5584 - PLIEGO PRESCRIPCIONES TÉCNICAS

Área de Arquitectura Tecnológica

Departamento de Seguridad

ÍNDICE

1 OBJETO

Servicio de oficina de concienciación en ciberseguridad para mejorar la cultura de seguridad, de forma que permita mitigar el nivel de riesgo frente a potenciales incidentes de ciberseguridad.

2 PRECIO POR UNIDADES

La empresa licitadora deberá especificar precios para:

- Precio fijo para todos los trabajos solicitados en las Fase I - Diagnostico y Fase II - Planificación, establecido en un máximo de 15.000,00 € (sin IVA).
- Precio fijo para todos los trabajos solicitados en la Fase III – Ejecución de los trabajos específicos, establecido en un máximo de 90.000,00 € (sin IVA).
- Precio/hora para trabajos bajo demanda: establecido en un máximo de 45,00 €/h (sin IVA).

3 ESPECIFICACIONES TÉCNICAS

3.1 Alcance

El alcance incluirá tanto trabajos específicos a realizar como una bolsa de horas disponible bajo demanda.

3.1.1 Trabajos específicos

Se persigue mejorar la cultura de ciberseguridad para mantener el nivel de riesgo frente a posibles incidentes en niveles aceptables para la organización. Para esto se fijan las siguientes tareas que serán ejecutadas en tres fases (Fases I, II y III) detalladas más adelante:

- **Identificación** de los diferentes colectivos, con necesidades similares en el ámbito de la ciberseguridad, y de este modo realizar actividades orientadas a las necesidades particulares de estos.

  Los perfiles mínimos para contemplar y que se estiman serán alrededor de unas 250 personas son:

  - Plantilla en general y nuevas incorporaciones de LANTIK S.A. M.P. (en adelante Lantik).
  - Personas especialmente sensibles a recibir ataques dirigidos (VAP).
  - Personal técnico: Personas Desarrolladoras, Administradoras, Operadoras y técnicas de ciberseguridad.
  - Gestores de la Seguridad: Dirección, Comité de Seguridad, Comité de Crisis (BCP) y Equipo de respuesta ante incidentes (ERI).

  Adicionalmente y una vez al año se preparará una concienciación off-line para estos 2 colectivos fuera del ámbito de las 250 personas:

- La ciudadanía que consume de sistemas de información construidos o gestionadas por Lantik para la Diputación Foral de Bizkaia en redes no controladas (Sede electrónica, web corporativa etc.). Este contenido debe ser conforme al Real Decreto 1112/2018, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público
- Empresas colaboradoras de Lantik en el ámbito de la política, procedimientos y normas que les aplican dentro de su ámbito de colaboración.

- **Desarrollo de un plan anual general y planes particulares por cada uno de los colectivos identificados** en la tarea anterior, donde se detallen las acciones a llevar a cabo para la formación, concienciación: simulacros, acciones puntuales, campañas, etc. Para ello se requerirá la toma de información sobre la cultura de seguridad existente en Lantik, entrevistando a diferentes áreas/personas clave de la organización con la finalidad de establecer un plan de transformación.
- **Concienciar** en materia de ciberseguridad a las personas usuarias y colectivos particulares identificados, para que adquieran unos hábitos de comportamiento seguro en los distintos entornos en los que desempeñan su actividad.
  - Que las personas usuarias puedan identificar los principales riesgos de seguridad que puedan afectar en cada momento a la seguridad de la organización y la suya propia, como podrían ser: phishing, ransomware, malware, ingeniería social, estafas, anomalías, etc.
  - Que las personas usuarias conozcan el contexto legislativo que les aplica en cada momento dentro del ámbito, como podrían ser: RD311/2022, RGPD, EIDAS, NIS, etc.
  - Reducir la probabilidad de sufrir incidentes de seguridad que impliquen pérdidas económicas, sanciones o pérdidas reputacionales.
  - Asegurar la confidencialidad, integridad y disponibilidad de la información que trata el personal de Lantik.
  - Diseñar las acciones de concienciación de forma anual adecuándolas al contexto de la situación vigente en cada momento y a las necesidades concretas que se hayan detectado tanto en el ámbito tecnológico (Por ejemplo – IA), como en el regulatorio (Por ejemplo – NIS 2).
  - La oficina de concienciación estará vigilante de las nuevas tecnologías o normativas que pueden incrementar el riesgo de la organización, por lo que trimestralmente emitirá un informe (“Informe de vigilancia tecnológica y normativa”) con aspectos a tener en consideración dentro de los planes de formación. En caso de que Lantik apruebe los planes se incorporaran de inmediato a los planes de transformación.
  - Los tipos de acciones de concienciación que se realizarán anualmente deberán disponer de al menos las siguientes acciones:
    - Una sesión formativa presencial u online (a criterio de Lantik), para cada uno de los colectivos definidos.
    - Una sesión formativa presencial u online (a criterio de Lantik), para cada uno de los colectivos definidos sobre cumplimiento dentro de su ámbito de responsabilidad. En este caso RGPD y ENS.

