



6237 – PLIEGO DE PRESCRIPCIONES TÉCNICAS

Área de Arquitectura Tecnológica

Área de Plataforma Tecnológica



ÍNDICE

1 ANTECEDENTES.....	6
2 OBJETO.....	6
3 ESPECIFICACIONES TÉCNICAS.....	7
3.1 Protección Anti-DDoS L7.....	7
3.1.1 Requisitos generales	7
3.2 Firewall de segundo nivel.....	10
3.2.1 Equipamiento.....	10
3.2.2 Características hardware mínimas de los equipos	10
3.2.3 Características de red	11
3.2.4 Identificación e integración de usuarios	11
3.2.5 Características generales de seguridad	12
3.2.6 Motor de routing avanzado	13
3.2.7 Protección ante vulnerabilidades	13
3.2.8 Filtrado de URL	13
3.2.9 Antivirus	14
3.2.10 Bloqueo de ficheros y datos sensibles	14
3.2.11 Tecnología de Sandboxing.....	15
3.2.12 Seguridad en DNS	15
3.2.13 Funciones SDWAN	16
3.2.14 VPN. Acceso Remoto.....	17
3.2.15 Procesamiento de logs.....	17
3.2.16 Consola de gestión centralizada	18



3.2.17	Cumplimiento de estándares.....	18
3.3	Solución SD-WAN	19
3.3.1	Requerimientos técnicos.....	19
3.3.2	Requerimientos de hardware	20
3.3.3	Requerimientos de seguridad.....	21
3.3.4	Tipología de sedes existentes	24
3.4	Solución SASE.....	24
3.4.1	Bundle base obligatorio.....	25
3.4.2	Arquitectura general	26
3.4.3	Requerimientos de gestión y visibilidad.....	27
3.4.4	Requerimientos de seguridad y cumplimiento	28
3.4.5	Requisitos Técnicos y Operativos	31
3.4.6	Protecciones SASE sobre IA.....	31
3.5	Servicio de implantación y migración	32
3.5.1	Horarios del servicio	33
3.5.2	Fases del servicio.....	33
3.5.3	Niveles de servicio – indicadores	35
3.6	Servicio gestionado de la solución	35
3.6.1	Metodología y planificación del servicio.....	35
3.6.2	Niveles de servicio – indicadores	36
3.6.3	Tareas específicas del servicio gestionado	37
3.6.4	Mantenimiento del equipamiento de seguridad y red	39
3.6.5	Fases del servicio.....	39
3.7	Bolsa de servicios profesionales especializados (bajo demanda)	40



3.7.1	Horario del servicio y control de trabajos.....	43
3.8	Pruebas de validación de las ofertas.....	44
4	CONDICIONES PARTICULARES.....	45
4.1	Equipo de trabajo.....	45
4.2	Modelo de gestión.....	45
4.2.1	Modelo organizativo.....	45
4.2.2	Modelo operativo.....	45
4.3	Documentación a entregar durante la duración del contrato.....	46
4.4	Propuesta técnica (estructura).....	47
4.5	Finalización del contrato.....	47
4.6	Perspectiva de género.....	48
4.7	Seguridad de la información.....	48
4.7.1	Deber de confidencialidad.....	48
4.7.2	Gestión interna de Lantik (medidas de securización interna) previas a la prestación 52	
4.7.3	Documentación.....	52
4.7.4	Auditoría, monitorización y reporte periódico del rendimiento de los controles de seguridad y notificación de evolución en la resolución de incidentes de seguridad a Lantik 52	
4.7.5	Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores”.....	53
4.7.6	Evidencia de buenas prácticas de seguridad, preferiblemente mediante certificación acreditada en una norma de referencia para la gestión de la seguridad de la información, en el entorno de prestación.....	53
4.7.7	Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica.....	54
4.7.8	Subcontratación.....	54



4.7.9	Mantenimiento y afección al servicio.....	55
4.7.10	Coordinación en caso de incidentes y desastres.....	56
4.7.11	Regulación de la finalización del contrato: transferencia de tecnología.....	57
4.7.12	Normativa de securización de entornos para prestación de servicio remoto	58
4.7.13	Informe periódico del cumplimiento de la “Normativa de securización de entornos para prestación de servicio remoto”	58
4.7.14	Monitorización de las conexiones remotas	58
4.7.15	Instalación de herramientas de seguridad	59
4.7.16	Evidencias de las buenas prácticas relativas al objetivo de control 11 “Seguridad Física y del entorno” de la norma de referencia ISO/IEC 27002 en el entorno de prestación	59
4.7.17	Teletrabajo	59
4.7.18	Certificación de inexistencia de vulnerabilidades de seguridad.....	60
4.7.19	Conformidad con el Esquema Nacional de Seguridad (ENS)	60
4.7.20	Declaración de ubicación	61
4.7.21	Transferencia Internacional de Datos Personales.....	61
4.7.22	Servicio asociado a la verificación electrónica de la identidad y tratamiento de datos de los tipos descritos en el artículo 46bis de la Ley 40/2015.....	61
4.7.23	Gestión de copias de seguridad y restauración de datos	62
4.7.24	Medidas de continuidad del servicio o proyecto	62
4.7.25	Registros de actividad.....	63
4.7.26	Claves criptográficas	63
4.7.27	Transparencia e información	64
4.7.28	Resolución del Contrato.....	64
4.7.29	Fuero.....	64

ANEXO A – TABLA DE CARACTERÍSTICAS 65



1 ANTECEDENTES

La Diputación Foral de Bizkaia (en adelante DFB), a través de Lantik S.A.M.P., gestiona la infraestructura tecnológica que da soporte a los servicios digitales ofrecidos por la Institución Foral y sus entidades dependientes. Esta infraestructura incluye los servicios de conectividad entre sedes, acceso a Internet, y medidas de seguridad para la protección de los sistemas y aplicaciones frente a ciberamenazas.

Con el fin de garantizar la continuidad del servicio, así como la evolución tecnológica de la infraestructura, se ha considerado conveniente la implantación de una solución avanzada de seguridad y conectividad basada en arquitecturas SASE y SD-WAN, modernizando el modelo de protección mediante los servicios avanzados de seguridad definidos en el presente expediente.

2 OBJETO

El objeto de este expediente es establecer las condiciones técnicas y económicas para la contratación de una solución integral de seguridad de las comunicaciones para la Diputación Foral de Bizkaia, sus entidades dependientes y otras organizaciones externas con conexión autorizada a recursos internos.:

Se trata de la contratación de una plataforma de seguridad gestionada basada en arquitectura SASE y solución SD-WAN para sedes corporativas. Incluye servicios SASE cloud, protección AntiDDoS de capa 7 del modelo OSI, solución SD-WAN en sedes con equipamiento corporativo bajo modalidad de pago por uso, suministro e implantación del firewall de segundo nivel, servicio de implantación y migración de la arquitectura completa, y gestión centralizada de la solución durante toda la vigencia del contrato.

La solución contemplará todos los componentes de seguridad cloud del modelo SASE, así como el suministro e implantación del firewall de segundo nivel y los servicios de implantación, migración y operación gestionada.

- **Protección AntiDDoS L7:** servicio independiente, diseñado para reforzar la defensa frente a ataques avanzados en la capa de aplicación. Incluye protección de aplicaciones web, APIs y portales públicos mediante WAF, mitigación frente a bots y mecanismos de inteligencia de amenazas actualizada.
- **Firewall de segundo nivel:** sustitución del clúster actual por nuevos equipos en alta disponibilidad (HA), con capacidades de inspección avanzada, protección ante vulnerabilidades y amenazas, cumplimiento del ENS y CCN-STIC, y garantizando la continuidad operativa tras el fin de soporte de los equipos actuales.
- **Solución SD-WAN gestionada:** despliegue bajo modelo de pago por uso de equipamiento en las sedes corporativas, con funciones de balanceo dinámico de enlaces, optimización de tráfico, QoS, seguridad integrada y monitorización centralizada del rendimiento de la red.
- **Plataforma SASE cloud:** integración de servicios de seguridad avanzados (SWG, FWaaS, CASB, ZTNA, entre otros) bajo una arquitectura nativa en la nube, con consola única de



gestión, soporte a usuarios en movilidad y protección uniforme frente a amenazas en navegación y acceso a aplicaciones privadas.

- **Servicios de implantación y migración:** planificación, despliegue progresivo y transición ordenada de las sedes y servicios hacia la nueva arquitectura de seguridad, garantizando la mínima interrupción operativa e integración de la telemetría y logs en el SOC de Lantik. **Este servicio (incluido el estudio previo) tendrá una duración de 36 meses desde el inicio del contrato.**
- **Servicios gestionados 24x7x365:** operación continua de toda la solución (SASE, SD-WAN, firewall y AntiDDoS), con soporte técnico especializado, gestión de incidencias y cambios, informes periódicos y cumplimiento estricto de acuerdos de nivel de servicio (SLA).

La solución deberá integrarse de manera transparente con los servicios MPLS y de navegación abierta a internet contratados por Lantik S.A. M.P., facilitando una transición hacia un modelo de seguridad más moderno basado en principios de Zero Trust. La arquitectura resultante deberá garantizar:

- Visibilidad y control de accesos remotos y tráfico distribuido.
- Protección frente a amenazas avanzadas en tiempo real.

Todos los elementos de seguridad HW/SW deberán contar certificación vigente registrada en el CCN-CERT, en su catálogo CPSTIC.

3 ESPECIFICACIONES TÉCNICAS

3.1 Protección Anti-DDoS L7

Este apartado extiende la protección perimetral más allá de las capas de red (L3/L4) incorporando medidas específicas de seguridad en la capa de aplicación (L7), esenciales para entornos web modernos y servicios expuestos a Internet.

La Diputación Foral de Bizkaia, a través de Lantik, prevé la incorporación de este servicio en una segunda capa de defensa complementaria al AntiDDoS tradicional, que deberá proteger de forma dinámica aplicaciones, APIs y portales públicos de ataques sofisticados en la capa de aplicación.

3.1.1 Requisitos generales

La solución deberá proveer un Firewall de Aplicaciones Web en modalidad SaaS (WAF-as-a-Service), eliminando la necesidad de infraestructura propia y garantizando un despliegue rápido en entornos de nube pública. Será fundamental que la solución asegure baja latencia, alta disponibilidad y continuidad operativa incluso bajo escenarios de ataque.

La solución deberá cumplir, como mínimo, con los siguientes requisitos:

- Despliegue en modalidad SaaS (WAF-as-a-Service).
- Baja latencia mediante nodos en la misma región de la aplicación.



- Alta disponibilidad y escalabilidad dinámica para adaptarse a incrementos de tráfico y nuevas aplicaciones o servicios.
- Continuidad de servicio bajo escenarios de ataque.
- Retención mínima de datos de seguridad durante 1 año.
- Soporte en modalidad 24x7x365.
- Gestión multitenant, con segmentación de políticas y visibilidad independiente por dominio o servicio.
- Aplicaciones web protegidas: hasta 100 aplicaciones corporativas críticas y de acceso público.
- Dominios y subdominios gestionados: hasta 100 dominios/subdominios con políticas de seguridad diferenciadas.
- Tráfico sostenido: capacidad mínima de 200 Mbps de tráfico legítimo inspeccionado, con protección ante ataques de hasta 10 Gbps sin degradación del servicio.
- Peticiones HTTP/HTTPS concurrentes: mínimo 100.000 solicitudes por segundo procesadas y analizadas con latencia añadida ≤ 10 ms.
- Protección de APIs: cobertura inicial para al menos 200 endpoints activos, con descubrimiento automático de nuevos endpoints.
- Usuarios concurrentes protegidos contra Account Takeover: mínimo 200.000 usuarios en servicios web y portales corporativos.

3.1.1.1 Capacidad y volumetría:

La solución debe proteger de manera integral frente a las principales amenazas de aplicaciones web, incluyendo vulnerabilidades del OWASP Top 10 y ataques de día cero, mediante un enfoque que combine firmas, validación y detección basada en aprendizaje automático.

Requisitos mínimos:

- Protección contra OWASP Top 10 (XSS, SQL Injection, CSRF, etc.).
- Detección de anomalías con machine learning para amenazas desconocidas.
- Validación de parámetros de entrada.
- Seguridad de cookies (firmado y protección contra envenenamiento).
- Análisis de archivos cargados (tipo, tamaño, malware, troyanos).
- Prevención de fuga de información en cabeceras y errores.

3.1.1.2 Protección de APIs

Dado el protagonismo de las APIs en arquitecturas modernas, el servicio deberá incorporar protección avanzada para interfaces REST, JSON, XML y OpenAPI, con descubrimiento automático de endpoints y validación de esquemas.



Requisitos mínimos:

- Descubrimiento automático de endpoints de API.
- Compatibilidad con OpenAPI 3.0, JSON y XML.
- Validación de esquemas y estructuras de datos.
- Soporte para tokens JWT en APIs móviles.
- API Gateway integrado con control de acceso, gestión de claves y limitación de solicitudes.

3.1.1.3 Seguridad del Cliente

El servicio debe incluir mecanismos para prevenir ataques que afecten directamente a la interacción del usuario con la aplicación, protegiendo tanto el navegador como las sesiones de usuario frente a amenazas avanzadas.

Requisitos mínimos:

- Protección contra ataques CSRF mediante tokens únicos por sesión.
- Defensa frente a MITB (ofuscación, cifrado, anti-keylogger, control AJAX).
- Control de acceso y limitación de solicitudes por cliente.
- Detección y protección contra robo de cuentas (account takeover).

3.1.1.4 Defensa contra Bots

El servicio deberá contar con capacidades inteligentes de defensa frente a bots, diferenciando el tráfico legítimo de motores de búsqueda de las actividades automatizadas maliciosas, aplicando contramedidas proactivas.

Requisitos mínimos:

- Mitigación de bots mediante machine learning.
- Verificación biométrica de interacción (ratón, teclado, scroll).
- Detección basada en umbrales de comportamiento.
- Distinción entre bots legítimos y maliciosos.
- Técnicas de engaño (bot deception) para identificación de crawlers.

3.1.1.5 Protección Adicional

Además de la seguridad de aplicaciones y APIs, el servicio debe incluir medidas adicionales que garanticen la continuidad del negocio y la optimización del rendimiento de las aplicaciones.

Requisitos mínimos:

- Bloqueo por reputación de IPs, listas blancas/negras y geolocalización (GeoIP).
- CDN integrado para optimización de entrega de contenido.



- Actualizaciones automáticas de seguridad.

3.1.1.6 Analítica y Visibilidad

La solución debe proporcionar herramientas de analítica avanzadas que permitan correlacionar incidentes y reducir falsos positivos, además de ofrecer visibilidad en tiempo real de los ataques y recomendaciones de mejora.

Requisitos mínimos:

- Threat Analytics con machine learning.
- Consola de incidentes con detalle de ataques y fuentes.
- Panel de Insights con recomendaciones de seguridad.
- Exportación de logs de ataques y tráfico a sistemas externos (SIEM, almacenamiento).

3.2 Firewall de segundo nivel

3.2.1 Equipamiento

Lantik dispone actualmente de un clúster de firewalls de segundo nivel basado en appliances de Check Point en arquitectura activo-pasivo, con cada nodo ubicado en uno de los dos CPDs. Estos dispositivos constituyen la segunda barrera de seguridad, que junto con la barrera perimetral delimita y protege la zona desmilitarizada (DMZ). Los equipos dispondrán de suscripción y soporte hasta el 30 de junio de 2027. Dado el papel crítico que desempeñan en la arquitectura de seguridad y la proximidad del fin de soporte, se considera necesario planificar y ejecutar la sustitución de ambos dispositivos por nuevos equipos que garanticen la continuidad operativa, la compatibilidad con las tecnologías de seguridad actuales y futuras, y el alineamiento con el modelo de red basado en SASE y SD-WAN.

Siguiendo la recomendación que cita el ENS en el Anexo II – Medidas de seguridad, bajo la categoría "Protección de las comunicaciones", en la medida COM-04, se recomienda disponer de distintos niveles de filtrado y protección, preferiblemente implementados con tecnologías de distintos fabricantes, con el objetivo de aumentar la eficacia frente a ataques que puedan explotar vulnerabilidades específicas de un determinado producto o fabricante.

Según esta recomendación de motor de diferente fabricante en los distintos niveles de filtrado, y la existencia en Lantik de una capa perimetral de fabricante Fortinet y Cisco, los firewalls ofertados NO podrán ser de dichos fabricantes para este entorno.

3.2.2 Características hardware mínimas de los equipos

Se desea adquirir 2 appliances físicos de firewall empresarial NGFW, cada uno de los cuales cumplirá los siguientes requisitos mínimos:

- 12 puertos RJ-45 1G/2.5G/5G/10G
- 10 puertos SFP/SFP+ 1G/10G
- 4 puertos SFP28 25G
- 2 puertos QSFP/QSFP28 40G/100G



- 1U de altura en rack
- SSD de 480 GB para sistema, configuración y logs
- Puertos dedicados para gestión y consola
- Interfaces dedicados para HA (sin uso de puertos de servicio)
- Arquitectura hardware separada entre plano de control y plano de datos
- Fuentes de alimentación redundadas hot-swap
- Flujo de aire front-to-back
- Configuración en HA activa/activa o activa/pasiva
- Throughput en tráfico real con App-ID, servicios de seguridad habilitados y logging: 15 Gbps
- Throughput con App-ID y logging activado: 29 Gbps
- 240.000 nuevas sesiones por segundo
- 2.500.000 sesiones concurrentes
- Al menos 1 sistema virtual incluido, ampliable hasta 11 con licencia

3.2.3 Características de red

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.
 - Y 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
- Soporte de protocolos dinámicos de routing RIP, OSPF y BGP4 así como routing estático.
- Soporte de DHCP, NAT y PAT.
- Soporte de monitorización SNMP v2, v3 y netflow..
- 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”

3.2.4 Identificación e integración de usuarios

Los equipos ofertados incluirán 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 por IP.
- Integración con sistemas de directorios para obtención de usuarios y grupos, incluyendo Microsoft Active Directory.
- Posibilidad de integración con sistemas multiusuario como 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.

3.2.5 Características generales de seguridad

Los equipos ofertados incluirán 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 procesamiento 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.
- Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 5100 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.
- 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 entrenados en la nube para proporcionar protección en tiempo real de amenazas desconocidas, URLs maliciosas, DNS, y seguridad IoT.
- Integrar machine learning (ML) en el núcleo del firewall para poder proporcionar una prevención de ataques sin firma internos para los ataques basados en archivos.



3.2.6 Motor de routing avanzado

Los equipos deben cumplir las siguientes características:

- Disponer de un motor avanzado de routing, que simplifique las operaciones con configuraciones basados en estándar similar al utilizado por otros fabricantes de routers.
- Permitir la configuración de perfiles para cada protocolo y el filtrado granular de cada perfil para multiples routers lógicos y sistemas virtuales.
- Permitir la redistribución de rutas con perfiles de redistribución.
- Permitir grupos de peers BGP y peers BGP que hereden configuraciones.
- 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.

3.2.7 Protección ante vulnerabilidades

Los equipos 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:

- 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 poder 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.
- Capacidad de creación de firmas de IPS a partir de la información de una firma de Snort, y que se permita importar de manera automática, un listado de reglas de Snort.
- Soporte en línea de Deep Learning y análisis en la nube.
- Prevención de Command and Control desconocido basado en Machine Learning desde la nube.

3.2.8 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.
- 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 loCs maliciosos, y permita automatizar la denegación del tráfico hacia/desde estos loCs en la política del firewall.
- Se requerirá que el fabricante ofrezca listas de IPs 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 web 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 poder configurar filtrado de URL multicategoría, esto es categorizar una URL con hasta 4 categorías, en función de su contenido, del dominio al que pertenecen etc y así poder definir políticas que permitan el acceso, pero limiten las posibilidades de navegación...
- Se deberá dotar a los equipos de modelos de Machine Learning 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 en 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.

3.2.9 Antivirus

Los equipos 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 al equipo las acciones oportunas.
- Los equipos 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 que permitan identificar muestras maliciosas desconocidas en tiempo real.

3.2.10 Bloqueo de ficheros y datos sensibles

- Los equipos propuestos deben tener la capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo, permitiendo al menos 100 tipos de ficheros identificables.
- Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.



- Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.
- Los equipos deben tener la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito, DNIs, etc. de forma que se evite la exfiltración de este tipo de datos.

3.2.11 Tecnología de Sandboxing

Los equipos 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 firewall se aprovechará, 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 10 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.

3.2.12 Seguridad en DNS

- Los equipos 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.
- Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).

