual instalación.

Se procederá a la realización de instalación de los últimos firmwares recomendados por el fabricante para garantizar el funcionamiento óptimo con la versión recomendada.

Migración/optimización de las reglas, configuraciones y servicios actuales.

Una vez preparado el equipo, con acceso a la gestión y con las actualizaciones de firmware, se procederá a la migración y optimización de las reglas actuales, creación de alias, NAT, interfaces y resto de configuraciones del sistema de firewalls de Parlamento de Navarra que se detallan en el Anexo V de este pliego, en el que se indican los servicios e infraestructura actual.

Este proceso deberá garantizar al menos el mismo nivel de acceso actual, pero mejorando la seguridad adaptando las reglas a un firewall de capa 7. Esta optimización se llevará a cabo de forma consensuado con el personal técnico que Parlamento de Navarra designe para este proyecto de cara a garantizar la mayor eficacia en las acciones a realizar.

Adicionalmente, se deberán implementar las políticas de QoS de cara a garantizar la disponibilidad de las redes WAN y su correcto balanceo, así como unas reglas genéricas que ayuden a la priorización del tráfico de más importante a menos.

Se deberá implementar el acceso con Múltiple Factor de Autenticación (MFA) mediante aplicación móvil para los Administradores del sistema como por ejemplo DUO. Este número de usuarios será en todo caso menor de 10.

En general, esta propuesta deberá ir encaminada a que Parlamento de Navarra pueda seguir prestando sus servicios más críticos (DNS, página web, servicios de streaming, intranet, etc.), garantizar los accesos necesarios a los diferentes sistemas con los mínimos permisos y privilegios necesarios, así como proteger las infraestructuras ante posibles ataques tanto externos como internos.

Creación de nuevas redes.

Con el fin de mejorar la seguridad mediante la segmentación de redes, se deberán crear las VLAN definidas posteriormente, dejándolas plenamente operativas a modo de prueba de

concepto. Estas VLAN con su direccionamiento IP servirán a su vez para el aprendizaje del proceso para el personal designado por Parlamento de Navarra para futuras intervenciones.

Las redes designadas para la nueva creación son:

- Red de parlamentarios: en esta red se colocarán todos los equipos de los parlamentarios que se conectan por una red wifi concreta y deben tener accesos limitados a: Impresoras, unidades de red compartidas y aplicación de gestión parlamentaria a través del navegador. Además de poder navegar por internet con las medidas generales de protección.
- Red de servidores. Únicamente su definición y la inclusión de un servidor para pruebas. Para ello consensuará con el personal técnico de Parlamento qué servidor o servicio es migrado a modo de prueba de concepto para futuras migraciones que serán llevadas a cabo por el personal de Parlamento de Navarra.
- Red de navegación para personal externo: en esta red se habilitará una VLAN definida y la navegación a internet aplicando un perfil de seguridad estándar para personal ajeno a Parlamento de Navarra. Esta red no tendrá acceso a ningún otro recurso interno, y servirá únicamente de propósito general para dar cobertura a personas u organizaciones externas a Parlamento como periodistas, u otros medios que necesiten únicamente una conexión a internet.

Configuración de VPN: punto a punto, equipos en remoto.

La empresa licitadora deberá realizar la configuración necesaria para que el servicio de VPN actual de Parlamento de Navarra pueda ser prestado con la nueva infraestructura.

Para ello se deberán configurar los servicios de VPN punto a punto basados en Ipsec, así como servicios de VPN, con o sin agente dependiendo de la solución, para el acceso remoto de diferentes perfiles. Se identifican al menos estos perfiles: administradores, usuarios internos del parlamento - teletrabajo, parlamentarios - asistentes y personal de empresas externas de soporte.

Las soluciones VPN implementadas deberán permitir validaciones de seguridad en los equipos clientes, de tal forma que se aumente la confianza de dichos equipos al consumir servicios de Parlamento de Navarra. Se valorará muy positivamente la implementación de la filosofía ZTNA, que ayude a mitigar los riesgos con procedencia tanto interna como externa.

