# Servicio para la planificación, despliegue, ejecución y seguimiento de los servicios del CSIRT de Cyberzaintza

Pliego de condiciones técnicas

# Índice


**1 Introducción ..... 4**

1.1 Perfil de la compañía ..... 4

**2 Objeto y Lotes del contrato ..... 6**

**3 Consideraciones previas ..... 6**

3.1 Privacidad y confidencialidad ..... 7

**4 Lote 1: "Suministro de renovación de licencias con soporte de fabricante de herramientas de inteligencia". 7**

4.1 Objeto ..... 7

4.2 Justificación de la tecnología ..... 7

4.3 Alcance ..... 8

**5 Lote 2: "Servicio de inteligencia de amenazas" ..... 8**

5.1 Objeto ..... 8

5.2 Requisitos ..... 8

5.3 Alcance ..... 8

5.4 Definición de una metodología de medición del riesgo basado en amenazas ..... 9

5.5 Vigilancia digital e Identificación de amenazas ..... 11

5.6 Análisis ..... 15

5.7 Producción de inteligencia y alerta temprana ..... 15

5.8 Desarrollo e integraciones ..... 17

5.9 Servicios adicionales bajo demanda ..... 18

5.10 Metodología y planificación ..... 18

5.11 Organización y equipo de trabajo ..... 19

5.12 Niveles de servicio ..... 24

5.13 Planes para la gestión adecuada del servicio ..... 27

**6 Lote 3: "Suministro de renovación de licencias y soporte del fabricante de la herramienta de EASM" .... 29**

6.1 Objeto ..... 29

6.2 Justificación de la tecnología ..... **¡Error! Marcador no definido.**

6.3 Alcance ..... 29

**7 Lote 4: "Servicios de despliegue y ejecución de una capacidad de preparación y respuesta a incidentes de ciberseguridad" ..... 33**

7.1 Objeto ..... 33

7.2 Requisitos ..... 33

7.3 Alcance ..... 33

7.4 Preparación ..... 34

7.5 Respuesta a incidentes ..... 39

7.6 Metodología y planificación ..... 43

7.7 Planes para la gestión adecuada del servicio ..... 44

7.8 Niveles de servicio ..... 46

7.9 Organización y equipo de trabajo ..... 49

7.10 Horario del servicio ..... 53

7.11 Equipamiento y software para el equipo de trabajo ..... 54

**8 Lote 5: "Servicio de campañas de phishing" ..... 54**

8.1 Objeto ..... 54

8.2 Requisitos ..... 54

8.3 Alcance ..... 54

8.4 Metodología y planificación ..... 57

8.5 Planes para la gestión adecuada del servicio ..... 58
8.6 Herramientas ..... ¡Error! Marcador no definido.
8.7 Organización y equipo de trabajo ..... 59
**9 Lote 6: "Oficina técnica para gestión de las iniciativas del Departamento de Operaciones" ..... 60**
9.1 Objeto ..... 60
9.2 Requisitos ..... 60
9.3 Alcance ..... 61
9.4 Incompatibilidades ..... 62
9.5 Metodología y planificación ..... 62
9.6 Planes para la gestión adecuada del servicio ..... 63
9.7 Herramientas ..... 64
9.8 Organización y equipo de trabajo ..... 64

# 1 Introducción

## 1.1 Perfil de la compañía

La Agencia Vasca de Ciberseguridad (Cyberzaintza), en adelante la Agencia, es un ente público de derecho privado del Sector Público de la Comunidad Autónoma Vasca. La Agencia se adscribe al departamento del Gobierno Vasco competente en materia de seguridad, a través de la persona titular de la Viceconsejería de Seguridad.

La Agencia tiene por objeto promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de su competencia, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración Pública, de su ciudadanía y de su tejido empresarial.

La LEY 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad en su Artículo 2 establece que las funciones que corresponden a la Agencia para el cumplimiento de su objeto son las siguientes:

- Promover una estrategia de ciberseguridad para el conjunto de las administraciones públicas de la Comunidad Autónoma Vasca, y potenciar y coordinar el alineamiento en la ciberseguridad en dicho conjunto.
- Impulsar un marco de estándares, directrices y normas técnicas de seguridad recomendables para el sector público vasco.
- Informar, con carácter preceptivo, en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Comunidad Autónoma Vasca en materia de ciberseguridad.
- Realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad desplegadas en el ámbito del sector público vasco.
- Prevenir y detectar incidentes de ciberseguridad en la Comunidad Autónoma Vasca y responder a ellos, estableciendo criterios y promoviendo el despliegue de las medidas de protección pertinentes ante las ciberamenazas y los riesgos inherentes sobre las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan, todo ello con respeto del marco competencial aplicable.
- Recoger los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en la Comunidad Autónoma Vasca en relación con el estado de la seguridad de la información, prestando especial atención a los sistemas considerados como críticos para el funcionamiento de los servicios públicos o la seguridad de las personas, con vistas a informar al Gobierno Vasco, así como a las administraciones públicas del territorio que intervengan en la prestación de dichos servicios críticos y esenciales, y proponer las medidas adecuadas llevando a cabo la gestión de riesgos en materia de ciberseguridad.
- Ejercer las funciones del equipo de respuesta a emergencias (CERT) dentro de las competencias de la Comunidad Autónoma Vasca. Dado que se trata de un fenómeno transfronterizo, es necesario colaborar con las administraciones y agencias de otros territorios con el objetivo de minimizar los daños y el tiempo de recuperación en caso de ciberataque.
- Coordinar los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y los equipos de respuesta a emergencias o las entidades equivalentes que actúen en su ámbito de actuación y de acuerdo a la legislación vigente, estableciendo modelos de colaboración con otros CSIRT estatales e internacionales. Asimismo, la Agencia ejercerá funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad en el ámbito del sector público vasco.

- Trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión Europea y reforzar las cadenas de suministro de dentro de la Unión Europea.
- Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información y servicios de tecnologías de la información.
- Garantizar un nivel adecuado de ciberseguridad en el uso de medios electrónicos.
- Organizar actividades de difusión, promoción, formación y concienciación en materia de ciberseguridad.
- Organizar actividades para promocionar el talento en la ciberseguridad, y participar en actividades de ciberseguridad, dando a conocer referentes, haciendo especial hincapié en las mujeres profesionales de la ciberseguridad.
- Proponer medidas técnicas de ciberseguridad en la utilización de los recursos informáticos y de las comunicaciones existentes, y proponer la formación en estas medidas del personal de la Administración de la Comunidad Autónoma Vasca y del propio personal de la Agencia.
- Actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas y, en particular, en las tareas de lucha contra las conductas ilícitas, incluidas la intervención directa y la obtención de pruebas electrónicas.
- Coordinar al sector público vasco en la elaboración de sus respectivos planes de ciberseguridad, así como en la consecución de los objetivos establecidos en los mismos.
- Poner sus servicios materiales y técnicos de ciberseguridad a disposición del sector público vasco.
- Impulsar la coordinación del sector público vasco en todo lo que se considere necesario para la consecución de los objetivos especificados en los planes de ciberseguridad, estableciendo para ello las líneas de colaboración que se entiendan necesarias.
- Ostentar la representación oficial del sector público vasco ante organismos internacionales, estatales y regionales en materia de ciberseguridad.
- Apoyar e impulsar la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial y en los sectores esenciales de la Comunidad Autónoma Vasca, como son el sector sanitario, el sector de emergencias y seguridad, el sector de servicios sociales y de intervención social, el sector educativo, el sector del transporte y el sector de la energía y las telecomunicaciones, o cualquier otro sector que pudiera considerarse sensible.
- Cualesquiera otras competencias que le sean conferidas por la legislación vigente o le sean expresamente delegadas o atribuidas.