3.2.13 Funciones SDWAN

En cumplimiento de la medida COM-04 del Esquema Nacional de Seguridad (ENS), que indica utilizar tecnologías de distintos fabricantes en los diferentes niveles de filtrado, los firewalls de segundo nivel no podrán ser del fabricante Fortinet, ya que la primera barrera perimetral de Lantik está basada en este fabricante. En caso de que la solución SD-WAN propuesta sea de Fortinet, el hub concentrador de túneles IPsec será el firewall perimetral FortiGate 3000F, sin que se admita la incorporación de un segundo concentrador de ese mismo fabricante en la segunda barrera.

Por el contrario, si se propone un fabricante distinto a Fortinet para la solución SD-WAN, el fabricante del firewall de segundo nivel deberá coincidir con el de la SD-WAN, y será este quien actúe como hub concentrador IPsec. En este caso, el concentrador deberá contar con los siguientes requisitos:

- Optimización de enlaces: Debe ofrecer capacidades de optimización del rendimiento del tráfico, incluyendo selección dinámica de rutas y priorización de tráfico.
- Soporte para redes híbridas: El sistema debe ser capaz de integrar múltiples tipos de conexiones WAN, incluyendo MPLS, Internet, LTE, y conexiones de fibra.
- Soporte para túneles IPsec: La solución debe ser capaz de establecer túneles IPsec entre sitios de manera segura, con soporte para cifrado y autenticación robustos, incluyendo autenticación post-cuántica con claves PPKs RFC 8784.
- Centralización en la gestión de políticas: Debe existir un sistema centralizado para la configuración y gestión de políticas de tráfico, permitiendo el control granular sobre el comportamiento de la red.
- Visibilidad de tráfico: La solución debe permitir monitoreo en tiempo real y proporcionar métricas detalladas sobre el rendimiento de la red, incluyendo latencia, disponibilidad y rendimiento de las aplicaciones.
- Seguridad de red integrada: El SD-WAN debe integrar capacidades de Next-Generation Firewall (NGFW), como inspección profunda de paquetes, prevención de intrusiones (IPS), y protección contra amenazas avanzadas.
- Redundancia de enlaces: Debe soportar la gestión de enlaces múltiples, tanto para la conectividad a Internet como MPLS, garantizando que el tráfico se desvíe automáticamente en caso de fallo de enlace.
- Control de la latencia y el jitter: La solución debe poder monitorizar la latencia y el jitter en tiempo real, y optimizar el tráfico en función de estos parámetros para garantizar un rendimiento consistente.
- Soporte para QoS: Debe permitir la priorización de aplicaciones críticas, como VoIP y videoconferencias, mediante políticas de Calidad de Servicio (QoS) configurables.



- Dashboards personalizados: Los usuarios deben poder personalizar dashboards de monitoreo para obtener visibilidad sobre el tráfico de la red, la seguridad y el rendimiento en tiempo real.
- Alertas y notificaciones: La solución debe ofrecer alertas personalizables sobre eventos críticos de seguridad o desempeño, como la caída de enlaces o la detección de actividades sospechosas.
- Reporting detallado: Debe generar informes detallados y fáciles de interpretar, sobre el tráfico de la red, el cumplimiento de las políticas, las amenazas detectadas y la disponibilidad de los enlaces.

3.2.14 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: sólo acceso web, acceso a aplicaciones específicas, a equipos, etc.

Se diferencia 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. a. La configuración de dichas VPN deberá soportar intercambio de claves precompartidas (PPK) post-cuánticas con posibilidad de agregar más de 5 PPK post cuánticos (PQ) a cada VPN IKEv2. Deberá ser compatible con los estándares RFC-8784, RFC-9242 y RFC-9370.

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:

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

3.2.15 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 del fabricante con objeto de mantener dichos logs a largo plazo.

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

- 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.
- Los logs de los datacenters deben almacenarse local e igualmente tener la capacidad de enviar esos logs a un entorno en nube del fabricante para su análisis.
- Los logs deberán contener al menos (tráfico, threats, URL, DNS, logs del sistema, etc..)



- El historial de almacenamiento de logs en la nube no será inferior a 1 año.
- Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecerían dentro de sus fronteras.

3.2.16 Consola de gestión centralizada

- La consola de gestión deberá estar ubicada en la nube con soporte íntegro del fabricante.
- 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.
- 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 y solución de SASE, para reducir los costes de operación y la curva de aprendizaje.
- Deberá permitir la gestión íntegra de la configuración de todo el parque de firewalls ofertados.
- Deberá permitir la gestión de la solución SASE con la posibilidad de realizar reglas que sean aplicadas a distintos entornos, ya sean firewalls o dicha solución SASE con el fin de no duplicar configuraciones y así evitar misconfig.
- Los logs de los firewalls deben almacenarse en la nube para una gestión más eficiente y deberán disponer de al menos de un histórico de 1 año de antigüedad.
- 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 con el fin de facilitarnos la causa raíz del incidente.
- 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.
- Gestión de la configuración indicando BPA (Best Practice Assessment) en todo momento.
- Dashboards que indiquen el grado de cumplimiento y adopción de la seguridad para identificar el grado de madurez de la configuración.
- Sistema de posture con reglas predefinidas y creación de reglas personalizables con posibilidad de bloqueo de configuraciones antes de aplicarse en los firewalls.
- Programación de upgrades de los firewalls y definir un scope para dicha programación.
- Posibilidad de crear reglas de notificación según la severidad de la alerta.
- Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecerían dentro de sus fronteras.
- Posibilidad de administrar los equipos físicos sin necesidad de utilizar una consola de gestión adicional.

3.2.17 Cumplimiento de estándares

El equipamiento ofertado para el firewall de segundo nivel cumplirá, como mínimo, con los siguientes estándares y certificaciones:



- Directiva de Baja Tensión (Low Voltage Directive 2014/35/EU)
- Directiva EMC (2014/30/EU)
- Directiva RoHS (2011/65/EU)
- Certificación Common Criteria
- Inclusión en guías CCN-STIC (ENS) de productos cualificados

Se deberá adjuntar documentación acreditativa correspondiente.

3.3 Solución SD-WAN

Según se explica en el apartado 3.2 Firewall de segundo nivel, teniendo en cuenta que la primera barrera perimetral de Lantik está basada en tecnología Fortinet (FortiGate 3000F), se establece que los firewalls de segundo nivel no podrán ser de dicho fabricante.

A partir de esta condición, se definen dos escenarios posibles para la solución SD-WAN:

- **Escenario 1:** Si la solución SD-WAN ofertada está basada en tecnología Fortinet, el concentrador de túneles IPsec deberá ser el propio firewall perimetral FortiGate 3000F existente. En este caso, no se podrá desplegar un concentrador SD-WAN adicional basado en Fortinet en la segunda barrera porque supondría un incumplimiento del ENS.

En este escenario la solución deberá incluir todas las suscripciones necesarias para habilitar en los equipos perimetrales FortiGate 3000F la funcionalidad de hub concentrador de la solución SD-WAN, garantizando el soporte oficial del fabricante y la plena compatibilidad con los equipos desplegados en las sedes remotas.

- **Escenario 2:** Si la solución SD-WAN propuesta esté basada en un fabricante distinto a Fortinet, se requerirá que el fabricante elegido para la sustitución del clúster de firewalls de segundo nivel sea el mismo que el de la solución SD-WAN. Esta condición tiene como objetivo garantizar la compatibilidad técnica en el establecimiento de los túneles Ipsec y unificar la tecnología empleada en ambos extremos del proceso de cifrado.

La solución SD-WAN ofertada deberá estar basada en equipamiento hardware dedicado, de manera que el servicio se preste sobre dispositivos físicos que dispongan de funcionalidades de tecnología SD-WAN. No se admitirán soluciones que se implementen únicamente en modalidad software o virtualizada. El adjudicatario deberá garantizar que el equipamiento proporcionado es de nueva fabricación, cuenta con soporte oficial del fabricante.

3.3.1 Requerimientos técnicos

El adjudicatario deberá desplegar una solución SD-WAN bajo modelo gestionado y pago por uso, adaptada a las necesidades de interconexión y optimización de tráfico entre sedes, CPDs e Internet. La solución incluirá:

- **Optimización de enlaces:** Debe ofrecer capacidades de optimización del rendimiento del tráfico, incluyendo selección dinámica de rutas y priorización de tráfico.
- **Soporte para redes híbridas:** El sistema debe ser capaz de integrar múltiples tipos de conexiones WAN, incluyendo MPLS, Internet, LTE, y conexiones de fibra.



- **Soporte para túneles IPsec:** La solución debe ser capaz de establecer túneles IPsec entre sitios de manera segura, con soporte para cifrado y autenticación robustos, incluyendo autenticación post -cuántica con claves PPKs RFC 8784.
- **Centralización en la gestión de políticas:** Debe existir un sistema centralizado para la configuración y gestión de políticas de tráfico, permitiendo el control granular sobre el comportamiento de la red.
- **Visibilidad de tráfico:** La solución debe permitir monitoreo en tiempo real y proporcionar métricas detalladas sobre el rendimiento de la red, incluyendo latencia, disponibilidad y rendimiento de las aplicaciones.
- **Seguridad de red integrada:** El SD-WAN debe integrar capacidades de Next-Generation Firewall (NGFW), como inspección profunda de paquetes, prevención de intrusiones (IPS), y protección contra amenazas avanzadas.
- **Redundancia de enlaces:** Debe soportar la gestión de enlaces múltiples, tanto para la conectividad a Internet como MPLS, garantizando que el tráfico se desvíe automáticamente en caso de fallo de enlace.
- **Control de la latencia y el jitter:** La solución debe poder monitorizar la latencia y el jitter en tiempo real, y optimizar el tráfico en función de estos parámetros para garantizar un rendimiento consistente.
- **Soporte para QoS:** Debe permitir la priorización de aplicaciones críticas, como VoIP y videoconferencias, mediante políticas de Calidad de Servicio (QoS) configurables.
- **Dashboards personalizados:** Los usuarios deben poder personalizar dashboards de monitoreo para obtener visibilidad sobre el tráfico de la red, la seguridad y el rendimiento en tiempo real.
- **Alertas y notificaciones:** La solución debe ofrecer alertas personalizables sobre eventos críticos de seguridad o desempeño, como la caída de enlaces o la detección de actividades sospechosas.
- **Reporting detallado:** Debe generar informes detallados y fáciles de interpretar, sobre el tráfico de la red, el cumplimiento de las políticas, las amenazas detectadas y la disponibilidad de los enlaces.
- **Monitorización:** Soporte de monitorización SNMP v2, v3 y netflow.
- **Consola de gestión centralizada:** la consola de gestión deberá ser única y estar centralizada para SD-WAN y SASE (al menos en la parte de políticas de seguridad) incluyendo todas las funcionalidades descritas sobre la misma.

3.3.2 Requerimientos de hardware

Los equipos de hardware que soporten la solución SD-WAN deberán cumplir, como mínimo, con las siguientes características:

- 7 puertos RJ-45 10/100/1000Mbps
- Puerto dedicado para gestión.
- Puerto de consola RJ45.
- Posibilidad de configuración en HA (A/P)
- Recursos hardware 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.
- Prestaciones o capacidad del firewall con la identificación de aplicaciones habilitada (es decir, trabajando a nivel 7 para todo el tráfico) Appmix y logging habilitado: 1.4 Gbps



- Prestaciones o capacidad con identificación de aplicación, con todos los servicios de seguridad habilitados, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, File Blocking, etc) como frente a amenazas desconocidas (Sandboxing) y Logging habilitado medidos en transacciones APPMix: 0.8 Gbps
- Nuevas sesiones por segundo: 11.000
- Número de sesiones totales: 64.000

3.3.3 Requerimientos de seguridad

3.3.3.1 Protección ante vulnerabilidades

Los equipos 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:

- En la protección ante vulnerabilidades se deberán usar criterios basados en la identificación tanto de la aplicación o en el sistema operativo, aplicando perfiles ajustados a cada caso sin afectar al rendimiento de los equipos.
- 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 poder 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 o sistema operativo 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.
- Capacidad de creación de firmas de IPS a partir de la información de una firma de Snort, y que se permita importar de manera automática, un listado de reglas de Snort.

3.3.3.2 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.
- 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 requerirá que el fabricante ofrezca listas de IPs 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 web que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales en función de las categorías de web visitadas.
- 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.

3.3.3.3 Antivirus

Los equipos 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 al equipo las acciones oportunas.
- Los equipos 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.

3.3.3.4 Bloqueo de ficheros y datos sensibles

- Los equipos propuestos deben tener la capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo, permitiendo al menos 100 tipos de ficheros identificables.
- Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.
- Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.
- Los equipos deben tener la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito, DNIs, etc. de forma que se evite la exfiltración de este tipo de datos.

3.3.3.5 Tecnología de Sandboxing

Los equipos 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 firewall se aprovechará, 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 10 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.

3.3.3.6 Seguridad en DNS

- Los equipos 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.
- Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).



3.3.4 Tipología de sedes existentes

A efectos de valoración económica, pero no vinculante, y conforme al modelo de pago por uso requerido para la solución SD-WAN, se establece la siguiente clasificación de sedes según el tramo de usuarios concurrentes. Esta tabla refleja la distribución actual de las sedes gestionadas por Lantik:

Tipo de sede	Rango de usuarios	Threat Protection Throughput mínimo	Nº de sedes
A	Hasta 20	750 Mbps	45
B	21-100	1 Gbps	63
C	Más de 100	2 Gbps	5

3.4 Solución SASE

La solución SASE deberá ser cloud-native, multi-tenant y estar basada en el mismo fabricante que la solución SD-WAN definida en el apartado 3.3 (Solución de SD-WAN), con el fin de garantizar una integración plena entre conectividad y seguridad. Esta unificación tecnológica permitirá:

- **Gestión centralizada** de políticas de seguridad desde una única consola, evitando duplicidades y reduciendo errores operativos.
- **Visibilidad unificada** del tráfico, tanto de usuarios como de sedes y aplicaciones, lo que facilita la correlación de eventos de seguridad y el diagnóstico de incidencias.
- **Compatibilidad nativa** entre los componentes de conectividad y seguridad, reduciendo riesgos de interoperabilidad y asegurando que las funcionalidades avanzadas (ZTNA, SWG, FWaaS, CASB, etc.) operen de forma consistente.
- **Simplificación operativa y reducción de costes**, al minimizar la necesidad de integraciones adicionales entre soluciones de distintos fabricantes.
- **Mayor resiliencia y trazabilidad**, al contar con una arquitectura homogénea que facilita la aplicación coherente de medidas de seguridad y la adaptación a futuros escenarios tecnológicos.
- Evaluación de riesgos de **cumplimiento normativo** (GDPR, PCI, SOC2, ISO, etc.)

El uso de fabricantes distintos para SASE y SD-WAN introduciría capas adicionales de complejidad, posibles incompatibilidades y pérdida de visibilidad, lo que va en contra de los principios de seguridad integrada, operación eficiente y continuidad de servicio que persigue este proyecto.

La propuesta deberá incluir como mínimo un bundle base de funcionalidades obligatorias, contemplar ampliaciones bajo demanda (usuarios y caudal), y ofrecer la posibilidad de incorporar funcionalidades adicionales mediante licencias complementarias (add-ons).



3.4.1 Bundle base obligatorio

La solución SASE deberá incluir de forma nativa y sin coste adicional los siguientes componentes, debidamente licenciados para el número de usuarios iniciales requerido por Lantik:

3.4.1.1 Zero Trust Network Access (ZTNA)

- Posibilidad de aplicar las mismas capacidades de seguridad para protección del tráfico de navegación y para protección del acceso a aplicaciones o recursos privados
- No limitación del acceso a un número determinado de aplicaciones privadas. Debe permitirse el acceso a tantas aplicaciones privadas como se estimen oportunas en cada momento.
- Posibilidad del uso de aplicaciones en las que la comunicación se inicia desde el CPD hacia el cliente, por ejemplo, aplicaciones de help-desk remoto, FTP activo o Voz sobre IP
- Para una mejor visibilidad y trazabilidad, la solución propuesta no debe hacer NAT del tráfico de los usuarios que acceden a las aplicaciones o recursos privados, de tal forma que estos vean la IP origen de los usuarios o dar trazabilidad por ID de usuario.
- Acceso seguro basado en identidad para aplicaciones privadas, sin necesidad de VPN tradicional.
- Capacidad de aplicar políticas de acceso condicional basadas en identidad, dispositivo, ubicación y nivel de riesgo.
- Autenticación multifactor (MFA).

3.4.1.2 Firewall-as-a-Service (FWaaS)

- Inspección de tráfico a nivel de capa 7 (aplicación) para todo el tráfico entrante y saliente.
- Reglas basadas en aplicaciones, usuarios/grupos y contenidos. Estas reglas deberán poder ser configurables con perfiles de seguridad.

3.4.1.3 Secure Web Gateway (SWG)

- Protección contra amenazas web en tiempo real (malware, phishing, URLs maliciosas).
- Control granular del uso de aplicaciones web y redes sociales.
- Capacidad de aplicar políticas de navegación seguras y filtrado de contenido.

3.4.1.4 Cloud Access Security Broker (CASB)

La solución deberá incluir al menos la modalidad inline como parte del bundle base, y opcionalmente permitir su ampliación con add-ons (CASB API y SSPM). En su modalidad inline, deberá garantizar:

- Descubrimiento y control de aplicaciones SaaS (Shadow IT).
- Identificación de al menos 80.000 aplicaciones SaaS, clasificadas por tipo y riesgo.
- Políticas de control para el uso de aplicaciones cloud (ej. subida/descarga de ficheros).

3.4.1.5 Funcionalidad SD-WAN integrada

La solución deberá contar con capacidades nativas de SD-WAN, sin necesidad de licencias adicionales, incluyendo:

- Establecimiento seguro de túneles entre sedes y la nube SASE.
- Balanceo inteligente de tráfico y selección dinámica de rutas.



- Optimización de la experiencia de usuario mediante monitorización en tiempo real de latencia, pérdida y jitter.

3.4.2 Arquitectura general

- La solución debe estar basada en una arquitectura cloud-native y multi-tenant, permitiendo alta disponibilidad y escalabilidad.
- La solución debe estar preparada para realizar ampliaciones bajo demanda, tanto en ancho de banda como en número de usuario.
- Debe ofrecer una consola centralizada para la administración de políticas, visibilidad y monitoreo.
- Deberá estar preparada para soportar todos los casos de uso, incluyendo ZTNA, SWG, FWaaS, CASB, DLP, SSPM, SD-WAN, etc.
- Mismas capacidades de seguridad tanto en navegación como en acceso a aplicaciones privadas incluyendo protección avanzada ante amenazas, Sandbox, IPS/IDS, Antivirus, Seguridad DNS, Filtrado avanzado de URLs.
- Múltiples opciones de acceso de usuarios: mediante agente, a través de proxy (archivo .pac), desde sedes, con dispositivos gestionados o no gestionados.
- Múltiples opciones de acceso a las aplicaciones privadas: que las aplicaciones puedan ver la dirección IP de los usuarios (normativa, trazabilidad) o que las aplicaciones no puedan ver la dirección IP origen de los usuarios.
- Control del uso de aplicaciones SaaS corporativas (compartición de archivos, descarga, subida, etc.)
- Detección de actividad de riesgo de los usuarios.
- Recursos dedicados, únicamente disponibles y siempre disponibles para su uso por Lantik.
- Recursos dedicados, sin compartir el plano de datos con terceros.
- La solución propuesta debe ofrecer direccionamiento IP público dedicado para Lantik, sin necesidad de configuraciones adicionales y aplicado directamente en la nube SASE al tráfico que se envía a Internet.
- Para mayor disponibilidad, una solución que permita desplegar la infraestructura SASE en 2 o más proveedores diferentes de nube pública.
- SLA de disponibilidad no menor a 99'999%.
- Comprometer un máximo 10 milisegundos para descifrado, inspección de seguridad y cifrado del tráfico, tanto para la navegación segura como para el acceso a aplicaciones privadas, en la descripción pública de sus niveles de servicio o bajo un NDA.
- Para mayor seguridad y para evitar fluctuaciones de rendimiento, el tránsito entre regiones/zonas/PoPs debe ser a través de internet si no a través de redes privadas. De tal forma que, si un usuario se conecta al PoP1 para acceder a un recurso que está conectado al PoP2, el tráfico entre PoP1 y PoP2 no pase por internet.
- La solución debe constar como mínimo de 1 PoP (puntos de presencia) en territorio español en modalidad de alta disponibilidad, de forma que cualquier contingencia en cada uno de los PoP sea cubierta de forma transparente y sin intervención necesaria por parte de un operador sin afectar al servicio.
- Separación de los planos de gestión, control y datos de tal forma que una indisponibilidad del plano de gestión no afecta al funcionamiento de usuarios conectados ni de usuarios, previamente aprovisionados, que quieran establecer una nueva conexión durante el período de indisponibilidad del plano de gestión.