Los accesos por VPN se deberán configurar con MFA para los grupos de personal interno de Parlamento de Navarra: usuarios internos del parlamento - teletrabajo, parlamentarios – asistentes. Este doble factor deberá ser lo más sencillo de uso para el usuario pudiéndose adoptar mediante la autenticación del sistema (Windows en dominio) y la adición de un certificado físico instalado en cada equipo.

La empresa licitante deberá proponer una solución que ayude a mitigar los riesgos de los equipos finales, en general portátiles con sistema operativo Windows, que se conectan en redes externas a las de parlamento. Esta solución deberá proponer la mejor solución para proteger estos equipos sin importar dónde o con qué medio estén conectados, garantizando que se cumplen las reglas de filtrado URL y protecciones comunes ante ataques, que ya están configuradas en los firewalls instalados en el Parlamento de Navarra.

Parlamento de Navarra dispone de un sistema de protección EDR desplegado en todos los equipos de Parlamento, tanto equipamiento fijo como equipamiento portátil. **No es objeto de este pliego ni de este apartado la sustitución del actual sistema EDR**, sino la de implementar una serie de mejoras que complementen el nivel de seguridad actual permitiendo la reducción de riesgos de los dispositivos portátiles. Esta serie de mejoras podrán contemplarse como elementos individuales o como complemento mejoras en el uso de mecanismos de VPN basados en la filosofía de ZTNA.

Se configurarán los diferentes servicios de forma que el personal técnico de Parlamento de Navarra pueda ampliar el servicio tanto en perfiles diferentes como en el número de usuarios o bien deshabilitarlos fácilmente.

Se acordará con el personal técnico designado por Parlamento de Navarra, la mejor forma de desplegar las configuraciones y/o agentes necesarios de cara a optimizar el proceso de adopción de la solución.

Documentación de la solución.

La empresa adjudicataria deberá proporcionar dentro de un plazo de 2 meses desde que finalicen las tareas de instalación y configuración, la documentación perteneciente al proyecto.

Esta documentación deberá contener al menos:

- Identificación con números de serie, modelo y firmware de todos los componentes utilizados. Deberán incluirse tanto los firewalls, como SFP, así como las licencias y suscripciones o cualquier otro elemento utilizado.
- Esquemas de conexionados físico de los equipos con el resto de la infraestructura de Parlamento de Navarra.
- Identificación física de todas las conexiones y el cableado utilizado, identificando origen y destino, velocidad de conexión y agregados si los hubiera.
- Descripción de la configuración inicial establecida.
- Descripción de las reglas del firewall configuradas, incluidas las suscripciones de seguridad, gestión de WAN, NAT, etc.
- Descripción de la configuración de las VPN configuradas y los equipos finales endpoints.

SERVICIOS DE FORMACIÓN.

La empresa adjudicataria proporcionará una formación técnica de la administración diaria de la solución técnica implantada.

La formación se impartirá al personal técnico que designe el Parlamento de Navarra con el objetivo de que éste sea capaz de realizar las tareas básicas diarias de configuración y mantenimiento de la solución.

El contenido de la formación incluirá los siguientes apartados:

- Administración del sistema
    - Creación de interfaces, enrutamiento, zonas, añadir VPN, modos de funcionamiento del firewall: en capa 2, 3, 7, etc.
    - Administración de usuarios del sistema, roles de acceso y permisos.
    - Administración HA, estados Activo/activo, Activo/pasivo, conmutación, monitorización interconexión de instancias, etc.
    - Administración de parches de seguridad y upgrades de versiones del sistema.
- Creación, administración y monitorización de reglas de filtrado avanzados, aplicaciones, grupos de URL, etc.
- Creación de reglas de clasificación y priorización de tráfico.
- Creación, administración y monitorización de VPN site to site con diferentes perfiles de seguridad y protocolos.
- Creación, administración y monitorización de VPN de usuarios, con creación de diferentes perfiles, roles, y securizando los accesos a los sistemas internos de los

usuarios finales. Creación de perfiles de seguridad de los equipos remotos y su validación.

