



4717 – PLIEGO PRESCRIPCIONES TÉCNICAS

Servicio gestionado de prevención, detección, triaje, orquestación y respuesta ante incidentes de seguridad

Área de Producción

Departamento de Seguridad



ÍNDICE

1	OBJETO	5
2	PRESUPUESTO	6
2.1	Ampliación	6
3	ESPECIFICACIONES TÉCNICAS.....	7
3.1	Especificaciones generales	7
3.1.1.	Servicio A: Servicio gestionado de prevención, detección, orquestación y respuesta ante incidentes de seguridad y servicio de ciberinteligencia y vigilancia de las marcas, personas y denominaciones del sector público foral del Territorio Histórico de Bizkaia.	7
3.1.2.	Servicio B: Oficina Técnica de Seguridad	12
3.2	Fases del servicio gestionado	13
3.2.1	Recogida de requerimientos.....	13
3.2.2	Diseño.	13
3.2.3	Implantación.	14
3.2.4	Prestación del servicio	14
3.2.5	Finalización y entrega del servicio	15
3.3	Entregables del servicio A	15
3.4	Modelo organizativo.....	16
4	CONDICIONES PARTICULARES	19
4.1	Plazo de entrega.....	19
4.2	Propuesta técnica (estructura).....	19
4.3	Penalizaciones	19
4.4	Prórroga	20
4.5	Instalación	20

4.6	Metodología y documentación	20
4.7	Modelo de gestion.....	20
4.7.1	Modelo Organizativo	20
4.7.2	Modelo Operativo	20
4.7.3	Gestión del Servicio	20
4.8	Forma de pago	21
4.9	Criterios de adjudicación	21
4.9.1	Criterios cuantificables automáticamente – Sobre B	21
4.9.2	Criterios no cuantificables automáticamente – Sobre C.....	25
4.10	Equipo de trabajo	26
4.11	Control de los trabajos	26
4.12	Confidencialidad	27
4.13	Propiedad intelectual	27
4.14	Metodología	27
4.15	Subcontratación	27
4.16	Perspectiva de género	28
4.17	Seguridad de la información	28
A.	Deber de confidencialidad.....	28
B.	Gestión interna de Lantik (medidas de securización interna) previas a la prestación	29
C.	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.....	30
D.	Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores”	30
E.	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.	30

F.	Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica.....	30
G.	Medidas de continuidad del servicio o proyecto	31
H.	Informe periódico del cumplimiento de la “Normativa de securización de entornos para prestación de servicio remoto”	31
I.	Evidencias de las buenas prácticas relativas al objetivo de control 11 “Seguridad Física y del entorno” de la norma de referencia ISO 27002 en el entorno de prestación.....	31
Anexo I – Acuerdos de Nivel de Servicio		33
	Monitorización de seguridad.....	33
	Operación del servicio.....	34

1 OBJETO

El objeto del presente pliego de prescripciones técnicas (desde este momento PPT) es la contratación para un periodo de dos años de los siguientes servicios:

- **Servicio gestionado** de prevención, detección, triaje, orquestación y respuesta ante incidentes de seguridad en modalidad 24x7x365 para toda la infraestructura de las tecnologías de información y comunicaciones (desde este momento TIC) , servicios y recursos tecnológicos del sector público foral del Territorio Histórico de Bizkaia (desde este momento Sector Público Foral), incluyendo la cooperación en la gestión, análisis y resolución de todos los incidentes de seguridad en los que participe Lantik.
- **Servicio de ciberinteligencia** y vigilancia de las marcas, personas, y denominaciones del sector público foral en la modalidad 24x7x365.
- **Servicio de “Oficina Técnica de Seguridad”** para la cooperación en programas/proyectos/ acciones/etc. dentro del ámbito de la seguridad de la información que se encuentren fuera de los servicios principales requerido en este PPT.

2 PRESUPUESTO

Se va a proceder a la contratación máxima por un importe neto de 1.080.000,00 €. Importe total 1.306.800,00 € IVA incluido (%21) para la duración del contrato: 2 (dos) años.

El presupuesto incluye TODOS los gastos para la provisión de TODOS los servicios solicitados en el pliego, además de TODAS las herramientas, licencias (Por ejemplo: Security Incident and Event Management (desde este momento SIEM) , Security Orchestration and Automated Response (desde este momento SOAR) , etc.) IaaS, hardware (sistemas, almacenamiento, comunicaciones, etc.), software (productos, etc.), personal, generales, financieros, transportes, dietas, desplazamientos, seguros, etc., y de cualquier otro tipo, necesarios para la totalidad de los servicios objeto del PPT.

En la oferta se deberá de presentar el **importe total de todos los servicios**:

- El servicio gestionado (A) que será el sumatorio del importe del Servicio gestionado de incidentes de seguridad y del Servicio de Ciberinteligencia.
- Servicio de “Oficina Técnica de Seguridad” (B), indicando en la oferta el precio/hora presupuestada para la oficina técnica.

El importe máximo se reparte de la siguiente forma:

- 800.000 euros IVA no incluido, en el servicio gestionado (A) de incidentes de seguridad y Servicio de ciberinteligencia y vigilancia de marcas.
- 280.000 euros, IVA no incluido, a consumir bajo demanda en el servicio de “Oficina Técnica de Seguridad” (B)
 - 70 €/hora máxima sin IVA, con un máximo de 4000 horas en el periodo del contrato.
 - En el caso de peticiones de urgencia que requieran el consumo de horas de Oficina Técnica en horario fuera del standard de Lantik (8x5), la hora podrá facturarse con el coeficiente de compensación de 1,5x.

Importe total para valorar = precio bienal A + (precio/hora B x4000)

Precio	Cantidad	Importe
Precio bienal A	1	Total A
Precio/hora B	4000	Total B
Importe total para valorar		Total A+Total B

Nota: Lantik S.A.M.P (desde este momento Lantik) se reserva el derecho de ejecutar solo las horas del Servicio de “Oficina Técnica de Seguridad” que sean necesarias durante la prestación del servicio hasta el máximo de 4000 horas en el periodo del contrato.

2.1 Ampliación

Debido a la evolución de la infraestructura tecnológica, servicios, proyectos, etc., podrían verse incrementados los sistemas, servicios o actuaciones necesarias a llevar a cabo, por lo que se considera incorporar la posibilidad de un incremento económico de hasta un 20% adicional.

3 ESPECIFICACIONES TÉCNICAS

A continuación, se enuncian las especificaciones técnicas de los servicios objeto del presente pliego.

Para la mejor preparación de este pliego, los licitadores tienen a su disposición documentación adicional con mayor nivel de detalle.

Para disponer de ella, se debe de solicitar explícitamente en la dirección de correo eskaintzak.lantik@bizkaia.eus con Asunto: "Expediente 4717 - Solicitud de información técnica adicional". Una vez finalizado el plazo de presentación, esta información deberá de ser destruida.

Lantik se reserva el derecho de proceder a la entrega de dicha documentación de forma presencial, si lo considerara oportuno.

3.1 Especificaciones generales

3.1.1. Servicio A: Servicio gestionado de prevención, detección, orquestación y respuesta ante incidentes de seguridad y servicio de ciberinteligencia y vigilancia de las marcas, personas y denominaciones del sector público foral del Territorio Histórico de Bizkaia.

A continuación, se indican las características principales del servicio:

- El servicio es "llave en mano".
- El servicio se ejecutará por fases, teniendo cada una de ellas sus entregables e hitos, tal y como se describe en detalle en el apartado "3.2 Fases del servicio".
- La empresa oferente debe de disponer de Certificado Gestión de Seguridad ISO/IEC 27.001 cuyo ámbito sea, al menos, el del servicio contratado.
- La empresa oferente debe de disponer de Certificado ENS para sistemas de información de nivel medio o superior cuya descripción sea, al menos, la del servicio contratado.
- La empresa oferente deberá estar constituido como CERT o CSIRT, formando parte de algunas de las asociaciones reconocidas CSIRT.ES, TF-CSIRT o FIRST.
- La empresa oferente deberá contar con al menos dos Centros de Servicios Gestionados SOC desde donde se provea el servicio ofrecido, redundados en diferentes localizaciones geográficas para garantizar la continuidad del servicio prestado. Dichos SOC deberán cumplir la normativa legal vigente referente al RGPD y ENS.
- Los sistemas y tecnologías necesarias para la provisión del servicio descrito en el presente pliego se podrán desplegar on-premise, en instalaciones de Lantik, o fuera de ellas, pero siempre dentro de infraestructura propiedad o gestionada por el proveedor, cumpliendo todos los requisitos legales y de seguridad aplicables.
- Los sistemas y tecnologías necesarias para la provisión del servicio deberán ser escalables, con el fin de poder responder a nuevas fuentes de información y datos, así como a nuevos escenarios de seguridad.
- Los sistemas y tecnologías necesarias para la provisión del servicio deberán tener contratado el soporte oficial del fabricante.
- Los logs de actividad y de incidentes detectados se podrán almacenar on-premise o en nube, siempre dentro de la infraestructura del proveedor, cumpliendo todos los requisitos legales y de seguridad aplicables. Los logs de actividad que gestionará el servicio serán los originados por la infraestructura y servicios TIC que gestiona Lantik.
- El servicio de ciberinteligencia y vigilancia de las marcas, personas, y denominaciones del sector público ubicado en el Territorio Histórico de Bizkaia en la modalidad 24x7x365; para 50 marcas, con el objetivo de detectar y prevenir de forma proactiva cualquier potencial amenaza que pueda darse contra los activos o reputación del sector público foral.
- La detección, triaje, comunicación, gestión, orquestación y respuesta de incidentes se realizará en modo 24x7x365 para incidentes clasificados como críticos, muy altos o altos según la tipología de clasificación que se definirá durante las primeras fases de despliegue del servicio.
 - El resto de los incidentes, tipo medio, bajo o muy bajo, se gestionarán en modalidad 8x5 según calendario laboral aplicable a Bilbao.