        - Material audiovisual (infografías, documentos, píldoras, etc.) que se realice a lo largo del año (al menos una al mes).
        - Dos juegos o iniciativas de gamificación para asentar el proceso de concienciación y fomentar la motivación.
        - Un concurso para testar el conocimiento en seguridad de la plantilla y que premie a la persona ganadora. El coste del premio correrá a cargo de la empresa adjudicataria.
    - Una plataforma que permita el consumo del material generado a demanda.

- **Entrenar** en materia de ciberseguridad a las personas usuarias y colectivos particulares identificados, para que adquieran soltura, se pongan en la situación y aprendan en base a simulacros en los distintos entornos en los que desempeñan su actividad. Los tipos de entrenamiento que se realizarán anualmente deberán disponer de al menos las siguientes acciones:
    - Un simulacro de planes de continuidad y gestión de crisis.
    - Un simulacro de Phishing general para todos los colectivos.
    - Un simulacro de ingeniería social no podrá ser de Phishing para cada uno de los colectivos definidos como, por ejemplo: Pretexting, Baiting, etc.

- **Sesiones aclaratorias y soporte a consultas**

  Se realizarán sesiones aclaratorias a consultas en materia de ciberseguridad a las personas usuarias y colectivos particulares identificados, de acuerdo con las campañas de formación, concienciación y entrenamientos realizados. Estas sesiones se realizarán utilizando los sistemas corporativos de Lantik.

  El soporte a consultas se gestionará a través de la plataforma.

  Se elaborarán FAQs , blogs, videos ,etc. que permitan compartir las dudas del personal/colectivos con el resto.

- **Evaluación**

  Se deberá realizar una evaluación continua del riesgo en ciberseguridad asociado a cada persona usuaria y colectivos particulares identificados. Como mínimo:

    - Se definirán KPIs de cada uno de los simulacros que se realicen.
    - Se medirá la valoración percibida del servicio por cada persona usuaria y colectivos particulares identificados.
    - Se dispondrá de un sistema de seguimiento y control que permita medir el grado de cumplimiento, la efectividad y el impacto de las acciones realizadas.
    - Se diseñará un cuadro de mando para realizar el seguimiento del grado de concienciación de todo el personal, colectivos identificados y el progreso de cada uno de estos.
    - Se planificarán y lanzarán comunicados personalizados a cada persona o colectivo.

3.1.2 Trabajos bajo demanda

Una vez finalizadas las Fases I y II (detalladas más adelante) y si Lantik viera oportuno ahondar en la **Concienciación** y el **Entrenamiento,** se podría solicitar la realización de más acciones que las anteriormente requeridas.

Estas acciones podrán estar orientadas tanto a los colectivos ya identificados como a cualquier otro grupo que pueda formar parte del sector público del Territorio Histórico de Bizkaia.