# 2 Objeto y Lotes del contrato

El objeto del presente Pliego de Condiciones Técnicas corresponde a un servicio para la planificación, despliegue, ejecución y seguimiento de los servicios del CSIRT de Cyberzaintza, siendo las líneas de actividad englobadas:

- **Inteligencia de amenazas**: la línea de acción de inteligencia de amenazas tiene como objetivo principal proporcionar a las organizaciones información relevante y procesable sobre posibles amenazas en el ámbito de la ciberseguridad. Esto les facilita anticiparse a ataques, tomar decisiones informadas y reforzar su protección.
- **Respuesta a incidentes (CSIRT)**: la línea de acción de respuesta a incidentes tiene como objetivo principal asistir a las organizaciones en la preparación para una respuesta adecuada a incidentes de ciberseguridad, así como, en el apoyo y coordinación en la gestión cuando se materialicen, identificando vías de proteger al resto de entidades.
- **Concienciación**: la línea de acción de concienciación tiene como objetivo principal fomentar una cultura sólida de ciberseguridad y elevar el nivel de conocimiento y compresión tanto de individuos como de organizaciones sobre los riesgos digitales presentes en el entorno actual. Además, busca promover comportamientos seguros y responsables en la utilización de la tecnología.

El presente expediente comprende varias ofertas diferentes por lo que se ha dividido en los siguientes lotes:

***Línea de servicio de inteligencia de amenazas (Lotes 1 y 2)***

- Lote 1: “Suministro de renovación de licencias y soporte del fabricante de herramientas de inteligencia”: se trata del suministro para la renovación y mantenimiento de las licencias actuales. De este modo, el adjudicatario deberá suministrar las licencias y su soporte de fabricante asociado, correspondientes a los sistemas vigentes de los diferentes fabricantes.
- Lote 2: “*Servicio de inteligencia de amenazas*”: consiste en la provisión integral de servicios, abarcando el soporte, operación y suministro de las plataformas/herramientas correspondientes al Servicio de Cyber Threat Intelligence necesarias para garantizar el adecuado funcionamiento de los servicios solicitados.

***Línea de servicio de seguridad ofensiva (Lotes 3)***

- Lote 3: “Servicio para la gestión proactiva de la superficie de exposición”.

***Línea de servicio de respuesta a incidentes - CSIRT (Lote 4)***

- Lote 4: “Servicio de despliegue y ejecución de una capacidad de preparación y respuesta a incidentes de ciberseguridad”.

***Línea de servicio de concienciación (Lote 5)***

- Lote 5: “Servicio de campañas de phishing”.

***Oficina técnica para la gestión de todos los servicios (Lote 6)***

- Lote 6: “Oficina técnica para gestión de las iniciativas del Departamento de Operaciones”.

# 3 Consideraciones previas

A continuación, se detallan diversas consideraciones que son pertinentes para todos los lotes del presente expediente:

## 3.1 Privacidad y confidencialidad

El contratista se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la ejecución del contrato, respecto a toda la información de Cyberzaintza que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

La información proporcionada por Cyberzaintza a la que tenga acceso el licitador, así como aquella que haya sido generada a petición de Cyberzaintza debe considerarse propiedad de Cyberzaintza y se debe asegurar su confidencialidad, integridad y disponibilidad, mediante los controles adecuados para que esta información solo pueda ser accedida por el personal de Cyberzaintza o quien éste designe durante la duración del contrato. El contratista solo podrá hacer uso de la citada información para las actividades descritas en el presente pliego de prescripciones técnicas. Cualquier uso no contemplado en este apartado, requerirá autorización expresa de Cyberzaintza.

# Línea de servicio de inteligencia de amenazas

# 4 Lote 1: "Suministro de renovación de licencias con soporte de fabricante de herramientas de inteligencia".

## 4.1 Objeto

Este lote tiene por objeto la contratación de la renovación y ampliación de los suministros de los distintos fabricantes del servicio actual según el listado de suministros descrito en el alcance del lote.

De este modo, el adjudicatario deberá suministrar las suscripciones y su soporte de fabricante.

## 4.2 Justificación de la tecnología

Se considera dar continuidad al servicio que se presta a Cyberzaintza con el suministro para la renovación y mantenimiento de las licencias correspondientes manteniendo la tecnología actual, ya que incorporar nuevas tecnologías, implicaría afección en los siguientes ámbitos:

- Afección en el ámbito técnico:
  - La introducción de nuevas plataformas/herramientas para el servicio, diferentes a las actuales, genera la necesidad de realizar maquetas y laboratorios de pruebas adicionales previos al inicio de la fase de despliegue, pruebas que ya se han completado con la tecnología instalada.
- Afección en el ámbito organizativo:
  - Se incrementa la complejidad y esfuerzo a realizar para el despliegue y la operación y mantenimiento del servicio (en el día a día) derivado de:
    - La necesidad de definir, con los diferentes grupos de soporte, procedimientos de operación y mantenimiento adicionales para las nuevas tecnologías, atendiendo a los modelos de relación y modelo de garantías del propio fabricante.
    - La necesidad de disponer de recursos expertos adicionales sobre la nueva tecnología, así como de garantizar la formación de los recursos actuales en el corto plazo.
- Afección en el ámbito económico:
  - Un mayor coste en recursos capacitación y esfuerzo de operación, tanto en la puesta en marcha de la nueva infraestructura como en la operación y mantenimiento posterior.

Es por ello que, el Lote 1 del presente expediente contempla el suministro para la renovación y mantenimiento de las licencias correspondientes al servicio, con el fin de facilitar la explotación y operación, garantizando los tiempos de respuesta actuales sin costes adicionales.

### 4.3 Alcance

A continuación, se describe el alcance del Lote 1 a través del presente expediente.

| Producto | Cantidad |
|---|---|
| Shodan (Licencia Corporate) | 1 |
| Brand24 (Licencia Enterprise) | 1 |
| Maxmind (GeoIP2 City Database) | 1 |
| Any Run (Licencia Hunter) | 1 |
| IntelX (Licencia Enterprise) | 1 |

La empresa adjudicataria deberá suministrar las licencias indicadas en el citado documento junto con el soporte de fabricante asociado.

Todas las licencias y soportes de fabricante asociados deberán ser oficiales y estar garantizadas por el fabricante durante el periodo solicitado para cada elemento.

El soporte de fabricante debe incluir, sin coste adicional, el acceso a las actualizaciones de parches, alertas de seguridad, y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.

## 5 Lote 2: “Servicio de inteligencia de amenazas”

### 5.1 Objeto

Este lote tiene por objeto la contratación de un servicio de inteligencia amenazas que permita identificar, analizar y mitigar las ciberamenazas con potencial impacto en los diferentes públicos objetivo de Cyberzaintza.

### 5.2 Requisitos

- El servicio se prestará en su totalidad en formato bilingüe: tanto en euskera como en castellano.
- El servicio se prestará en horario laboral de 09:00 a 17:00 de lunes a viernes.
- Los materiales se generarán siguiendo las pautas del manual de identidad de marca de la Agencia.
- El adjudicatario asumirá los gastos derivados de los desplazamientos, dietas y otros costos asociados a la disposición de medios necesarios para estos y, en general, para la ejecución del proyecto en las condiciones de presencialidad indicadas.

### 5.3 Alcance

El alcance del lote comprende lo siguiente:

- Servicio de inteligencia de amenazas que incluye las tareas que se describen en el presente pliego.
- Stack tecnológico. Plataformas y herramientas como servicio que soporten dichas tareas, incluyendo:
    - Salvo que se indique lo contrario, credenciales y licencias de acceso será para todo el equipo de trabajo asignado por el proveedor al contrato.