- El servicio deberá gestionar de forma completa del ciclo de vida de los incidentes de seguridad, desde su detección hasta su resolución y según escenarios y procedimientos establecidos, interactuando de forma autónoma con el resto de los servicios y áreas de Lantik, notificando sus acciones al Departamento de Seguridad; tanto en los incidentes detectados por el propio servicio como los notificados por terceros y que estén dentro del ámbito establecido.
 - Se deberá automatizar la gestión de estos incidentes, según escenarios definidos empleando diferentes tácticas y herramientas de scripting y SOAR.
 - Tras la resolución de incidente, se plantearán las lecciones aprendidas/retrospectivas para su estudio y, si procede, se realizará el diseño de procedimientos e incorporación de los mismos en los procesos de mejora dentro de los repositorios de información de Lantik.
- Tanto de forma preventiva como reactiva ante incidentes de seguridad, siempre siguiendo procedimientos establecidos junto a Lantik, el servicio operará en horario 24x7x365 los recursos técnicos gestionados por Lantik dedicados a la reducción del riesgo, tales como Firewalls, plataformas antimalware, proxys, etc.; siempre notificando sus acciones al Departamento de Seguridad y esperando conformidad en aquellas que no estén definidas en un determinado escenario de gestión de incidente modelado con anterioridad en las primeras fases de implantación del servicio.
- La empresa proveedora deberá describir todas las plataformas/herramientas propuestas (incluyendo herramientas SIEM y SOAR a desplegar) para la prestación del servicio, detallando al menos:
 - Nombre del producto y versión inicial con las que se iniciará el servicio
 - Funcionalidades que proporciona.
 - Arquitectura de integración de la herramienta para cumplir objetivos del servicio.
 - Metodologías y estándares que se seguirán para el desarrollo del servicio y evolución de la herramienta.
- La empresa oferente deberá describir la ubicación desde la que prestará el servicio y su Centro de operaciones de Seguridad (desde este momento SOC) , así como las características de la infraestructura utilizada para proporcionarlo y todas las consideraciones que estime oportunas, para garantizar la disponibilidad, integridad, confidencialidad, trazabilidad y no repudio de la información gestionada. Por este motivo, al menos se deberá detallar:
 - Descripción general de recursos a asignar a este servicio.
 - La ubicación física del SOC principal y posibles SOC's alternativos donde se realizará el servicio.
 - Certificaciones del personal del SOC, detallando sus perfiles profesionales.
 - Los sistemas de control de acceso físico a la infraestructura del servicio.
 - Red de gestión (aislada o compartida).
 - Existencia de un centro de gestión alternativo y planes de contingencia.
 - La seguridad de las líneas de conexión y canales de comunicación.
 - La seguridad en el acceso a las herramientas.
 - Arquitectura de red de seguridad para el SOC.
 - Certificaciones y cumplimiento de normativas de seguridad.
- El registro y la gestión de tareas realizadas, así como el registro y control de las incidencias y peticiones del servicio, se recogerán mediante procedimientos de Lantik.
- Se deberá rellenar la siguiente tabla, sobre las características de la empresa oferente:

Empresa	Certificados ISO 27001 el ámbito del servicio (SI/NO)	Certificado ENS en el ámbito del servicio (SI/NO)	Constituido como CERT/CSIRT (SI/NO)	Asociaciones reconocidas de las que forma parte	Centros SOC y ubicación	Visita a instalaciones de Lantik (SI/NO)
	(se deberá aportar fotocopia)	(se deberá aportar fotocopia)	(se deberá aportar fotocopia)	(se deberá aportar evidencia)		(aportar documento acreditativo)

Los objetivos principales del servicio son:

- Prevención, detección, triaje, orquestación y respuesta ante incidentes de seguridad en modalidad 24x7x365 durante todo el ciclo de vida de estos (desde su detección a su resolución).
 - Este objetivo requerirá, en su caso, la actuación de un Equipo de Respuesta a Incidentes (desde este momento ERI) conformado por recursos del proveedor, pudiendo actuar de forma autónoma según escenarios consensuados y apoyado, en su caso, por personal de Lantik; pudiéndose requerir la presencia física de recursos del proveedor en emplazamientos del Sector Público Foral.
- Vigilancia de las marcas, personas, y denominaciones del sector público foral en la modalidad 24x7x365.
- Centro de operaciones de seguridad en modalidad 24x7x365.
- Gestión proactiva de vulnerabilidades y amenazas (threat hunting) en activos y servicios tecnológicos gestionados por Lantik:
 - Auditoría técnica continua de la infraestructura del Sector Público Foral para detección proactiva de vulnerabilidades que puedan presentar.
 - Test de intrusión y vulnerabilidades periódicos automatizados en los servicios tecnológicos del Sector Público Foral.
 - Se realizará, al menos, un test de intrusión completo (automatizado y manual) anual en un servicio seleccionado por Lantik.
 - En la oferta el proveedor deberá indicar el número de test de intrusiones completos incluidos en el servicio.
- Evaluación continua de la configuración de seguridad y monitorización de la integridad de la configuración de la infraestructura tecnológica gestionada por Lantik.
 - Cooperación en la resolución de los defectos detectados.
- Vigilancia periódica del cumplimiento técnico para la normativa aplicable.

Para cumplir estos objetivos, el servicio deberá constar, al menos, de:

- Un servicio de monitorización y soporte a la gestión de incidentes de seguridad en modalidad 24x7x365 con las siguientes características:
 - Provisión, despliegue e integración de herramientas (incluyendo, al menos, herramientas SIEM y SOAR) en modalidad de servicio (herramientas propiedad de la empresa proveedora) que gestione todo el ámbito del servicio y entorno tecnológico del Sector Público Foral.Las soluciones SIEM y SOAR desplegadas deberán cumplir al menos los siguientes requisitos:
 - La solución SIEM aportada por la empresa oferente deberá disponer de certificación "Common Criteria" en alguna de las versiones del producto.
 - Deberá aportar un conjunto suficiente de conectores, reglas de correlación y alertas completo y suficiente desde el inicio para la correcta gestión de la seguridad de acuerdo con las necesidades de Lantik. Gestionando aproximadamente 12.000 eventos por segundo (en adelante, EPS) o 200 Gigabytes de logs diarios.
 - Deberá ser escalable de forma sencilla para poder soportar la gestión de nuevas fuentes de información y datos durante el periodo del contrato; así como nuevos escenarios de gestión de incidentes de seguridad.
 - Deberá permitir la automatización de operaciones de seguridad para la gestión de incidentes y respuesta inmediata y gestionada ante incidentes de seguridad, según la definición de escenarios y/o tácticas automatizadas (en adelante, playbooks) acordadas.
 - Poder realizar conexión a redes colaborativas de intercambio de datos de seguridad como DXL, OTX u otra de características similares para automatizar

el despliegue de detección y protección de IOC.

- Debe permitir ver en tiempo real el ciclo de vida de eventos e incidentes de seguridad, así como la salud de seguridad de la infraestructura y activos monitorizados, desde un punto de gestión centralizado, con una consola única de supervisión y gestión y diseño de cuadros de mando de acuerdo con diferentes roles acordados al inicio del servicio (técnico, dirección, etc.) para la gestión tanto del estado de seguridad de los activos dentro del alcance del servicio como de la salud del propio servicio..
- Debe permitir capacidades de análisis de comportamiento de usuarios y perfilado por aprendizaje (machine learning).
- Debe disponer de capacidades forenses de incidentes de forma nativa.
- Debe disponer de capacidades de análisis de flujos en capa 7 de forma nativa.
- Debe permitir la monitorización y retención de trazas para permitir detectar y analizar incidentes de seguridad dentro de, al menos, los siguientes casos de uso:
 - Trazabilidad y respuesta automática antes eventos generados siguiendo escenarios acordados para el servicio.
 - Trazabilidad y detección de sistemas comprometidos y/o infectados por programas malignos (malware) o intentos de compromiso de los mismos.
 - Aportación de información adicional y de contexto para validar y/o descartar automáticamente por falsos positivos las alertas proporcionadas por la infraestructura de seguridad (por ejemplo, creación de reglas IPS, reglas WAF, políticas FW...).
 - Monitorización de conexiones a la red, a elementos críticos de la infraestructura y transmisiones anormales de datos que puedan ocasionar un incidente de seguridad.
 - Trazabilidad de cambios en sistemas críticos.
 - Trazabilidad de acciones realizadas con cuentas privilegiadas en diversos sistemas.
 - Trazabilidad del uso de aplicaciones y servicios, detectando incidentes y ataques que puedan sufrir.
 - Trazabilidad del estado de seguridad y protección de los activos.

