5821 - PLIEGO DE PRESCRIPCIONES TÉCNICAS

Área de Arquitectura Tecnológica

Departamento de Seguridad

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

ÍNDICE

1 OBJETO 4

2 PRECIO POR UNIDADES 4

3 ESPECIFICACIONES TÉCNICAS 4

3.1 Alcance 4

3.2 Equipo técnico 5

3.3 Fases del servicio 14

3.4 Características del servicio 15

3.4.1 Coordinación 15

3.4.2 Horario del servicio 15

3.4.3 Dedicación 15

3.4.4 Modalidad de trabajo 16

3.4.5 Control de los trabajos 16

4 CONDICIONES PARTICULARES 17

4.1 Equipo de trabajo 17

4.2 Metodología y documentación 18

4.3 Propiedad Intelectual 18

4.4 Finalización del contrato 18

4.5 Perspectiva de género 19

4.6 Seguridad de la información 19

4.6.1 Contrato, acuerdo de confidencialidad, Normativa de seguridad para empresas proveedoras, y protección de datos de carácter personal 19

4.6.2 Deber de confidencialidad 19

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

4.6.3 Gestión interna de Lantik S.A. M.P. (medidas de securización interna) previas a la prestación 23

4.6.4 Documentación 23

4.6.5 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 23

4.6.6 Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores” 24

4.6.7 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. ... 24

4.6.8 Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica 25

4.6.9 Subcontratación 25

4.6.10 Coordinación en caso de incidentes y desastres 26

4.6.11 Regulación de la finalización del contrato: transferencia de tecnología 27

4.6.12 Normativa de securización de entornos para prestación de servicio remoto 28

4.6.13 Informe periódico del cumplimiento de la “Normativa de securización de entornos para prestación de servicio remoto” 28

4.6.14 Monitorización de las conexiones remotas 28

4.6.15 Instalación de herramientas de seguridad 28

4.6.16 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 29

4.6.17 Teletrabajo 29

4.6.18 Certificación de inexistencia de vulnerabilidades de seguridad 30

4.6.19 Resolución del Contrato 30

4.6.20 Fuero 30

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

1 OBJETO

Contratación de Servicios de oficina técnica en materia de ciberseguridad.

2 PRECIO POR UNIDADES

La empresa licitadora deberá especificar precios/hora para los siguientes perfiles:

- Gestor de proyectos: establecido en un máximo de 60,00 €/h (sin IVA).
- Experto: establecido en un máximo de 80,00 €/h (sin IVA).
- Senior: establecido en un máximo de 60,00 €/h (sin IVA).
- Junior: establecido en un máximo de 50,00 €/h (sin IVA).

3 ESPECIFICACIONES TÉCNICAS

Debido a la necesidad de realizar nuevos proyectos en el ámbito de la Seguridad de la información, se ve necesaria la contratación de un servicio que permita dar respuesta a los retos que se le plantean.

3.1 Alcance

Las actividades principales del servicio girarán en torno a la realización de proyectos de ciberseguridad. No pretende ser un listado con una relación exhaustiva de tareas, ya que se deberán acometer los trabajos necesarios para lograr los objetivos marcados en función de las necesidades:

- Trabajos de consultoría en materia de ciberseguridad.
- Planificar, gestionar y participar en la realización de proyectos en los que el Departamento de Seguridad deba de tener representación.
- Velar por el cumplimiento normativo especialmente, pero no exclusivamente, en materia de ENS, RGPD, ISO 27001 y NIS2.
- Ejercer de DPO *as a service* (*DPOaaS*) en caso de que Lantik así lo requiera.
- Realizar análisis y gestión de riesgos, así como el Análisis de Impacto en el Negocio (BIA).
- Valoración del impacto de los ciberincidentes que puedan ocurrir y documentación y archivo de los informes relacionados.
- Elaborar documentación y procedimientos de seguridad de la información.
- Realizar labores de auditoría interna como análisis GAP y revisiones periódicas del cumplimiento de los controles establecidos (control interno).
- Al menos, anualmente se deberá elaborar un informe directivo de la situación del riesgo en Lantik, partiendo de la inteligencia de las fuentes de información que Lantik S.A. M.P. en adelante Lantik) detalle para cada periodo. Entre otras fuentes de información podrá solicitarse que se tengan en cuenta los informes del SOC de Lantik, los informes de incidentes del periodo, fuentes oficiales (como ENISA, CCN-CERT, INCIBE o BCSC...), resultados de los simulacros realizados por Lantik, los análisis de riesgos del Sector Público Foral de Bizkaia, los análisis de impacto en el negocio, etc. En base a esta información, el servicio deberá plantear un plan de acción anual a ejecutar durante el periodo siguiente que dé respuesta a los riesgos identificados.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Para abordar los trabajos será necesario:

- Que Lantik plantee la necesidad.
- Antes de comenzar con el trabajo, la empresa adjudicataria estimará y validará con Lantik el nº de horas por perfil que inicialmente se prevea que se vayan a consumir.
- Si se prevé una desviación en las horas estimadas según se esté realizando el servicio, se deberá informar, explicar su motivación y recibir el vºbº de Lantik antes de continuar, ajustando la planificación a la nueva estimación.

3.2 Equipo técnico

El equipo técnico corresponde a las personas, adscritas al contrato, que deben acreditar unos conocimientos y/o experiencia mínimos para garantizar una correcta ejecución del servicio. Si estas se identificasen mediante identificativos no personales en las tablas solicitadas para la verificación de los requisitos, deberán ser detalladas con nombre y apellidos una vez se firme el contrato.

Para la correcta ejecución del objeto de contrato será necesario contar con un equipo técnico estable compuesto por ocho (8) personas que cubran la siguiente experiencia y certificaciones en vigor:

Una (1) persona gestora de proyectos

Deberá cumplir todos los siguientes requisitos:

- Experiencia: Al menos 3 años como coordinadora de proyectos de seguridad de la información.
- Certificación PMP.

Una (1) persona abogada experta

Deberá cumplir todos los siguientes requisitos:

- Grado en Derecho o equivalente.
- Experiencia: Al menos 5 años como consultora LOPD/LOPDGDD/RGPD y Seguridad de la Información (en especial ISO27001 y ENS), acreditando no menos de los siguientes años de dedicación distribuidos de la siguiente manera:
    - LOPD/LOPDGDD/RGPD: 3 años
    - ENS: 2 años
- Certificación DPO.
- Al menos una de las siguientes certificaciones:
    - ISO 27001 Lead auditor
    - CSX-P - Cybersecurity Practitioner
    - CRISC - Certified in Risk and Information Systems Control
    - CISSP – Certified Information Systems Security Professional
    - CISM - Certified Information Security Manager
    - CISA – Certified Information System Auditor

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Una (1) persona ingeniera experta

Deberá cumplir todos los siguientes requisitos:

- Grado en Ingeniería Informática, Telecomunicaciones, Matemáticas, Ciberseguridad o equivalente.
- Experiencia: Al menos 5 años como consultora LOPD/LOPDGDD/RGPD y Seguridad de la Información (en especial ISO27001 y ENS), acreditando no menos de los siguientes años de dedicación distribuidos de la siguiente manera:
    - ENS: 4 años
    - LOPD/LOPDGDD/RGPD: 1 año
- La certificación "ISO 27001 Lead auditor".