- Capacidad de multitenant, pudiendo crear y administrar múltiples tenants desde la consola única de gestión. Cada tenant debe tener infraestructura dedicada e independiente de los otros tenants y direccionamiento IP público dedicado por tenant y diferente entre tenants

3.4.3 Requerimientos de gestión y visibilidad

La solución deberá acompañarse de una consola unificada en nube para gestionar y monitorizar las soluciones de SASE y SD-WAN. Las funcionalidades requeridas son las siguientes:

- Consola para monitoreo de eventos, políticas y tráfico de red.
- Consola de gestión desde la que configurar, monitorizar y mantener los casos de uso SASE principales, incluyendo expresamente Proxy en la nube, SWG, FWaaS, ZTNA, SD-WAN, CASB en línea).
- Consolidación de los logs en un punto común en nube de fabricante, al menos para las funcionalidades de navegación en internet y acceso a aplicaciones privadas. En ambos casos (navegación y acceso a recursos privados) la solución debe correlacionar automáticamente los logs relativos a una misma sesión, es decir, si para una sesión el tráfico pasa por el servicio de proxy o de firewall, por inspección de URL y por inspección de amenazas, tales logs deben correlacionarse automáticamente para simplificar el análisis de un posible problema o incidente de seguridad. El histórico de los logs no deberá ser inferior a una retención de 1 año, incluida en la oferta.
- Permitir configurar distintos tipos de autenticación para diferentes propósitos, estableciendo un orden de prioridad entre ellos, de tal forma que se compruebe cada tipo de autenticación en función de su orden de prioridad hasta que uno de ellos autentique correctamente al usuario. Mínimamente tiene que estar soportado autenticaciones contra AD, SamL y OIDC.
- Capacidad de evaluar la configuración e identificar áreas de mejora, incluyendo la detección de objetos configurados pero que no se están usando, la detección de reglas configuradas pero que no se están usando o la presencia de reglas demasiado permisivas.
- Deberá permitir la gestión de la solución SASE con la posibilidad de realizar reglas que sean aplicadas a distintos entornos, ya sean firewalls o dicha solución SASE con el fin de no duplicar configuraciones y así evitar misconfig.
- Los logs de los firewalls deben almacenarse en la nube para una gestión más eficiente y deberán disponer de al menos de un histórico de 1 año de antigüedad.
- Evaluar la configuración de la consola 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, RAM con el fin de facilitarnos la causa raíz del incidente así como posibles caídas de los nodos de SASE.
- 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.
- Gestión de la configuración indicando BPA (Best Practice Assessment) en todo momento.
- Dashboards que indiquen el grado de cumplimiento y adopción de la seguridad para identificar el grado de madurez de la configuración.
- Programación de upgrades de los firewalls y definir un scope para dicha programación.
- Posibilidad de crear reglas de notificación según la severidad de la alerta.



- Informes detallados sobre uso de aplicaciones, cumplimiento y seguridad.
- Soporte para integración con SIEM, SOAR y herramientas de terceros.
- Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecerían dentro de sus fronteras.

3.4.4 Requerimientos de seguridad y cumplimiento

La solución propuesta deberá disponer de las funcionalidades de seguridad igual o superiores que las descritas para el punto 4.3 “Solución SD-WAN”. Deberá ofrecer:

- Las mismas capacidades de seguridad en la navegación segura y en el acceso a apps privadas
- Las firmas creadas en base al contenido malicioso del archivo (payload) y no simplemente en base a hashes del archivo
- Capacidad de detonar archivos Mac OS X y Android .apk
- Una funcionalidad de Sandbox capaz de inspeccionar tanto archivos descargados desde (inbound) como archivos subidos (outbound) a servidores, ya sean servidores internos o sitios públicos en Internet
- Capacidades de seguridad DNS capaces de detectar al menos las siguientes amenazas: dominios estratégicamente envejecidos, ataques de CNAME cloaking, detección de la reputación de subdominios, detección de dominios almacenados (stockpiled domains), ataques de tunelización DNS ultra-lenta (ultra-slow DNS tunneling), ataques NXNS (NXNSAttack), ataques de dangling DNS.
- Funcionalidades de seguridad basadas en soluciones propias, no en acuerdos de reventa de terceras soluciones (acuerdos OEM) ni en soluciones opensource
- La capacidad de detectar la aplicación a nivel 7 independientemente del puerto de nivel 4 por el que aplicación se comunica, tanto en la navegación como en el acceso a aplicaciones privadas
- Poder forzar un cambio dinámico de políticas aplicadas si, una vez establecida la sesión, se modifica la postura de seguridad del dispositivo. Este cambio dinámico de políticas debe estar disponible tanto para la navegación a internet como para el acceso a aplicaciones privadas
- Capacidad de detectar y detener 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
- Capacidad de RBI, entregadas desde la misma nube SASE que el resto de los casos de uso y gestionadas desde la misma consola común.
- Auditoría completa de actividades administrativas y de usuario.

3.4.4.1 Protección ante vulnerabilidades

Los equipos 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:



- 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 poder 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.
- Soporte en línea de Deep Learning y análisis en la nube.
- Prevención de Command and Control desconocido basado en Machine Learning desde la nube.

3.4.4.2 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.
- 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 requerirá que el fabricante ofrezca listas de IPs 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 poder configurar filtrado de URL multicategoría, esto es categorizar una URL con hasta 4 categorías, en función de su contenido, del dominio al que pertenecen etc y así poder definir políticas que permitan el acceso, pero limiten las posibilidades de navegación...
- Se deberá dotar a los equipos de modelos de Machine Learning 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 en 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.



3.4.4.3 Antivirus

Los equipos 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 al equipo las acciones oportunas.
- La infraestructura debe 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 que permitan identificar muestras maliciosas desconocidas en tiempo real.

3.4.4.4 Tecnología de Sandboxing

La infraestructura propuesta debe 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.
- La infraestructura se aprovechará, 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 10 minutos, también lo desconocido sea convertido en conocido en el contexto de protección en el puesto.
- La infraestructura debe 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 detección 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.

3.4.4.5 Seguridad en DNS

- La infraestructura propuesta 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.
- Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).

3.4.5 Requisitos Técnicos y Operativos

- Alta disponibilidad garantizada (SLA de al menos 99.999%).
- Integración con proveedores de identidad (Azure AD).
- Soporte para dispositivos gestionados y no gestionados.
- Respecto de estos últimos:
 - Capacidades de protección del dato corporativo (DLP) con notificaciones a los usuarios (user coaching) en dispositivos no gestionados. Se acepta el uso de agentes ligeros o navegadores corporativos, pero no se acepta que el tráfico deba descifrarse.
 - Capacidad de mostrar enlaces personalizados (portal de aplicaciones), que pueden ser tanto de aplicaciones públicas como privadas, a las que tienen acceso los usuarios que se conectan desde dispositivos no gestionados. Se acepta el uso de agentes ligeros o navegadores corporativos.

3.4.6 Protecciones SASE sobre IA

La solución deberá contar con la posibilidad de activar capacidades de protección en el uso de herramientas de IA:

- **Detección** del uso de herramientas de IA en SaaS.
- **Clasificación y etiquetado** (categorización) del riesgo de herramientas de IA usadas.
- **Aplicación de reglas uso** (bloqueo, autorización condicionada y uso autorizado).



- **Reportes de uso:** informes o paneles de control con datos de uso de las herramientas de IA autorizadas y bloqueadas.

3.5 Servicio de implantación y migración

El servicio abarcará la planificación, diseño, coordinación, despliegue y puesta en marcha de la solución SASE y SD-WAN, la migración del clúster de firewalls de nivel 2 y la protección frente a ataques de denegación de servicio AntiDDoS de capa7.

Se regirá por los hitos/plazos definidos en el apartado “3.5.2. Fases del servicio”.

La empresa adjudicataria deberá aportar servicios profesionales propios y del fabricante, garantizando que el personal técnico asignado disponga de certificaciones de nivel avanzado o especialista emitidas por los fabricantes de las soluciones propuestas. Igualmente, se exigirá que el fabricante realice la fase inicial de los pilotos, con el objetivo de verificar la correcta instalación, parametrización y funcionamiento de la solución en el entorno de Lantik, así como su plena compatibilidad con la infraestructura existente. Los pilotos se darán por finalizados con el visto bueno de Lantik, quedando documentado en un informe conjunto fabricante-empresa adjudicataria cuya aprobación marcará el inicio del despliegue definitivo. A partir de ese momento, la empresa adjudicataria asumirá en exclusiva la responsabilidad de la implantación final de la solución, quedando este compromiso reflejado expresamente en la documentación técnica de la oferta.

Durante la fase de implantación y migración, se deberá nombrar un equipo de coordinación dedicado 100%, de al menos 3 personas de la empresa adjudicataria, el cual será responsable de la interlocución con Lantik para la correcta gestión, gobernanza y operativa de la fase de implantación y migración, así como cualquier tipo de necesidad que surja. En este equipo deberán estar representados, como mínimo, los siguientes roles: dirección, redes, seguridad, sistemas, observabilidad, soporte, etc. En este equipo, deberá existir, como mínimo, perfiles con experiencia mínima de 3 años en la gestión de servicios de seguridad y comunicaciones, formación técnica acreditada en ITIL u otras metodologías de gestión de servicios, así como certificaciones técnicas relevantes en las tecnologías ofertadas. Lantik establecerá la periodicidad de reuniones necesarias, en cada momento, con este equipo de coordinación.

Durante el avance de la implantación y migración, la empresa adjudicataria deberá garantizar que toda la telemetría, eventos, logs y métricas generadas se envíen e integren en el SOC actual de Lantik. Esta integración deberá realizarse en los formatos y canales que Lantik determine, de forma que se asegure su correcta ingesta, correlación y monitorización centralizada, conforme a los procedimientos y capacidades del SOC existente.

Durante la fase de implantación y migración, la empresa adjudicataria deberá garantizar la integración de las nuevas herramientas y soluciones con las plataformas corporativas.

La empresa oferente podrá solicitar por el cauce establecido la relación de plataformas y sistemas con los que integrarse con Lantik, S.A. M.P.



3.5.1 Horarios del servicio

Se establecen las siguientes necesidades:

- Horario
 - Invierno: de 7:00 a 17:00.
 - Verano (agosto): de 7:00 a 15:00.
 - Excepto días festivos en Bilbao y 24 y 31 de diciembre.
 - Por necesidades específicas de la implantación y migración de cada sede específica, la mayoría de las intervenciones planificadas se realizarán fuera del horario establecido previamente.
- Un número de teléfono móvil del servicio con disponibilidad 24x7x365.
- Tiempo de atención de cualquier incidencia ≤ 5 minutos.
- Resolución de incidencias con prioridad muy urgentes ≤ 30 minutos.
- Resolución de incidencias urgentes ≤ 4 horas.
- Resolución de incidencias normales ≤ 8 horas.

3.5.2 Fases del servicio.

La implantación y/o migración de las soluciones se organizará en fases sucesivas, cada una con actividades definidas e hitos con fecha límite, cuyo cumplimiento será validado por Lantik antes de avanzar a la siguiente. Estas fases podrán contemplar tanto escenarios de migración de servicios existentes como instalación de nuevas capacidades que no dispongan de una solución previa.

1. Análisis y diseño:

Alcance:

- Revisión detallada de la topología de red actual, políticas de seguridad existentes y requerimientos funcionales y operativos.
- Diseño de la arquitectura basada en las tecnologías solicitadas, alineada con las necesidades de conectividad segura y gestión centralizada.
- Elaboración del plan de migración, priorizando entornos con mayor exposición o vulnerabilidad.

Se establecerán los siguientes hitos y entregables:

- Hito 1: Servicio AntiDDoS: este servicio deberá quedar activado y puesto en marcha en un plazo inferior a 4 meses desde la firma del contrato.
- Hito 2: Plataforma de FW de 2º nivel: la plataforma deberá ser instalada, puesta en marcha y con las reglas/políticas actuales migradas antes del 30 de junio de 2027. Las tareas a realizar serán:
 - Configuración base de la solución en un entorno de pruebas controlado.
 - Planificación técnica para la sustitución del clúster de firewalls de nivel 2.



- Migración del clúster de firewalls de nivel 2, garantizando la continuidad del servicio mediante una transición controlada y validaciones de alta disponibilidad, tráfico y reglas de seguridad/políticas que existen actualmente en el entorno de producción.
- Hito 3: Transición bajo demanda de las sedes a tecnología SASE/SD-WAN:
 - La empresa adjudicataria dispondrá de 36 meses desde la firma de contrato para realizar dicha transición. Este plazo se subdividirá en:
 - Hito 3.1: Hasta un máximo de 6 meses desde inicio de contrato para realizar el Plan de proyecto (planificación detallada y cronograma) y diseño de la arquitectura y plan de migración (documento técnico validado por Lantik).
 - Hito 3.2: Tras el Hito 3.1 y hasta la fecha fin de contrato para la ejecución del proyecto de transición. Se realizarán las siguientes actividades:
 - Implantación progresiva de SASE/SD-WAN en ubicaciones críticas.
 - Ejecución de pruebas de conectividad, rendimiento y seguridad, generando evidencias documentadas que permitan comparar los resultados obtenidos con la plataforma anterior frente a la nueva solución implantada, de modo que se valide objetivamente la mejora en capacidad, disponibilidad y nivel de protección.

2. Devolución del servicio:

Alcance:

- Soporte técnico post-despliegue y estabilización.
- Transferencia de conocimiento y entrega de documentación técnica.
- Verificación de telemetría, eventos, métricas en el SOC de Lantik, integración con plataforma de observabilidad y monitorización, CMDB y herramientas de automatización y orquestación.
- Lantik será la responsable de dar el Visto Bueno final a la implantación.

La planificación detallada deberá ser validada por Lantik antes del inicio del despliegue, y deberá garantizarse la mínima afectación al servicio.

Lantik podrá ampliar los plazos máximos de los hitos mediante acuerdo expreso y motivado, en caso de concurrir causas internas de planificación, coordinación con otros proyectos corporativos o necesidades organizativas. Esta ampliación no supondrá derecho a compensación económica para la empresa adjudicataria.



3.5.3 Niveles de servicio – indicadores

Cada hito contará con un indicador de control:

- **Ind1:** Activación y validación del servicio AntiDDoS L7 $\leq$ 4 meses desde firma.
- **Ind2:** Migración del clúster de firewalls de nivel 2 finalizada y validada por Lantik $\leq$ 30/06/2027.
- **Ind3:** Entrega y validación del plan de proyecto (Diseño de la arquitectura y plan de migración) dentro de los 6 meses tras firma de contrato.
- **Ind4:** Implantación progresiva de SASE/SD-WAN validada en sedes prioritarias $\leq$ 18 meses tras entrega de plan de proyecto.
- **Ind5:** Integración completa en el SOC, monitorización/observabilidad y CMDB (logs, telemetría, métricas) $\leq$ 24 meses tras firma de contrato.
- **Ind6:** Entrega de documentación técnica y transferencia de conocimiento $\leq$ 36 meses tras firma de contrato.

3.6 Servicio gestionado de la solución

El servicio gestionado, que comenzará su servicio tras la primera implantación en producción objeto del contrato, constituye un modelo de provisión en el que la instalación, gestión, operación, resolución de incidencias, atención de peticiones y mantenimiento del equipamiento son responsabilidad de la empresa adjudicataria.

3.6.1 Metodología y planificación del servicio

La empresa adjudicataria deberá:

- Nombrar un equipo de coordinación dedicado 100%, de al menos 3 personas de la empresa adjudicataria, el cual será responsable de la interlocución con Lantik para la correcta gestión, gobernanza y operativa del servicio, así como cualquier tipo de necesidad que surja. En este equipo deberán estar representados, como mínimo, los siguientes roles: dirección, redes, seguridad, identidad, sistemas, observabilidad, soporte, etc. Este equipo, será responsable tanto de la coordinación operativa como del escalado de incidencias y la interlocución con el fabricante. En este equipo, deberá existir, como mínimo, perfiles con experiencia mínima de 3 años en la gestión de servicios de seguridad y comunicaciones, formación técnica acreditada en ITIL u otras metodologías de gestión de servicios, así como certificaciones técnicas relevantes en las tecnologías ofertadas. Lantik establecerá la periodicidad de reuniones necesarias, en cada momento, con este equipo de coordinación.
- Facilitar, como mínimo:
 - Un número de teléfono móvil y una dirección de correo electrónico en el siguiente horario:
 - Invierno: de 7:00 a 17:00.
 - Verano (agosto): de 7:00 a 15:00.
 - Excepto días festivos en Bilbao y 24 y 31 de diciembre.



- Por necesidades específicas de las operativas a realizar, pudiera ser necesario que alguna intervención se tuviera que realizar fuera del horario establecido previamente.
 - Un número de teléfono móvil del servicio con disponibilidad 24x7x365.
- Asegurar que el personal técnico adscrito a prestar el servicio mantenga un nivel de dedicación suficiente para garantizar el cumplimiento de los objetivos de calidad y los plazos acordados, debiendo la empresa adjudicataria acreditar dicha dedicación mediante informes periódicos de actividad, registro de horas y evidencias de los entregables realizados.
- Integrarse con las herramientas de gestión de incidencias/peticiones que determine Lantik, de manera que quede registro y se pueda calcular el grado de cumplimiento de los indicadores establecido en el apartado a continuación (3.6.2).
- Asegurar la prestación del servicio desde las dependencias de la empresa adjudicataria, garantizando la seguridad y confidencialidad de la información.
- Atender requerimientos de presencialidad: en caso necesario, el personal deberá acudir a Lantik, dependencias de la DFB u organismos forales en un plazo máximo de 1 hora desde el aviso. En caso de las dependencias de Bilbao, el plazo máximo es de 30 minutos.
- Mantener a su personal permanentemente formado en las tecnologías requeridas, siendo este coste asumido por la empresa adjudicataria.
- Realizar, como mínimo, una reunión mensual de seguimiento durante la primera semana de cada mes, aportando un informe detallado de las actuaciones del mes vencido y formalizando acta de la reunión.

3.6.2 Niveles de servicio – indicadores

Los tiempos se medirán desde la notificación de la incidencia o petición por parte de Lantik hasta el inicio de la resolución (*tiempo de atención*) y hasta la finalización de la misma (*tiempo de resolución*).

No computarán en los tiempos de resolución los retrasos atribuibles a:

- Solicitud de aprobación o información pendiente por parte de Lantik.
- Intervención de terceros ajenos a la adjudicataria.

Incidencias

- **Inc1:** Tiempo de atención de cualquier incidencia ≤ 5 minutos.
- **Inc2:** Resolución de incidencias con prioridad muy urgentes ≤ 30 minutos.
- **Inc3:** Resolución de incidencias urgentes ≤ 4 horas.
- **Inc4:** Resolución de incidencias normales ≤ 8 horas.
- **Inc5:** Disponibilidad del servicio de incidencias 24x7x365.

Peticiones de servicio

- **Inp6:** Tiempo de atención de cualquier petición ≤ 15 minutos.
- **Inp7:** Resolución de peticiones muy urgentes ≤ 1 hora.



- **Inp8:** Resolución de peticiones urgentes ≤ 8 horas.
- **Inp9:** Resolución de peticiones normales ≤ 16 horas.
- **Inp10:** Disponibilidad del servicio de peticiones 24x7x365.

Control adicional

- **Inp11:** Realización de reunión mensual de seguimiento con entrega de informe.

Lantik se reserva el derecho, de común acuerdo con la empresa adjudicataria, de modificar los SLA establecidos, incluso para una incidencia o petición concreta.

La empresa adjudicataria deberá identificar y analizar problemas raíz cuando varias incidencias deriven de una misma causa.

Toda actuación deberá quedar registrada en las herramientas de gestión definidas por Lantik.

El grado de cumplimiento de los indicadores servirá como base para la aplicación de penalizaciones, en su caso.