- Se deberá rellenar la siguiente tabla sobre la solución SIEM Aportada:

Nombre Solución SIEM	Versión SIEM	Common Criteria (SI/NO) y Versión certificada	Soporte Oficial fabricante (SI/NO). Detallando número de licencia o evidencia de contrato en vigor con fabricante
Ref. 1			

- Se deberá rellenar la siguiente tabla sobre la solución SOAR Aportada:

Nombre Solución SOAR	Versión SOAR	Soporte Oficial fabricante (SI/NO). Detallando número de licencia o evidencia de contrato en vigor con fabricante
Ref. 1		

- Administración y explotación de los sistemas desplegados por parte de la empresa proveedora, incluyendo la incorporación de nuevas fuentes de datos cuando se requiera, incorporación de nuevas reglas de alerta y correlación, actualizaciones de la plataforma, o evolución de los informes y cuadros de mando.
 - Mantenimiento de un histórico de eventos de al menos 3 meses en tiempo real no comprimido (caliente), 1 año en almacenamiento comprimido de rápido acceso y 2 años comprimido en almacenamiento offline; con el objeto de poder realizar investigaciones forenses. El espacio de almacenamiento necesario correrá a cargo del proveedor.
- Servicio de gestión, operación y monitorización en modalidad 24x7x365 de la infraestructura de seguridad propiedad de Lantik (Firewalls, Proxies web, proxies correo, solución antivirus y antimalware corporativa, IPS, WAF...), incluyendo en este servicio el despliegue de nuevas políticas, reglas y firmas en dicha infraestructura. Esta operativa se realizará tanto de forma proactiva en operativa habitual de seguridad para prevenir incidentes, como reactiva, cuando sea necesario operar dicha infraestructura para activar salvaguardas necesarias ante amenazas o incidentes de seguridad, según escenarios y protocolo definido entre ambas partes al inicio del contrato.
- Servicio de Ciberinteligencia y vigilancia de marca: Detección continuada, para 50 marcas, en modalidad 24x7x365 de amenazas y ataques potenciales que puedan sufrir el Sector Público Foral, para ello se deberá vigilar cualquier canal que pueda proporcionar información (internet, medios de comunicación...), empleando diversas técnicas (OSINT, SIGINT, GEOINT, HUMINT...); incluyendo colaboración o consulta con entidades tipo CERT.
- Servicio de Equipo de Respuesta ante Incidentes (ERI): soporte completo a la gestión de incidentes de seguridad durante todo su ciclo de vida que puedan producirse, en modalidad 24x7x365, mediante la investigación en detalle de los incidentes (origen sistemas afectados, patrones...) y la realización y ejecución de propuestas de medidas de contención y resolución de los incidentes en colaboración, en su caso, con personal de Lantik. Tras la resolución se realizará el informe del incidente en el formato que Lantik determine, donde se incluirán además propuestas de mejora y lecciones aprendidas.
- A partir del hito de puesta en marcha del servicio, y durante los 4 meses siguientes, Lantik puede requerir a la empresa adjudicataria la presencia periódica según necesidades de un recurso local en instalaciones de Lantik con soporte 8x5 y emergencias, para el despliegue del servicio, gestión de incidentes, operación de plataformas de seguridad y traslado de conocimiento.
 - Durante todo el contrato, y en formato 24x7x365, el proveedor deberá disponer de recursos locales especializados en el servicio prestado, con posibilidad de acudir en un plazo de dos horas a instalaciones del Sector Público Foral en caso de ser necesario para dar respuesta a incidentes como parte del ERI.
- Servicio de gestión proactiva de vulnerabilidades y amenazas en activos y servicios del Sector Público Foral:
 - Realización de análisis automatizados de intrusión y escaneos automatizados de vulnerabilidades, de forma periódica y bajo demanda a petición de Lantik. Se deberá indicar la periodicidad en la oferta, debiendo ser la periodicidad mínima de dichos escaneos trimestral.
 - Se realizará, al menos, un análisis anual de intrusión completo (automatizado y manual) en un servicio seleccionado por Lantik. Se deberá indicar en la oferta el número adicional de test de intrusión completos anuales ofertados por el proveedor.
 - Gestión del ciclo de vida completo de las vulnerabilidades (detección, análisis, remediación, cierre).

- Se controlará la conexión de nuevos elementos de infraestructura (todo tipo de elementos. En el caso de equipos de personas usuarias será necesario validar solo la imagen modelo), generando un informe negativo para aquellos elementos que no cumplan con los criterios/configuración mínima establecida de seguridad.
- Se deberá disponer de un cuadro de mando según diferentes roles acordados al inicio del servicio (técnico, dirección, etc.), donde se pueda visualizar de forma continua el estado de salud del servicio y de la seguridad de los activos dentro del alcance, con indicadores a consensuar entre el proveedor y Lantik, entre los que se deberán incluir, al menos, los siguientes indicadores, guardando el valor actual y un histórico de cada uno de ellos:
 - Índice de Nivel de Riesgo al que está sometida la organización según criterio normalizado consensuado con Lantik en las primeras fases del servicio.
 - Número de vulnerabilidades críticas y graves según criterios normalizados como CVE o CVSS detectadas y no solventadas.
 - Número de ataques recibidos, diferenciados por ventana de ataque.
 - Número de incidentes de seguridad abiertos, junto con su grado de criticidad.
 - % de disponibilidad de la herramienta SIEM.
 - Número de Eventos por Segundo tratados.
 - Información mostrada en el cuadro de mandos exportable en un formato entendible para otras herramientas de análisis de datos como puede ser PowerBI.
- La gestión y supervisión del servicio se realizará en base a los acuerdos de nivel de servicio, informes y entregables,
- Soporte técnico al mantenimiento y evolución de los procedimientos de Lantik en materia de Seguridad de la Información, plasmados en el Plan de Calidad.

3.1.2. Servicio B: Oficina Técnica de Seguridad

Provisión de una Oficina Técnica de Seguridad para la ejecución de diferentes tipos de servicios de seguridad según necesidades. Por ejemplo: test de intrusión completos adicionales a los incluidos en el servicio, consultoría y despliegue de controles técnicos de seguridad, desarrollo de políticas y procedimientos de seguridad, formación en materia de seguridad o cualquier otra tarea relacionada solicitada por el Departamento de Seguridad.

Lantik podrá solicitar hasta un máximo de 4000 horas a lo largo de la duración del contrato y según sus necesidades, al precio/hora ofertada por la empresa licitante.

La realización de los proyectos asociadas a la Oficina Técnica de Seguridad se comunicará según se generen las necesidades de acuerdo con escenarios de riesgo. Por parte de la empresa adjudicataria, exigirá:

- La valoración previa, en esfuerzo (horas).
- Aceptación por parte de Lantik de esta valoración.
- Gestión del proyecto/tareas encomendadas de acuerdo con la metodología de proyectos ágil vigente en Lantik.

3.2 Fases del servicio gestionado

La propuesta presentada, debe desarrollarse en las fases que se describen a continuación, incluyendo una planificación detallada, para cada una de ellas.

Las Fases de recogida de requerimientos, diseño e implantación del servicio se deberán de completar en el tiempo máximo de 12 semanas desde la solicitud de inicio de los servicios.

3.2.1 Recogida de requerimientos

Durante esta actividad se deberán llevar a cabo:

- Recopilación de información necesaria para la implantación de los servicios en las condiciones indicadas.
- Evaluación de la situación respecto los servicios que se van a proporcionar, análisis diferencial y propuesta de planificación de puesta en marcha del servicio.
- Realización del primer análisis de activos y vulnerabilidades, de los requeridos como parte del servicio, que sirva como línea base de este.

El hito de finalización de esta fase será la entrega de un documento recopilatorio de toda la información necesaria para implantar el servicio y el resultado del primer análisis de activos, vulnerabilidades encontradas y plan de mitigación correspondiente.