Dos (2) personas ingenieras senior

Ambas deberán cumplir todos los siguientes requisitos:

- Grado en Ingeniería Informática, Telecomunicaciones, Matemáticas, Ciberseguridad o equivalente.
- Experiencia: Al menos 3 años como consultoras LOPD/LOPDGDD/RGPD y Seguridad de la Información (en especial ISO27001 y ENS), acreditando no menos de los siguientes años de dedicación distribuidos de la siguiente manera:
    - ENS: 2,5 años
    - LOPD/LOPDGDD/RGPD: 6 meses
- Cada persona deberá disponer de al menos una de las siguientes titulaciones/certificaciones:
    - Máster en Ciberseguridad/seguridad de la información con un mínimo de 60 créditos.
    - CSX-P - Cybersecurity Practitioner
    - CRISC - Certified in Risk and Information Systems Control
    - CISSP – Certified Information Systems Security Professional
    - CISM - Certified Information Security Manager
    - CISA – Certified Information System Auditor
    - ISO 27001 Lead auditor

Una (1) persona abogada senior

Deberá cumplir todos los siguientes requisitos:

- Grado en derecho o equivalente
- Experiencia: Al menos 3 años como consultora LOPD/LOPDGDD/RGPD y Seguridad de la Información (en especial ISO27001 y ENS), acreditando no menos de los siguientes años de dedicación distribuidos de la siguiente manera:
    - LOPD/LOPDGDD/RGPD: 2,5 años
    - ENS: 6 meses
- Certificación DPO.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Una (1) persona abogada junior

Deberá cumplir todos los siguientes requisitos:

- Grado en derecho o equivalente
- Experiencia como consultora de seguridad de al menos 1 año.

Una (1) persona ingeniera junior

Deberá cumplir los siguientes requisitos:

- Grado en Ingeniería Informática, Telecomunicaciones, Matemáticas, Ciberseguridad o equivalente.
- Experiencia como consultora de seguridad de al menos 1 año.

La información del equipo técnico 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 RESUMEN y DETALLE. Las ofertas que no incluyan las tablas serán excluidas de la licitación.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

TABLA DETALLE Persona Gestora de proyectos

Id. (1)	Descripción del proyecto	Cliente / Entidad	Periodo		Al menos 3 años como coordinadora de proyectos de seguridad de la información	
			Fecha inicio (2)	Fecha fin (2)	Meses	Descripción de tareas realizadas
1			mm/aaaa	mm/aaaa	∑ meses	
...			mm/aaaa	mm/aaaa	∑ meses	
TOTAL					∑ 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.

Además, se deberá aportar la certificación PMP.

TABLA RESUMEN 1: Personas expertas

Id. (1)	Experiencia de 5 años		Titulación	Certificación DPO (2)	ISO 27001 Lead auditor (2)	Al menos una: CSX-P, CRISC, CISSP, CISM, CISA o ISO 27001 Lead Auditor (2)
	LOPD/LOPDGDD/RGPD	ENS				
2 (abogada)	(meses)	(meses)		(fecha certificado)	-	(fecha certificado)
3 (ingeniera)	(meses)	(meses)		-	(fecha certificado)	-

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

(2) Presentar certificación

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

TABLA DETALLE 1: Personas expertas (dos tablas, una por cada persona)

Id. (1)	Descripción del proyecto	Cliente/Entidad	Periodo		Experiencia de al menos 5 años			
					LOPD/LOPDGDD/RGPD		ENS	
			Fecha inicio (2)	Fecha fin (2)	Meses	Descripción de tareas realizadas	Meses	Descripción de tareas realizadas
x			mm/aaaa	mm/aaaa	∑ meses		∑ meses	
...			mm/aaaa	mm/aaaa	∑ meses		∑ meses	
TOTAL					∑ meses (3)		∑ meses (3)	

(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) El total de meses deberá coincidir con el dato de la TABLA RESUMEN 1.