  - Interfaz de programación de aplicación (API), con un número ilimitado de peticiones y sin limitaciones ni restricciones, para el acceso automatizado para, al menos, una integración.
- Equipo de trabajo asociado al servicio.
- Transferencia del conocimiento asociada al servicio prestado en base, principalmente, al uso, administración y configuración del mismo.
- Soporte asociado durante toda la prestación del servicio.

En este apartado se describe el alcance de los servicios solicitados, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por Cyberzaintza, cubriendo los aspectos de tareas a realizar y los resultados esperados.

| Definición de metodología de medición del riesgo | Vigilancia digital e Identificación de amenazas | Análisis | Producción de inteligencia y Alerta temprana | Desarrollo e integraciones |
|---|---|---|---|---|
| | • Monitorización de disponibilidad de activos<br>• Detección de fugas de credenciales<br>• Detección de información sensible expuesta<br>• Detección de dominios nuevos registrados con fines maliciosos<br>• Detección de campañas de phishing, smishing y malware<br>• Detección de ataques<br>• Detección de fraudes | | • Generación,entrenamiento, explotación y mantenimiento de modelos de inteligencia artificial en el ámbito de la ciberseguridad.<br>• Generación de alertas previstas<br>• Generación de alertas imprevistas<br>• Generación de eventos en MISP<br>• Generación de boletines<br>• Generación de informes de inteligencia de amenazas y cibercrimen<br>• Generación de informes de estado | |

A continuación, se describen las tareas generales que se ejecutarán dentro del contrato. **Para cada una de las tareas referidas a continuación, el licitador deberá presentar y detallar de manera exhaustiva las herramientas / plataformas que utilizará para la prestación del servicio, destacando sus funcionalidades y limitaciones de manera explícita.** El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

## 5.4 Definición de una metodología de medición del riesgo basado en amenazas

Los licitadores deberán proponer una metodología lógica que permita evaluar de manera común y objetiva el nivel de riesgo basado en amenazas tanto de Euskadi a nivel global, como de sus públicos objetivo (Administración Pública, Empresas y Ciudadanía), y de las entidades a las que Cyberzaintza presta servicio, a partir del modelo de inteligencia.

Dicha metodología contemplará al menos:

- Los públicos objetivo de Cyberzaintza: Administración Pública, Empresas y Ciudadanía.
- Una propuesta de algoritmo basado en evidencias fiables y de calidad, obtenidas cumpliendo toda la normativa de aplicación para Cyberzaintza.
- La metodología incluirá un listado de al menos 30 ámbitos de evaluación diferentes con el objetivo de que el sistema sea exhaustivo y completo.
- La identificación de amenazas en el ámbito de la ciberseguridad, identificando las más activas por cada uno de los públicos objetivo a modo de «Threat landscape», así como por cada uno de los sectores estratégicos.

- La identificación de requisitos para el modelo de inteligencia, los cuales deberán ser agrupados según criterio común y que permitan identificar las amenazas anteriormente mencionadas a partir de orígenes propuestos.
- La identificación de sistemas comprometidos bajo criterios concretos como por ejemplo infección por botnets o stealers, emisión de phishing o spam, emisión de ataques DDOS, etc.
- La identificación de sistemas vulnerables bajo criterios concretos, como por ejemplo accesos remotos, sistemas desactualizados, errores de configuración, certificados vulnerables, etc.
- Deberá ir alineada con los estándares de ciberseguridad de aplicación a los públicos objetivos de la Agencia.
- Deberá, así mismo, detallar diferentes ámbitos de evaluación, ponderando cada uno de ellos, de modo que finalmente se obtenga tanto una puntuación general del colectivo, una puntuación por cada uno de los ámbitos de evaluación individuales, y una puntuación a título individual de un dominio, una entidad, etc.
- Deberá especificar toda la información a recopilar y almacenar, así como los tiempos de retención, etc.

A continuación, se muestra un ejemplo de ámbito de evaluación que podría formar parte de la metodología:

- Descripción: el objetivo es evaluar el nivel de protección de los dominios de Euskadi.
- Requisito principal: Identificar cuántos dominios pertenecientes al TLD .EUS pueden ser fácilmente suplantados.
- Grupo al que pertenece el requisito: Dominios seguros.
- Requisitos secundarios:
  - Primer requisito secundario: Determinar cuántos dominios pertenecientes al TLD .EUS no tienen SPF.
  - Segundo requisito secundario: Determinar cuántos dominios pertenecientes al TLD .EUS no tienen DKIM.
  - Tercer requisito secundario: Determinar cuántos dominios pertenecientes al TLD .EUS no tienen DMARC.
- Muestra: los 16.500 dominios pertenecientes al TLD .EUS.
- Ponderación individual, de modo que un dominio pueda tener un nivel de riesgo máximo de 200 puntos en este grupo de «Dominios seguros»:
  - Ausencia de SPF: 100 puntos de riesgo.
  - Ausencia de DKIM: 60 puntos.
  - Ausencia de DMARC: 40 puntos.
- Ponderación colectiva por cada requisito secundario: una vez identificados cuántos dominios no tienen SPF, DKIM y DMARC se calculará el nivel de riesgo de cada uno de los requisitos secundarios de acuerdo a los siguientes criterios:
  - Ausencia de registro ≤ 5%: Puntuación A.
  - Ausencia de registro > 5% y ≤ 10: Puntuación B.
  - Ausencia de registro > 10% y ≤ 20: Puntuación C.
  - Ausencia de registro > 20% y ≤ 30: Puntuación D.
  - Ausencia de registro > 30% y ≤ 40: Puntuación E.
  - Ausencia de registro > 40%: Puntuación F.
  - Etc.
- Ponderación general de grupo. A partir de los valores obtenidos en el punto anterior se obtendrá un nivel de riesgo general de grupo de requisito de acuerdo a los siguientes criterios:
  - Si SPF ≤ E, grupo dominios seguros será Riesgo Muy Alto.
  - …….
  - …….

    - …….
    - Si SPF ≥ B y DKIM ≥ B y DMARC ≥ C será Riesgo Muy Bajo.
- De este modo, el TLD .EUS puede tener un nivel de riesgo Muy Bajo, pudiendo estar el SPF con puntuación A, el DKIM con puntuación B y el DMARC con puntuación C, pero un dominio concreto puede tener un nivel de riesgo Muy Alto ya que puede tener los 3 registros sin configurar, o viceversa.
- Esta valoración deberá ir así mismo relacionada con las amenazas más activas en Euskadi en ese momento, de modo que si hubiera alguna cuyos TTP incluyeran la suplantación de correos como método de propagación de fraude, se aplicaría un factor de corrección que incrementaría el nivel de riesgo en el grupo «Dominio seguros», por ejemplo, de Muy Alto a Crítico.

**Los licitadores deberán proponer un listado de ámbitos de evaluación, desarrollando 2 de ellos de acuerdo a la estructura descrita o similar.**

El adjudicatario del servicio desarrollará una propuesta completa, que tras previa validación por parte de Cyberzaintza, será implementada en el ELK de Cyberzaintza por el equipo de trabajo asignado al servicio.