3.6.3 Tareas específicas del servicio gestionado

La empresa adjudicataria deberá asumir, entre otras, las siguientes funciones

- **Funciones transversales de observabilidad y mejora continua:**
 - Asegurar la observabilidad de todos los componentes gestionados.
 - Proporcionar cuadros de mando en tiempo real sobre disponibilidad, capacidad, rendimiento, seguridad y uso de recursos, accesibles desde consola centralizada.
 - Mantener un histórico de métricas para análisis de tendencias y generación de informes evolutivos.
 - Aplicar un enfoque proactivo, detectando de forma temprana cualquier tipo de afección y proponiendo o ejecutando mejoras para garantizar la continuidad y optimización del servicio.
 - Realizar automatizaciones de aquellas situaciones o casos de uso que lo requieran para un mejor funcionamiento, rendimiento, calidad, etc.
 - Emitir informes periódicos con recomendaciones técnicas y plan de acción para la evolución de la solución.
 - En caso de que fuera necesario crear algo específico, se deberán entregar a Lantik todos los fuentes y configuraciones para su uso indefinido por parte de Lantik, incluso una vez finalizado el contrato. Así mismo, se deberá poner en marcha en Lantik antes de la finalización del contrato.
- **Firewall de segundo nivel**
 - Administración de reglas y objetos de red.
 - Monitorización 24x7 y detección de fallos.
 - Gestión de actualizaciones de firmware y resolución de vulnerabilidades.
 - Pruebas de failover y validación de rendimiento.



- Documentación y trazabilidad de configuraciones.
- Soporte técnico y escalado al fabricante cuando corresponda.
- Revisión periódica de políticas y recomendaciones de mejora.
- **Solución SASE**
 - Administración centralizada de políticas y perfiles de acceso.
 - Control de identidades y accesos (SSO, MFA, etc.).
 - Gestión integral de identidades (integración con IGA Sailpoint) y accesos (SSO, MFA, perfiles de usuario), incluyendo altas, bajas y modificaciones en coordinación con los procesos corporativos de gestión de personal.
 - Asegurar que los cambios en identidades o permisos se realicen de forma trazable y auditable, minimizando el impacto en la continuidad del servicio.
 - Monitorización de tráfico y detección de anomalías.
 - Actualización y evolución del servicio según amenazas emergentes.
 - Soporte técnico y gestión de incidencias.
 - Generación de informes de seguridad y cumplimiento normativo.
- **Red SD-WAN**
 - Gestión de nodos y enlaces (altas, bajas, modificaciones).
 - Monitorización continua de latencia, jitter, pérdida y uso de enlaces.
 - Definición de políticas de enrutamiento y priorización de tráfico.
 - Escalabilidad bajo demanda.
 - Validación de seguridad en tránsito y cifrado.
 - Soporte y resolución de incidencias con trazabilidad completa.
 - Informes operativos sobre estado y eficiencia del servicio.
- **Protección AntiDDoS capa 7**
 - Administración de políticas de protección de servicios HTTP/S, APIs y aplicaciones expuestas.
 - Actualización de firmas y reglas de detección de ataques.
 - Monitorización bidireccional en tiempo real y respuesta inmediata.
 - Análisis forense y restauración de tráfico legítimo en caso de ataque.
 - Informes sobre intentos bloqueados y efectividad de mitigación.
 - Revisión de políticas ante nuevos vectores de ataque.



3.6.4 Mantenimiento del equipamiento de seguridad y red

El mantenimiento forma parte del servicio gestionado e incluye las tareas preventivas y correctivas necesarias para garantizar la disponibilidad del clúster de firewalls de segundo nivel y de los equipos con funcionalidades SD-WAN.

Mantenimiento preventivo

- Auditoría general anual de inventario, firmware y condiciones de operación en CPDs.
- Revisión anual del estado físico, ventilación, alimentación y conexionado.
- Validación periódica de la configuración de clústeres y pruebas de failover.
- Monitorización de logs y generación de alertas tempranas.
- Entrega de informes de auditoría y revisiones.

Mantenimiento correctivo

- Resolución de incidencias de hardware o fallos de software.
- Sustitución de piezas originales del fabricante (con características iguales o superiores).
- Gestión de garantías y RMA con fabricantes.
- Actualización de firmware previa aprobación de Lantik.
- Verificación de funcionamiento tras la intervención.

Niveles de servicio – indicadores (mantenimiento)

- **Ind12:** Recepción de incidencias críticas – 24x7.
- **Ind13:** Recepción de incidencias normales – L-V laborables 8:00–20:00.
- **Ind14:** Tiempo de respuesta ≤ 15 minutos desde el aviso.
- **Ind15:** Tiempo de diagnóstico y resolución ≤ 4 horas (crítico).
- **Ind16:** Tiempo de diagnóstico y resolución $\leq$ siguiente día laborable (normal).

3.6.5 Fases del servicio

Fase 1: Devolución del servicio

- Un mes antes de la finalización del contrato, la empresa adjudicataria colaborará con Lantik y con la nueva adjudicataria, o quien determine Lantik, en el traspaso de conocimiento.
- Se entregarán todos los documentos de trabajo, documentación técnica y cuadros de mando necesarios para garantizar la continuidad del servicio.
- La responsabilidad de prestación integral del servicio se mantendrá hasta la finalización del contrato.



3.7 Bolsa de servicios profesionales especializados (bajo demanda)

La empresa adjudicataria deberá poner a disposición de Lantik una bolsa de horas técnica destinada a la ejecución de tareas especializadas bajo demanda, a lo largo de toda la vigencia del contrato. Esta bolsa permitirá cubrir necesidades no previstas en el servicio gestionado, así como actuaciones puntuales que requieran personal técnico adicional. Será Lantik quien decida si estas necesidades están previstas o no en el servicio gestionado.

La realización de estos trabajos por parte de la empresa adjudicataria exigirá:

- La valoración previa, en horas, por perfiles y plazos, por parte de la empresa adjudicataria se deberá responder en un plazo máximo de 2 días laborables.
- La aceptación por parte de Lantik de esta valoración.
- El plazo de comienzo de los trabajos una vez aceptada la valoración no podrá ser superior a 10 días laborables.

A su finalización, la empresa adjudicataria facturará los trabajos en base a la valoración aceptada.

De esta bolsa se irá detrayendo en base a las peticiones que Lantik realice a la empresa adjudicataria, en función de los **perfiles** que se indican a continuación:

- Perfil de especialista en seguridad:
Profesional con experiencia demostrable en el diseño, implementación, operación y optimización de soluciones de ciberseguridad de ámbito corporativo. Su ámbito de actuación deberá cubrir:
 - Análisis y gestión de riesgos de seguridad.
 - Implementación y operación de soluciones de protección perimetral (firewalls de nueva generación, IPS/IDS, AntiDDoS, etc.).
 - Administración de arquitecturas de seguridad basadas en SASE (ZTNA, SWG, CASB, FWaaS).
 - Gestión y monitorización de entornos SD-WAN seguros.
 - Detección avanzada de amenazas, respuesta ante incidentes y elaboración de informes de mejora continua.

Se requiere experiencia mínima de 3 años en entornos de ciberseguridad y operación de infraestructuras seguras.

- Perfil especializado en sistemas (Servidores y Comunicaciones)
Perfil técnico con capacidades para diseñar, integrar, administrar y mantener infraestructuras TIC, tanto físicas como virtualizadas. Deberá tener experiencia en redes corporativas, servicios cloud, virtualización y configuración de herramientas de monitorización y automatización.

Se requiere una experiencia mínima de 3 años en administración de sistemas y operación de entornos TI híbridos, así como experiencia demostrable en proyectos de migración o integración de soluciones SD-WAN, SASE y AntiDDoS.



- Técnico/a de soporte:

Especialista en resolución de incidencias, mantenimiento operativo, gestión de tickets y soporte a personas usuarias, incluyendo conocimiento técnico avanzado de las soluciones solicitadas en esta licitación. Participará en tareas de configuración básica, documentación y asistencia técnica de segundo nivel.

Se requiere una experiencia mínima de 2 años en funciones de soporte técnico o asistencia a personas usuarias.

- Técnico de formación:

Responsable de diseñar, documentar e impartir sesiones formativas orientadas a personas usuarias finales o personal técnico. Las formaciones podrán ser presenciales o telemáticas, y deberán incluir documentación específica, material de apoyo y ejercicios prácticos.

Se requiere una experiencia mínima de 2 años en diseño e impartición de formación técnica, especialmente en entornos TIC o de ciberseguridad.

La información de los perfiles se deberá aportar de una forma clara, estructurada en las tablas descritas a continuación, que aporten toda la información de la experiencia en cada uno de los epígrafes solicitados.

Es requisito que todas las empresas licitadoras presenten debidamente cumplimentadas las tablas DETALLE. Las ofertas que no incluyan las tablas serán excluidas de la licitación.

- TABLA DETALLE 1: Perfil de especialista en seguridad:

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo (Mínimo 3 años en entornos de ciberseguridad y operación de infraestructuras seguras.)			Experiencia (Descripción y tareas)
			Fecha inicio (2)	Fecha fin (2)	Suma	
1			mm/aaaa	mm/aaaa	Σ meses	
1			mm/aaaa	mm/aaaa	Σ meses	
...			mm/aaaa	mm/aaaa	Σ meses	
	TOTAL				Σ meses	

(1) Identificador: nº correlativo que identifica a cada persona del equipo

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.



TABLA DETALLE 2: Perfil especializado en sistemas (Servidores y Comunicaciones)

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo (Mínimo 3 años en administración de sistemas y operación de entornos TI híbridos)			Experiencia Descripción y tareas (indicar si proyectos de migración o integración de soluciones SD-WAN, SASE y AntiDDoS)
			Fecha inicio (2)	Fecha fin (2)	Suma	
2			mm/aaaa	mm/aaaa	Σ meses	
2			mm/aaaa	mm/aaaa	Σ meses	
...			mm/aaaa	mm/aaaa	Σ meses	
	TOTAL				Σ meses	

(1) Identificador: nº correlativo que identifica a cada persona del equipo

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.

TABLA DETALLE 3: Técnico de soporte

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo (Mínimo 2 años en funciones de soporte técnico o asistencia a personas usuarias)			Experiencia Descripción y tareas
			Fecha inicio (2)	Fecha fin (2)	Suma	
3			mm/aaaa	mm/aaaa	Σ meses	
3			mm/aaaa	mm/aaaa	Σ meses	
...			mm/aaaa	mm/aaaa	Σ meses	
	TOTAL				Σ meses	

(1) Identificador: nº correlativo que identifica a cada persona del equipo

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.



TABLA DETALLE 4: Técnico de formación

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo (Mínimo 2 años en diseño e impartición de formación técnica, especialmente en entornos TIC o de ciberseguridad)			Experiencia
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción y tareas
4			mm/aaaa	mm/aaaa	Σ meses	
4			mm/aaaa	mm/aaaa	Σ meses	
...			mm/aaaa	mm/aaaa	Σ meses	
	TOTAL				Σ meses	

(1) Identificador: nº correlativo que identifica a cada persona del equipo

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.

3.7.1 Horario del servicio y control de trabajos

Horario obligatorio:

- Invierno: de 8:00 a 17:00.
- Verano (agosto): de 8:00 a 15:00.
- Excepto días festivos en Bilbao y 24 y 31 de diciembre.

Control de los trabajos:

- Los trabajos se desarrollarán en los locales de la empresa adjudicataria, garantizando seguridad y confidencialidad de la información, o bien en Lantik cuando se requiera.
- La empresa adjudicataria designará una persona responsable con visión global del servicio.
- Lantik podrá solicitar que el servicio se preste de manera presencial. En tal caso:
 - Presencialidad en Bilbao: ≤ 30 minutos desde la notificación (**Ind17**).
 - Presencialidad en otras ubicaciones de Bizkaia: ≤ 1 hora desde la notificación (**Ind18**).
- Para servicios fuera del horario definido, el precio de la hora será el estipulado en remoto con un coeficiente de 1,5.



- El modelo de contacto será mediante correo electrónico (canal formal de notificación), complementado con un número de teléfono y al menos dos personas de referencia. Durante la vigencia del contrato se podrán incorporar nuevas vías de comunicación (p. ej. herramienta de ticketing de Lantik o JIRA).
- Lantik designará personas responsables para aspectos organizativos, funcionales y técnicos, que actuarán como interlocutores y podrán realizar controles de calidad de los trabajos entregados.
- La empresa adjudicataria deberá presentar un informe mensual con el cálculo de los indicadores y el desglose del consumo de horas, indicando actuaciones realizadas, fechas, descripción y tiempos dedicados. Este informe deberá remitirse a Lantik con al menos dos días hábiles de antelación al cierre de mes.
- En caso de que fuera necesario crear algún desarrollo específico, se deberán entregar a Lantik todos los fuentes para su uso indefinido por parte de Lantik, incluso una vez finalizado el contrato. Así mismo, se deberá poner en marcha antes de la finalización del presente contrato.

3.8 Pruebas de validación de las ofertas

Durante el proceso de valoración, Lantik podrá solicitar una demo técnica de las **soluciones ofertadas** con objeto de poder realizar las pruebas que estime oportunas para verificar el cumplimiento de los requerimientos establecidos. Se deberá incluir la correspondiente documentación técnica acreditativa de sus características, así como los manuales de funcionamiento y/o utilización, y tienen que estar a disposición de Lantik en un plazo máximo de 15 días naturales tras ser solicitados. La demo técnica, se realizará por cuenta de la empresa ofertante, sin coste alguno para Lantik. El incumplimiento de esta condición podrá conllevar la desestimación de la oferta presentada.

Demostración del Producto

La empresa licitadora deberá, previa solicitud formal por parte de Lantik, realizar una demostración operativa de las **soluciones ofertadas**. Dicha demostración deberá reproducir las funcionalidades descritas en el pliego técnico, y permitirá la verificación de que el producto cumple con los requisitos y especificaciones solicitadas.

Pruebas de Integración con la infraestructura tecnológica de Lantik

Se podrá exigir la realización de pruebas de integración de las soluciones ofertadas, con las infraestructuras tecnológicas de Lantik, como, por ejemplo:

- Plataforma de observabilidad y monitorización.
- CMDB.
- Herramientas de automatización y orquestación.

Resultado de las Pruebas

Lantik se reserva el derecho de excluir del proceso de valoración técnica a la empresa oferente, si, tras la demostración o las pruebas de integración, se constata que el producto ofertado no cumple con los requisitos técnicos y funcionales descritos en este pliego.



4 CONDICIONES PARTICULARES

4.1 Equipo de trabajo

La empresa adjudicataria deberá poner a disposición de Lantik los perfiles necesarios para la correcta ejecución de todos los servicios objeto de esta licitación:

- Todos los miembros del equipo deberán hablar castellano y/o euskera como lengua nativa o ser capaces de comunicarse de manera fluida en castellano y/o euskera. En caso de incluir recursos que no cumplan este requisito, la empresa adjudicataria deberá proporcionar, a petición de Lantik, intérpretes que faciliten la comunicación sin cargo adicional.
- Lantik podrá solicitar la sustitución de cualquier persona del equipo de trabajo que, aun teniendo los conocimientos técnicos requeridos, no disponga de las aptitudes necesarias para el trabajo en equipo o para garantizar un mínimo de calidad en los trabajos realizados.
- La empresa adjudicataria deberá mantener permanentemente formado a su personal en las tecnologías requeridas. El coste de esta formación, así como el tiempo de dedicación, correrán a cargo de la adjudicataria.

4.2 Modelo de gestión

4.2.1 Modelo organizativo

La empresa licitadora deberá detallar en su propuesta la organización del equipo de trabajo, funciones y responsabilidades asignadas, distinguiendo claramente entre los perfiles dedicados a las fases de implantación y migración, y aquellos destinados a la prestación del servicio gestionado.

Deberá identificarse un responsable global de servicios, que actuará como interlocutor único con Lantik y coordinará tanto los trabajos de despliegue como la operación posterior.

4.2.2 Modelo operativo

La empresa licitadora deberá describir, como mínimo:

- Propuesta de funcionamiento que cubra todas las actividades del servicio, diferenciando:
 - **Implantación y migración:** planificación, coordinación con Lantik, pruebas de validación y puesta en producción.
 - **Servicio gestionado:** operación, monitorización, resolución de incidencias, mantenimiento y soporte.
- Propuesta de seguimiento del servicio, incluyendo reuniones periódicas, informes de avance en la fase de implantación y seguimiento mensual en la fase gestionada.

En el ámbito de la seguridad, información relevante sobre la certificación ENS (si se dispone de ella), detallando los ámbitos específicos cubiertos y su relación con el objeto del contrato.



4.3 Documentación a entregar durante la duración del contrato

La empresa adjudicataria deberá entregar en los 15 primeros días de cada mes un informe que recoja los parámetros de nivel de servicio indicados en su oferta, su grado de cumplimiento en el mes precedente y la penalización resultante por su incumplimiento.

- **Indicadores de servicio (KPIs).**

La empresa licitadora deberá definir los indicadores de servicio diferenciando entre:

- KPIs asociados al servicio de implantación y migración, vinculados al cumplimiento de fases, plazos y entregables del proyecto.
- KPIs asociados al servicio gestionado, vinculados al cumplimiento de los niveles de servicio (SLA), tiempos de atención, resolución de incidencias, disponibilidad y calidad del servicio en la fase de operación.

- **Descripción de fases del servicio, incluyendo:**

- **Para el servicio de implantación y migración:** descripción de las fases del proyecto y sus plazos:
 - Fase 1 – Análisis y diseño.
 - Fase 2 – Preparación y migración de los firewalls de segundo nivel.
 - Fase 3 – Despliegue.
 - Fase 4 – Devolución del servicio.
- **Para el servicio gestionado:** descripción de las fases de prestación del servicio:
 - Fase 1: Diagnóstico y transferencia.
 - Fase 2: Ejecución del servicio gestionado.
 - Fase 3: Devolución del servicio.
- Plan de proyecto (planificación detallada y cronograma) y diseño de la arquitectura y plan de migración (documento técnico validado por Lantik) de implantación de la solución SD-WAN y SASE.
- Se deberá realizar un cuadro de mando referente a las soluciones de AntiDDoS L7 y de las tecnologías SASE y SD-WAN consensuado con Lantik.



4.4 Propuesta técnica (estructura)

A efectos de la correcta evaluación de los criterios no cuantificables automáticamente, la **propuesta técnica presentada en el Sobre C** deberá tener una extensión máxima de 100 páginas y deberá contener como mínimo los siguientes apartados, de acuerdo con lo descrito en las especificaciones técnicas del Pliego de Prescripciones Técnicas:

1. Arquitectura y diseño de la solución

- Capacidades del servicio AntiDDoS L7.
- Estrategia de migración del firewall de segundo nivel.
- Descripción de los componentes y funcionalidades de la solución SASE.
- Diseño de despliegue de la solución SD-WAN (topología, modos de operación y gestión del tráfico).
- Tabla de características técnicas solicitadas (ANEXO A).

2. Estrategia de integración y plan de implantación

- Integración con el directorio corporativo y sistemas de autenticación de Lantik.
- Compatibilidad con sistemas de monitorización, gestión de eventos y herramientas de seguridad existentes.
- Cronograma detallado de implantación con hitos, tareas y responsables.
- Descripción de las actividades de migración (SD-WAN, SASE, Firewall).
- Procedimientos de pruebas piloto, validación funcional y reversión.

3. Modelo de soporte y servicio gestionado

- Organización del servicio 24x7, niveles de soporte y mecanismos de escalado.
- Alcance del servicio gestionado en relación con la operación continua de la solución.
- Procedimientos de actualización, resolución de incidencias y gestión de cambios.

4. Bolsa de servicios profesionales especializados

- Descripción del servicio
- Tablas DETALLE de los perfiles presentados

Todos los elementos de seguridad HW/SW deberán contar certificación vigente registrada en el CCN-CERT, en su catálogo CPSTIC y se deberá incluir la documentación de evidencia en el sobre C.

Se podrán incluir anexos adicionales con carácter informativo, pero **la información contenida en dichos anexos no será valorada** en los criterios no cuantificables automáticamente.

4.5 Finalización del contrato

Se considerará que las obligaciones contractuales han finalizado cuando concurra alguna de las siguientes circunstancias:

- Alcance de la fecha de terminación del contrato o del importe total adjudicado.
- Decisión expresa de Lantik de dar por finalizado el servicio.



4.6 Perspectiva de género

Las empresas licitadoras, en la elaboración y presentación de sus respectivas propuestas deberán hacer un uso no sexista del lenguaje. Asimismo, la empresa adjudicataria, a lo largo de la vigencia del contrato, deberá hacer un uso no sexista del lenguaje en cualquier documento definitivo escrito o digital, así como, deberá desagregar los datos por sexo en cualquier estadística referida a personas que se genere, todo ello al amparo del artículo 2.3 de la Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres en el que se señalan los principios generales que deberán respetarse.