Para ello se contará con una bolsa de 3.000 horas que se comportará de la siguiente manera:

- Lantik solicitará la valoración de un trabajo específico. Se aportará tanta información como se tenga para una buena comprensión del nuevo trabajo a realizar.
- La empresa adjudicataria elaborará un cuadro de valoración detallado en horas y plazo que permita la aprobación por parte de Lantik.
- La empresa adjudicataria necesitará de la aceptación por parte de Lantik de esta valoración para realizar las acciones que se le hayan requerido.

3.2 Características del servicio

- Todos los contenidos y acciones que se realicen deberán tener posibilidad de realizarse en euskera y/o castellano. A criterio de Lantik se podrán solicitar en uno o los dos idiomas.
- Cada acción se adaptará al perfil y las necesidades de los diferentes colectivos, teniendo en cuenta su nivel de conocimiento, su rol y sus funciones dentro de la organización.
- Los contenidos y acciones incluirán contenidos variados en el ámbito de la ciberseguridad: teóricos y prácticos, basados en normas, estándares y recomendaciones reconocidas, noticias, sucesos, incidentes relevantes, entre otros.
- Contará con al menos una plataforma y recursos didácticos estimulantes que faciliten el aprendizaje y la evaluación de las personas usuarias, tales como vídeos, juegos, simulaciones, cuestionarios, etc., en ambos idiomas, euskera y castellano. Todas las actuaciones técnicas y operativas sobre las plataformas propuestas son responsabilidad de la empresa proveedora.
- Deberá llevarse a cabo en modalidades diferentes según el objetivo perseguido en cada caso: charlas online o presenciales, píldoras multimedia, juegos, simulacros, concursos, entrenamientos, etc.
- Los diseños se realizarán de acuerdo con la imagen corporativa de Lantik.
- El informe de seguimiento del servicio se emitirá el día 25 del mes para la revisión por parte de Lantik. En caso de ser festivo, la entrega se realizará el primer día hábil anterior a dicha fecha. Este informe contendrá al menos:
    - Actividades realizadas en el periodo.
    - Bolsa de horas consumida por actividad adicional en el periodo.
    - Análisis de situación y, si fuese necesario, las medidas a tomar para solventar los impedimentos detectados para la consecución de los objetivos acordados.

- Posibles mejoras en el servicio.

- Adicionalmente, cada año se desarrollará un informe de retrospectiva del servicio a modo de memoria. Este informe contendrá al menos:
  - Actividades realizadas en el periodo.
  - Bolsa de horas consumida por actividad adicional en el periodo.
  - Análisis de situación y, si fuese necesario, las medidas a tomar para solventar los impedimentos detectados para la consecución de los objetivos acordados.
  - ¿Qué debemos de dejar de hacer?
  - ¿Qué debemos de empezar a hacer?
  - ¿Qué debemos de continuar haciendo?
  - ¿Qué debemos de hacer menos?
  - ¿Qué debemos de hacer más?
  - Se revisarán y ajustarán los planes de concienciación, entrenamientos para ajustarlos al nuevo contexto.

3.3 Fases del servicio

Las fechas de ejecución entre fases pueden solaparse entre sí en caso de que se requiera.

3.3.1 Fase I – Diagnóstico

En esta fase se realizarán conjuntamente entre Lantik y la empresa adjudicataria las siguientes acciones:

- Revisión del alcance del servicio, la estructura de gestión, las exigencias del servicio y la organización de este.
- Identificación de los diferentes colectivos y sus necesidades particulares en materia de formación y concienciación. La propuesta de Lantik será el punto de partida, y sobre esta se debe valorar la oferta (apartado 3.1.1. Trabajos específicos - Identificación).
- Obtención de información sobre las iniciativas de formación que se han llevado a cabo en el ámbito de seguridad hasta la fecha en Lantik.
- Gestionar el traslado de información para el registro de las formaciones realizadas y otros requisitos, de acuerdo con los procedimientos, instrucciones técnicas y buenas prácticas en el ámbito de la formación y concienciación del Plan de Calidad de Lantik.

La duración de esta fase no podrá superar los 15 días laborables.