## 5.5 Vigilancia digital e Identificación de amenazas

El servicio, que debe ir alineado con la metodología de medición propuesta, por lo que la plataforma de inteligencia de amenazas propuesta por el licitador debe integrar y administrar múltiples fuentes de inteligencia de ciberamenazas, incluyendo, pero no limitándose a los siguientes tipos:

- Fuentes propias del contratista, información que proceda de mecanismos de detección propios como, por ejemplo, análisis e investigaciones de eventos de ciberseguridad, generación de iocs basados en análisis de malware, entre otros.
- Fuentes de terceros, datos que provengan de la detección y recolección de otras fuentes propietarias distintas a las propias del contratista.
- Fuentes abiertas (OSINT), datos recolectados a partir de fuentes de acceso público como medios de comunicación, redes sociales e información pública de fuentes gubernamentales, entre otros.
- Foros privados, datos recolectados en foros solo accesibles para usuarios registrados y verificados.
- Fuentes de deep y dark web, datos recolectados de fuentes que no están indexadas, o que no son accesibles a través de mecanismos tradicionales.
- Paste sites, datos recolectados de servicios de alojamiento de contenidos donde los usuarios pueden almacenar texto sin formato. Por ejemplo, sitios como PasteBin, Exploit-db o HasteBin, entre otros.
- Repositorios de código, datos recolectados de servicios de alojamiento y compartición de código fuente como pueden ser GitHub o Bitbucket, entre otros.
- Fuentes HUMINT, aquellas derivadas de la inteligencia recogida y proporcionada por inteligencia humana.

Dicho listado será actualizado a lo largo de la ejecución del servicio y deberá permitir identificar y recolectar información que pueda afectar a los diferentes públicos objetivos de Cyberzaintza, como, por ejemplo:

- Ciberamenazas.
- Campañas de malware.
- Campañas de phishing.
- Campañas de smishing.
- Fugas de credenciales.

- Fugas de información sensible.
- Incidentes de ciberseguridad.
- Amenazas directas realizadas.
- Posibles fraudes online.
- Etc.

La plataforma de inteligencia de amenazas deberá cumplir así mismo los siguientes requisitos:

- Credenciales y licencia de acceso para todo el equipo asignado por el proveedor.
- Interfaz de programación de aplicación (API), con un número ilimitado de peticiones y sin limitaciones, ni restricciones para el acceso automatizado.
- Recopilación de información en tiempo real.
- Capacidad para realizar búsquedas complejas en tiempo real. Así mismo, deberá permitir hacerlo sobre un histórico de datos. Dicho histórico de datos debe ser de, al menos, 12 meses al inicio de la prestación del servicio. Sin perjuicio de lo anterior, desde el inicio del servicio se debe generar un histórico de datos que permita consultar los datos que se han generado durante la vigencia del contrato.
- Soporte multi-idioma de la información.
- Posibilidad de activar y configurar alertas automáticas a diferentes destinatarios y a través de diferentes métodos.
- Debe incluir información accionable como:
  - Listado de recomendaciones para responder a amenazas, que vayan alineadas con estándares de ciberseguridad.
  - Reglas de yara, sigma, etc.
  - Indicadores de compromiso.
- Soporte 8x5 durante la prestación del servicio.

El licitador deberá indicar de manera expresa si la plataforma de inteligencia de amenazas cubre una serie de **casos de uso obligatorios**, para lo cual deberá completar la tabla detallada contenida en la pestaña titulada "Casos de uso" del archivo Excel Anexo II – PCT_Requisitos Técnicos_Lote2.xlsx correspondiente a los requerimientos solicitados en el Lote 2 del presente expediente.

Así mismo, podrá incluir casos de uso adicionales no especificados, pero que vayan alineados con el objeto del contrato.

Para garantizar el cumplimiento de los casos de uso designados como Req.XX, el licitador deberá proporcionar las evidencias pertinentes, consistentes en:

- Capturas de pantalla que acrediten la funcionalidad requerida.
- Breve descripción del contenido de cada captura, explicando su relación con el requisito evaluado. Esta información se incluirá en un anexo específico, en el que cada evidencia estará numerada según el orden exacto de los requisitos Req.XX establecidos en la documentación del procedimiento.

El incumplimiento de las condiciones formales de presentación establecidas en este documento podrá afectar a la valoración de la oferta pudiendo llegar a la exclusión de esta.

Con el objetivo de validar que la plataforma de inteligencia cubre los casos de uso obligatorios solicitados, Cyberzaintza se reserva el derecho a solicitar una prueba de las capacidades técnicas de cualquiera de las soluciones propuestas por el licitador propuesto como adjudicatario, coincidiendo con la fase de acreditación de requisitos previos.

En caso de que así sea requerido:

- Los costes para la realización de esas pruebas serán íntegramente asumidos por el propuesto como adjudicatario que, además, deberá facilitar el soporte que sea solicitado por Cyberzaintza para la realización de dicha prueba.
- El periodo de prueba no podrá superar los 30 días naturales y deberá realizarse en los 45 días siguientes a la publicación de la propuesta de adjudicación de la Mesa de Contratación.
- En caso de que el resultado de la prueba no sea satisfactorio porque se evidencie que la solución no cumple con los requisitos establecidos en este PCT, el licitador será descartado como posible adjudicatario por incumplimiento del PCT.

### 5.5.1 Monitorización de disponibilidad de activos

En el alcance de la actividad de monitorización de activos se contempla la monitorización de la disponibilidad de un listado de hasta 1.000 dominios. Dicha monitorización permitirá al menos la identificación de caídas de servicio de las páginas web, si bien se valorarán funcionalidades adicionales.

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades. El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

### 5.5.2 Detección de fugas de credenciales

En el alcance de la actividad de detección de fugas de credenciales se contempla la identificación en los siguientes casos para un total de al menos 1.000 dominios:

- Equipos comprometidos por troyanos, backdoors, y malware en general. Dicha información debe ser detectada de manera exclusiva por parte del contratista a partir de diferentes métodos como sinkholing, acceso privado a logs, etc., es decir, que no esté disponible en fuentes abiertas o de forma pública. Para este caso, es obligatorio que el adjudicatario del servicio aporte información de detalle entre la que se incluya nombre de usuario, contraseña, activos afectados, dirección IP desde la que se ha exfiltrado la información, fecha de cuándo se ha producido el leak, el malware responsable, etc.
- Bases de datos expuestas o recopilatorios de contraseñas, para el cual se deberá indicar los usuarios afectados y la fecha de cuándo se ha producido el leak.

**La información deberá estar disponible en tiempos inferiores a 48 horas a partir de la exfiltración y poder consumirse de manera automatizada a través de la API. Así mismo, debe establecer mecanismos para reducir al mínimo los falsos positivos.**

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades. El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

### 5.5.3 Detección de información sensible expuesta

En el alcance de la actividad contempla la detección de fugas de información que afecten a un listado de al menos 1.000 entidades. Esto es, supongamos que se produce una fuga de información en la que aparecen documentos con información sensible como nóminas, facturas, credenciales de accesos a bases de datos, etc. pertenecientes a la entidad monitorizada. El adjudicatario del servicio deberá tener la capacidad de detectar este tipo de fugas.

**Así mismo, el adjudicatario del servicio deberá tener la capacidad de detectar fugas de información sensible en repositorios de Github atendiendo a los casos de uso de Cyberzaintza.**

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades. El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

### 5.5.4 Detección de dominios nuevos registrados con fines maliciosos

En el alcance de la actividad se contempla la monitorización, detección y envío diario del listado de dominios registrados que sean similares a los establecidos en un listado de al menos 1.000 entidades, evaluando previamente la probabilidad de que hayan sido registrados con fines maliciosos. Dicha monitorización se realizará en distintos TLD y previo a la alerta se realizará un enriquecimiento y análisis de la información que aporte contexto a Cyberzaintza de cara a tomar potenciales medidas de desmantelamiento.

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades. El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

### 5.5.5 Detección de campañas de phishing, smishing y malware

En el alcance de la actividad se contempla la identificación de campañas de phishing, smishing y malware con impacto en Euskadi.

Cyberzaintza acordará con la entidad adjudicataria los criterios exactos, si bien como norma general serán campañas en castellano o euskera que suplanten a entidades públicas de Euskadi o a compañías y servicios de uso mayoritario por parte de los diferentes públicos objetivos de la Agencia.