3.2.2 Diseño.

Durante esta actividad se deberán:

- Inventariar los activos que se monitorizan e integran con el servicio, distinguiendo cuales de ellos serán también operados por el proveedor.
- Análisis en profundidad de Infraestructura, servicios y recursos ubicados en las redes de Lantik.
- Diseño de reglas y conectores necesarios para el servicio en la herramienta SIEM.
- Diseño inicial de playbooks y/o escenarios automatizados de respuesta ante incidentes de seguridad.
- Definir los procesos que se llevarán a cabo por el servicio para cumplir todos los objetivos marcados en el presente pliego, incluyendo su puesta en marcha y las interacciones entre los diferentes agentes que participan.
- Si fuera necesario, adaptación del servicio según el marco normativo y las buenas prácticas. Principalmente ENS, Reglamento General de protección de datos e ISO 27001.
- Análisis y mejora (o desarrollo cuando sea necesario) del Plan de respuesta a incidente de la organización y todos los procedimientos asociados para la interacción con el presente servicio.
- Definición de los procedimientos iniciales de puesta en marcha, monitorización, gestión y explotación de los sistemas de seguridad dentro del ámbito de este pliego
- Definición del plan de comunicación y escalado del servicio (tanto para incidentes de seguridad como incidencias de las plataformas operadas).
- Si fuera necesario, definir las herramientas necesarias para desarrollar los procesos.
- Definición de objetivos, métricas e indicadores que permitan evaluar la eficiencia de los procesos definidos.
- Definir las responsabilidades y modelo de relación. Se determinarán claramente dentro de los flujos de proceso cuales son los roles y responsabilidades del proveedor y Lantik.

- Definir los informes necesarios y periodicidad de estos, para cubrir al menos los siguientes objetivos:
 - Seguimiento de los objetivos de eficiencia de los procesos.
 - Cumplimiento de Acuerdos de Nivel de Servicio.
 - Cuadro de mando Seguridad.
- Definir la arquitectura tecnológica, que soporte los procesos y procedimientos definidos.
- Definir un plan de continuidad del servicio.

El hito de finalización de esta fase será la entrega de un documento de diseño completo de la solución del servicio a implantar, tanto la solución técnica como los procedimientos del servicio de acuerdo con los puntos anteriores.

3.2.3 Implantación.

Durante esta actividad se deberán:

- Aplicar los procesos y procedimientos definidos en la fase de diseño.
- La empresa proveedora será responsable de la implantación de las herramientas, tecnologías y procedimientos necesarios para cumplir los objetivos del servicio.
 - En esta fase deberá implantarse de forma completa la solución SIEM e iniciar el proceso de automatización de las respuestas a la gestión de incidente según escenarios definidos
- La empresa proveedora será responsable de planificar las actividades destinadas a la formación de los roles identificados en Lantik.
- Lantik será responsable de:
 - Realizar las pruebas de integración, el despliegue y la implantación de los agentes o configuraciones en los sistemas terminales para la generación y envío de los eventos.
 - Implantar y divulgar los procesos y procedimientos definidos dentro de la organización.

El hito de finalización de esta fase será la implantación efectiva del servicio según la definición realizada en las dos fases anteriores, incluyendo la puesta en producción de la herramienta SIEM y la entrega de un documento que evidencia dicha implantación. A partir de aquí se considera que el servicio se pone en marcha.

3.2.4 Prestación del servicio

Durante esta actividad se deberán realizar los siguientes servicios:

- Completar de forma efectiva la automatización de la respuesta ante incidentes de seguridad, empleando la herramienta SOAR, de acuerdo con los escenarios definidos en la fase de diseño.
 - Esta acción de automatización se deberá finalizar antes de concluir el primer año de prestación del servicio.
- Operación de las herramientas propiedad del proveedor necesarias para alcanzar los objetivos del servicio.
 - En el transcurso del servicio Lantik podrá solicitar la inclusión o exclusión de nuevos elementos en el sistema de monitorización e información mostrada en los cuadros de mando del servicio, de acuerdo con sus necesidades operativas; así como la inclusión de nuevos escenarios de gestión de incidentes de seguridad, incluyendo la posible automatización de la respuesta a los mismos.
- Gestión y operación de las plataformas de seguridad propiedad de Lantik, según el alcance

- del servicio, en modalidad 24x7x365.
 - En el transcurso del servicio Lantik podrá solicitar la inclusión o exclusión de nuevos elementos para su gestión u operación, de acuerdo con sus necesidades operativas.
- Realización de servicios de Ciberinteligencia y vigilancia de marcas definidos, en modalidad 24x7x365.
- Realización de análisis de vulnerabilidades periódicas determinadas en el servicio
 - Incluyendo gestión de estas vulnerabilidades (propuesta de solución, resolución de dudas y propuesta de mejora).
- Análisis, Respuesta y seguimiento de los incidentes de seguridad detectados o reportados durante todo el ciclo de vida de estos.
 - En modo 24x7x365 aquellas clasificadas como críticas, muy altas o altas.
 - En modo 8x5 el resto de los casos.
- Atender las peticiones de servicio solicitadas por Lantik en materia de análisis y tratamiento de riesgos y gestión de incidentes.
- Mantenimiento del inventario de activos monitorizados y fuentes de datos.
- Presentación de informes definidos en la fase de diseño.
- Ejecución de los proyectos encargados a la Oficina Técnica de Seguridad.
- Reuniones periódicas de seguimiento y coordinación del servicio mínima mensual entre las personas coordinadoras por ambas partes.

Al ser esta fase la propia de prestación de servicio, se considera finalizada a la finalización del contrato.

3.2.5 Finalización y entrega del servicio

Durante esta actividad, se deberán realizar los siguientes servicios:

- Recopilación y entrega de toda la información generada por el servicio (informes, conectores, reglas, escenarios, playbooks...) en un formato exportable.
- Entrega de los logs y eventos disponibles en un formato reutilizable según periodicidad de mantenimiento acordada; eliminándolos de forma segura por la parte del proveedor después de realizar dicha entrega; se deberá entregar a Lantik un certificado de dicha eliminación.
- Desinstalación ordenada de todos los sistemas propiedad del proveedor de los CPD de Lantik, así como la vuelta atrás de la configuración que haya sido necesaria realizar en los sistemas propiedad de Lantik para dar el servicio, si fuera necesario y si Lantik así lo determina.

El hito de finalización de esta fase será la firma de un documento de fin de servicio.

3.3 Entregables del servicio A

Se deben proporcionar, entre otros, los siguientes entregables por parte de la empresa proveedora:

- Diseño y arquitectura de la solución tecnológica.
- Definición de roles y responsabilidades del servicio.
- Documentación sobre la plataforma de operación y gestión de incidentes de servicio implantada.
 - Cualquier conector desarrollado para dicha plataforma durante el desarrollo del servicio será considerado propiedad de Lantik.
 - Guías y/o procedimientos de configuración de la infraestructura para envío de eventos.
 - Manual técnico de la solución implantada.
- Diseño y manual del cuadro de mando e implantación de las herramientas.
- Actas de reuniones que se celebren.
- Informes técnicos, de seguimiento y acuerdos de nivel de servicio periódicos.
- Definición de los procedimientos para la gestión de las incidencias y peticiones de servicio

enumerados en el catálogo. Incluyendo:

- Procedimiento de gestión de cambios y solicitudes de servicio.
 - Manual de usuario de las herramientas implantadas, para gestión de incidencias de servicio.
- Plan de Continuidad del servicio.
- Documentación de tareas de la Oficina Técnica de Seguridad

3.4 Modelo organizativo

La empresa adjudicataria deberá disponer de la organización necesaria para acometer con éxito los servicios solicitados.

3.4.1 Equipo técnico

Se deberá de contar como mínimo con:

- Un perfil gestor del servicio, en horario 8x5, con las siguientes funciones principales:
 - Control y seguimiento de los servicios, asistencia a las reuniones periódicas de coordinación, etc.
 - Gestión habitual del ciclo de vida de las tareas encomendadas al servicio y Oficina Técnica de seguridad, siguiendo metodologías ágiles empleadas en Lantik.
 - Centralizar y coordinar las relaciones con Lantik.
 - Aseguramiento de la calidad del servicio, mejora continua y ANS.
 - Debido a la naturaleza del servicio, se nombrará al menos dos personas que respondan a este perfil.
- Un perfil técnico de referencia del servicio en horario 24x7x365, con las siguientes funciones principales:
 - Control y seguimiento técnico del servicio, con asistencia a las reuniones periódicas de coordinación.
 - Propuestas de mejora del servicio de acuerdo con escenarios de riesgo y amenazas.
 - Presentación de informes y análisis solicitados.
 - Gestión técnica de las tareas encomendadas a la Oficina Técnica de Seguridad.
 - Durante todo el contrato, y en 24x7x365, deberá acudir en un plazo de dos horas a instalaciones del Sector Público Foral en caso de ser necesario para dar respuesta a incidentes como parte del ERI.
 - Debido a la naturaleza del servicio, se nombrará al menos dos personas que respondan a este perfil.
- Perfiles técnicos de SOC y Ciberinteligencia en horario 24x7x365, para la realización de las tareas propias del servicio como la monitorización de alertas de ciberseguridad y herramientas propietarias del proveedor, operación de la infraestructura de seguridad gestionada por Lantik, y Ciberinteligencia.
- Perfiles de Equipo ERI, en horario 24x7x365, para la gestión y cooperación en la resolución de incidentes de seguridad detectados, durante el ciclo de vida completo de los mismos, debiendo poder acudir en el plazo de dos horas desde la notificación a instalaciones del Sector Público Foral al menos una persona de este perfil.

- Perfiles técnicos necesarios para acometer las tareas encomendadas a la Oficina Técnica de Seguridad.