Los entregables mínimos de esta fase son:

- Informe de colectivos y necesidades identificadas (“Informe de colectivos y necesidades”) para cada uno de ellos.
- Informe de diagnóstico de la situación actual ("Informe de situación actual”).

3.3.2 Fase II - Planificación

En la oferta técnica (Sobre C) se deberá incluir un “Plan de Gestión del Cambio Inicial” cuyo principal objetivo es definir la transición que Lantik debe realizar para trasformar su modelo actual al deseado.

Como no se podrá partir de una fase de diagnóstico previo, se debe de asumir que la situación de partida de Lantik es de un nivel 2 (básico) y se pretende llegar al menos a un nivel 5 (avanzado), de acuerdo con el marco DIGCOMP en el área de Seguridad (4.1 “Proteger los dispositivos” y 4.2 “Proteger los datos personales y la privacidad.”)

Una vez firmado el contrato y realizada la Fase I, la empresa adjudicataria partiendo del “Informe de colectivos y necesidades” y del “Informe de situación actual”, deberá presentar un plan de gestión actualizado (“Plan de Gestión del Cambio”) cuyo principal objetivo es definir la transición que Lantik debe realizar para trasformar su modelo actual al deseado.

Durante la ejecución de esta fase y de acuerdo con el “Plan de Gestión del Cambio”, se deberá desarrollar un plan de acción personalizado.

El “Plan de Gestión del Cambio” debe incluir al menos:

- Objetivos que se persiguen
- Con qué periodicidad se ejecutará cada acción.
- En qué fechas se realizarán
- En qué tema se centrarán
- Colectivo al que irá dirigido
- Cómo se medirá su consecución (deberán ser cuantificables mediante indicadores).

Deberán establecerse métricas para valorar, al menos:

- Nivel de participación.
- Control de asistencia.
- Índice de satisfacción con la formación recibida.
- Evolución en la concienciación de seguridad.
- Número de actividades realizadas por tipología.

Toda esta información deberá estar disponible para Lantik a través de un cuadro de mando.

La duración de esta fase no podrá superar los 20 días laborables.

Los entregables mínimos de esta fase son:

- Plan de gestión del cambio (transformación) cuyo principal objetivo es definir la transición que Lantik debe de realizar para trasformar su modelo actual al deseado.
- Diseño del cuadro de mando.

3.3.3 Fase III – Ejecución de los trabajos específicos

El objetivo de esta fase es ejecutar y gestionar las acciones de acuerdo con el plan establecido en las fases anteriores (Fases I y II).

El uso de la plataforma estará disponible en todo momento para las personas usuarias durante la duración de esta fase.

Los entregables mínimos de esta fase son:

- Informe de vigilancia tecnológica y normativa, con periodicidad trimestral.
- Retrospectiva anual del servicio:
    - Servicio como tal
    - Mejora de cada colectivo

Toda la formación irá acompañada de material auxiliar de soporte.

3.3.4 Fase IV – Ejecución de trabajos bajo demanda

Lantik podrá incorporar nuevas acciones de acuerdo con las bolsas de horas reservadas para concienciar y/o entrenar.

La Fase III y la Fase IV pueden coincidir temporalmente.

3.3.5 Fase V – Devolución del servicio

Un mes antes de la finalización del contrato 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. Además, deberá extraer los datos de la plataforma actual en un formato intercambiable y facilitársela a la nueva empresa adjudicataria, o a quien Lantik determine para poder ser cargados en otra plataforma, si así lo determina Lantik.

La empresa adjudicataria tendrá en cuenta lo siguiente:

- La empresa adjudicataria continuará con la responsabilidad de prestación integral 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.

3.4 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 como mínimo por cuatro (4) personas y como máximo por cinco (5) ya que la "Dirección del servicio" se puede cubrir con una de las tres personas "Consultoras Senior" solicitadas o ser una más.

Deberán cubrir la siguiente experiencia y certificaciones:

Una persona Consultora Senior de Comunicación/Formación

- Deberá acreditar una experiencia de al menos 1.000h/año de media en los últimos 3 años en la elaboración de contenidos de formación.