La empresa adjudicataria presentará en la justificación final de la realización de la prestación objeto del contrato, en su caso, una memoria sobre el impacto de género de la contratación, con los indicadores y datos desagregados por sexo de las personas usuarias o beneficiarias, o del personal prestador del servicio, que posibiliten evaluar la eficacia de las medidas de igualdad aplicadas.

4.7 Seguridad de la información

Contrato, acuerdo de confidencialidad, Normativa de seguridad para empresas proveedoras, y protección de datos de carácter personal

En el contrato a firmar se incluirá:

- Acuerdo de confidencialidad.
- Conocimiento y compromiso de cumplimiento por parte de la empresa adjudicataria de:
 - [Política de seguridad de la información de Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia.](#)
 - [Norma NCS-1/1 "Norma de Política de Seguridad: Código de Conducta Informático para Proveedores".](#)
 - [Norma NCS-1/2 "Normativa de Seguridad de la Información para Proveedores".](#)

El acuse de recibo y compromiso de cumplimiento de las normativas internas existentes en Lantik S.A. M.P., previa a la prestación del servicio, deberá realizarse por todo el personal interviniente en el mismo (tanto el de la empresa proveedora y como el de posibles subcontrataciones que haga esta), de lo cual se encargará de recoger y custodiar la empresa proveedora que responderá en su nombre.

4.7.1 Deber de confidencialidad

I. Prohibición expresa de acceso a datos privados o confidenciales

Para la realización de los trabajos objeto del presente contrato es posible que el personal de la empresa adjudicataria tenga acceso a locales donde se realizan tratamientos de datos de carácter personal, a soportes o recursos que los contengan o a otro tipo de documentación de carácter privado o confidencial, para la realización de trabajos que no impliquen directamente un tratamiento de este tipo de datos. En particular, será considerado como Información Confidencial todo el know how o saber hacer resultante de la ejecución de los servicios contratados, debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato. De este



modo, se considerará confidencial, a todos los efectos, toda la información y documentación relativa a Lantik S.A. M.P. y/o que esta trate a cuenta de terceros, así como los buenos usos, prácticas y procedimientos internos, que pudiera conocer la empresa adjudicataria con motivo de la ejecución del contrato. En la misma línea, se confiere el carácter confidencial a aquella información a la que tenga acceso con ocasión de la ejecución del contrato, que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal, incluyendo, expresamente, toda la información asociada a medidas de seguridad y de protección, configuraciones desarrolladas, protecciones del servicio y aplicaciones, elementos y descripciones de infraestructura y arquitectura, procesos de autenticación y protocolos de seguridad, comunicaciones, incidencias, informes de terceros, controles de capacidad y evaluaciones de las disponibilidades implicadas, análisis automáticos, redes y protecciones del perímetro, elementos adscritos a la continuidad, registros de actividad y protecciones asociadas, protocolos de copias y restauraciones, elementos de mantenimiento y garantías implicadas, y cuantos otros elementos puedan considerarse un riesgo a los efectos del servicio contratado o la información vinculada al mismo. En cualquier caso, se prohíbe expresamente el acceso a este tipo de datos, ni a ningún dato que no sea objeto de tratamiento del presente. Con ello, la empresa adjudicataria se compromete a no divulgar, no ceder o exponer la información titularidad de Lantik S.A. M.P. y/o que esta trate a cuenta de terceros, sin su previo consentimiento expreso y por escrito. Asimismo, la empresa adjudicataria deberá abstenerse de emplear la documentación y/o información conocida o facilitada durante la ejecución del contrato para fines ajenos a los propios de la ejecución del contrato.

Cuando el contrato no requiera el acceso al sistema de información de Lantik S.A. M.P. pero suponga el acceso a sus instalaciones, la empresa adjudicataria se compromete a mantener plena confidencialidad de la información que pudiera conocer de manera accidental por los accesos a las instalaciones, y especialmente, aquella que pueda suponer un riesgo para Lantik S.A. M.P. y/o para terceros en caso de ser conocida y/o pueda suponer una brecha de seguridad.

II. Deber de secreto

El personal de la empresa adjudicataria deberá observar en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos de carácter privado o confidencial, a los que pudiera tener acceso incidentalmente en el cumplimiento de las tareas encomendadas.

El personal de la empresa adjudicataria queda obligado a no revelar, transferir, ceder o comunicar de cualquier forma este tipo de datos a terceras personas, obligación que se mantendrá aún finalizada su relación con esta.

La empresa adjudicataria se compromete a comunicar y hacer cumplir a su personal las obligaciones establecidas en el presente pliego y, en concreto, las relativas al deber de secreto.

Si se produjera una incidencia durante la ejecución del contrato que conllevará un acceso accidental o incidental a Datos Personales no contemplados en el presente pliego, la empresa adjudicataria deberá ponerlo en conocimiento de Lantik S.A. M.P., en concreto, a la persona interlocutora del contrato, con la mayor diligencia y a más tardar en el plazo de 72 horas.

Serán motivos de resolución del contrato la vulneración del deber de secreto por la empresa adjudicataria o su personal.



III. Garantía de confidencialidad

La empresa adjudicataria certifica que el personal a su cargo ha firmado una cláusula de confidencialidad por la cual se comprometen a no revelar la información que conozcan en función de su cargo o cometido durante la prestación del contrato y posteriormente al mismo. Así como que conoce las medidas de seguridad tendentes a garantizar el cumplimiento de la normativa relativa a protección de los datos de carácter personal.

IV. Tratamiento de datos para la gestión de los servicios de contratación de Lantik

En cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LANTIK S.A. M.P. como responsable del tratamiento, informa al personal de la empresa adjudicataria que sus datos de carácter personal serán tratados e incorporados a su actividad de tratamiento que tiene como finalidad la gestión de los servicios de contratación de Lantik. El tratamiento de dichos datos es necesario para el cumplimiento de una obligación legal y no se comunicarán los datos a terceros salvo obligación legal. Las personas interesadas podrán ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, en la medida que sean aplicables, ante el responsable del tratamiento (<https://lantik.bizkaia.eus/es/aviso-legal>) y podrán consultar información adicional y detallada sobre protección de datos en <https://lantik.bizkaia.eus/es/-/gestion-de-los-servicios-de-contratacion-de-lantik>.

En caso de que la empresa adjudicataria facilitara datos personales de terceros, incluidos los relativos al personal a su servicio, previamente a su inclusión deberá informar a las personas interesadas de los extremos establecidos en el párrafo anterior.

V. Medidas de seguridad

La empresa adjudicataria garantizará que la información de la que disponga por razón de la prestación del servicio no pueda ser visible por personas no autorizadas. Así, los lugares donde almacene, guarde o conserve la información deberán ser aptos para garantizar el deber de confidencialidad.

Asimismo, la empresa adjudicataria se compromete a no revelar, transferir, ceder o de otra forma comunicar información confidencial o datos personales, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación a ningún tercero (exceptuándose las cesiones autorizadas por ley).

La empresa adjudicataria comunicará a Lantik S.A. M.P. toda filtración de información de la que tenga o llegue a tener conocimiento, producida por la vulneración del presente acuerdo de confidencialidad de las personas que hayan accedido a la información. Tal comunicación no exime a la empresa adjudicataria de su responsabilidad, pero si la incumple dará lugar a cuantas responsabilidades se deriven de dicha omisión en particular.

El presente acuerdo no supondrá, en ningún caso, la concesión de permiso o derecho expreso o implícito para el uso de licencias o derechos de autor, propiedad de la parte que revele la



información. El receptor de la información se compromete a no copiar, reproducir, ni por cualquier otro procedimiento, ceder información o material facilitado por Lantik S.A. M.P. o al que hubiere tenido acceso, así como a no permitir a ninguna otra persona, empresa o institución la copia, reproducción o divulgación, sea total, parcial o de cualquier forma, de información o materiales facilitados por Lantik S.A. M.P. o a los que se hubieren tenido acceso en cualquier momento y que obren en poder de la empresa adjudicataria, sin la autorización previa de Lantik S.A. M.P., manifestada expresamente y por escrito.

Con el fin de coordinar y ser eficientes ante cualquier ciberincidente o ajuste de seguridad que se requiera, una vez haya sido firmado el contrato, la empresa adjudicataria debe indicar quién ocupa el rol de responsable de seguridad en su organización. Para ello, notificará por escrito a la persona responsable del contrato de Lantik S.A. M.P. el nombre, apellidos, correo electrónico y teléfono de la persona o servicio que desempeñe este rol.

Por parte de Lantik S.A. M.P, el contacto en relación a la gestión de cualquier ciberincidente o ajuste de seguridad en el ámbito o servicio objeto del pliego será:

Contacto: Área de plataforma tecnológica (Operación)

Teléfono: 944 068 989

Correo electrónico: alertas.operacion@bizkaia.eus

Dirección: Avenida Sabino Arana, 44 48013 Bilbao (Bizkaia)

Las partes acuerdan que en el caso de que sea necesario contactar a la otra parte para aclarar cualquier aspecto relacionado con la seguridad incluyendo cualquier duda, aspecto técnico o cualquier incidencia durante la prestación del servicio, se deberá realizar a las personas de contacto referidas anteriormente.

El personal de Lantik S.A. M.P, tendrá los siguientes roles y funciones en el ámbito de la seguridad:

- Transmitir a la empresa adjudicataria los requisitos y medidas de seguridad.
- En su caso, dar instrucciones y coordinar las actuaciones de mantenimiento.
- Dar instrucciones y coordinar las actuaciones en caso de que se produzca un incidente de seguridad de la información o desastre.
- En su caso, comprobar el cumplimiento del presente contrato, pudiendo requerir para ello la documentación que sea necesaria para acreditarlo.

El personal de la empresa adjudicataria tendrá los siguientes roles y funciones en el ámbito de la seguridad:

- Atender y asegurarse del cumplimiento de las medidas de seguridad que Lantik S.A. M.P. pudiera establecer.



- Transmitir a Lantik S.A. M.P., el cumplimiento de los requisitos y medidas de seguridad requeridos, realizando en caso necesario, las salvedades u observaciones que pudieran ser oportunas.
- En su caso, atender a las peticiones realizadas por el personal responsable de Lantik S.A. M.P., en materia de mantenimiento.
- Comunicar con antelación a la persona responsable de Lantik S.A. M.P., de cualquier actuación planificada que pudiera afectar a la disponibilidad, confidencialidad, integridad, autenticidad o trazabilidad de la información o servicios de la entidad.
- Comunicar a la persona responsable de Lantik S.A. M.P., cualquier incidente de seguridad de la información que se produzca a la mayor brevedad.
- Atender a las instrucciones dadas por Lantik S.A. M.P., en caso de que se produzca un incidente de seguridad de la información o desastre.
- Proporcionar la documentación o evidencias que sean necesarias para acreditar el cumplimiento del presente contrato.

4.7.2 Gestión interna de Lantik (medidas de securización interna) previas a la prestación

Lantik S.A. M.P. establecerá los mecanismos de control y securización interna que considere en su propia infraestructura, por ejemplo, asignación de usuarios temporales, rutado específico, perímetros de seguridad, etc.

4.7.3 Documentación

En caso de que la empresa adjudicataria preste en el ámbito del contrato un producto o servicio soportado por sistemas de información propios, deberá proporcionar a requerimiento de Lantik S.A. M.P. la información necesaria sobre la arquitectura de seguridad de dicho sistema de información, con el objeto de facilitar a esta el cumplimiento de sus obligaciones.

4.7.4 Auditoría, monitorización y reporte periódico del rendimiento de los controles de seguridad y notificación de evolución en la resolución de incidentes de seguridad a Lantik

Lantik S.A. M.P. se reserva el derecho de auditar y monitorizar las actividades realizadas por la empresa adjudicataria durante el servicio con el objetivo de prevenir y detectar incidentes de seguridad.

La empresa adjudicataria del servicio deberá remitir a requerimiento de Lantik S.A. M.P., sin perjuicio de otros plazos establecidos en el pliego, información sobre el nivel de rendimiento de los controles de seguridad establecidos, así como información de los incidentes no graves ocurridos en el periodo.



4.7.5 Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores”

La empresa adjudicataria del servicio deberá remitir, a requerimiento de Lantik S.A. M.P., información sobre el nivel de cumplimiento de lo establecido en la Normativa de Seguridad para Proveedores.

4.7.6 Evidencia de buenas prácticas de seguridad, preferiblemente mediante certificación acreditada en una norma de referencia para la gestión de la seguridad de la información, en el entorno de prestación.

A requerimiento de Lantik S.A. M.P., la empresa adjudicataria del servicio deberá aportar evidencias de buenas prácticas de seguridad en el servicio, preferiblemente mediante certificado de la implantación y uso de un modelo de gestión de la seguridad de la información en base las normas de referencia existentes para la gestión de la seguridad de la información, como por ejemplo la ISO/IEC 27001.

En el caso de que el alcance del contrato esté relacionado con la prestación de un producto o servicio correspondiente al diseño, instalación, configuración, puesta en marcha o mantenimiento de un sistema de información sobre el que se soporten servicios relacionados con la gestión de las competencias de Lantik S.A. M.P. (o de cualquier otra entidad del Sector Público a la que Lantik S.A. M.P. preste servicio) o desarrollen o ayuden a desarrollar el Procedimiento Administrativo regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la empresa adjudicataria deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados.

Con carácter general deberá prestarse especial atención a la observancia de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante “Esquema Nacional de Seguridad”) en particular las medidas de seguridad establecidas en su Anexo II, en las dimensiones de seguridad que le apliquen y según el nivel de clasificación determinado en cada caso. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el Esquema Nacional de Seguridad, se aplicarán las medidas de seguridad indicadas en su Anexo II, ya sean pertenecientes al marco organizativo, operacional o de protección.

De este modo, con el fin de facilitar la realización de los controles periódicos exigidos para el cumplimiento de la citada legislación, la empresa adjudicataria deberá proporcionar a Lantik S.A. M.P. tras la firma del contrato:

- Bajo petición de Lantik S.A. M.P., la empresa adjudicataria proporcionará el detalle de la Declaración de Aplicabilidad y, en su caso, de las medidas compensatorias y complementarias de vigilancia utilizadas.
- Bajo petición de Lantik S.A. M.P. mecanismos y funcionalidades que permitan a Lantik S.A. M.P. conocer y analizar los controles llevados a cabo por parte de la empresa adjudicataria (auditorías de seguridad, informes de hacking ético, renovación de certificaciones de seguridad, utilización de componentes cualificados o certificados, etc.).



4.7.7 Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica

Las empresas adjudicatarias deben garantizar la seguridad de los productos o servicios que suministren. Para ello, los productos o servicios deben superar un proceso de cualificación y estar incluidos en el Catálogo de Productos y Servicios TIC del Centro Criptológico Nacional (CPSTIC), o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento establecidos en el artículo 19 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En caso de que la empresa adjudicataria no cumpliera lo anteriormente expuesto, dicha empresa deberá asumir el compromiso de certificar los servicios/componentes antes indicados en un plazo de seis meses a contar a partir de la adjudicación del pliego.

La empresa adjudicataria del servicio deberá realizar las acciones necesarias para concienciar regularmente al personal interviniente en la prestación del servicio acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

Se formará regularmente al personal interviniente en la prestación del servicio en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

Con carácter general, la empresa adjudicataria aplicará las medidas de seguridad correspondientes a un sistema de información de categoría MEDIA, según lo establecido en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Asimismo, deberá cumplir con las obligaciones exigidas para los prestadores de servicios por las entidades públicas.

Con carácter general, el intercambio de información confidencial se realizará de acuerdo a lo establecido en la normativa de clasificación de la información de Lantik S.A. M.P. La empresa adjudicataria deberá atender las peticiones y requisitos que pudiera realizar el personal de Lantik S.A. M.P para dicho intercambio.

4.7.8 Subcontratación

En caso de exista una cadena de subcontratación para la prestación del producto o servicio, la empresa adjudicataria deberá disponer de una documentación que detalle claramente los elementos que forman parte de la cadena de subcontratación, así como las implicaciones derivadas de cualquier cambio o modificación que pueda sufrir algún eslabón de dicha cadena, todo ello previo conocimiento y aceptación por Lantik S.A. M.P. Si el producto o servicio objeto de contrato está sujeto al cumplimiento del Esquema Nacional de Seguridad según lo estipulado en el punto "Evidencia de buenas prácticas de seguridad acreditada en una norma de referencia para la gestión de la seguridad de la información en el entorno de prestación", la empresa adjudicataria deberá asegurar que los sistemas de información de las empresas subcontratadas son conformes con el Esquema Nacional de Seguridad en lo que respecta a los servicios que afecten a Lantik S.A. M.P., por lo que el contenido del presente documento resultará asimismo de aplicación a la cadena de suministro de la empresa adjudicataria.



4.7.9 Mantenimiento y afección al servicio

En caso de que el contrato incluya la prestación de servicios de mantenimiento a los sistemas de información y comunicaciones de Lantik S.A. M.P., los requisitos de nivel de servicio, consecuencias de su incumplimiento y mecanismos de seguimiento del servicio serán los establecidos en el pliego de prescripciones técnicas.

La coordinación de las labores de mantenimiento o de cualquier actuación que pueda impactar negativamente sobre la información o servicios de Lantik S.A. M.P. tendrá en cuenta los siguientes requerimientos:

- La coordinación la realizarán las personas responsables de Lantik S.A. M.P. y la empresa adjudicataria.
- La empresa adjudicataria estará obligada a seguir las indicaciones de la persona responsable del servicio de Lantik S.A. M.P. para cualquier actuación en la que se puedan ver afectados los sistemas de información y comunicaciones de Lantik S.A. M.P.
- La empresa adjudicataria deberá comunicar por escrito y con antelación suficiente a la persona responsable de servicio de Lantik S.A. M.P. cualquier actuación planificada que pudiera afectar a la disponibilidad, confidencialidad, integridad, autenticidad o trazabilidad de la información o servicios de Lantik S.A. M.P. La comunicación incluirá la previsión de actuaciones a realizar, fecha y hora prevista de actuación, riesgos asociados y, en su caso, medidas de seguridad. Estas actuaciones deberán ser aprobadas por el personal responsable de Lantik S.A. M.P. de forma previa a su ejecución.
- En actuaciones relacionadas con mantenimiento correctivo, la persona responsable del servicio de Lantik S.A. M.P. podrá requerir la realización de determinadas acciones en un periodo concreto o el envío por parte de la empresa adjudicataria de una previsión de actuaciones a realizar, fecha y hora, riesgos asociados y, en su caso, medidas de seguridad.

Será obligatorio que la empresa adjudicataria disponga de un registro operativo de las peticiones o actuaciones de mantenimiento requeridas por Lantik S.A. M.P., empleando, en su caso, la herramienta señalada por esta. Las peticiones de servicio mantendrán un flujo con el comunicante, debiendo proceder a su cierre cuando se hubiera comunicado al mismo y no se considere ninguna acción adicional. Se incluirá necesariamente en el registro:

- Hora de inicio de incidencia y hora de finalización (incluyendo la hora en la que se produce la incidencia, la hora en la que se notifica y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.
- Tiempos de resolución.
- Conclusiones y mejora.

En caso de que así lo requiera Lantik S.A. M.P., la empresa adjudicataria proporcionará:



- Informe donde se detallen las actuaciones realizadas y, en su caso, las deficiencias detectadas y plan de corrección.
- Mecanismo para hacer seguimiento de todas las incidencias de mantenimiento tanto preventivo como correctivo.

4.7.10 Coordinación en caso de incidentes y desastres

En caso de que la empresa adjudicataria tenga acceso a la información de Lantik S.A. M.P. o información que trate Lantik, S.A. M.P o su actuación pueda afectar a los servicios de la entidad, debe atenerse a lo indicado en la presente cláusula en caso de que se produzca una incidencia de seguridad, entendiendo como tal, cualquier acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traduzca en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.

La empresa adjudicataria deberá, a través de su Persona de Contacto, notificar al interlocutor de Lantik identificado en el pliego, tan pronto como sea consciente, de cualquier incidente de seguridad que pueda afectar a los activos de información y servicios y en general sistemas de información y comunicaciones de Lantik S.A. M.P.