- Monitorización del sistema: estado, carga, interfaces, conexiones concurrentes, usuarios, alertas.
- Administración de las suscripciones, configuraciones, updates, estado y alertas.
- Creación de cuadros de mando: uso de aplicaciones, usuarios más activos, riesgos y en general del estado del equipo.
- Gestión de la seguridad e incidentes, creación de alertas, IDS/IPS, identificación, análisis y soluciones de ataques producidos y respuesta automática ante los mismos.

Esta formación no deberá ser menor a 15 horas, pudiéndose realizar de forma remota y distribuyéndose de forma que no sea superior a 3 horas por día.

SERVICIOS DE SOPORTE.

La empresa adjudicataria prestará el servicio de soporte una vez terminado el proceso de puesta en marcha. A su vez resolverá las principales incidencias que puedan surgir durante la operación de los firewalls.

Este soporte deberá cubrir al menos los siguientes aspectos:

- **Soporte con el fabricante de los equipos**. Todos los soportes estarán vigentes el tiempo de duración del contrato. Este soporte cubrirá al menos lo siguiente:
    - Reemplazo de hardware defectuoso: Siendo posible el reemplazo en el siguiente día laborable, NBD.
    - Acceso a repositorios del fabricante para aplicar actualizaciones, tanto del sistema base como de cualquier suscripción activa.
    - Acceso a bases de conocimiento del fabricante.
    - Apertura y seguimiento de la incidencia con el fabricante en caso de no resolverse con los medios propios del partner.
- Consultas sobre el sistema instalado:
    - Nuevas versiones del producto.
    - Parches.
    - Funcionalidades (nuevas o ya adquiridas por el cliente).
    - Dudas al respecto del funcionamiento de la plataforma.

  El personal técnico de Parlamento de Navarra tendrá la capacidad de realizar peticiones y consultas incluidas en los servicios de soporte todas aquellas intervenciones lógicas, que tengan impacto en los servicios dentro del alcance de la propuesta, para las cuales no sea necesaria la adquisición de nuevo hardware,

software o licencias adicionales y aquella que su esfuerzo se estime en un tiempo igual o inferior a 4h.

- Intervenciones remotas para la resolución de incidencias.
- Ante amenazas críticas se aplicarán medidas en la configuración del sistema para la mitigación de dichas amenazas.
- **Una actualización de versión anual de todos los sistemas**.
- **Realización de los upgrade de versiones de los sistemas ante vulnerabilidades críticas, recomendación del fabricante.**
- **Monitorización del sistema.** Se deberán monitorizar los siguientes servicios en 24x7:
    - Estado de las máquinas.
    - Fallos en el clúster de HA (Si lo hay).
    - Estado de la CPU.
    - Estado de la Memoria.
    - Error de Paquetes.
    - Sesiones.
    - Estado de las Interfaces.
    - Así como **incidentes graves de seguridad**. Con notificación al personal de Parlamento para que puedan actuar y ayuda a la subsanación.
- Se podrán requerir técnicos especializados con soporte presencial en caso de emergencia en menos de 3 horas.

3. PROPUESTA DEL LICITANTE.

Las empresas licitadoras deberán presentar una documentación técnica del proyecto en la que se describan claramente y mediante capítulos separados cada uno de los elementos exigidos y de valoración.

A su vez deberá presentar una oferta económica en la que quede reflejado el coste unitario de cada uno de los elementos y los servicios ofertados, según indica el Anexo II del PCR.

A modo de resumen de la oferta y con carácter vinculante a la misma, se deberán rellenar las siguientes tablas en las que se especifican las características de la oferta, así como de la documentación presentada (Anexo IV).