La empresa proveedora deberá designar varias personas que cumplan los diferentes perfiles.

El equipo de trabajo deberá acreditar una experiencia suficiente en los servicios solicitados, exigiéndose como mínimo:

- El perfil gestor del servicio asignado por la empresa oferente deberá haber dirigido o estar dirigiendo al menos dos (2) servicios de seguridad gestionada durante al menos seis meses ininterrumpidos cada uno de ellos en los últimos tres años (2019,2020,2021); aportando referencias de los mismos (tipo de proyecto, breve descripción del mismo, empresa, persona y datos de contacto, año de comienzo, duración).
- Al menos una de las personas que respondan al perfil de gestor del servicio deberá disponer de certificados o formación en gestión de proyectos, como PMP, PMI-ACP, ICAgile o Scrum máster.
- Al menos dos personas de entre los perfiles técnicos de referencia y/o SOC asignados al servicio deberán disponer, en caso de que existan, de certificados vigentes en la tecnología SIEM ofertada. En caso de no existir certificados, se deberá aportar evidencias de formación específica en dichas tecnologías.
- Al menos dos personas de entre los perfiles técnicas de referencia y/o SOC asignados al servicio deberán disponer, en caso de que existan, de certificados vigentes en la tecnología SOAR ofertada. En caso de no existir certificados, se deberá aportar evidencias de formación específica en dichas tecnologías.
- De entre el personal técnico asignado al servicio: técnico de referencia, SOC, Ciberinteligencia y/o ERI se deberá disponer de, al menos, un certificado de cada tipo de los siguientes tres tipos de certificados:
 - Certificados de fabricantes de Firewalls de red de acuerdo con la tecnología empleada en Lantik.
 - Certificados de seguridad ofensiva de las entidades EC Council, Offensive Security, GIAC, CompTIA; como, por ejemplo, EC Council Certified Ethical Hacker, EC Council Certified Penetration Testing Professional, EC Council Licensed penetration tester, CompTIA PenTest+, Offensive Security OSCP, Offensive Security OSWE. Offensive Security OSWP, Offensive Security OSEP, GIAC Penetration tester, GIAC Web Application Penetration Tester, GIAC Mobile Device Security Analyst, GIAC Exploit Researcher and Advanced Penetration Tester, GIAC Assessing and Auditing Wireless Networks, GIAC Cloud penetration Tester.
 - Certificados de análisis forense de incidentes y seguridad defensiva de las entidades EC Council, Offensive Security, CompTIA, GIAC o ISC2 como, por ejemplo, Offensive Security OSDA, EC Council Certified Network Defender, EC Council Certified Threat Intelligence Analyst, EC Council certified Incident Handler, EC Council forensic investigator,, EC Council Certified soc analyst, EC Council disaster recovery profesional, CompTIA Cybersecurity Analyst (CySA+), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler, GIAC Enterprise Vulnerability Assessor,, GIAC Open Source Intelligence, GIAC Certified Intrusion Analyst, GIAC Continuous Monitoring Certification, GIAC Defensible Security Architecture, GIAC Certified Detection Analyst, GIAC Security Operations Certified, GIAC Web Application Defender, GIAC Clud Security Automation, GIAC Battlefield Forensics and Acquisition, GIAC Certirified Forensic Examiner, GIAC Defending Advanced Threats, GIAC Certified Enterprise Defender, GIAC Information Security Professional, GIAC Network Forensic analyst, GIAC Cyber Threat Intelligence, GIAC Reverse Engineering Malware, ISC2 SSCP, ISC2 CCSP.

Esta información deberá aportarse en el siguiente cuadro resumen.

Se deberá rellenar la siguiente tabla sobre solvencia técnica profesional:

Id. (1)	Nombre y apellidos	Función (2)	Titulación académica	Superior (Si/No)	Servicios en los que ha participado (3)	Certificaciones o formación (4)	N.º de meses en la empresa
1							
2							
3							
n							

- (1) Identificador: nº correlativo que identifica a cada persona del equipo
- (2) Función que desempeñará mayoritariamente en el servicio (gestor del servicio, Técnico de referencia, técnico de SOC/Ciberinteligencia/ERI). Deberán estar todas las funciones en el equipo presentado y si alguna persona desempeña 2 o más roles, se deberán indicar todos ellos
- (3) Indicar responsabilidad y referencia del servicio, así como el tiempo que ha permanecido participando en el servicio
- (4) Certificaciones o formaciones que atesora esa persona miembro del equipo de trabajo, Indicando el tipo de cada certificación (Gestión de proyectos, SIEM, SOAR, Firewall, seguridad ofensiva, seguridad defensiva, análisis forense)

3.4.2 Responsabilidades de la empresa adjudicataria

- Puesta en marcha y cumplimiento del nivel de servicio.
- Disponer, gestionar y mantener actualizada la infraestructura necesaria para la prestación del servicio.
- Entregar a Lantik la información y documentos anteriormente indicados e indicadores que permitan el control continuo del servicio.
- Garantizar la capacidad del servicio asignado los medios o recursos que fueren necesarios para la adecuada prestación de este.
- Monitorizar la prestación del servicio de acuerdo con los ANS.

4 CONDICIONES PARTICULARES

4.1 Plazo de entrega

El objeto del presente expediente deberá entrar en servicio a la firma de contrato y tendrá una duración de 2 (dos) años.

4.2 Propuesta técnica (estructura)

De cara a la correcta valoración de los criterios no cuantificables automáticamente (sobre C), la propuesta técnica presentada por la empresa licitadora en el **sobre C deberá ajustarse como máximo a 50 páginas** a una sola cara, tamaño de letra mínimo equivalente al tipo "Arial" de 10 pt y con márgenes de al menos 2,5 cm, y deberá contener como mínimo los siguientes apartados:

- Introducción
- Descripción servicio
 - Herramientas que desplegar en el servicio
 - Modelo organizativo
 - Modelo operativo
 - Gestión del servicio
 - Fases de implantación del servicio

No contabilizará en las 50 páginas la información necesaria para acreditar el apartado "Equipo técnico", los cuadros resumen, ni los modelos de entregables, en caso de presentarlos. Se podrán añadir anexos a modo informativo, pero en ningún caso la información contenida en ellos será considerada para la valoración de los criterios no cuantificables automáticamente.

4.3 Penalizaciones

Se podrán aplicar las siguientes penalizaciones en el servicio A: Servicio gestionado:

- Penalización de 2.000,00 euros (sin IVA) por cada incidente de criticidad alta que no sea comunicado en el Tiempo máximo de notificación de incidentes especificado. Por cada 6 horas adicionales de no comunicación se añadirán 500,00 euros (sin IVA) de penalización.
- Penalización de 1.500,00 euros (sin IVA) por cada dos incidentes de criticidad media que no sean comunicados en el tiempo máximo de notificación de incidentes especificado.
- Penalización de 1.000,00 euros (sin IVA) por cada tres incidentes de criticidad baja que no sean comunicados en el tiempo máximo de notificación de incidentes especificado.
- Penalización de 1.000,00 euros (sin IVA) cada vez que el % trimestral de falsos positivos en incidentes se vea superado.
- Penalización de 2.000,00 euros (sin IVA) por cada vez que un falso negativo de criticidad alta (incidente real no comunicado) supere el número máximo de falsos negativos anuales especificado.
- Penalización de 500,00 euros (sin IVA) cada informe solicitado por Lantik que supere el tiempo máximo de generación especificado.
- Penalización de 500,00 euros (sin IVA) por cada punto porcentual inferior al porcentaje trimestral de disponibilidad especificado.

El incumplimiento reiterado podría suponer la rescisión total del contrato.
En caso de que el pago por parte de Lantik estuviera realizado con anterioridad, la empresa adjudicataria abonará a Lantik el importe de la penalización.

4.4 Prórroga

El contrato será prorrogable opcionalmente por periodos mensuales, hasta un máximo de 36 meses. Las horas del servicio de Oficina Técnica se ampliarán en proporción al periodo prorrogado, en base una regla de tres, tomando como patrón que 36 meses suponen 6000 horas (las máximas contempladas).

Para que la renovación surta efecto, Lantik, deberá comunicar por escrito a la empresa adjudicataria su intención de prorrogar el contrato. En el caso de prórroga se mantendrán los precios.

4.5 Instalación

La instalación del hardware, software, licencias, etc., necesarias para la prestación de este servicio, corre a cargo de la empresa adjudicataria; excluyendo la infraestructura propiedad de Lantik. Estas tareas de instalación serán acordadas con Lantik al inicio del contrato, pudiéndose estas acciones llevar a cabo en horario 24x7.

4.6 Metodología y documentación

La empresa adjudicataria estará obligada a cumplir los procedimientos, normas y estándares establecidos por Lantik relativos al servicio demandado.

4.7 Modelo de gestion

El modelo de gestión, cuya propuesta inicial deberá ser planteada por la empresa licitadora, deberá incluir los siguientes elementos:

4.7.1 Modelo Organizativo

La empresa licitadora presentará la estructura organizativa que compondrá el equipo de trabajo propuesto para la prestación del servicio.