La coordinación de las labores de resolución del incidente tendrá en cuenta los siguientes requerimientos:

- La coordinación la realizarán las personas responsables de Lantik S.A. M.P. y la Persona de Contacto designada en la empresa adjudicataria.
- La empresa adjudicataria estará obligada a seguir las indicaciones de la persona responsable de Lantik S.A. M.P. para la resolución de la incidencia.
- La persona responsable de Lantik S.A. M.P. podrá requerir la realización de determinadas acciones en un periodo concreto o el envío por parte de la empresa adjudicataria de una previsión de actuaciones a realizar, fecha y hora, riesgos asociados y, en su caso, medidas de seguridad.

Será obligatorio que la empresa adjudicataria disponga de un registro operativo de las incidencias de seguridad ocurridas en el marco del presente contrato, empleando, en su caso, la herramienta señalada por Lantik S.A. M.P. Las incidencias mantendrán un flujo con el comunicante, debiendo proceder a su cierre cuando se hubiera comunicado al mismo y no se considere ninguna acción adicional. Se incluirá necesariamente en el registro:

- Hora de inicio de incidencia y hora de finalización (incluyendo la hora en la que se produce la incidencia, la hora en la que se notifica y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.
- Tiempos de resolución.
- Conclusiones y mejora.



En este sentido se tendrán en cuenta los puntos requeridos por la normativa aplicable, para la identificación, gestión y registro de incidencias, que puedan afectar al servicio, incluyendo:

- Reglamento general de protección de datos.
- Guía CCN-STIC-817 Gestión de ciberincidentes.
- Guía nacional de notificación y gestión de ciberincidentes.

En caso de que la incidencia afecte a datos de carácter personal, será de aplicación lo establecido en el capítulo referente a protección de datos personales.

En cualquier caso, la resolución de un incidente de seguridad, especialmente cuando sea de peligrosidad alta o superior, requerirá la participación de la empresa adjudicataria de los servicios afectados para evaluar el impacto de la incidencia y adoptar las medidas necesarias de contención, mitigación, respuesta y recuperación.

Estas actividades, por su especialización, podrán requerir el concurso de su CSIRT de referencia, en este caso el CCN-CERT del Centro Criptológico Nacional especialmente cuando el incidente hubiere afectado a sistemas que traten información de naturaleza administrativa o datos de los ciudadanos administrados. Dicha respuesta deberá gozar por tanto de las preceptivas medidas de seguridad y confidencialidad de la actuación administrativa que exige el art. 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y que obliga a que tal conocimiento solo pueda extenderse a un organismo de las administraciones públicas, como el Centro Criptológico Nacional.

4.7.11 Regulación de la finalización del contrato: transferencia de tecnología

Durante la ejecución del contrato, la empresa adjudicataria se compromete a facilitar a las personas designadas por Lantik S.A. M.P. toda la información y documentación que estas soliciten para disponer de un total conocimiento técnico de las circunstancias en las que se desarrollan los servicios, sus actividades y, en general, de todas las operaciones técnicas, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos.

Una vez finalizado el contrato, la empresa adjudicataria deberá desarrollar las acciones precisas para la transferencia del conocimiento y de la información, implicados en el servicio. Asimismo, la empresa adjudicataria debe realizar, en el plazo máximo de un (1) mes:

- a. Devolver a Lantik S.A. M.P. la información confidencial y, si procede, los soportes donde conste, una vez cumplida la prestación. La devolución debe comportar el borrado total y seguro de la información confidencial existente en los equipos informáticos utilizados por la empresa adjudicataria.

No obstante, Lantik S.A. M.P. podrá requerir a la empresa adjudicataria para que en vez de la opción a), cumpla con la b) o con la c) siguientes:

- b. Devolver a la empresa que designe por escrito Lantik S.A. M.P., la información confidencial y, si procede, los soportes donde conste, una vez cumplida prestación. La



devolución debe comportar el borrado total y seguro de la información confidencial existente en los equipos informáticos utilizados por la empresa adjudicataria.

- c. Destruir de manera segura los datos, una vez cumplida la prestación.

La empresa adjudicataria deberá certificar la destrucción final de los datos de manera segura por escrito, entregando el certificado correspondiente a Lantik S.A. M.P.

En caso de imposibilidad de cumplimiento del plazo establecido, la empresa adjudicataria realizará un requerimiento de prórroga debidamente justificado a Lantik S.A. M.P. quien, en su caso, podrá conceder o rechazarlo.

Cuando sea necesario, para el proceso de restitución y transferencia tecnológica la empresa adjudicataria presentará una planificación detallada, contemplando los medios que serán empleados, las acciones de contingencia diseñadas y los riesgos que pudieran presentarse en el proceso. Cuando sea necesario, y especialmente cuando existiera una nueva entidad adjudicataria, se incluirá el periodo de transición destinado a la gestión organizada del proceso de transferencia y restitución.

Esta cláusula será obligatoria cuando la finalización del servicio fuera anticipada, siendo responsabilidad de la entidad adjudicataria saliente, una transferencia y restitución ordenada.

4.7.12 Normativa de securización de entornos para prestación de servicio remoto

Se deberá conocer y dar compromiso de cumplimiento por parte de la empresa adjudicataria del servicio la norma NCS-1/3 relativa a la "Normativa de securización de entornos para prestación de servicio remoto".

4.7.13 Informe periódico del cumplimiento de la "Normativa de securización de entornos para prestación de servicio remoto"

La empresa adjudicataria del servicio deberá remitir a requerimiento de Lantik S.A. M.P., información sobre el nivel de cumplimiento de lo establecido en la Normativa de securización de entornos para prestación de servicio remoto; para ello deberá cumplimentar el Formato cuestionario normativa securización de entornos que le será entregado, por la persona responsable del servicio o proyecto por parte de Lantik S.A. M.P. y que está disponible en el Plan de Calidad.

4.7.14 Monitorización de las conexiones remotas

Lantik S.A. M.P. monitorizará las conexiones remotas a sus sistemas de información. La empresa adjudicataria notificará este hecho a su personal, de modo que sean informados de que sus actuaciones pueden ser auditadas en caso necesario por Lantik S.A. M.P. para la comprobación del cumplimiento del conjunto de medidas de seguridad especificados en el presente documento y demás normativa referenciada.



4.7.15 Instalación de herramientas de seguridad

Lantik se reserva el derecho de instalación de herramientas de seguridad y monitorización, en los equipos propiedad de la entidad adjudicataria que vayan a conectarse al dominio Bizkaia.

4.7.16 Evidencias de las buenas prácticas relativas al objetivo de control 11 “Seguridad Física y del entorno” de la norma de referencia ISO/IEC 27002 en el entorno de prestación

La empresa adjudicataria del servicio deberá evidenciar a requerimiento del Dpto. de Seguridad de Lantik S.A. M.P., el grado de cumplimiento de las buenas prácticas de seguridad física establecidas en el dominio 11 “Seguridad Física y del entorno” de la norma de referencia ISO27002; así como informar de los incidentes no graves ocurridos en el periodo. Los incidentes graves deberán ser notificados al Dpto. de Seguridad de Lantik S.A. M.P. a la mayor brevedad.

4.7.17 Teletrabajo

En aquellos supuestos en los que el servicio se preste en modalidad de teletrabajo o remota en un entorno no corporativo, la empresa adjudicataria del servicio objeto del presente pliego deberá garantizar el mismo nivel de seguridad, garantizando el uso de medidas de seguridad. Para tal fin, deberá observar las recomendaciones establecidas en “Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo” de la Agencia Española de Protección de Datos y el informe “CCN-CERT BP/18 Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia” del Centro Criptológico Nacional.

En este sentido, la empresa adjudicataria deberá como mínimo utilizar las siguientes medidas de seguridad y/o medidas análogas, tales como:

- El personal de la empresa adjudicataria no podrá descargar a sus equipos en conexión remota información confidencial ni datos de carácter personal de los que Lantik S.A. M.P. sea responsable ni imprimir dicha información, salvo que tenga autorización expresa por parte de Lantik S.A. M.P. Tomará todas las precauciones necesarias para evitar acceso por personal no autorizado (familiares, compañeras/os, etc.) a su dispositivo y, por tanto, a la información almacenada.
- La empresa adjudicataria deberá disponer de una política o normativa de seguridad que incluya consejos y recomendaciones a su personal relativos a situaciones de teletrabajo o acceso remoto para mantener la seguridad de la información. Esta documentación deberá ser conocida por todas las personas que participen como resultado de la adjudicación.
- Si el equipamiento (portátil, móvil, tablet) empleado para la conexión remota a los sistemas de información de Lantik S.A. M.P. no es proporcionado por esta, la empresa adjudicataria se asegurará de que dicho equipamiento cumple los requerimientos de seguridad generales especificados en el presente documento y en la normativa referenciada. En particular, el equipamiento deberá incluir como mínimo las siguientes medidas de seguridad:
 - o Software antimalware y protección mediante firewall activados y actualizados.
 - o Tendrá instaladas exclusivamente las aplicaciones software que sean necesarias para que el personal desarrolle sus funciones. Estas aplicaciones deberán ser aprobadas por la propia entidad y descargadas de repositorios fiables.



- o El sistema operativo y las aplicaciones software deberán estar actualizados.
- o Cifrado de disco duro (algoritmo AES, con longitud de clave mínima de 128 bits) en caso de que Lantik S.A. M.P. hubiera autorizado al personal de la empresa adjudicataria a descargarse a su dispositivo información sensible o datos personales.
- o Conexión remota a los sistemas de información de Lantik S.A. M.P. exclusivamente a través de las herramientas autorizadas por Lantik S.A. M.P. referenciadas con anterioridad.
- o No tendrá elementos externos conectados, como memorias USB, lectores CD/DVD, etc.

El personal no podrá almacenar credenciales de acceso en claro en los dispositivos que emplee para el acceso remoto a los sistemas de información de Lantik S.A. M.P. En caso de que el almacenamiento de credenciales sea necesario, empleará un contenedor cifrado o herramienta de gestión de contraseñas que soporte algoritmo de encriptación simétrica AES con una longitud de clave mínima de 128 bits.

4.7.18 Certificación de inexistencia de vulnerabilidades de seguridad

La empresa adjudicataria se comprometerá en la firma del contrato a mantener actualizada y libre de vulnerabilidades de seguridad la infraestructura TI de su propiedad empleada durante la prestación del servicio.

4.7.19 Conformidad con el Esquema Nacional de Seguridad (ENS)

De conformidad con el ENS, todo sistema que suministre un servicio en la nube a organismos del sector público deberá cumplir las medidas de seguridad definidas en las guías CCN-STIC que le sean de aplicación.

Cuando el contrato contemple, total o parcialmente, el uso de sistemas *cloud on-premise*, la empresa adjudicataria deberá cumplir lo establecido en la Guía CCN-STIC-858 Implantación de sistemas SaaS en modo local (on-premise). De este modo, deberá aportar los siguientes documentos:

- Guía de instalación (dirigida a administradores).
- Guía de uso seguro (dirigida a usuarios).
- Guía de relación entre empresa proveedora y Lantik S.A M.P.

El servicio en la nube debe contar con una certificación de seguridad reconocida por el ENECSTI.

En caso de que exista un Perfil de Cumplimiento Específico aprobado por el CCN para el servicio proporcionado, Lantik S.A. M.P. podrá acogerse a este, siendo entonces de aplicación la declaración de aplicabilidad asociada a este perfil en concreto.



4.7.20 Declaración de ubicación

Tal y como se establece en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, considerando la naturaleza del servicio, la empresa adjudicataria deberá facilitar la identificación de la ubicación de los sistemas de información vinculados con los servicios objeto del contrato, incluyendo todas las ubicaciones asociadas al almacenamiento y prestación del servicio, contemplando todas las actividades implicadas, tales como recogida, almacenamiento, procesamiento y gestión.

Es necesario que la empresa adjudicataria identifique a todas las entidades subcontratadas que participarán en la ejecución de los servicios objeto del contrato, durante la vigencia del mismo, debiendo identificar la ubicación y los servicios concretos prestados por cada una de ellas. La subcontratación quedará en todo caso sometida a las disposiciones contenidas en la normativa de protección de datos, sin excepción.

Se considerarán, a todos los efectos, las limitaciones establecidas en la normativa de protección de datos relativas a transferencias internacionales de datos, siendo condición esencial el cumplimiento de tales previsiones, que se extenderán a las entidades subcontratadas. Esta obligación se considera esencial al contrato y se mantendrá durante toda la vigencia del mismo.

Cualquier modificación a lo largo del contrato relativa a las exigencias establecidas en el presente apartado, deberá ser comunicada sin dilación, a Lantik S.A. M.P.

4.7.21 Transferencia Internacional de Datos Personales

No podrán realizarse transferencias a un tercer país u organización internacional fuera de la Unión Europea, salvo en los supuestos específicamente autorizados por el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), siendo la única excepción contemplada, la transferencia a países, organizaciones o territorios que hayan sido declarados con un nivel adecuado de protección por parte de las autoridades de control en materia de protección de datos, o cuando sea precisa la transferencia en cumplimiento de una obligación legal, convenio internacional o requerimiento judicial.

La entidad adjudicataria deberá comunicar sin dilación indebida, cualquier cambio en relación a las condiciones para la transferencia de datos personales, especialmente la pérdida de la condición de "nivel adecuado de protección" para transferencia internacional, conforme al RGPD. Se considera expresamente incluidos los supuestos en los que la Comisión determine la pérdida de adecuación de un país, organización, entidad o empresa, incluidas aquellas que dejen de estar adheridas a eventuales acuerdos internacionales que permitan transferencias internacionales de datos.

4.7.22 Servicio asociado a la verificación electrónica de la identidad y tratamiento de datos de los tipos descritos en el artículo 46bis de la Ley 40/2015

Considerando lo dispuesto en la Ley 39/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en el caso de que el servicio licitado por Lantik S.A. M.P. incluya un sistema de identificación mediante clave concertada a los efectos de lo descrito el artículo 9.2c) de la precitada ley, será necesario que la empresa adjudicataria incluya o facilite la identificación de la ubicación y prestación del servicio, así como



los recursos técnicos que vayan a ser asignados para la recogida, almacenamiento, tratamiento y gestión, los cuales solo podrán estar ubicados en el territorio de la Unión Europea, según lo dispuesto en el artículo 122.2c) de la ley 9/2017, de 8 de noviembre de Contratos del Sector Público. Cuando estuvieran implicadas categorías especiales de datos, según lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), la ubicación se circunscribirá al territorio nacional.

Asimismo, considerando lo dispuesto en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en los casos en que el servicio licitado por Lantik S.A. M.P. afectara a datos relativos al censo electoral, padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de las persona usuarias del Sistema Nacional de Salud, será necesario que la entidad adjudicataria comunique a Lantik S.A. M.P. la ubicación y prestación del servicio, que solo podrá prestarse dentro del territorio de la Unión Europea.

A todos los efectos, cuando el servicio licitado permitiera la subcontratación, esta quedará sometida en idénticos términos a lo descrito. Por ello, será necesario declarar expresamente la localización de los servicios o recursos concernientes a los procesos subcontratados. Cuando existieran varios subcontratados, será necesario declararlo de cada uno de ellos, de manera individualizada.

Cuando el contrato ya hubiera sido adjudicado, y existiera una modificación que afectara a la ubicación o prestación del servicio, incluyendo cambios en la subcontratación, deberán ser comunicados sin demora, a Lantik S.A. M.P. identificando claramente los cambios producidos, quedando estáa facultada para resolver el contrato.

La empresa adjudicataria será a todos los efectos responsable directo de los incumplimientos derivados de tal subcontratación y de las obligaciones declaradas.

4.7.23 Gestión de copias de seguridad y restauración de datos

La empresa adjudicataria deberá disponer de los mecanismos necesarios para implementar una política de respaldo y de pruebas de recuperación que contemplen como mínimo los siguientes requisitos:

- Identificación del alcance de los respaldos.
- Política de copias de seguridad.
- Medidas de cifrado de información en respaldo.
- Procedimiento de solicitud de restauraciones de respaldo.
- Realización de pruebas de restauración.
- Traslado de copias de seguridad (si aplica).

4.7.24 Medidas de continuidad del servicio o proyecto

La empresa licitadora deberá disponer de un Plan de Continuidad para el servicio que garantice que se cumplan los Acuerdos de Nivel de Servicio especificados en el pliego técnico. Este plan se activará ante la indisponibilidad total o parcial de los recursos principales, que por cualquier motivo provoque la indisponibilidad de los servicios objeto del contrato e incluirá:



- La identificación y descripción de los medios alternativos planificados para la provisión de los servicios, personal alternativo, existencia o planificación de instalaciones y medios de comunicación alternativos, etc.
- Realización de, al menos, una prueba de recuperación anual.
- Actualización de la documentación del plan de recuperación ante desastres tanto como sea necesario.

Bajo requerimiento de Lantik S.A. M.P. la empresa licitadora deberá presentar:

- Evidencias de disponer de un Plan de Continuidad para el servicio (p.ej. Certificaciones, compromiso de la empresa proveedora...).
- Informe final de pruebas anuales del Plan de Continuidad, así como un plan de trabajo con acciones correctivas si se detectaran eventos o acciones a corregir.

4.7.25 Registros de actividad

La empresa adjudicataria dispondrá de los registros de actividad de las personas usuarias que permiten monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.

La empresa adjudicataria será responsable de:

- Realizar la configuración necesaria para llevar a cabo el registro de las actividades de las personas usuarias.
- Definir y establecer las medidas de seguridad necesarias para la protección de los registros.
- Mantener los registros durante un periodo no inferior a dos (2) años.

En caso de que así lo requiera Lantik S.A. M.P., la empresa adjudicataria pondrá a disposición de esta los registros de actividad correspondientes a las personas usuarias cuyo acceso al sistema cloud esté incluido en el ámbito del contrato.

4.7.26 Claves criptográficas

En caso de conservar claves criptográficas en su infraestructura, la empresa adjudicataria pondrá en conocimiento de Lantik S.A. M.P. las medidas implementadas para proteger las claves criptográficas durante todo su ciclo de vida.

El servicio deberá disponer de mecanismos de cifra que permitan que la información del usuario esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo. Los mecanismos criptográficos deberán cumplir con lo especificado en la guía CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.

El proveedor deberá cumplir uno de los siguientes casos:



- Ser capaz de garantizar el funcionamiento de los mecanismos de cifra sin que las claves sean almacenadas en la nube. Estas estarán en disposición de Lantik S.A. M.P. quien es la persona encargada de su gestión y almacenamiento.
- Almacenar las claves del cifrado en módulos de seguridad de hardware denominados dispositivos HSM (Hardware Security Modules), no accesibles por terceros. Dichos dispositivos deberán estar cualificados por el Centro Criptológico Nacional (CCN) e incluidos en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN (bajo metodología LINCE), o en su defecto, estén certificados en Common Criteria o LINCE. ..dispongan de una declaración de seguridad (ST) que cumpla los requisitos definidos en la [Guía de Seguridad CCN-STIC 140](#).

4.7.27 Transparencia e información

La empresa adjudicataria proporcionará a Lantik S.,A. M.P. información relativa a:

- Herramientas de seguridad de que dispone, incluyendo aquellas destinadas a la monitorización, análisis, recuperación y notificación de incidentes de seguridad.
- Tipo de virtualización utilizada y nivel y mecanismos de segregación de los datos o aplicaciones de Lantik S.A. M.P. alojadas en la nube.
- Mecanismos y procedimientos de borrado seguro de la información almacenada por la empresa adjudicataria, que serán utilizados en el momento de terminación del vínculo contractual.
- Bajo petición de Lantik S.A. M.P., características del hardware contratado: tamaño de disco, memoria RAM, tipo de procesador, CPU o transferencia de datos. La empresa adjudicataria asegurará la existencia de servicios que permitan monitorizar el uso de estas capacidades por parte de Lantik S.A. M.P.
- Ubicación geográfica de sus datos (incluidos backups y almacenamiento de logs), antes y durante el suministro del servicio.
- El acceso y análisis de logs, registros de acceso y cualquier otra información que pudiera ser solicitada por parte de Lantik S.A. M.P. para garantizar el cumplimiento de sus obligaciones legales. En caso de incidente de seguridad, toda la información requerida (configuración, logs, etc...) de los equipos físicos, dispositivos de red, servicios compartidos y dispositivos de seguridad debe ser entregada a Lantik S.A. M.P.

4.7.28 Resolución del Contrato

El incumplimiento por parte de la empresa adjudicataria de cualesquiera de las presentes disposiciones podrá ser motivo de resolución del contrato de manera unilateral.

4.7.29 Fuero

Ambas partes se someten, con renuncia a su fuero propio si lo tuvieran, a los Juzgados y Tribunales de Bilbao para la interpretación de cualquier cuestión litigiosa que se derive de este contrato.