TABLA RESUMEN 2: Personas senior

Id. (1)	Experiencia de 3 años		Titulación	Certificación DPO (2)	Al menos una: CSX-P, CRISC, CISSP, CISM, CISA, ISO 27001 lead Auditor o Máster en Ciberseguridad (2)
	LOPD/LOPDGDD/RGPD	ENS			
4 (ingeniera)	(meses)	(meses)		-	(fecha certificado)
5 (ingeniera)	(meses)	(meses)		-	(fecha certificado)
6 (abogada)	(meses)	(meses)		(fecha certificado)	-

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

(2) Presentar certificación

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

TABLA DETALLE 2: Personas senior (tres tablas, una por cada persona)

Id. (1)	Descripción del proyecto	Cliente/Entidad	Periodo		Experiencia de al menos 3 años			
			Fecha inicio (2)	Fecha fin (2)	LOPD/LOPDGDD/RGPD		ENS	
					Meses	Descripción de tareas realizadas	Meses	Descripción de tareas realizadas
x			mm/aaaa	mm/aaaa	∑ meses		∑ meses	
...			mm/aaaa	mm/aaaa	∑ meses		∑ meses	
TOTAL					∑ meses (3)		∑ meses (3)	

(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) El total de meses deberá coincidir con el dato de la TABLA RESUMEN 2.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

TABLA RESUMEN 3: Personas junior

Id. (1)	Experiencia de 1 año	Titulación
7	(meses)	
8	(meses)	

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

TABLA DETALLE 3: Personas junior

Id. (1)	Descripción del proyecto	Cliente/Entidad	Periodo		Experiencia de al menos 1 año	
			Fecha inicio (2)	Fecha fin (2)	Meses	Descripción de tareas realizadas
x			mm/aaaa	mm/aaaa	∑ meses	
...			mm/aaaa	mm/aaaa	∑ meses	
TOTAL					∑ meses (3)	

(1) Identificador: nº correlativo que identifica a cada persona del equipo (mismo identificador que en la TABLA RESUMEN).

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

(3) El total de meses deberá coincidir con el dato de la TABLA RESUMEN 3.

3.3 Fases del servicio

FASE 1: diagnóstico y transferencia

En esta fase se realizará una revisión conjunta entre Lantik y la empresa adjudicataria del alcance del servicio, la estructura de gestión, las exigencias del servicio y la organización de este; con el fin de realizar una transferencia de conocimientos estructurada, mediante la ejecución de un plan de reuniones específicas y formación funcional en aquellos casos que se requiera.

Se recopilarán los procedimientos, instrucciones técnicas, buenas prácticas, y los indicadores definidos.

Salvo que la empresa contratista del anterior contrato y la nueva empresa adjudicataria resultasen coincidentes, la Fase 1 del presente contrato —diagnóstico y transferencia—, coincidirá con la Fase 3 del contrato anterior —devolución del servicio— y tendrá una duración de 3 meses.

La adjudicataria deberá colaborar activamente con Lantik y con la anterior contratista, o quien determine Lantik, para el traspaso de conocimiento.

Los servicios incluidos en esta fase no serán facturables y su duración no podrá ser superior a tres meses.

FASE 2: inicio del servicio - ejecución

El objetivo de esta fase es ejecutar y gestionar los servicios del contrato y garantizar la calidad del servicio mediante el desarrollo de las actividades indicadas.

La fase 2 comenzará tan pronto como la empresa adjudicataria esté en condiciones de ejecutar los trabajos asignados. Es posible que las fases 1 y 2 se solapen, ya que no todos los servicios del pliego requieren el mismo tiempo para su transferencia.

FASE 3: devolución del servicio

Tres meses antes de la finalización del contrato, el adjudicatario deberá entregar un Plan de Devolución del Servicio. Durante este tiempo, la empresa adjudicataria deberá colaborar activamente con Lantik y la nueva empresa adjudicataria, o quien determine Lantik, para el traspaso de conocimiento; con el fin de que la nueva empresa adjudicataria se pueda hacer cargo del servicio.

En esta fase la empresa adjudicataria pondrá a disposición de Lantik los documentos de trabajo y la documentación técnica necesaria que no haya entregado durante la ejecución del contrato (FASE 2) para poder volver a asumir el mantenimiento delegado.