Así mismo, el adjudicatario del servicio montará y gestionará para Cyberzaintza una red de spamtraps que contribuya a la detección de este tipo de campañas. Para ello, registrará y mantendrá un total de 30 dominios en diferentes TLD, cuyos nombres se acordarán previamente. **El licitador deberá proponer un planteamiento de red de spamtraps,** presentando y detallando de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades.

### 5.5.6 Detección de ataques

En el alcance de la actividad se contempla la identificación de ataques que se estén produciendo en el ámbito de Euskadi para lo cual el adjudicatario montará y gestionará para Cyberzaintza una honeynet.

**El licitador deberá proponer un planteamiento de una red de honeypots,** presentando y detallando de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades.

Así mismo, se valorará el despliegue de cualquier otro tipo de soluciones que contribuyan a este objetivo.

### 5.5.7 Detección de fraudes

En el alcance de la actividad se contempla la identificación de fraudes con impacto en los diferentes públicos objetivo de la Agencia.

Cyberzaintza acordará con la entidad adjudicataria los criterios exactos, si bien como norma general serán campañas en castellano o euskera que suplanten a entidades públicas de Euskadi o a compañías y servicios de uso mayoritario por parte de los diferentes públicos objetivos de la Agencia.

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades y funcionalidades. El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

## 5.6 Análisis

Como continuación a la fase de vigilancia digital e identificación de amenazas se contempla una fase de análisis que permita realizar el correspondiente enriquecimiento y triaje para valorar la idoneidad de continuar con la fase de producción de inteligencia y alerta temprana.

El licitador deberá indicar de manera expresa si la plataforma de inteligencia de amenazas cubre una serie de **casos de uso obligatorios**, para lo cual deberá completar la tabla detallada contenida en la pestaña titulada "Casos de uso" del archivo Excel Anexo II – PCT_Requisitos Técnicos_Lote2.xlsx correspondiente a los requerimientos solicitados en el Lote 2 del presente expediente.

Así mismo, podrá incluir casos de uso adicionales no especificados, pero que vayan alineados con el objeto del contrato.

En el caso de que resulte adjudicatario del servicio deberá implementar todos los casos de uso en la plataforma de inteligencia de amenazas.

Una vez enriquecida la información y realizado el triaje, se realizarán las acciones que se consideren oportunas como realizar una alerta temprana, tomar acciones técnicas para proteger a los diferentes públicos objetivo de Cyberzaintza, etc.

## 5.7 Producción de inteligencia y alerta temprana

### 5.7.1 Generación, entrenamiento, explotación y mantenimiento de modelos de inteligencia artificial en el ámbito de la ciberseguridad

El equipo de trabajo asignado al servicio generará, entrenará, explotará y mantendrá modelos de inteligencia artificial específicos en el ámbito de la ciberseguridad que contribuyan a la prestación de los servicios de Cyberzaintza, en base las particularidades de los mismos, y que se ejecutarán de manera local. A modo de contexto, se referencia un modelo específico para la generación avisos y alertas, un modelo específico para la generación de boletines, un modelo para la generación recomendaciones en base a diferentes tipologías de incidentes, etc. A efectos informativos, se estima la utilización de crawl4ai, Microsoft markitdown, ollama y herramientas similares para el desarrollo de los modelos.

### 5.7.2 Generación de alertas

El equipo de trabajo asignado al servicio generará, publicará y difundirá alertas correspondientes en su mayoría a vulnerabilidades con potencial afección en los diferentes públicos objetivos de la Agencia

A modo de ejemplo, se indican una serie de alertas:

- https://www.ciberseguridad.eus/ultima-hora/vulnerabilidades-en-cisco-adaptive-security-appliance-y-firepower-threat-defense
- https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-en-citrix-uberagent

- https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-critica-en-pan-os-de-palo-alto

### 5.7.3 Generación de alertas imprevistas

En el caso de que sea necesario, el equipo de trabajo asignado al servicio generará, publicará y difundirá alertas instantáneas. Dicha alerta tendrá como mínimo la siguiente información:

- Título.
- Resumen de la información encontrada y análisis de la misma.
- Justificación de la alerta y un análisis del impacto y de las posibles consecuencias de esta información, que deberá estar contextualizada estableciendo enlaces con casos precedentes o con cualquier otra información previa que pueda estar relacionada.
- Recomendaciones para mitigar el riesgo o incluso neutralizarlo.

A modo de ejemplo, se indican una serie de posibles alertas:

- Una de las entidades a monitorizar sufre un incidente de ciberseguridad y el atacante publica información sensible.
- Una de las entidades monitorizar es fijada como objetivo de un ataque de denegación de servicio.
- La web de alguno de las entidades a monitorizar sufre un defacement.
- Una de las entidades a monitorizar sufre una amenaza directa en redes sociales.
- Un proveedor de entidades públicas sufre un incidente de ransomware.

### 5.7.4 Generación de eventos en la plataforma de intercambio de información sobre ciberamenazas (MISP)

El equipo de trabajo asignado al servicio generará, validará, publicará y difundirá eventos con indicadores de compromiso en el MISP de Cyberzaintza, plataforma de intercambio de información sobre ciberamenazas a la que se conectan entidades de los diferentes públicos de la Agencia para consumir la información.

Así mismo, se encargarán de la gestión, mantenimiento y actualización de la plataforma y los feeds generados a partir de la información de la misma.

### 5.7.5 Generación de boletines

El equipo de trabajo asignado al servicio generará, validará, publicará y difundirá periódicamente diferentes boletines atendiendo a los públicos objetivos de Cyberzaintza, los cuales se generan a partir de información pública de ciberseguridad y de información del modelo de inteligencia de Cyberzaintza. Sirva a modo de referencia que en la actualidad se generan 6 boletines, si bien se prevé el incremento de dicha cantidad.

A modo de ejemplo, se comparte una muestra de boletín englobado dentro de esta casuística:

- https://www.ciberseguridad.eus/boletin-cibereguraldia-ciberseguridad/ciber-eguraldia-abril-2024

El adjudicatario del servicio automatizará la generación de los boletines con el objetivo de que sean personalizados para cada una de las entidades destinatarias de los mismos.

### 5.7.6 Generación de informes de situación

Se contempla el envío de un informe semanal en el día y hora convenidos, el cual incluirá un resumen ejecutivo con todo lo sucedido esa semana, junto con la información más relevante

relacionada durante ese periodo en el ámbito de la ciberinteligencia. Cyberzaintza aportará la plantilla que deberá ser utilizada.

### 5.7.7 Generación de informes de inteligencia de amenazas y cibercrimen

Se contempla la elaboración de informes especializados. Dichos informes requerirán la aportación del conocimiento especializado del equipo de especialistas del adjudicatario, obtenido como resultado de las diferentes investigaciones en las que han participado.

A modo de ejemplo, se comparte una muestra de informe englobado dentro de esta casuística:

- https://www.ciberseguridad.eus/empresa-segura/utilidades-empresa/guias-estudios-informes/situacion-de-la-ciberseguridad-en-euskadi-4-trimestre-2022
- https://www.ciberseguridad.eus/empresa-segura/utilidades-empresa/guias-estudios-informes/noname057-16
- https://www.ciberseguridad.eus/empresa-segura/utilidades-empresa/guias-estudios-informes/cactus-ransomware

Otros ejemplos de informe de estas características pueden ser el análisis de la actividad en los últimos 3 meses de un threat actor con impacto en un sector concreto, el análisis de amenazas en el ámbito de la ciberseguridad relacionadas con procesos electorales, el análisis de amenazas en el ámbito de la ciberseguridad más activas relacionadas con el sector salud, la identificación de riesgos más habituales en un sector, etc.