ANEXO A – TABLA DE CARACTERÍSTICAS

		[Indicar Nombre de la EMPRESA]	
Sección	Especificaciones técnicas requeridas	Cumple (Si / No)	Comentarios
AntiDDoS L7			
Requisitos mínimos	Despliegue en modalidad SaaS (WAF-as-a-Service).		
	Baja latencia mediante nodos en la misma región de la aplicación.		
	Alta disponibilidad y escalabilidad dinámica para adaptarse a incrementos de tráfico y nuevas aplicaciones o servicios.		
	Continuidad de servicio bajo escenarios de ataque.		
	Retención mínima de datos de seguridad durante 1 año.		
	Soporte en modalidad 24x7x365.		
	Gestión multitenant, con segmentación de políticas y visibilidad independiente por dominio o servicio.		
	Aplicaciones web protegidas: hasta 100 aplicaciones corporativas críticas y de acceso público.		
	Dominios y subdominios gestionados: hasta 100 dominios/subdominios con políticas de seguridad diferenciadas.		
	Tráfico sostenido: capacidad mínima de 200 Mbps de tráfico legítimo inspeccionado, con protección ante ataques de hasta 10 Gbps sin degradación del servicio.		
	Peticiones HTTP/HTTPS concurrentes: mínimo 100.000 solicitudes por segundo procesadas y analizadas con latencia añadida ≤ 10 ms.		
	Protección de APIs: cobertura inicial para al menos 200 endpoints activos, con descubrimiento automático de nuevos endpoints.		
	Usuarios concurrentes protegidos contra Account Takeover: mínimo 200.000 usuarios en servicios web y portales corporativos.		
Capacidad y volumetría	Protección contra OWASP Top 10 (XSS, SQL Injection, CSRF, etc.).		
	Detección de anomalías con machine learning para amenazas desconocidas.		
	Validación de parámetros de entrada.		
	Seguridad de cookies (firmado y protección contra envenenamiento).		
	Análisis de archivos cargados (tipo, tamaño, malware, troyanos).		
	Prevención de fuga de información en cabeceras y errores.		
Protección de APIs	Descubrimiento automático de endpoints de API.		
	Compatibilidad con OpenAPI 3.0, JSON y XML.		
	Validación de esquemas y estructuras de datos.		
	Soporte para tokens JWT en APIs móviles.		
	API Gateway integrado con control de acceso, gestión de claves y limitación de solicitudes.		



Seguridad del cliente	Protección contra ataques CSRF mediante tokens únicos por sesión.		
	Defensa frente a MITB (ofuscación, cifrado, anti-keylogger, control AJAX).		
	Control de acceso y limitación de solicitudes por cliente.		
	Detección y protección contra robo de cuentas (account takeover).		
Defensa contra bots	Mitigación de bots mediante machine learning.		
	Verificación biométrica de interacción (ratón, teclado, scroll).		
	Detección basada en umbrales de comportamiento.		
	Distinción entre bots legítimos y maliciosos.		
	Técnicas de engaño (bot deception) para identificación de crawlers.		
Protección Adicional	Bloqueo por reputación de IPs, listas blancas/negras y geolocalización (GeoIP).		
	CDN integrado para optimización de entrega de contenido.		
	Actualizaciones automáticas de seguridad.		
Analítica y visibilidad	Threat Analytics con machine learning.		
	Consola de incidentes con detalle de ataques y fuentes.		
	Panel de Insights con recomendaciones de seguridad.		
	Exportación de logs de ataques y tráfico a sistemas externos (SIEM, almacenamiento).		
Firewall de segundo nivel			
Características hardware mínimas de los equipos	12 puertos RJ-45 1G/2.5G/5G/10G		
	10 puertos SFP/SFP+ 1G/10G		
	4 puertos SFP28 25G		
	2 puertos QSFP/QSFP28 40G/100G		
	1U de altura en rack		
	SSD de 480 GB para sistema, configuración y logs		
	Puertos dedicados para gestión y consola		
	Interfaces dedicados para HA (sin uso de puertos de servicio)		
	Arquitectura hardware separada entre plano de control y plano de datos		
	Fuentes de alimentación redundadas hot-swap		
	Flujo de aire front-to-back		
	Configuración en HA activa/activa o activa/pasiva		
	Throughput en tráfico real con App-ID, servicios de seguridad habilitados y logging: 15 Gbps		



	Throughput con App-ID y logging activado: 29 Gbps		
	240.000 nuevas sesiones por segundo		
	2.500.000 sesiones concurrentes		
	Al menos 1 sistema virtual incluido, ampliable hasta 11 con licencia		
Características de red	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. - Y 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		
	Soporte de protocolos dinámicos de routing RIP, OSPF y BGP4 así como routing estático.		
	Soporte de DHCP, NAT y PAT.		
	Soporte de monitorización SNMP v2, v3 y netflow..		
	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"		
Identificación e integración de usuarios	Posibilidad de aplicar políticas basadas en usuarios y grupos en vez de por IP.		
	Integración con sistemas de directorios para obtención de usuarios y grupos, incluyendo Microsoft Active Directory.		
	Posibilidad de integración con sistemas multiusuario como 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.		
Características generales de seguridad	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.		
	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.		



	Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 5100 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.		
	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 entrenados en la nube para proporcionar protección en tiempo real de amenazas desconocidas, URLs maliciosas, DNS, y seguridad IoT.		
	Integrar machine learning (ML) en el núcleo del firewall para poder proporcionar una prevención de ataques sin firma internos para los ataques basados en archivos.		
Motor de routing avanzado	Disponer de un motor avanzado de routing, que simplifique las operaciones con configuraciones basados en estándar similar al utilizado por otros fabricantes de routers.		
	Permitir la configuración de perfiles para cada protocolo y el filtrado granular de cada perfil para multiples routers lógicos y sistemas virtuales.		
	Permitir la redistribución de rutas con perfiles de redistribución.		
	Permitir grupos de peers BGP y peers BGP que hereden configuraciones.		
	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	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 poder 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.		
	Capacidad de creación de firmas de IPS a partir de la información de una firma de Snort, y que se permita importar de manera automática, un listado de reglas de Snort.		
	Soporte en línea de Deep Learning y análisis en la nube.		
	Prevención de Command and Control desconocido basado en Machine Learning desde la nube.		
Filtrado de URL	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.		
	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 requerirá que el fabricante ofrezca listas de IPs 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 web 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 poder configurar filtrado de URL multicategoría, esto es categorizar una URL con hasta 4 categorías, en función de su contenido, del dominio al que pertenecen etc y así poder definir políticas que permitan el acceso pero limiten las posibilidades de navegación...		
	Se deberá dotar a los equipos de modelos de Machine Learning 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 en 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.		
Antivirus	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 al equipo las acciones oportunas.		
	Los equipos 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 que permitan identificar muestras maliciosas desconocidas en tiempo real.		
Bloqueo de ficheros y datos sensibles	Los equipos propuestos deben tener la capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo, permitiendo al menos 100 tipos de ficheros identificables.		
	Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.		
	Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.		
	Los equipos deben tener la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito, DNIs, etc. de forma que se evite la exfiltración de este tipo de datos.		
Tecnología de sandboxing	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 firewall se aprovechará, 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 10 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 equipos 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.		
	Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).		
Funciones de SDWAN	Optimización de enlaces: Debe ofrecer capacidades de optimización del rendimiento del tráfico, incluyendo selección dinámica de rutas y priorización de tráfico.		
	Soporte para redes híbridas: El sistema debe ser capaz de integrar múltiples tipos de conexiones WAN, incluyendo MPLS, Internet, LTE, y conexiones de fibra.		
	Soporte para túneles IPsec: La solución debe ser capaz de establecer túneles IPsec entre sitios de manera segura, con soporte para cifrado y autenticación robustos, incluyendo autenticación post-cuántica con claves PPKs RFC 8784.		
	Centralización en la gestión de políticas: Debe existir un sistema centralizado para la configuración y gestión de políticas de tráfico, permitiendo el control granular sobre el comportamiento de la red.		
	Visibilidad de tráfico: La solución debe permitir monitoreo en tiempo real y proporcionar métricas detalladas sobre el		



	rendimiento de la red, incluyendo latencia, disponibilidad y rendimiento de las aplicaciones.		
	Seguridad de red integrada: El SD-WAN debe integrar capacidades de Next-Generation Firewall (NGFW), como inspección profunda de paquetes, prevención de intrusiones (IPS), y protección contra amenazas avanzadas.		
	Redundancia de enlaces: Debe soportar la gestión de enlaces múltiples, tanto para la conectividad a Internet como MPLS, garantizando que el tráfico se desvíe automáticamente en caso de fallo de enlace.		
	Control de la latencia y el jitter: La solución debe poder monitorizar la latencia y el jitter en tiempo real, y optimizar el tráfico en función de estos parámetros para garantizar un rendimiento consistente.		
	Soporte para QoS: Debe permitir la priorización de aplicaciones críticas, como VoIP y videoconferencias, mediante políticas de Calidad de Servicio (QoS) configurables.		
	Dashboards personalizados: Los usuarios deben poder personalizar dashboards de monitoreo para obtener visibilidad sobre el tráfico de la red, la seguridad y el rendimiento en tiempo real.		
	Alertas y notificaciones: La solución debe ofrecer alertas personalizables sobre eventos críticos de seguridad o desempeño, como la caída de enlaces o la detección de actividades sospechosas.		
	Reporting detallado: Debe generar informes detallados y fáciles de interpretar, sobre el tráfico de la red, el cumplimiento de las políticas, las amenazas detectadas y la disponibilidad de los enlaces.		
VPN Acceso Remoto	Conexiones punto a punto (Site2Site, L2L): La solución posibilitará el establecimiento de conexiones punto a punto mediante protocolos estándar de conexiones remotas privadas IPSEC. a. La configuración de dichas VPN deberá soportar intercambio de claves precompartidas (PPK) post-cuánticas con posibilidad de agregar más de 5 PPK post cuánticos (PQ) a cada VPN IKEv2. Deberá ser compatible con los estándares RFC-8784, RFC-9242 y RFC-9370.		
	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: - Integración con cualquier tipo de repositorio corporativo de usuarios (Microsoft Active Directory, LDAP, Radius, SAML, etc.)		
Procesamiento de logs	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.		
	Los logs de los datacenters deben almacenarse local e igualmente tener la capacidad de enviar esos logs a un entorno en nube del fabricante para su análisis.		
	Los logs deberán contener al menos (tráfico, threats, URL, DNS, logs del sistema, etc..)		
	El historial de almacenamiento de logs en la nube no será inferior a 1 año.		



	Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecerían dentro de sus fronteras.		
Consola de gestión centralizada	La consola de gestión deberá estar ubicada en la nube con soporte íntegro del fabricante.		
	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.		
	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 y solución de SASE, para reducir los costes de operación y la curva de aprendizaje.		
	Deberá permitir la gestión íntegra de la configuración de todo el parque de firewalls ofertados.		
	Deberá permitir la gestión de la solución SASE con la posibilidad de realizar reglas que sean aplicadas a distintos entornos, ya sean firewalls o dicha solución SASE con el fin de no duplicar configuraciones y así evitar misconfig.		
	Los logs de los firewalls deben almacenarse en la nube para una gestión más eficiente y deberán disponer de al menos de un histórico de 1 año de antigüedad.		
	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 con el fin de facilitarnos la causa raíz del incidente.		
	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.		
	Gestión de la configuración indicando BPA (Best Practice Assessment) en todo momento.		
	Dashboards que indiquen el grado de cumplimiento y adopción de la seguridad para identificar el grado de madurez de la configuración.		
	Sistema de posture con reglas predefinidas y creación de reglas personalizables con posibilidad de bloqueo de configuraciones antes de aplicarse en los firewalls.		
	Programación de upgrades de los firewalls y definir un scope para dicha programación.		
	Posibilidad de crear reglas de notificación según la severidad de la alerta.		
	Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecerían dentro de sus fronteras.		



	Posibilidad de administrar los equipos físicos sin necesidad de utilizar una consola de gestión adicional.		
Cumplimiento de estándares	Directiva de Baja Tensión (Low Voltage Directive 2014/35/EU)		
	Directiva EMC (2014/30/EU)		
	Directiva RoHS (2011/65/EU)		
	Certificación Common Criteria		
	Inclusión en guías CCN-STIC (ENS) de productos cualificados		
SD-WAN			
Requerimientos técnicos	Optimización de enlaces: Debe ofrecer capacidades de optimización del rendimiento del tráfico, incluyendo selección dinámica de rutas y priorización de tráfico.		
	Soporte para redes híbridas: El sistema debe ser capaz de integrar múltiples tipos de conexiones WAN, incluyendo MPLS, Internet, LTE, y conexiones de fibra.		
	Soporte para túneles IPsec: La solución debe ser capaz de establecer túneles IPsec entre sitios de manera segura, con soporte para cifrado y autenticación robustos, incluyendo autenticación post -cuántica con claves PPKs RFC 8784.		
	Centralización en la gestión de políticas: Debe existir un sistema centralizado para la configuración y gestión de políticas de tráfico, permitiendo el control granular sobre el comportamiento de la red.		
	Visibilidad de tráfico: La solución debe permitir monitoreo en tiempo real y proporcionar métricas detalladas sobre el rendimiento de la red, incluyendo latencia, disponibilidad y rendimiento de las aplicaciones.		
	Seguridad de red integrada: El SD-WAN debe integrar capacidades de Next-Generation Firewall (NGFW), como inspección profunda de paquetes, prevención de intrusiones (IPS), y protección contra amenazas avanzadas.		
	Redundancia de enlaces: Debe soportar la gestión de enlaces múltiples, tanto para la conectividad a Internet como MPLS, garantizando que el tráfico se desvíe automáticamente en caso de fallo de enlace.		
	Control de la latencia y el jitter: La solución debe poder monitorizar la latencia y el jitter en tiempo real, y optimizar el tráfico en función de estos parámetros para garantizar un rendimiento consistente.		
	Soporte para QoS: Debe permitir la priorización de aplicaciones críticas, como VoIP y videoconferencias, mediante políticas de Calidad de Servicio (QoS) configurables.		
	Dashboards personalizados: Los usuarios deben poder personalizar dashboards de monitoreo para obtener visibilidad sobre el tráfico de la red, la seguridad y el rendimiento en tiempo real.		
	Alertas y notificaciones: La solución debe ofrecer alertas personalizables sobre eventos críticos de seguridad o desempeño, como la caída de enlaces o la detección de actividades sospechosas.		
	Reporting detallado: Debe generar informes detallados y fáciles de interpretar, sobre el tráfico de la red, el		



	cumplimiento de las políticas, las amenazas detectadas y la disponibilidad de los enlaces.		
	Monitorización: Soporte de monitorización SNMP v2, v3 y netflow.		
	Consola de gestión centralizada: la consola de gestión deberá ser única y estar centralizada para SD-WAN y SASE (al menos en la parte de políticas de seguridad) incluyendo todas las funcionalidades descritas sobre la misma.		
Requerimientos de hardware	7 puertos RJ-45 10/100/1000Mbps		
	Puerto dedicado para gestión.		
	Puerto de consola RJ45.		
	Posibilidad de configuración en HA (A/P)		
	Recursos hardware 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.		
	Prestaciones o capacidad del firewall con la identificación de aplicaciones habilitada (es decir, trabajando a nivel 7 para todo el tráfico) Appmix y logging habilitado: 1.4 Gbps		
	Prestaciones o capacidad con identificación de aplicación, con todos los servicios de seguridad habilitados, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, File Blocking, etc) como frente a amenazas desconocidas (Sandboxing) y Logging habilitado medidos en transacciones APPMix: 0.8 Gbps		
	Nuevas sesiones por segundo: 11.000		
	Número de sesiones totales: 64.000		
Protección ante vulnerabilidades	En la protección ante vulnerabilidades se deberán usar criterios basados en la identificación tanto de la aplicación o en el sistema operativo, aplicando perfiles ajustados a cada caso sin afectar al rendimiento de los equipos.		
	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 poder 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 o sistema operativo 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.		
	Capacidad de creación de firmas de IPS a partir de la información de una firma de Snort, y que se permita importar de manera automática, un listado de reglas de Snort.		
Filtrado de URL	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. 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 requerirá que el fabricante ofrezca listas de IPs 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 web que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales en función de las categorías de web visitadas. 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.		
Antivirus	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 al equipo las acciones oportunas. Los equipos 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.		
Bloqueo de ficheros y datos sensibles	Los equipos propuestos deben tener la capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo, permitiendo al menos 100 tipos de ficheros identificables. Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes. Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia		



	URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.		
	Los equipos deben tener la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito, DNIs, etc. de forma que se evite la exfiltración de este tipo de datos.		
Tecnología de Sandboxing	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 firewall se aprovechará, 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 10 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.		
Seguridad en DNS	Los equipos 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.		
	Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).		
SASE			



Zero Trust Network (ZTNA)	Posibilidad de aplicar las mismas capacidades de seguridad para protección del tráfico de navegación y para protección del acceso a aplicaciones o recursos privados		
	No limitación del acceso a un número determinado de aplicaciones privadas. Debe permitirse el acceso a tantas aplicaciones privadas como se estimen oportunas en cada momento.		
	Posibilidad del uso de aplicaciones en las que la comunicación se inicia desde el CPD hacia el cliente, por ejemplo, aplicaciones de help-desk remoto, FTP activo o Voz sobre IP		
	Para una mejor visibilidad y trazabilidad, la solución propuesta no debe hacer NAT del tráfico de los usuarios que acceden a las aplicaciones o recursos privados, de tal forma que estos vean la IP origen de los usuarios o dar trazabilidad por ID de usuario.		
	Acceso seguro basado en identidad para aplicaciones privadas, sin necesidad de VPN tradicional.		
	Capacidad de aplicar políticas de acceso condicional basadas en identidad, dispositivo, ubicación y nivel de riesgo.		
	Autenticación multifactor (MFA).		
Firewall-as-a-service (FWaaS)	Inspección de tráfico a nivel de capa 7 (aplicación) para todo el tráfico entrante y saliente.		
	Reglas basadas en aplicaciones, usuarios/grupos y contenidos. Estas reglas deberán poder ser configurables con perfiles de seguridad		
Secure Web Gateway (SWG)	Protección contra amenazas web en tiempo real (malware, phishing, URLs maliciosas).		
	Control granular del uso de aplicaciones web y redes sociales.		
	Capacidad de aplicar políticas de navegación seguras y filtrado de contenido.		
Cloud Access Security Broker (CASB)	Descubrimiento y control de aplicaciones SaaS (Shadow IT).		
	Identificación de al menos 80.000 aplicaciones SaaS, clasificadas por tipo y riesgo.		
	Políticas de control para el uso de aplicaciones cloud (ej. subida/descarga de ficheros).		
Funcionalidad SD-WAN integrada	Establecimiento seguro de túneles entre sedes y la nube SASE.		
	Balanceo inteligente de tráfico y selección dinámica de rutas.		
	Optimización de la experiencia de usuario mediante monitorización en tiempo real de latencia, pérdida y jitter.		
Arquitectura general	La solución debe estar basada en una arquitectura cloud-native y multi-tenant, permitiendo alta disponibilidad y escalabilidad.		
	La solución debe estar preparada para realizar ampliaciones bajo demanda, tanto en ancho de banda como en número de usuario.		
	Debe ofrecer una consola centralizada para la administración de políticas, visibilidad y monitoreo.		
	Deberá estar preparada para soportar todos los casos de uso, incluyendo ZTNA, SWG, FWaaS, CASB, DLP, SSPM, SD-WAN, etc.		