En ella se incluirán las líneas generales de la composición del equipo de trabajo describiendo la estructura organizativa del mismo en función de los servicios y actividades a desempeñar.

4.7.2 Modelo Operativo

La empresa licitadora presentará un modelo operativo para el servicio y describirá los procedimientos y tecnología asociados al servicio mediante una propuesta de funcionamiento y operación de los mismos.

4.7.3 Gestión del Servicio

La empresa licitadora será responsable de proporcionar de forma periódica los informes acordados y que serán utilizados como parte del seguimiento.

La empresa licitadora deberá proponer modelos de informes y de notificación de incidentes y eventos del servicio; así como diferentes informes de la salud de seguridad del Sector Público Foral y del propio servicio y del cuadro de mandos requerido en el mismo.

La empresa adjudicataria utilizará los sistemas de Lantik para el registro de incidencias, consultas y problemas, así como para la gestión de las peticiones asignadas. La información se actualizará periódicamente pudiendo ser diaria, semanal o mensual según necesidades.

Se realizarán los trabajos objeto del presente contrato siguiendo la metodología definida por Lantik.

4.8 Forma de pago

La empresa adjudicataria emitirá dos facturas al final de cada trimestre por cada uno de los servicios desglosados a continuación:

- Precio fijo trimestral que será el importe presentado para el servicio gestionado (A) dividido entre 8 trimestres.
- Horas correspondientes a las tareas entregadas y validadas por Lantik relacionadas con el servicio de Oficina Técnica (número de horas x precio/hora B).

Lantik, realizará los pagos de las facturas en los 30 días siguientes a la fecha de recepción de dicha factura, a conformidad.

4.9 Criterios de adjudicación

Para la adjudicación se tendrán en cuenta los siguientes criterios de valoración:

4.9.1 Criterios cuantificables automáticamente – Sobre B

Criterio valoración económica: Hasta un máximo de 40 puntos.

- Se valorará con hasta un máximo de 30 puntos: Servicio Gestionado, incluyendo servicio de ciberinteligencia.

Se puntuará con un total de 25 puntos la hipotética oferta cuyo precio coincida con la media aritmética del precio de las ofertas presentadas y aceptadas por Lantik.

A las ofertas cuyo precio sea superior a la media aritmética mencionada, se las puntuará de forma proporcional con respecto a la media aritmética (con un máximo de 25 puntos).

$$P_i = \frac{Of_m}{Of_i} \cdot 25$$

Siendo:

- P_i : Puntuación de la oferta valorada i
- Of_i : Oferta (precio) comprometida por el licitador i
- Of_m : Media aritmética de las ofertas presentadas y aceptadas por Lantik

A las ofertas cuyo precio sea inferior a la media aritmética de las ofertas se les otorgará una puntuación total de 25 puntos más un incremento de hasta 5 puntos.

$$Incr. P_i = \frac{Of_m - Of_i}{Of_m - Of_e} \cdot 5$$

Siendo:

- *Incr. P_i : Incremento de puntuación de la oferta valorada i*
- *Of $_i$: Oferta (precio) comprometida por el licitador i*
- *Of $_m$: Media aritmética de las ofertas presentadas y aceptadas por Lantik*
- *Ofe: Oferta más económica de las ofertas presentadas y aceptadas por Lantik*

- Se valorará con hasta un máximo de 10 puntos la hora de Oficina Técnica

Se puntuará con un total de 8 puntos la hipotética oferta cuyo precio/hora coincida con la media aritmética del precio/hora de las ofertas presentadas y aceptadas por Lantik.

A las ofertas cuyo precio/hora sea superior a la media aritmética mencionada, se las puntuará de forma proporcional con respecto a la media aritmética (con un máximo de 8 puntos).

$$P_i = \frac{Of_m}{Of_i} \cdot 8$$

Siendo:

- *P_i : Puntuación de la oferta valorada i*
- *Of $_i$: Oferta (precio/hora) comprometida por el licitador i*
- *Of $_m$: Media aritmética de las ofertas presentadas y aceptadas por Lantik*

A las ofertas cuyo precio/hora sea inferior a la media aritmética de las ofertas se les otorgará una puntuación total de 8 puntos más un incremento de hasta 2 puntos.

$$Incr. P_i = \frac{Of_m - Of_i}{Of_m - Ofe} \cdot 2$$

Siendo:

- *Incr. P_i : Incremento de puntuación de la oferta valorada i*
- *Of $_i$: Oferta (precio/hora) comprometida por el licitador i*
- *Of $_m$: Media aritmética de las ofertas presentadas y aceptadas por Lantik*
- *Ofe: Oferta más económica de las ofertas presentadas y aceptadas por Lantik*

Se considerarán desproporcionadas o temerarias las ofertas que se encuentren recogidas en los supuestos especificados en el artículo 85 del Real Decreto 1098/2001 de 12 de octubre por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas.

Criterio Social: hasta un máximo de 10 puntos

Criterio Compromiso de integrar la plantilla que ejecutará el contrato mediante personal con contratos indefinidos.

Se valorará con un máximo de 10 puntos las propuestas de los licitadores o licitadoras que impliquen compromiso de integrar la plantilla que ejecutará el contrato mediante personal con contratos indefinidos. Se otorgará la máxima puntuación a la empresa con mayor compromiso de contratación indefinida y el resto de las propuestas de manera decreciente y proporcional, siempre que superen el mínimo (25%) que se ha establecido como condición esencial de ejecución.

$$P_i = \frac{CIP - 25\%}{MPL - 25\%} \cdot 10$$

Siendo:

- P_i = Puntuación de la oferta valorada i
- CIP = Contratación Indefinida a la que se compromete el licitador o licitadora para la ejecución del contrato
- MPL = Mejor oferta de los licitadores o licitadoras

Aquellas licitadoras que oferten un porcentaje de contratación indefinida menor al considerado como condición esencial serán excluidas.

Criterio Compromiso de Acuerdos de Nivel de Servicio (ANS): Hasta un máximo de 15 Puntos

El compromiso de ANS se valorará como sigue, de acuerdo con los criterios y requisitos explicitados en el anexo I del presente documento:

- **Monitorización de seguridad** Hasta un máximo de 12 puntos, distribuidos de la siguiente forma
 - Número de análisis de intrusión completos anuales, Hasta un máximo de 1 punto
 - Para 4 análisis completos anuales: 1 punto
 - Para 3 análisis completos anuales: 0,75 puntos
 - Para 2 análisis completos anuales: 0,25 puntos
 - Tiempo máximo de notificación de incidentes. Hasta un máximo de 7 puntos
 - Para incidentes de nivel alto, hasta un máximo de 4 puntos
 - Notificación en 30 minutos o menos: 4 puntos
 - Notificación entre más 30 minutos y 1 hora: 3 puntos
 - Notificación entre más de 1 hora y 2 horas: 2 puntos
 - Notificación entre más de 2 horas y 3 horas: 1 punto
 - Notificación entre más de 3 horas y menos de 4 horas: 0,5 puntos
 - Para incidentes de nivel medio, hasta un máximo de 2 puntos
 - Notificación en 24 horas o menos: 2 puntos
 - Notificación entre más 24 horas y 48 horas: 1 punto
 - Notificación entre más de 48 horas y menos de 72 horas: 0,5 puntos
 - Notificación entre más de 72 horas y menos de 96 horas: 0,25 puntos
 - Para incidentes de nivel bajo, hasta un máximo de 1 punto
 - Notificación en 72 horas o menos: 1 punto
 - Notificación entre más de 72 horas y 120 horas: 0,5 puntos
 - Notificación entre más de 120 horas y menos de 168 horas: 0,25 puntos

- % trimestral de falsos positivos en incidentes Hasta un máximo de 1 punto
 - Para un porcentaje del 5% o menos: 1 punto
 - Para un porcentaje entre más del 5% y el 15%: 0,5 puntos
 - Para un porcentaje entre más del 15% y el menos del 25%: 0,1 puntos
- Número máximo de falsos negativos anuales Hasta un máximo de 2 puntos
 - Para incidentes de nivel alto, hasta un máximo de 1,5 puntos
 - Para 0 incidente: 1,5 puntos
 - Para 1 incidente: 0,5 puntos
 - Para incidentes de nivel medio, hasta un máximo de 0,5 puntos
 - Para 0 incidentes : 0,5 puntos
 - Para 1 incidentes : 0,3 puntos
 - Para 2 incidentes: 0,2 puntos
 - Para 3 incidentes: 0,1 puntos
- Tiempo máximo de generación de un informe por petición explícita de Lantik. Hasta un máximo de 1 punto
 - Para un tiempo de 24 horas o menos: 1 punto
 - Para un tiempo entre más de 24 horas y 72 horas: 0,5 puntos
 - Para un tiempo entre más de 72 horas y menos de 168 horas: 0,25 puntos

Para realizar la adjudicación, será requisito rellenar correctamente la siguiente tabla e incluirla en el sobre B. En caso contrario, se podrá desestimar la oferta presentada.