En función del perfil al que estén dirigidos y el nivel de detalle de los informes, se identifican tres tipos:

- Estratégico. Proporciona una visión amplia del entorno de las amenazas, evaluación de su impacto y riesgo de las mismas. No contiene un detalle técnico amplio, pero sí cubre temas relevantes sobre el contexto enfocado a su uso por parte de la Dirección. Debe estar orientado a apoyar y mejorar, mediante un mejor contexto en la toma de decisiones.
- Táctico. Permite la priorización y mitigación de amenazas, al proporcionar información agregada de ataques específicos, relaciones entre diferentes TTPs y, probablemente, avisos o alertas sobre ataques inminentes. Permite un seguimiento a alto nivel en cambios identificados en TTPs, campañas, actores, etc. y con ello la identificación tanto de medidas de mitigación como oportunidades de lanzamiento de nuevas acciones que permitan captar nueva información de inteligencia sobre las amenazas. La táctica se relaciona en forma directa con la resolución de problemas. En este sentido, se trata del “qué” hacer frente a una situación determinada, evaluando en forma racional una serie de variables que se ajustarán con la experiencia.
- Operacional o técnico. Proporciona información técnica sobre las amenazas, información accionable a través de IOCs y TTPs condicionadas por la fiabilidad de la información y permitiendo la identificación de patrones sobre las amenazas. Dirigido particularmente a personal técnico y a acciones de detección y mitigación a corto plazo. Estos informes incluirán un detalle técnico elevado que permita comprender las amenazas en sus diferentes fases, vectores de ataque, etc.

Se estima la generación de 4 informes anuales de esta tipología.

## 5.8 Desarrollo e integraciones

El servicio incluirá una bolsa de 1700 horas anuales, que podrán ejecutarse según necesidad y facturadas según trabajos realizados, siendo el objetivo principal la evolución y el mantenimiento de la aplicación web interna de clientes de la Agencia. De no consumirse, las horas se podrán utilizar en caso necesario cuando se consuman las otras bolsas de horas, aplicando el precio de adjudicación de cada una de las bolsas.

## 5.9 Servicios adicionales bajo demanda

El servicio incluirá una bolsa de 510 horas anuales para actividades que tengan relación directa con el contrato, pero queden fuera del alcance inicial del mismo y que serán consumidas según necesidad.

A continuación, se expone, a modo de ejemplo, una relación enunciativa y no limitativa de tareas que podrían solicitarse:

- Consultoría técnica.
- Consultoría tecnológica sobre herramientas que contribuyan a evolucionar el modelo de inteligencia de Cyberzaintza.
- Despliegue de nuevas capacidades alineadas con el objetivo del contrato.
- Operativos de inteligencia.
- Apoyo en la respuesta a incidentes.
- Etc.

## 5.10 Metodología y planificación

Los licitantes deberán realizar una **propuesta de metodología y de plan de trabajo** que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas. Así mismo deberá incluir:

### 5.10.1 Fases de trabajo

Los licitadores deberán realizar una propuesta de plan de trabajo que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas.

#### 5.10.1.1 Inicio del servicio

El licitador deberá describir en su propuesta técnica (Plan de Inicio del Servicio) los recursos de gestión específicos que aportará en la fase de entrada al servicio, así como los que tiene que aportar Cyberzaintza.

Esta fase pondrá un especial énfasis en la gestión del cambio de todos los aspectos implicados, con especial foco en la metodología, la configuración inicial, la formación al equipo de trabajo, y el resto de los aspectos que corresponda.

Como primera actividad asociada al contrato se establecerá una reunión de “lanzamiento del servicio” entre la empresa adjudicataria y Cyberzaintza, en el cual se identificarán los interlocutores de ambas partes.

En esta reunión además se definirán el resto de las condiciones que afectan a la ejecución del servicio, si existiesen, y se establecerán los procedimientos de trabajo a ejecutar, en base a la propuesta presentada, que deberá ser aprobado por Cyberzaintza.

#### 5.10.1.2 Seguimiento del servicio

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista se reunirá con la dirección técnica del proyecto de Cyberzaintza con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato.

Cyberzaintza podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento y la correcta ejecución del objeto del contrato, si bien se estima una reunión mensual. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

En dichas reuniones se revisarán al menos los siguientes puntos:

- Trabajos realizados en el periodo anterior.
- Trabajos planificados para el siguiente periodo.
- Seguimiento económico del contrato.
- Incidencias surgidas y áreas de mejora.

El responsable de Cyberzaintza tiene las más amplias atribuciones, y sus órdenes e instrucciones serán debidamente ejecutivas.

El adjudicatario deberá proporcionar la información requerida por Cyberzaintza para conocer la situación y desarrollo de las actividades solicitadas. Las discrepancias sobre el desarrollo de los servicios serán resueltas al nivel más elevado de representación.

El incumplimiento por parte del adjudicatario de lo establecido en el presente pliego de Bases Técnicas y cuando dicho incumplimiento sea reiterativo o se refiera a órdenes que le hayan sido impartidas por escrito y advirtiéndole que son esenciales para el buen fin del contrato, se considerará causa de resolución del mismo.

#### 5.10.1.3 Devolución del servicio

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, a prestar apoyo, y realizar la transferencia del conocimiento, documentación técnica y administrativa necesaria para el traspaso del servicio, etc. al siguiente adjudicatario del contrato, en caso de que éste sea distinto al adjudicatario del presente pliego.

Asimismo, durante el último mes de servicio, el adjudicatario del presente contrato deberá facilitar al adjudicatario entrante acceso en modo lectura a las plataformas de servicio para el conocimiento y aprendizaje de reglas creadas, configuraciones y políticas, indicadores de servicio, garantizando con ello una transición efectiva del servicio con el inicio del siguiente contrato.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de Cyberzaintza cuando se produzca la finalización del contrato.

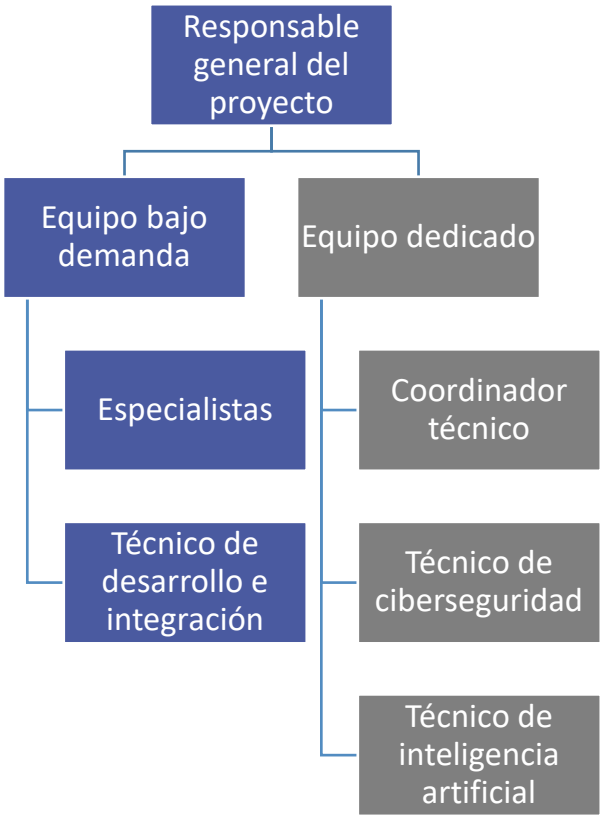
Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por Cyberzaintza con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

## 5.11 Organización y equipo de trabajo

El equipo de trabajo encargado de ejecutar las tareas especificadas en el ámbito de este contrato deberá respetar el siguiente organigrama:




El licitador se compromete, en caso de ser adjudicatario, a mantener el equipo, según lo establecido en el Documento de Propuesta Técnica, y durante el periodo fijado en cada actividad específica. Los recursos asignados a la ejecución del contrato deberán estar asignados desde el inicio del mismo. En el caso de modificación o sustitución de recursos, deberá comunicarlo previamente a Cyberzaintza, con la antelación necesaria en función de la criticidad del servicio, y en cualquier caso cumpliendo los niveles de servicio, y Cyberzaintza aprobará o rechazará dicha modificación o sustitución. En todo caso el sustituto o sustitutos tendrán un perfil igual o superior al ofertado, o recurso a sustituir.