Una persona Consultora Senior de Ciberseguridad y Tecnología

- Deberá acreditar una experiencia de al menos 300h/año de media en los últimos 3 años en la elaboración de contenidos de formación relacionados con la seguridad de la información.
- Deberá disponer de al menos una de las siguientes certificaciones de ISACA:
  - 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

Una persona Consultora Senior en la gestión de la Información y Protección de Datos

- Deberá acreditar una experiencia de al menos 300h/año de media en los últimos 3 años en la elaboración de contenidos de formación relacionados con la seguridad de la información.
- Deberá estar certificada como DPO.

Dirección del Servicio: La dirección del servicio podrá estar a cargo de una de las tres personas Consultoras Senior mencionadas anteriormente, siempre que cumplan con la experiencia requerida a continuación, o bien otra persona con la experiencia solicitada:

- Deberá acreditar una experiencia de al menos 3 años en gestión de proyectos.

Una persona Consultora Junior

- Deberá acreditar una experiencia de al menos 150h/año de media en los últimos 2 años en la elaboración de contenidos de formación relacionados con la seguridad de la información.

Se valorarán certificaciones y/o titulaciones. Las certificaciones/titulaciones son personales y se deberán identificar con el mismo identificativo que el presentado en las tablas que se describen a continuación. **Esta información únicamente se deberá aportar en el Sobre B por ser un criterio cuantificable automáticamente.**

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.

TABLA RESUMEN 1: entre 4 y 5 personas, dependiendo de si la Dirección del servicio la asume una persona Consultora Senior o una nueva incorporación.

Id. (1)	1.000h/año de media en los últimos 3 años en la elaboración de contenidos de formación	300h/año de media en los últimos 3 años en la elaboración de contenidos de formación relacionados con la seguridad de la información	3 años en gestión de proyectos	150h/año de media en los últimos 2 años en la elaboración de contenidos de formación relacionados con la seguridad de la información	Certificación ISACA (2)	Certificación DPO (2)	Certificación PMP (2)
1	(horas)		(horas)				(Fecha certificado)
2		(horas)	(horas)		Nombre certificación y Fecha certificado		(Fecha certificado)
3		(horas)	(horas)			(Fecha certificado)	(Fecha certificado)
…				(horas)			

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

(2) Presentar certificación

TABLA DETALLE 1: persona Consultora Senior de Comunicación/Formación

Id. (1)	Descripción del proyecto	Cliente (Entidad/Persona de contacto)	Periodo		Al menos 1.000h/año de media en los últimos 3 años en la elaboración de contenidos de formación
			Año	Horas	Descripción de tareas realizadas
1			aaaa	h	
…			aaaa	h	
Total				∑ horas (2)	

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

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

TABLA DETALLE 2: persona Consultora Senior de Ciberseguridad y Tecnología

Id. (1)	Descripción del proyecto	Cliente (Entidad/Persona de contacto)	Periodo		Al menos 300h/año de media en los últimos 3 años en la elaboración de contenidos de formación relacionados con la seguridad de la información
			Año	Horas	Descripción de tareas realizadas
2			aaaa	h	
…			aaaa	h	
Total				∑ horas (2)	

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

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

TABLA DETALLE 3: persona Consultora Senior en la gestión de la Información y Protección de Datos

Id. (1)	Descripción del proyecto	Cliente (Entidad/Persona de contacto)	Periodo		Al menos 300h/año de media en los últimos 3 años en la elaboración de contenidos de formación relacionados con la seguridad de la información
			Año	Horas	Descripción de tareas realizadas
3			aaaa	h	
…			aaaa	h	
Total				∑ horas (2)	

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

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

TABLA DETALLE 4: persona que asume las labores de Dirección del servicio. Puede ser un nuevo identificativo si se trata de una nueva persona o si la persona que asume las labores es una de las tres Consultoras Senior mencionadas anteriormente, se le pondrá el mismo identificativo que en su tabla.