Criterios	Valor
Compromisos de ANS	
Número de análisis de intrusión completos anuales	(en número)
Tiempo máximo de notificación de incidentes	
Criticidad alta	(en horas naturales)
Criticidad media	(en horas naturales)
Criticidad baja	(en horas naturales)
% trimestral de falsos positivos	(en porcentaje)
Número máximo de falsos negativos anuales	(en número)
Tiempo máximo de generación de informe	(en horas naturales)

- **Operación del servicio** Hasta un máximo de 3 puntos
 - % trimestral de disponibilidad del servicio Hasta un máximo de 2 puntos
 - Para un porcentaje del 99% o más: 2 puntos
 - Para un porcentaje entre menos el 99% y el 98.5 %: 1.5 puntos
 - Para un porcentaje entre menos del 98.5% y el 97.5%: 1 punto
 - Para un porcentaje entre menos del 97.5% y el 96.5%: 0.5 puntos
 - Para un porcentaje entre menos del 96.5% y más del 95%: 0,2 puntos
 - Tiempo máximo desde aviso para ejecutar una operación hasta su implantación definitiva en la infraestructura de seguridad propiedad de Lantik Hasta un máximo de 0,5 puntos
 - Para un tiempo de 30 minutos o menos: 0,5 puntos

- Para un tiempo entre más de 30 minutos y 60 minutos: 0,25 puntos
- Para tiempo entre más de 60 minutos y menos de 120 minutos: 0,1 puntos
- Tiempo máximo de resolución de fallos o mantenimiento relacionados con el servicio
Hasta un máximo de 0,5 puntos
 - Para un tiempo de 8 horas o menos: 0,5 puntos
 - Para un tiempo entre más de 8 horas y 16 horas: 0,25 puntos
 - Para tiempo entre más de 16 horas y menos de 24 horas: 0,1 puntos

Para realizar la adjudicación, será requisito rellenar correctamente la siguiente tabla e incluirla en el sobre B. En caso contrario, se podrá desestimar la oferta presentada.

Criterios	Valor
Operación del servicio	
% trimestral de disponibilidad de servicio	(en porcentaje)
Tiempo máximo de ejecución de tareas en infraestructura de Lantik	(en horas naturales)
Tiempo máximo de resolución de fallos o mantenimiento del servicio	(en horas naturales)

El detalle de cada uno de estos ANS se describe en la tabla adjunta del [Anexo I.](#) del PPT

4.9.2 Criterios no cuantificables automáticamente – Sobre C

Propuesta técnica: Hasta un máximo de 35 puntos

En ningún caso se deberá incluir en este sobre información cuantificable por fórmula.

Se puntuarán la valoración de la gestión del servicio, el modelo operativo, el modelo organizativo y la forma en la que se abordarán las fases de despliegue del mismo.

Criterio	Puntos
Gestión del servicio	7 puntos
Modelo operativo	13 puntos
Modelo organizativo	10 puntos
Fases de despliegue	5 puntos

Quedaran automáticamente excluidas del proceso de valoración las ofertas que no alcancen una valoración mínima de 18 puntos en este apartado.

La adjudicación se hará a aquella oferta que sumando los puntos obtenidos en los apartados anteriores (4.9.1 y 4.9.2), resulte superior.

4.10 Equipo de trabajo

El equipo de trabajo estará compuesto por las personas suficientes para cubrir los perfiles indicados en el apartado "Equipo técnico". La empresa proveedora deberá indicar qué perfil o perfiles son cubiertos por cada persona comprendida inicialmente en la oferta.

La empresa adjudicataria podrá añadir los perfiles que considere necesarios para la correcta ejecución de los servicios, teniendo en cuenta posibles fluctuaciones en la carga de trabajo. Deberá garantizar la gestión de un equipo variable que se adecue a la demanda del servicio en función de las necesidades de cada momento.

Cualquier cambio en la composición del equipo de trabajo durante la vigencia del contrato deberá notificarse previamente a Lantik y contar con la autorización expresa del Departamento de Seguridad. Así mismo, cualquier cambio en el equipo técnico deberá justificarse y las sustituciones deberán realizarse con una persona de cualificación técnica igual o superior a la solicitada. La empresa adjudicataria tendrá obligación de formar a la persona cuya incorporación haya sido aprobada por el Departamento de Seguridad, entre otros, con los conocimientos generales y específicos de las labores a realizar, la situación actual de las mismas, la normativa aplicable, los procedimientos de trabajo a seguir, los roles y responsabilidades del equipo, etc. La empresa adjudicataria lo hará por sus propios medios, sin coste adicional para Lantik.

Todos los miembros del equipo de trabajo deberán hablar castellano y/o euskera como lengua nativa o ser capaces de comunicarse en castellano y/o euskera de forma fluida. En caso de incluir recursos que no cumplan este perfil, la empresa adjudicataria deberá proporcionar, a petición de Lantik, intérpretes que faciliten la comunicación sin cargo adicional para Lantik.

4.11 Control de los trabajos

La empresa licitadora, en el ejercicio de una actividad empresarial propia, contará con patrimonio, instrumentos, maquinaria y organización estables y mantendrá a sus trabajadores dentro de su ámbito de poder de dirección, conservando respecto a ellos los derechos, obligaciones, riesgos y responsabilidades inherentes a su condición de empleador, aunque se coordinen con Lantik, pudiendo ésta incluso facilitar cierto equipamiento común (servidores informáticos,...) para su labor, cuando sea necesario el traslado de sus empleados a Lantik, para poder ejercer la actividad, no enervando todo ello el que la empresa licitadora ejerza las funciones inherentes a su condición de empresario, al existir una justificación técnica, objetiva y razonable de las condiciones del trabajo a desarrollar para dar cumplimiento al objeto del contrato.

Corresponderá a la empresa licitadora la negociación y pago de los salarios a los miembros del equipo, la concesión a los mismos de los permisos, licencias y vacaciones, la gestión de las sustituciones, respetando la cobertura de los servicios exigida e informando de ello a Lantik, y la vigilancia del efectivo cumplimiento de las obligaciones en materia de prevención de riesgos laborales, de Seguridad Social y en general de todas las que legalmente correspondan. Para ello, la empresa licitadora nombrará un interlocutor para la gestión de este contrato.

La empresa contratada deberá nombrar una persona coordinadora para que actúe de interlocutor con el responsable del servicio de Lantik. Dicha persona coordinadora verificará el nivel de calidad del servicio, visando y entregando los informes necesarios.

Los trabajos se desarrollarán en los locales de la empresa contratada mediante conexión con la

infraestructura de Lantik. Los equipos, licencias, comunicaciones (incluso con la red de Lantik) y los desplazamientos necesarios del personal de la empresa serán a cargo de la empresa contratada. Todos los trabajos se realizarán bajo la supervisión, y en su caso participación, del personal que Lantik establezca.

Las reuniones entre Lantik y la empresa adjudicada se efectuarán tanto en Lantik como en los locales de la empresa dependiendo de los convocados.

Lantik se reserva el derecho de realizar las auditorias y solicitar informes y evidencias que considere necesarios para el desarrollo seguro y adecuado del servicio.

4.12 Confidencialidad

La empresa adjudicataria se obliga a guardar secreto sobre la información y documentación proporcionada o confiada a su personal, o que llegue a su conocimiento como consecuencia de la realización del trabajo.

La contravención de esta cláusula será motivo suficiente para promover la rescisión del contrato.

4.13 Propiedad intelectual

Cualquier conector, política, regla, software, documentación o cualquier otro elemento que sean creados durante el desarrollo del servicio será considerado propiedad de Lantik.

El título de propiedad de todos los productos generados objeto del presente pliego corresponde a Lantik. Todos los trabajos realizados por la empresa adjudicataria pasarán a ser propiedad de Lantik, quien podrá utilizarlos indefinidamente sin ninguna restricción ni costo adicional. A estos efectos tendrán la misma consideración todas las adaptaciones o adiciones realizadas por la empresa adjudicataria a un software propiedad de Lantik, dentro del ámbito del presente contrato.

La empresa adjudicataria protegerá todas las propiedades intelectuales de Lantik.

La empresa adjudicataria garantizará a Lantik que tiene todos los derechos de propiedad intelectual de los productos que oferta bien directamente o bien indirectamente, mediante los correspondientes acuerdos con sus empresas proveedoras. Por tanto, se obliga a dejar indemne a Lantik de cualquier reclamación de tercero que, frente a ella, pueda suscitarse por dicho concepto.

4.14 Metodología

La empresa contratada realizará los trabajos objeto del presente contrato siguiendo la metodología oficial de Lantik y su documentación correspondiente.

4.15 Subcontratación

Las empresas licitadoras deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de las empresas subcontratistas a las que se vaya a encomendar su realización.

4.16 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.

4.17 Seguridad de la información

Para garantizar la seguridad de Información se deben cumplir los siguientes apartados durante todo el servicio a prestar:

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

En el contrato a firmar se incluirá el acuerdo de confidencialidad, y el conocimiento y compromiso de cumplimiento de la Normativa de Seguridad y Código de Conducta Informático para proveedores.