Cyberzaintza podrá solicitar el cambio de los recursos asignado a los servicios, por inadecuación de los recursos o por incumplir los requisitos tanto de solvencia como técnicos exigidos, o haber declarado el contratista unas circunstancias que no son veraces, en cuyo caso podrá conllevar la rescisión del contrato y adjudicación al licitador siguiente en las calificaciones.

### 5.11.1 Roles y ámbito de responsabilidad

- Responsable general del proyecto: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del pliego y se encargará de la relación profesional entre el proveedor y Cyberzaintza.

Dicho rol deberá cumplir los siguientes requisitos:

- Tener una buena capacidad de planificación.
- Habilidades de comunicación efectiva.
- Conocimientos sólidos en metodologías de gestión de proyectos.
- Habilidad de resolución de problemas.
- Buena orientación a los resultados.

Tendrá las siguientes funciones:

- Controlar los Procesos de Gestión ITIL y establecer los indicadores de control de gestión y los informes de gestión.
- Mantener y actualizar con Cyberzaintza los Acuerdos de Niveles de Servicio (ANS).
- Coordinar las funciones del servicio y la correcta ejecución de los procesos de gestión.
- Mejora continua del servicio.

Debe presentar experiencia contrastable de al menos 5 años en tareas similares y es imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.

- Especialista (bajo demanda)

Las personas con rol de Especialista realizarán las siguientes tareas:

- Definirán la metodología de medición del riesgo basado en ciberamenazas.
- Planificarán, desplegarán y configurarán todo el stack tecnológico asociado al servicio.
- Harán transferencia del conocimiento a todo el equipo asignado al servicio.
- Proporcionarán asesoramiento experto en su área de especialización al equipo que preste el servicio de manera presencial en Cyberzaintza.
- Generarán los informes de inteligencia de amenazas y cibercrimen.
- Contribuirán en la mejora continua del servicio.

Deben presentar experiencia contrastable en las tareas que son objeto del contrato. Deberán tener al menos 5 años de experiencia en las funciones indicadas y tener conocimientos sólidos sobre ciberseguridad, ciberinteligencia, análisis de malware, respuesta a incidentes de ciberseguridad, redes, sistemas, etc.

- Coordinador técnico (dedicado)

Perfil de ciberseguridad altamente cualificado en ciberinteligencia y en el stack tecnológico ofertado para el servicio. Deberá tener al menos 5 años de experiencia en el objeto del contrato.

Dicho rol deberá cumplir además los siguientes requisitos:

- Tener una buena capacidad de organización.
- Habilidades de comunicación efectiva.
- Habilidad de resolución de problemas.
- Buena orientación a los resultados.

Tendrá las siguientes funciones:

- Seguimiento, supervisión, priorización y evolución de las actividades realizadas.
- Contribuir en la definición de métricas y seguimiento de las mismas, identificando ámbitos de mejora en la prestación del servicio.
- Creación y mantenimiento de procedimientos operativos para la mejora continua del servicio.
- Creación, mantenimiento e implantación de casos de uso.
- Investigación, análisis y caracterización de amenazas y ataques mediante los frameworks de Mitre ATT&CK y Diamond Model.
- Elaboración de inteligencia accionable para prevenir, detectar y responder a incidentes: reglas de yara, snort, sigma, etc.
- Tareas descritas en el presente pliego.
- Apoyo a los diferentes servicios que presta la dirección de operaciones de Cyberzaintza.

- Técnico de ciberseguridad (dedicado)

Perfil de ciberseguridad con una orientación principalmente a la operación y a la ciberinteligencia, y con experiencia en el stack tecnológico ofertado para el servicio. Debe presentar experiencia contrastable de al menos 3 años en el ámbito de la ciberseguridad.

- Técnico de inteligencia artificial (dedicado)

Perfil de ciberseguridad con experiencia en inteligencia artificial con una orientación principalmente a la creación, entrenamiento, explotación y mantenimiento de modelos locales de inteligencia artificial. Debe presentar experiencia contrastable de al menos 12 meses en este ámbito.

- Técnico de integración y desarrollo (bajo demanda)

Perfil de integración y desarrollo con amplia experiencia full stack en las tareas que se describen a continuación:

  - Identificación de requisitos funcionales y de diseño.
  - Diseño responsivo de interfaces.
  - Desarrollo de soluciones web y funcionalidades, usando buenas prácticas.
  - Mantenimiento evolutivo y correctivo de herramientas.
  - Programación en PHP, HTML, CSS, Bootstrap y conocimientos sólidos de JavaScript con jQuery.
  - Gestión y explotación de bases de datos: MySQL.
  - Mantenimiento de versiones de código con GIT.
  - Integración de sistemas utilizando para ello multitud de APIs, preferiblemente de diferentes servicios tales como ELK, MISP, etc.
  - Desarrollo de scripts a medida.
  - Crear y mantener la documentación.
  - Apoyo a los diferentes servicios que presta la dirección de operaciones de Cyberzaintza.

Deberá tener al menos 5 años de experiencia en las funciones indicadas.

### 5.11.2 Dimensionamiento y dedicación

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad establecida en la siguiente tabla para cada uno de los roles, cumpliendo para ello con la dedicación indicada durante la ejecución del contrato:

| | % Dedicación | Año 1 | Año 2 | Año 3 | Año 4 | Año 5 | Total contrato | Formato |
|---|---|---|---|---|---|---|---|---|
| **Responsable del servicio** | La necesaria para realizar el seguimiento del servicio. | | | | | | | Recurso nominal |
| **Especialista** | **Bajo demanda** | 510 horas | 510 horas | 510 horas | 510 horas | 510 horas | **2.550 horas** | Pool de especialistas |
| **Coordinador técnico dedicado** | **100%** | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | **8.500 horas** | Recurso nominal |
| **Técnico de ciberseguridad dedicado** | **100%** | 6.400 horas | 6.400 horas | 6.400 horas | 6.400 horas | 6.400 horas | **34.000 horas** | Recursos nominales |
| **Técnico de inteligenci** | **100%** | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | **8.500 horas** | Recurso nominal |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **a artificial dedicado** | | | | | | | | |
| **Técnico de integración y desarrollo dedicado** | **Bajo demanda** | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | **8.500 horas** | Recurso nominal |

### 5.11.3 Equipamiento y software para el equipo de trabajo

El adjudicatario del servicio proveerá y mantendrá todo el equipamiento necesario para la prestación del servicio, lo que incluye para cada uno de los integrantes nominales dedicados al servicio:

- Portátil con las características suficientes para la prestación del servicio, mínimo 16gb de RAM. Cyberzaintza requerirá la instalación de diferentes agentes de ciberseguridad.
- 2 monitores.
- Elevador para el portátil.
- Teléfono móvil.
- Licencia de Office 365 de tipo E3.

En el caso de evolución del tratamiento de la identidad por parte de Cyberzaintza, el adjudicatario deberá adaptarse a los nuevos requisitos.

El equipo asignado al servicio cumplirá la política y directrices de seguridad de Cyberzaintza.

### 5.11.4 Horario del servicio

El servicio se prestará en formato 8x5.