	Mismas capacidades de seguridad tanto en navegación como en acceso a aplicaciones privadas incluyendo protección avanzada ante amenazas, Sandbox, IPS/IDS, Antivirus, Seguridad DNS, Filtrado avanzado de URLs.		
	Múltiples opciones de acceso de usuarios: mediante agente, a través de proxy (archivo .pac), desde sedes, con dispositivos gestionados o no gestionados.		
	Múltiples opciones de acceso a las aplicaciones privadas: que las aplicaciones puedan ver la dirección IP de los usuarios (normativa, trazabilidad) o que las aplicaciones no puedan ver la dirección IP origen de los usuarios.		
	Control del uso de aplicaciones SaaS corporativas (compartición de archivos, descarga, subida, etc.)		
	Detección de actividad de riesgo de los usuarios.		
	Recursos dedicados, únicamente disponibles y siempre disponibles para su uso por Lantik.		
	Recursos dedicados, sin compartir el plano de datos con terceros.		
	La solución propuesta debe ofrecer direccionamiento IP público dedicado para Lantik, sin necesidad de configuraciones adicionales y aplicado directamente en la nube SASE al tráfico que se envía a Internet.		
	Para mayor disponibilidad, una solución que permita desplegar la infraestructura SASE en 2 o más proveedores diferentes de nube pública.		
	SLA de disponibilidad no menor a 99'999%.		
	Comprometer un máximo 10 milisegundos para descifrado, inspección de seguridad y cifrado del tráfico, tanto para la navegación segura como para el acceso a aplicaciones privadas, en la descripción pública de sus niveles de servicio o bajo un NDA.		
	Para mayor seguridad y para evitar fluctuaciones de rendimiento, el tránsito entre regiones/zonas/PoPs debe ser a través de internet si no a través de redes privadas. De tal forma que, si un usuario se conecta al PoP1 para acceder a un recurso que está conectado al PoP2, el tráfico entre PoP1 y PoP2 no pase por internet.		
	La solución debe constar como mínimo de 1 PoP (puntos de presencia) en territorio español en modalidad de alta disponibilidad, de forma que cualquier contingencia en cada uno de los PoP sea cubierta de forma transparente y sin intervención necesaria por parte de un operador sin afectar al servicio.		
	Separación de los planos de gestión, control y datos de tal forma que una indisponibilidad del plano de gestión no afecta al funcionamiento de usuarios conectados ni de usuarios, previamente aprovisionados, que quieran establecer una nueva conexión durante el período de indisponibilidad del plano de gestión.		
	Capacidad de multitenant, pudiendo crear y administrar múltiples tenants desde la consola única de gestión. Cada tenant debe tener infraestructura dedicada e independiente de los otros tenants y direccionamiento IP público dedicado por tenant y diferente entre tenants		
Requerimientos de gestión y visibilidad	Consola para monitoreo de eventos, políticas y tráfico de red.		
	Consola de gestión desde la que configurar, monitorizar y mantener los casos de uso SASE principales, incluyendo		



expresamente Proxy en la nube, SWG, FWaaS, ZTNA, SD-WAN, CASB en línea).		
Consolidación de los logs en un punto común en nube de fabricante, al menos para las funcionalidades de navegación en internet y acceso a aplicaciones privadas. En ambos casos (navegación y acceso a recursos privados) la solución debe correlacionar automáticamente los logs relativos a una misma sesión, es decir, si para una sesión el tráfico pasa por el servicio de proxy o de firewall, por inspección de URL y por inspección de amenazas, tales logs deben correlacionarse automáticamente para simplificar el análisis de un posible problema o incidente de seguridad. El histórico de los logs no deberá ser inferior a una retención de 1 año, incluida en la oferta.		
Permitir configurar distintos tipos de autenticación para diferentes propósitos, estableciendo un orden de prioridad entre ellos, de tal forma que se compruebe cada tipo de autenticación en función de su orden de prioridad hasta que uno de ellos autentique correctamente al usuario. Mínimamente tiene que estar soportado autenticaciones contra AD, SAML y OIDC.		
Capacidad de evaluar la configuración e identificar áreas de mejora, incluyendo la detección de objetos configurados pero que no se están usando, la detección de reglas configuradas pero que no se están usando o la presencia de reglas demasiado permisivas.		
Deberá permitir la gestión de la solución SASE con la posibilidad de realizar reglas que sean aplicadas a distintos entornos, ya sean firewalls o dicha solución SASE con el fin de no duplicar configuraciones y así evitar misconfig.		
Los logs de los firewalls deben almacenarse en la nube para una gestión más eficiente y deberán disponer de al menos de un histórico de 1 año de antigüedad.		
Evaluar la configuración de la consola 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, RAM con el fin de facilitarnos la causa raíz del incidente, así como posibles caídas de los nodos de SASE.		
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.		
Gestión de la configuración indicando BPA (Best Practice Assessment) en todo momento.		
Dashboards que indiquen el grado de cumplimiento y adopción de la seguridad para identificar el grado de madurez de la configuración.		
Programación de upgrades de los firewalls y definir un scope para dicha programación.		
Posibilidad de crear reglas de notificación según la severidad de la alerta.		
Informes detallados sobre uso de aplicaciones, cumplimiento y seguridad.		
Soporte para integración con SIEM, SOAR y herramientas de terceros.		



	Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, la consola y logs en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que la información enviada a esta nube permanecería dentro de sus fronteras.		
Requerimientos de seguridad y cumplimiento	Las mismas capacidades de seguridad en la navegación segura y en el acceso a apps privadas		
	Las firmas creadas en base al contenido malicioso del archivo (payload) y no simplemente en base a hashes del archivo		
	Capacidad de detonar archivos Mac OS X y Android .apk		
	Una funcionalidad de Sandbox capaz de inspeccionar tanto archivos descargados desde (inbound) como archivos subidos (outbound) a servidores, ya sean servidores internos o sitios públicos en Internet		
	Capacidades de seguridad DNS capaces de detectar al menos las siguientes amenazas: dominios estratégicamente envejecidos, ataques de CNAME cloaking, detección de la reputación de subdominios, detección de dominios almacenados (stockpiled domains), ataques de tunelización DNS ultra-lenta (ultra-slow DNS tunneling), ataques NXNS (NXNSAttack), ataques de dangling DNS.		
	Funcionalidades de seguridad basadas en soluciones propias, no en acuerdos de reventa de terceras soluciones (acuerdos OEM) ni en soluciones opensource		
	La capacidad de detectar la aplicación a nivel 7 independientemente del puerto de nivel 4 por el que aplicación se comunica, tanto en la navegación como en el acceso a aplicaciones privadas		
	Poder forzar un cambio dinámico de políticas aplicadas si, una vez establecida la sesión, se modifica la postura de seguridad del dispositivo. Este cambio dinámico de políticas debe estar disponible tanto para la navegación a internet como para el acceso a aplicaciones privadas		
	Capacidad de detectar y detener 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		
	Capacidad de RBI, entregadas desde la misma nube SASE que el resto de los casos de uso y gestionadas desde la misma consola común.		
Protección ante vulnerabilidades	Auditoría completa de actividades administrativas y de usuario.		
	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 poder 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.		
	Soporte en línea de Deep Learning y análisis en la nube.		
	Prevención de Command and Control desconocido basado en Machine Learning desde la nube.		
Filtrado de URL	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.		
	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 requerirá que el fabricante ofrezca listas de IPs 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 poder configurar filtrado de URL multicategoría, esto es categorizar una URL con hasta 4 categorías, en función de su contenido, del dominio al que pertenecen etc y así poder definir políticas que permitan el acceso, pero limiten las posibilidades de navegación...		
	Se deberá dotar a los equipos de modelos de Machine Learning 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 en 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.		
Antivirus	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 al equipo las acciones oportunas.		
	La infraestructura debe 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 que permitan identificar muestras maliciosas desconocidas en tiempo real.		
Tecnología de sandboxing	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.		
	La infraestructura se aprovechará, 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 10 minutos, también lo desconocido sea convertido en conocido en el contexto de protección en el puesto.		
	La infraestructura debe 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	La infraestructura propuesta 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.		
	Consola web de administración en la nube, donde poder visualizar cuadros de mando con información sobre el tráfico DNS, tipos de ataque, frecuencia de acceso, contexto (whois, threat intelligence...).		
Requisitos técnicos y operativos	Alta disponibilidad garantizada (SLA de al menos 99.999%).		
	Integración con proveedores de identidad (Azure AD).		
	Soporte para dispositivos gestionados y no gestionados.		
	Respecto de estos últimos: - Capacidades de protección del dato corporativo (DLP) con notificaciones a los usuarios (user coaching) en dispositivos no gestionados. Se acepta el uso de agentes ligeros o navegadores corporativos, pero no se acepta que el tráfico deba descifrarse. - Capacidad de mostrar enlaces personalizados (portal de aplicaciones), que pueden ser tanto de aplicaciones públicas como privadas, a las que tienen acceso los usuarios que se conectan desde dispositivos no gestionados. Se acepta el uso de agentes ligeros o navegadores corporativos.		
Implantación y migración			
Fases	Planificación/diseño y plan de migración por riesgo/criticidad		
	Entorno de pruebas; instalación inicial SD-WAN; preparación AntiDDoS L7		
	Sustitución clúster FW 2º nivel con continuidad y validación HA		
	Despliegue por fases con pruebas de conectividad, rendimiento y seguridad		
	Puesta en marcha AntiDDoS L7 alineada a servicios expuestos		
Devolución del servicio	Soporte post-despliegue, transferencia de conocimiento y documentación		
Plazo	Plazo máximo de ejecución: 18 meses (sin prórroga)		
Observabilidad	El adjudicatario deberá garantizar la integración de las nuevas herramientas y soluciones con las plataformas corporativas ya existentes en Lantik, incluyendo la plataforma de observabilidad y monitorización, la CMDB y las herramientas de automatización y orquestación, asegurando dicha interoperabilidad desde el inicio del servicio y sin requerir desarrollos adicionales por parte de Lantik		
SOC	Integración de telemetría/eventos/logs/métricas en el SOC de Lantik		



Horarios del servicio	Horario:		
	- Invierno: de 7:00 a 17:00. - Verano (agosto): de 7:00 a 15:00. - Excepto días festivos en Bilbao y 24 y 31 de diciembre. - Por necesidades específicas de la implantación y migración de cada sede específica, pudiera ser necesario que alguna intervención planificada se tuviera que realizar fuera del horario establecido previamente.		
	Un número de teléfono móvil del servicio con disponibilidad 24x7x365.		
	Tiempo de atención de cualquier incidencia ≤ 5 minutos.		
	Resolución de incidencias con prioridad muy urgentes ≤ 30 minutos.		
	Resolución de incidencias urgentes ≤ 4 horas.		
	Resolución de incidencias normales ≤ 8 horas.		
Niveles de servicio - indicadores	Ind1: Activación y validación del servicio AntiDDoS L7 ≤ 4 meses desde firma.		
	Ind2: Migración del clúster de firewalls de nivel 2 finalizada y validada por Lantik ≤ 30/06/2027		
	Ind3: Entrega y validación del plan de proyecto (Diseño de la arquitectura y plan de migración) dentro de los 6 meses tras firma de contrato.		
	Ind4: Implantación progresiva de SASE/SD-WAN validada en sedes prioritarias ≤ 18 meses tras entrega de plan de proyecto.		
	Ind5: Integración completa en el SOC, monitorización/observabilidad y CMDB (logs, telemetría, métricas) ≤ 24 meses tras firma de contrato.		
	Ind6: Entrega de documentación técnica y transferencia de conocimiento ≤ 24 meses tras firma de contrato.		
Servicio gestionado SASE y SD-WAN (24x7x365)			
Metodología y planificación del servicio	Un equipo de coordinación dedicado 100%, de al menos 3 personas de la empresa adjudicataria, el cual será responsable de la interlocución con Lantik para la correcta gestión, gobernanza y operativa del servicio, así como cualquier tipo de necesidad que surja. En este equipo deberán estar representados, como mínimo, los siguientes roles: dirección, redes, seguridad, identidad, sistemas, observabilidad, soporte, etc. Este equipo, será responsable tanto de la coordinación operativa como del escalado de incidencias y la interlocución con el fabricante. En este equipo, deberá existir, como mínimo, perfiles con experiencia mínima de 3 años en la gestión de servicios de seguridad y comunicaciones, formación técnica acreditada en ITIL u otras metodologías de gestión de servicios, así como certificaciones técnicas relevantes		



	en las tecnologías ofertadas. Lantik establecerá la periodicidad de reuniones necesarias, en cada momento, con este equipo de coordinación.		
	Canales: móvil/email (L-V 07:00–17:00 – invierno y L-V 7:00-15:00 - verano) y móvil de servicio 24x7x365		
	Asegurar que el personal técnico adscrito a prestar el servicio mantenga un nivel de dedicación suficiente para garantizar el cumplimiento de los objetivos de calidad y los plazos acordados, debiendo la empresa adjudicataria acreditar dicha dedicación mediante informes periódicos de actividad, registro de horas y evidencias de los entregables realizados.		
	Integrarse con las herramientas de gestión de incidencias/peticiones que determine Lantik, de manera que quede registro y se pueda calcular el grado de cumplimiento de los indicadores establecidos en el apartado siguiente.		
	Asegurar la prestación del servicio desde las dependencias de la empresa adjudicataria, garantizando la seguridad y confidencialidad de la información.		
	Atender requerimientos de presencialidad: en caso necesario, el personal deberá acudir a Lantik, dependencias de la DFB u organismos forales en un plazo máximo de 1 hora desde el aviso. En caso de las dependencias de Bilbao, el plazo máximo es de 30 minutos.		
	Mantener a su personal permanentemente formado en las tecnologías requeridas, siendo este coste asumido por la empresa adjudicataria.		
	Realizar, como mínimo, una reunión mensual de seguimiento durante la primera semana de cada mes, aportando un informe detallado de las actuaciones del mes vencido y formalizando acta de la reunión.		
Niveles de servicio - indicadores	Inc1: Tiempo de atención de cualquier incidencia ≤ 5 minutos.		
	Inc2: Resolución de incidencias con prioridad muy urgentes ≤ 30 minutos.		
	Inc3: Resolución de incidencias urgentes ≤ 4 horas.		
	Inc4: Resolución de incidencias normales ≤ 8 horas.		
	Inc5: Disponibilidad del servicio de incidencias 24x7x365.		
	Inp6: Tiempo de atención de cualquier petición ≤ 15 minutos.		
	Inp7: Resolución de peticiones muy urgentes ≤ 1 hora.		
	Inp8: Resolución de peticiones urgentes ≤ 8 horas.		
	Inp9: Resolución de peticiones normales ≤ 16 horas.		
	Inp10: Disponibilidad del servicio de peticiones 24x7x365.		
	Inp11: Realización de reunión mensual de seguimiento con entrega de informe.		
Funciones transversales de observabilidad y mejora continua	Asegurar la observabilidad de todos los componentes gestionados.		
	Proporcionar cuadros de mando en tiempo real sobre disponibilidad, capacidad, rendimiento, seguridad y uso de recursos, accesibles desde consola centralizada.		



	Mantener un histórico de métricas para análisis de tendencias y generación de informes evolutivos.		
	Aplicar un enfoque proactivo, detectando de forma temprana cualquier tipo de afección y proponiendo o ejecutando mejoras para garantizar la continuidad y optimización del servicio.		
	Realizar automatizaciones de aquellas situaciones o casos de uso que lo requieran para un mejor funcionamiento, rendimiento, calidad, etc.		
	En caso de que fuera necesario crear algún desarrollo, se deberán entregar a Lantik todos los fuentes y configuraciones para su uso indefinido por parte de Lantik, incluso una vez finalizado el contrato. Así mismo, se deberá poner en marcha en Lantik antes de la finalización del contrato.		
	Emitir informes periódicos con recomendaciones técnicas y plan de acción para la evolución de la solución.		
Tareas específicas con el firewall de 2º nivel	- Administración de reglas y objetos de red. - Monitorización 24x7 y detección de fallos. - Gestión de actualizaciones de firmware y resolución de vulnerabilidades. - Pruebas de failover y validación de rendimiento. - Documentación y trazabilidad de configuraciones. - Soporte técnico y escalado al fabricante cuando corresponda. - Revisión periódica de políticas y recomendaciones de mejora.		
Tareas específicas de la solución SASE	- Administración centralizada de políticas y perfiles de acceso. - Control de identidades y accesos (SSO, MFA, etc.). - Gestión integral de identidades (integración con IGA Sailpoint) y accesos (SSO, MFA, perfiles de usuario), incluyendo altas, bajas y modificaciones en coordinación con los procesos corporativos de gestión de personal. - Asegurar que los cambios en identidades o permisos se realicen de forma trazable y auditable, minimizando el impacto en la continuidad del servicio. - Monitorización de tráfico y detección de anomalías. - Actualización y evolución del servicio según amenazas emergentes. - Soporte técnico y gestión de incidencias. - Generación de informes de seguridad y cumplimiento normativo.		
Tareas específicas de la solución de red SD-WAN	- Gestión de nodos y enlaces (altas, bajas, modificaciones). - Monitorización continua de latencia, jitter, pérdida y uso de enlaces. - Definición de políticas de enrutamiento y priorización de tráfico. - Escalabilidad bajo demanda. - Validación de seguridad en tránsito y cifrado. - Soporte y resolución de incidencias con trazabilidad completa.		



	- Informes operativos sobre estado y eficiencia del servicio.		
Tareas específicas de la solución de protección AntiDDoS de capa 7	- Administración de políticas de protección de servicios HTTP/S, APIs y aplicaciones expuestas. - Actualización de firmas y reglas de detección de ataques. - Monitorización bidireccional en tiempo real y respuesta inmediata. - Análisis forense y restauración de tráfico legítimo en caso de ataque. - Informes sobre intentos bloqueados y efectividad de mitigación. - Revisión de políticas ante nuevos vectores de ataque.		
Documentación			
Documentación	Entrega de resumen ejecutivo de la solución (Sobre C)		Entregar documento en sobre C
	Descripción de la arquitectura global de la solución (SASE, SD-WAN y AntiDDoS L7), incluyendo funcionalidades y diseño de despliegue (Sobre C)		Entregar documento en sobre C
	Estrategia de integración con el entorno de LANTIK (autenticación, monitorización, sustitución FW segundo nivel) (Sobre C)		Entregar documento en sobre C
	Plan de implantación y fases del proyecto: tareas, responsables, cronograma y entregables (Sobre C)		Entregar documento en sobre C
	Informe de actividades de migración (SD-WAN, activación de SASE, sustitución FW, pruebas piloto, validación y reversión) (Sobre C)		Entregar documento en sobre C
	Modelo de soporte, mantenimiento y servicio gestionado: organización, niveles de soporte y escalado (Sobre C)		Entregar documento en sobre C
	Plan de supervisión y control de la postura de seguridad: informes de telemetría, cumplimiento, riesgos e indicadores (Sobre C)		Entregar documento en sobre C
	Informe de escalabilidad y flexibilidad de la solución (usuarios, sedes, entornos híbridos y movilidad) (Sobre C)		Entregar documento en sobre C
	Entrega mensual de informe de cumplimiento de SLA, parámetros de servicio y penalizaciones (Durante la vigencia del contrato)		Entregar en los 15 primeros días de cada mes
	certificación vigente registrada en el CCN-CERT, en su catálogo CPSTIC		Entregar documento en sobre C



Para cualquier aclaración o ampliación de información se deben dirigir a:

Lantik S.A. M.P.
Sabino Arana, 44 – 48013 Bilbao
ppt.pt.lantik@bizkaia.eus
Teléfono: 944068900

A la fecha de firma electrónica

#FL#

Sin./Fdo.: JOSE IGNACIO HERNANDEZ GARCIA - 2026-06-08
IKUSPEGI TEKNOLOGIKOKO ARLOA
VISIÓN TECNOLÓGICA

Sin./Fdo.: IRATXE GOBANTES FURUNDARENA - 2026-06-08
SISTEMAK
SISTEMAS

Sin./Fdo.: BALBINO ZUBIAGA URBIETA - 2026-06-09
SEGURTASUN SAILA
DEPARTAMENTO DE SEGURIDAD

Sin./Fdo.: MARTIN BERASATEGUI MEJIAS - 2026-06-09
ARKITEKTURA TEKNOLOGIKOKO ARLOA
ÁREA DE ARQUITECTURA TECNOLÓGICA

Sin./Fdo.: JAVIER AZUMENDI CALABAZA - 2026-06-09
PLATAFORMA TEKNOLOGIKOKO ARLOA
ÁREA DE PLATAFORMA TECNOLÓGICA

Sin./Fdo.: IMANOL SAUTO AVELLANAL - 2026-06-09
SEGURTASUN ETA TEKONOLOGIA UNITATEKO ZUZENDARITZA
DIRECCIÓN DE UNIDAD DE SEGURIDAD Y TECNOLOGÍA





Sabino Arana, 44
48013 BILBAO (Bizkaia)

Tel: (+34) 944 068 900
Fax: (+34) 944 068 800

e-mail: LANTIK S.A. M.P.@bizkaia.eus
<http://LANTIK S.A. M.P..bizkaia.eus>



ER-2023/2005
El Diseño, el Desarrollo y el Mantenimiento de Aplicaciones Informáticas.
ER-0739/2006
La Compra de Bienes y Servicios y el Suministro e Instalación de Equipamiento Informático para la Diputación Foral de Bizkaia.
ER-0811/2008
La Atención al Cliente.