El acuse de recibo y compromiso de cumplimiento de las normativas internas existentes en Lantik, 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 ésta), de lo cual se encargará de recoger y custodiar la empresa proveedora que responderá en su nombre.

A. 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 cualquier caso, se prohíbe expresamente el acceso a este tipo de datos.

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 ésta. 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.

III. Medidas de seguridad

La empresa adjudicataria se compromete a cumplir todo lo dispuesto en la legislación vigente sobre protección de datos que le sea de aplicación y a actuar de acuerdo con las instrucciones de Lantik. En concreto:

El personal de la empresa adjudicataria está obligado a respetar las medidas de seguridad de los locales a los que accede, sin que de su permanencia o paso por ellos pueda derivarse una merma de las condiciones de seguridad originales (cierre de puertas y ventanas, conexión de alarmas, etc.).

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.

Con el fin de coordinar y ser eficientes ante cualquier ciberincidente o ajuste de seguridad que se requiera, la empresa adjudicataria, debe de indicar quien ocupa el rol de responsable de seguridad en su organización. Se incluirá en la oferta el nombre, apellidos, correo electrónico y teléfono de la persona o servicio que desempeñe este rol.

IV. 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.

V. Responsabilidad y causas de resolución del contrato

La empresa adjudicataria que incumpla lo establecido en los apartados anteriores será considerada responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido, así como de cualquier reclamación que por las personas interesadas se interponga ante la Agencia de Protección de Datos competente y de la indemnización que, en su caso, se reconozca a la persona afectada que ejercite la acción de responsabilidad por el daño o lesión que sufra en sus bienes o derechos.

Serán motivos de resolución del contrato la vulneración del deber de secreto por la empresa adjudicataria o su personal, así como el incumplimiento de la normativa sobre protección de datos de carácter personal."

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

Lantik. 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.

- C. 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 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 del Dpto. de Seguridad de Lantik, información sobre el nivel de rendimiento de los controles de seguridad establecidos, así como información de los incidentes no graves ocurridos en el periodo. Los incidentes graves deberán ser notificados a la mayor brevedad.

- D. Informe periódico del cumplimiento de la "Normativa de Seguridad para Proveedores"

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

- E. 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 del Dpto. de Seguridad de Lantik.

, 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 27001.

- F. Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica

La empresa adjudicataria del servicio 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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La empresa adjudicataria del servicio asumirá el cumplimiento de lo establecido en el Esquema Nacional de Seguridad (ENS) y las medidas establecidas en el Anexo II del ENS correspondientes a un nivel de clasificación MEDIO, en las dimensiones de seguridad que le apliquen , además de la [obligaciones exigidas para los prestadores de servicios a las entidades públicas](#) .

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. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán las medidas de seguridad indicadas en su Anexo II, ya sean pertenecientes al marco organizativo, operacional o de protección.

G. Medidas de continuidad del servicio o proyecto

Para asegurar la continuidad y disponibilidad del servicio o proyecto contratado, la empresa oferente deberá plasmar en la oferta presentada los siguientes puntos:

- Niveles de disponibilidad de los elementos (personas, equipos...) ofertados para el servicio, en el caso de que no se indique niveles de servicio mínimos requeridos
- Persona interlocutora por parte de la empresa proveedora en caso de incidentes de seguridad
- Procedimiento de notificación y aprobación de cambio en el servicio o proyecto contratado.

En el caso que se indique que para el servicio o proyecto contratado son necesarios niveles de servicio mínimos, bien por sus propias características o por el impacto en servicios que preste Lantik con compromisos de nivel de servicio, se deberán presentar evidencias de disponer de un Plan de Continuidad para el servicio (p.ej. Certificaciones, compromiso de la empresa proveedora...) que garantice que se cumplan esos niveles de servicio.

H. 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 del Dpto. de Seguridad de Lantik, 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 y que está disponible en el Plan de Calidad.

I. Evidencias de las buenas prácticas relativas al objetivo de control 11 "Seguridad Física y del entorno" de la norma de referencia ISO 27002 en el entorno de prestación

La empresa adjudicataria del servicio deberá evidenciar a requerimiento del Dpto. de Seguridad de Lantik, el grado de cumplimiento de las buenas prácticas de seguridad física establecidas en el objetivo de control 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 a la mayor brevedad.

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

Balbino Zubiaga Urbieta

Lantik S.A.M.P.
Sabino Arana, 44 – 48013 Bilbao
balbino.zubiaga@bizkaia.eus
Teléfono: 944068800

Iñaki Moreno Fernandez

Lantik S.A.M.P.
Sabino Arana, 44 – 48013 Bilbao
inaki.moreno@bizkaia.eus
Teléfono: 944068800

Sin./Fdo.: BALBINO ZUBIAGA URBIETA - 2022-03-10
SEGURTASUN SAILA
DEPARTAMENTO DE SEGURIDAD

Sin./Fdo.: JAVIER AZUMENDI CALABAZA - 2022-03-10
EKOIZPENA ARLOA
ÁREA DE PRODUCCIÓN

Sin./Fdo.: IMANOL SAUTO AVELLANAL - 2022-03-10
TEKNOLOGIA ETA EZAGUTZA UNITATEKO ZUZENDARITZA
DIRECCIÓN UNIDAD DE TECNOLOGÍA Y CONOCIMIENTO

Anexo I – Acuerdos de Nivel de Servicio

La empresa adjudicataria deberá especificar los referentes a los diferentes niveles de servicio requeridos:

Monitorización de seguridad

La monitorización de seguridad se valorará según los siguientes criterios:

- Número de análisis de intrusión completos anuales; la empresa proveedora puede ofertar un número mayor adicional al obligatorio de análisis de intrusión completos (automatizados y manuales) de servicios.
- Tiempo máximo de notificación de incidente; se refiere al tiempo transcurrido desde que se produce un incidente o ataque, y éste es detectado y notificado a Lantik. Según la sistemática aplicada en Lantik, los incidentes se categorizan en criticidad alta, media y baja siguiendo los escenarios y criterios definidos en las primeras fases de implantación del servicio y tomando como referencia la clasificación del CVE (Common Vulnerabilities and Exposures) y CVSS (Common Vulnerability Scoring System). En caso de que el incidente o ataque no esté categorizado dentro de estos criterios o escenarios definidos, se clasificará como alta.
- Todos los tiempos deberán ser identificados en horas naturales, indicando siempre el escenario más desfavorable.
- Los valores dados por la empresa adjudicataria deberán cumplir las siguientes restricciones:
 - El tiempo máximo permitido de notificación de una incidencia de criticidad alta será de 4 horas naturales.
 - El tiempo máximo permitido de notificación de una incidencia de criticidad media será de 96 horas naturales.
 - El tiempo máximo permitido de notificación de una incidencia de criticidad baja será de 168 horas naturales.
- % trimestral de falsos positivos en incidentes; se refiere al porcentaje de incidentes “no reales” que se notifiquen durante la monitorización de seguridad durante el periodo de explotación del servicio del servicio (no durante las fases iniciales, donde se entiende que el número de falsos positivos podrá ser mayor. Es un valor mensual resultado de las incidencias “no reales” / incidencias notificadas. El valor indicado deberá ser siempre menor a un 25%.
- Número máximo de falsos negativos anuales, se refiere al porcentaje de incidentes que no sean detectados por el servicio; este valor no deberá ser superior a 2 incidentes de criticidad alta anuales u 4 incidentes de criticidad media anuales.
- Tiempo máximo de generación de un informe por petición explícita de Lantik; se refiere al tiempo máximo en el que se dispondrá de un informe desde que este es solicitado por Lantik.
 - El tiempo máximo será identificado en horas naturales, indicando siempre el escenario más desfavorable y no podrá ser mayor de 168 horas naturales

Operación del servicio

La operación del servicio se valorará según los siguientes criterios:

- % trimestral de disponibilidad del servicio; se refiere al % en tiempo en el que el servicio de seguridad gestionada se encontrará operativo; no podrá ser menor del 95% del servicio en el año natural en horario 24x7
- Tiempo máximo de ejecución de tareas en los sistemas de seguridad propiedad de Lantik; se refiere al tiempo transcurrido desde que se necesita realizar una operativa habitual en un sistema de seguridad propiedad de Lantik y esta es efectivamente ejecutada por el proveedor. La necesidad se puede conocer, bien por una incidencia de seguridad detectada por el servicio o bien por comunicación de Lantik al proveedor. Este tiempo no podrá ser mayor a 120 minutos.
- Tiempo máximo de resolución de fallos o mantenimiento relacionados con el servicio; se refiere al tiempo al tiempo transcurrido desde que se detecta un fallo o una necesidad de mantenimiento en el servicio de seguridad gestionada (bien por parte de Lantik o del proveedor) y este atendido y resuelto. Este tiempo no podrá ser mayor a 24 horas.



Sabino Arana, 44
48013 BILBAO (Bizkaia)

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

e-mail: lantik@bizkaia.eus
<http://lantik.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.