Para confeccionar el Plan de Devolución del Servicio, la empresa adjudicataria tendrá en cuenta lo siguiente:

- La empresa adjudicataria continuará con la responsabilidad de prestación integral del servicio.
- La empresa adjudicataria se compromete a poner los medios para minimizar el impacto en el servicio debido a las actividades de esta fase.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

- La empresa adjudicataria se compromete a colaborar activamente con Lantik y la nueva empresa adjudicataria para facilitar la correcta transferencia de conocimiento en el plazo previsto.
- La empresa adjudicataria verificará que la documentación está actualizada.

3.4 Características del servicio

La empresa adjudicataria deberá disponer de la organización necesaria para poder acometer con éxito el servicio solicitado.

3.4.1 Coordinación

La persona “Gestora de proyectos” solicitada en el apartado “Equipo técnico” realizará las labores de coordinación, que sin perjuicio de que le sean encomendadas otras tareas, serán las siguientes:

- Gestión y seguimiento de proyectos
  - Actualización de la herramienta corporativa de Lantik con el estado de cada tarea.
  - Elaboración de informes sobre la evolución del servicio y su correcta ejecución.
  - Reuniones periódicas de coordinación con el equipo de Lantik.
  - Gestión del equipo que conforma el servicio.
  - Elaboración del informe de seguimiento mensual (informe especificado en el apartado “Control de los trabajos”).
- Proponer mejoras que incrementen la calidad del servicio.
- Propuesta de acciones correctoras.
- Aseguramiento de la mejora continua.

3.4.2 Horario del servicio

El horario mínimo obligatorio del servicio, aplicable a todas las semanas del año con excepción de los días festivos en Bilbao y el 24 y 31 de diciembre, será de lunes a viernes de 8:00 a 15:00.

El tiempo de respuesta dentro del horario de servicio deberá ser inmediato. (Definido como el tiempo que pasa desde que se envía una comunicación y se recibe una respuesta).

Es requisito contar con una disponibilidad de atención 24/7 basada en tener acceso al teléfono móvil de una persona responsable, para poder informar sobre emergencias o situaciones imprevistas y que así pueda organizar el equipo necesario para manejar la situación. Este contacto deberá estar disponible durante toda la vigencia de contrato independientemente de periodos vacacionales.

Lantik podrá solicitar intervenciones bien planificadas bien por necesidades urgentes del servicio fuera del horario establecido, facturándose estas con un coeficiente de 1,5 sobre los precios unitarios establecidos.

3.4.3 Dedicación

Se establecen las siguientes condiciones para la prestación del servicio:

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

- Las dos personas expertas deberán tener disponibilidad total en la franja horaria descrita en el apartado “Horario del servicio”.
- A todas las reuniones que se celebren con Lantik deberá asistir al menos una de las personas expertas solicitadas.
- En periodos vacacionales es necesario que al menos un experto y un senior de competencias complementarias (derecho/ingeniería) estén disponibles para que el servicio quede cubierto.
- La no asistencia a una reunión planificada deberá ser avisada con al menos una semana de antelación. La cancelación de una reunión planificada podrá conllevar penalización.

3.4.4 Modalidad de trabajo

Los trabajos se desarrollarán en los locales de la empresa contratada, desde las que se garantizará la adecuada seguridad y confidencialidad de la información.

Los equipos, licencias, comunicaciones (incluso con la red de Lantik) y desplazamientos necesarios del personal de la empresa serán a cargo de la empresa contratada.

Si bien el trabajo se desempeñará con carácter ordinario en remoto, Lantik podrá requerir para cualquier componente del equipo técnico:

- Que el trabajo sea desempeñado puntualmente de forma presencial en las instalaciones de Lantik, siempre que Lantik así lo solicite con una semana mínima de preaviso.
- Reuniones presenciales semanales (día y hora prefijadas conjuntamente) para una correcta ejecución del servicio.