Id. (1)	Descripción del proyecto	Cliente (Entidad/Persona de contacto)	Periodo		Al menos 3 años en gestión de proyectos	
			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 horas deberá coincidir con el dato de la TABLA RESUMEN

TABLA DETALLE 5: persona Consultora Junior

Id. (1)	Descripción del proyecto	Cliente (Entidad/Persona de contacto)	Periodo		Al menos 150h/año de media en los últimos 2 años en la elaboración de contenidos de formación relacionados con la seguridad de la información
			Año	Horas	Descripción de tareas realizadas
y			aaaa	h	
…			aaaa	h	
Total				∑ horas (2)	

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

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

4 CONDICIONES PARTICULARES

4.1 Horario del servicio

El horario de la prestación de servicio será todos los días laborales del territorio histórico de Bizkaia, en horario de 08:00 a 15:00.

Si Lantik solicitara la realización de algún trabajo fuera del horario de servicio, estos se podrán facturar con un coeficiente de 1,5 sobre el precio/hora establecido.

4.2 Modalidad de trabajo

Los trabajos se desarrollarán en los locales de la empresa contratada mediante conexión con los ordenadores de Lantik. 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, se podrá requerir 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.

Todas las acciones planificadas como presenciales se harán de modo presencial sin necesidad de preaviso porque ya existe un acuerdo previo.

Cuando la modalidad de trabajo de forma sea necesaria de forma presencial y continuada en el tiempo, Lantik deberá avisar con un mes de antelación.

4.3 Requisitos técnicos de la plataforma

El servicio debe proveer de una plataforma para el consumo de la formación, que debe cumplir los siguientes requisitos:

- Acceso multidispositivo.
- La generación de videos y la plataforma debe contemplar la inclusión de subtítulos, transcripción y audio descripción cuando sea necesario por accesibilidad.
- Acceso desde los navegadores homologados en Lantik (mínimo a las dos últimas versiones de los navegadores Microsoft Edge, Mozilla Firefox y Google Chrome).
- Deberá de integrase con la identificación Active Directory / Azure Active Directory y la mensajería corporativa (M365).

Ofrecerá un soporte de dinamización y consultas. Las consultas que se realicen a través de la plataforma se gestionarán diariamente de modo que no quede ninguna pendiente para el siguiente día hábil, salvo que entre fuera del horario de prestación de servicio establecido días laborables en el territorio histórico de Bizkaia en horario de 08:00 a 15:00 o en la última hora, en cuyo caso se respondería el siguiente día laborable.

Dispondrá de soporte para la gestión de consultas.

4.4 Equipo de trabajo

El equipo de trabajo estará integrado, como mínimo, por las personas especificadas en el apartado "Equipo técnico". Durante la ejecución del contrato, la empresa adjudicataria podrá incorporar los perfiles que juzgue necesarios para garantizar la adecuada prestación del servicio, considerando posibles variaciones en la carga de trabajo.

Se 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 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.

Del mismo modo, cualquier modificación en la composición del "Equipo de trabajo" a lo largo de la duración del contrato, especialmente cuando se trate de personas que dejan el equipo y tienen acceso a los sistemas de Lantik, debe ser comunicada con la mayor brevedad posible.

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 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 evolución tecnológica y el riesgo que ello conlleva en la seguridad, es responsabilidad de la empresa adjudicataria la formación continua del personal adscrito al contrato.

4.5 Estructura de la oferta técnica (sobre C)

De cara a la valoración de los criterios no cuantificables automáticamente (sobre C), la propuesta técnica presentada por la empresa licitadora en el **sobre C debe ajustarse como máximo a 40 páginas** en 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
- Modelo organizativo
  - Equipo: 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.
- Modelo operativo: se describirán las fases y los trabajos a realizar en cada una de ellas
  - Fase I – Diagnóstico
  - Fase II - Planificación

- Fase III - Ejecución
  - Trabajos específicos
  - Trabajos bajo demanda
  - Soporte a consultas
  - Evaluación
- Seguimiento del servicio: cuadros de mando, informes, comités, …

No contabilizará en las 40 páginas la información necesaria para acreditar el apartado “Equipo técnico”.