3.4.5 Control de los trabajos

Para el control de los trabajos se utilizará el siguiente sistema de funcionamiento:

- Lantik nombrará una o varias personas responsables para los aspectos organizativos, funcionales y técnicos. Estas personas actuarán como interlocutoras con la empresa adjudicataria, y acudirán a cuantas reuniones de seguimiento se propongan. Asimismo, se encargarán de realizar cuantos controles consideren oportunos para garantizar la calidad del producto entregado y dar el visto bueno a los trabajos.
- Todas las personas responsables deberán tener un canal de comunicación fluido para solventar cualquier aspecto que pueda surgir durante la ejecución del contrato.
- La persona coordinadora deberá asegurar que la herramienta corporativa de Lantik (en principio JIRA) se encuentra actualizada en todo momento con la información de las tareas a realizar, su planificación y estado actual, de acuerdo con las instrucciones de Lantik.
- Se establecerán objetivos mensuales cuyo avance se revisará junto con Lantik quincenalmente.
- Adicionalmente, de forma trimestral, se organizará un comité de seguimiento para que el servicio contratado exponga el resumen de las tareas realizadas en el periodo y se analicen posibles mejoras en el servicio.
- Además, se realizarán informes de seguimiento que la empresa adjudicataria podrá proponer, pero como mínimo se establecerá la siguiente forma de proceder que será la base para que la empresa adjudicataria pueda emitir factura mensualmente.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

- El informe de seguimiento mensual será una hoja de cálculo que incluya: Relación de todos los trabajos finalizados y en curso en los que se haya trabajado en el periodo.
- Horas imputadas en el periodo, horas estimadas iniciales y las horas acumuladas totales para cada entregable.
- El número de horas se diferenciará por cada perfil.
- Deberá incluirse el precio sin IVA que supone cada entregable, tanto de las horas consumidas durante el mes en curso como el total acumulado para cada entregable.
- Desviación producida sobre lo planificado.
- Los totales mensuales deberán incluirse en una hoja adicional de seguimiento para controlar el número de horas restantes disponibles en el contrato.

- El informe de seguimiento mensual se entregará como máximo, dos días hábiles antes del último día de cada mes.
- Si bien podrán facturarse entregables en curso, no se aceptará su facturación si Lantik no ha supervisado los avances realizados en el mismo.
- Lantik podrá rechazar las horas facturadas si considera que no se corresponden con el avance y calidad del trabajo entregado.

4 CONDICIONES PARTICULARES

4.1 Equipo de trabajo

El equipo de trabajo estará compuesto como mínimo por las personas indicadas en el apartado “Equipo técnico”.

La empresa adjudicataria deberá añadir los perfiles que considere necesarios para la correcta ejecución del servicio, teniendo en cuenta posibles fluctuaciones en la carga de trabajo.

Se deberá garantizar una gestión adecuada de las personas profesionales cuyo perfil se ajustará a las tareas a ejecutar en el servicio en cada momento.

Cualquier cambio en el equipo técnico deberá justificarse (con la presentación de la información solicitada en las tablas del equipo técnico) y las sustituciones deberán realizarse con un perfil 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 Lantik, entre otros, con los conocimientos generales y específicos de las labores a realizar, la situación actual de las mismas, 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.

Así mismo, cualquier cambio en la composición del equipo de trabajo durante la vigencia del contrato, con especial mención en las personas que abandonan el equipo y no solo las sustituciones, deberá notificarse previamente a Lantik, y contar con la autorización expresa de Lantik.

Todos los miembros del equipo de trabajo deberán hablar castellano y/o euskera como lengua nativa o ser capaces de comunicase 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.

Lantik podrá solicitar la sustitución de cualquier persona del equipo de trabajo, aunque cumpla con el conocimiento técnico requerido, si no tuviese las aptitudes necesarias para la realización de los trabajos

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

en equipo y/o un mínimo de calidad en los trabajos realizados. Si se llegase a esta situación, se informará a la persona responsable de la empresa adjudicataria con las evidencias oportunas.

Debido a la continua evolución tecnológica es responsabilidad de la empresa adjudicataria la formación continua del personal adscrito al contrato.

4.2 Metodología y documentación

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

No obstante, las propuestas deberán incluir una explicación de la metodología que propone la empresa licitadora para poder desarrollar el proceso de forma global.

4.3 Propiedad Intelectual

De conformidad con lo previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, el título de propiedad de todos los productos generados objeto del presente pliego corresponde a Lantik, tanto de las aplicaciones, como de cualquier otro objeto de información que se desarrolle. 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.

Todo software de aplicación, operativo, o cualquier otro cuya propiedad intelectual o industrial corresponda o haya sido licenciado a la empresa adjudicataria por terceros o que haya sido desarrollado y adquirido por la empresa adjudicataria y utilizado en la prestación de los servicios objeto del presente contrato será, y seguirá siendo, propiedad de la empresa adjudicataria.

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 lo tanto, se obliga a dejar indemne a Lantik de cualquier reclamación de tercero que, frente a ella, pueda suscitarse por dicho concepto.

4.4 Finalización del contrato

Se habrán cumplido con las obligaciones contractuales, cuando alguna de las siguientes circunstancias se dé primero:

- Se alcance la fecha de terminación del contrato o se alcance el importe máximo adjudicado.
- Lantik decida dar por terminado el servicio.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

4.5 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.

4.6 Seguridad de la información

4.6.1 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 y protección de datos de Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia.
  - Norma Interna NCS-1/1 “Norma de Política de Seguridad: Código de Conducta Informático para entidades proveedoras"
  - Norma Interna NCS-1/2 “Normativa de Seguridad de la Información para entidades proveedoras"

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.

4.6.2 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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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 compromete a no revelar la información que conozca 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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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.

4.6.3 Gestión interna de Lantik S.A. M.P. (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.

4.6.4 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.

4.6.5 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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

los controles de seguridad establecidos, así como información de los incidentes no graves ocurridos en el periodo.

4.6.6 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.

4.6.7 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.

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 el ámbito de la Administración Electrónica. En este caso, la empresa adjudicataria asumirá el cumplimiento de lo establecido en 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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

adjudicataria (auditorías de seguridad, informes de hacking ético, renovación de certificaciones de seguridad, utilización de componentes cualificados o certificados, etc.).

4.6.8 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 desde 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.

4.6.9 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

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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.

4.6.10 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:

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

- 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.

4.6.11 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.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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.

4.6.12 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”.

4.6.13 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.

4.6.14 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.

4.6.15 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.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

4.6.16 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.

4.6.17 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:
    - Software antimalware y protección mediante firewall activados y actualizados.
    - 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.
    - El sistema operativo y las aplicaciones software deberán estar actualizados.
    - 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.
    - 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.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

- 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.

4.6.18 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.

4.6.19 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.

4.6.20 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.

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

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

Lantik S.A. M.P.

Sabino Arana, 44 – 48013 Bilbao

ppt.sc.lantik@bizkaia.eus

Teléfono: 944068900

#FI#
Sin./Fdo.: BALBINO ZUBIAGA URBIETA - 2025-06-17
SEGURTASUN SAILA
DEPARTAMENTO DE SEGURIDAD

Sin./Fdo.: MARTIN BERASATEGUI MEJIAS - 2025-06-17
ARKITEKTURA TEKNOLOGIKOKO ARLOA
ÁREA DE ARQUITECTURA TECNOLÓGICA

Sin./Fdo.: IMANOL SAUTO AVELLANAL - 2025-06-17
SEGURTASUN ETA TEKONOLOGIA UNITATEKO ZUZENDARITZA
DIRECCIÓN DE UNIDAD DE SEGURIDAD Y TECNOLOGÍA

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Egiaztapen Kode Elektronikoa / Código de Verificación Electrónica: WRW0-VZLJ-G25Z-QG8D
Egiaztapen helbidea / Dirección de verificación: www.lantik.bizkaia.eus

Bizkaia
lantik

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.