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.

4.6 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.
- Lantik decida dar por terminado el servicio.

4.7 Propiedad Intelectual

El título de propiedad de todos los productos generados objeto del presente pliego corresponde a Lantik. Todos los trabajos realizados por la empresa adjudicataria bajo el contrato resultante de este pliego 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 material 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.

4.8 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.

4.9 Seguridad de la información

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

En el contrato a firmar se incluirá:

- Acuerdo de confidencialidad.
- Conocimiento y compromiso de cumplimiento por parte de la empresa adjudicataria de:
  - Política de seguridad de la información y protección de datos de Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia.
  - Norma NCS-1/1 “Norma de Política de Seguridad: Código de Conducta Informático para Proveedores”.
  - Norma NCS-1/2 “Normativa de Seguridad de la Información para Proveedores”.

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

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 particular, será considerado como Información Confidencial todo el know how o saber hacer resultante de la ejecución de los servicios contratados, debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato. De este modo, se considerará confidencial, a todos los efectos, toda la información y documentación relativa a Lantik S.A. M.P. y/o que esta trate a cuenta de terceros, así como los buenos usos, prácticas y procedimientos internos, que pudiera conocer la empresa adjudicataria con motivo de la ejecución del contrato. En la misma línea, se confiere el carácter confidencial a aquella información a la que tenga acceso con ocasión de la ejecución del contrato, que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal, incluyendo, expresamente, toda la información asociada a medidas de seguridad y de protección, configuraciones desarrolladas, protecciones del servicio y aplicaciones, elementos y descripciones de infraestructura y arquitectura, procesos de autenticación y protocolos de seguridad, comunicaciones, incidencias, informes de terceros, controles de capacidad y evaluaciones de las disponibilidades implicadas, análisis automáticos, redes y protecciones del perímetro, elementos adscritos a la

continuidad, registros de actividad y protecciones asociadas, protocolos de copias y restauraciones, elementos de mantenimiento y garantías implicadas, y cuantos otros elementos puedan considerarse un riesgo a los efectos del servicio contratado o la información vinculada al mismo. En cualquier caso, se prohíbe expresamente el acceso a este tipo de datos, ni a ningún dato que no sea objeto de tratamiento del presente. Con ello, la empresa adjudicataria se compromete a no divulgar, no ceder o exponer la información titularidad de Lantik S.A. M.P. y /o que esta trate a cuenta de terceros, sin su previo consentimiento expreso y por escrito. Asimismo, la empresa adjudicataria deberá abstenerse de emplear la documentación y/o información conocida o facilitada durante la ejecución del contrato para fines ajenos a los propios de la ejecución del contrato.

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

II. Deber de secreto

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

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

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

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

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

III. Garantía de confidencialidad

La empresa adjudicataria certifica que el personal a su cargo ha firmado una cláusula de confidencialidad por la cual se 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.

B. 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".

C. 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.

D. 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.

E. 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.

F. 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.

G. 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.

o Conexión remota a los sistemas de información de Lantik S.A. M.P. exclusivamente a través de las herramientas autorizadas por Lantik S.A. M.P. referenciadas con anterioridad.

o No tendrá elementos externos conectados, como memorias USB, lectores CD/DVD, etc.

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

H. 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.

I. 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.

J. 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.

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

Sin./Fdo.: BALBINO ZUBIAGA URBIETA - 2024-09-24
SEGURTASUN SAILA
DEPARTAMENTO DE SEGURIDAD

Sin./Fdo.: MARTIN BERASATEGUI MEJIAS - 2024-09-24
ARKITEKTURA TEKNOLOGIKOKO ARLOA
ÁREA DE ARQUITECTURA TECNOLÓGICA

Sin./Fdo.: IMANOL SAUTO AVELLANAL - 2024-09-24
SEGURTASUN ETA TEKONOLOGIA UNITATEKO ZUZENDARITZA
DIRECCIÓN DE UNIDAD DE SEGURIDAD Y TECNOLOGÍA

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.