### 5.11.5 Modelo de prestación del servicio

Debido a la naturaleza sensible de la información que se va a gestionar dentro del alcance del contrato, el acceso a los sistemas y la necesidad de coordinación con otras áreas de Cyberzaintza, se hace necesario que el equipo realice la actividad en los siguientes términos:

- Las reuniones mensuales de seguimiento se llevarán a cabo exclusivamente de manera presencial en las oficinas de Cyberzaintza y será necesaria la asistencia del Responsable general del proyecto.
- Los roles que corresponden al equipo dedicado prestarán el servicio en las instalaciones del adjudicatario, con la realización de actividades de manera presencial en las instalaciones de Cyberzaintza al menos dos días a la semana para al menos el 50% del equipo. Los días específicos para trabajar físicamente en la oficina serán acordados con el responsable del servicio, y en caso de desacuerdo, la Agencia determinará los días correspondientes. Además, puede haber ocasiones en las que la Agencia solicite una presencia física más frecuente debido a la importancia crítica de las tareas a realizar o por necesidades puntuales.

### 5.11.6 Requerimientos fuera del horario habitual

Ante casos de emergencia o necesidades imprevistas relacionadas con incidentes de alto impacto, operativos especiales como elecciones, conflictos bélicos, etc. se establecen 100 horas anuales para asistencia adicional que podrán solicitarse fuera del horario habitual, incluyendo en horario nocturno y/o festivo.

## 5.12 Niveles de servicio

Los niveles de servicio ofertados deberán cumplir los indicados en este pliego. Adicionalmente el licitador podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados por la empresa adjudicataria y Cyberzaintza.

| CÓDIGO | PROCESO | INDICADOR DE SERVICIO | DESCRIPCIÓN | VALOR OBJETIVO | PERIODO DE CÓMPUTO | PENALIZACIÓN |
|---|---|---|---|---|---|---|
| *1* | *Gestión adecuada del servicio* | *Despliegue y configuración de todos los entornos.* | *Se deberán desplegar y configurar todos los entornos / herramientas / sistemas necesarios para la correcta prestación del servicio, en el plazo establecido.* | 30 días | Mensual | 5% de la facturación mensual hasta que se solucione. |
| *2* | *Gestión adecuada del servicio* | *Sustitución de integrante del equipo de trabajo a petición de Cyberzaintza* | *Cyberzaintza podrá solicitar en cualquier momento la sustitución de cualquier integrante del equipo de trabajo asociado al servicio, en caso de que determine que no disponga de la experiencia o no realice las tareas con el nivel de calidad adecuado, debiendo ser reemplazo por el adjudicatario del servicio teniendo como límite el tiempo máximo establecido.* | 30 días | Cada vez que se solicite | 5% de la facturación mensual hasta que se solucione. |
| *3* | *Gestión adecuada del servicio* | *Reposición de integrante del equipo de trabajo en el caso de que se vaya de la entidad adjudicataria.* | *En el caso de que un integrante del equipo de trabajo asociado al servicio abandone la entidad adjudicataria, ésta deberá reponerlo teniendo como límite el tiempo máximo establecido, asumiendo así mismo su personal interno la ejecución de tareas que venía realizando en Cyberzaintza.* | 30 días | Cada vez que se solicite | 5% de la facturación mensual hasta que se solucione. |
| *4* | *Gestión adecuada del servicio* | *Plan de formación* | *El adjudicatario del servicio deberá proponer y ejecutar un plan de formación de acuerdo a los requisitos establecidos por Cyberzaintza en el apartado correspondiente.* | 100% del equipo asignado al contrato. | Anualmente | 5% de la facturación mensual hasta que se solucione. |
| *5* | *Gestión adecuada del servicio* | *Certificación técnica* | *Personal del equipo dedicado con certificación técnica en ciberinteligencia en vigor de acuerdo con el Plan de formación.* | Mínimo 2 para las certificaciones de ELK y mínimo 4 para ATT&CK Cyber Threat Intelligence Certification o Certified Threat Intelligence Analyst (CTIA). | 12 meses a partir del inicio del contrato | 5% de la facturación mensual hasta que se solucione. |

| | | | | | | |
|---|---|---|---|---|---|---|
| *6* | *Gestión adecuada del servicio* | *Certificación lingüística* | *Personal del equipo dedicado con certificación lingüística en vigor de acuerdo con el Plan de formación.* | Mínimo 2 personas con B2 de euskera. | 12 meses a partir del inicio del contrato | 5% de la facturación mensual hasta que se solucione. |
| *7* | *Devolución del servicio* | *Devolución del servicio* | *Deberán cumplirse las condiciones establecidas relativas a la devolución del servicio.* | - | Finalización del contrato | No se procederá a realizar el pago de la última factura mensual del servicio hasta que se cumplan las condiciones establecidas |
| *8* | *Definición de una metodología de medición del riesgo basado en amenazas* | *Definición de la metodología* | *Deberán definir la metodología de medición del riesgo basado en amenazas en el plazo máximo establecido.* | 3 meses | 3 meses a partir del inicio del contrato | 5% de la facturación mensual hasta que se solucione. |
| *9* | *Definición de una metodología de medición del riesgo basado en amenazas* | *Implementación de la metodología* | *Deberán implementar la metodología de medición del riesgo basado en amenazas en el plazo máximo establecido, tomando como punto de partida el indicador de servicio 5.* | 6 meses | 6 meses a partir del indicador de servicio anterior. | 5% de la facturación mensual hasta que se solucione. |
| *10* | *Vigilancia digital e Identificación de amenazas:* | *Configuración de casos de uso obligatorios* | *Deberán configurarse y confirmar el funcionamiento adecuado de los casos de uso solicitados en el apartado 5.2.* | 1 mes | 1 mes a partir del inicio del contrato | 3% de la facturación mensual. |
| *11* | *Vigilancia digital e Identificación de amenazas:* | *Desarrollo y configuración de nuevos casos de uso* | *Deberán desarrollarse e implementarse nuevos casos de uso durante la vigencia del contrato.* | 12 al año, mínimo. | Anual | 5% de la facturación mensual. |
| *12* | *Vigilancia digital e Identificación de amenazas:* | *Monitorización de disponibilidad de activos* | *Se deberán identificar las caídas de servicio de los activos monitorizados.* | 99% | Mensual | 5% de la facturación mensual. |
| *13* | *Vigilancia digital e Identificación de amenazas:* | *Detección de fugas de credenciales (cantidad)* | *Se deberán identificar como mínimo la cantidad de nuevas fugas de credenciales indicadas.* | 50 | Mensual | 3% de la facturación mensual. |
| *14* | *Vigilancia digital e Identificación de amenazas:* | *Detección de fugas de credenciales válidas (calidad)* | *El porcentaje de falsos positivos con respecto a las credenciales identificadas debe ser inferior al indicado.* | 60% | Mensual | 1% de la facturación mensual. |
| *15* | *Vigilancia digital e Identificación de amenazas:* | *Detección de fugas de credenciales (tiempo de notificación)* | *Se deberán reportar las fugas de credenciales en el plazo máximo indicado.* | 24 horas | Mensual | 3% de la facturación mensual. |
| *16* | *Vigilancia digital e Identificación de amenazas:* | *Detección de información sensible expuesta* | *Se deberá detectar la información sensible expuesta.* | 95% | Mensual | 1% de la facturación mensual. |
| *17* | *Vigilancia digital e Identificación de amenazas:* | *Detección de dominios nuevos registrados con fines maliciosos* | *Se deberán detectar los dominios nuevos registrados con fines maliciosos.* | 95% | Mensual | 1% de la facturación mensual. |

| | | | | | | |
|---|---|---|---|---|---|---|
| *18* | *Vigilancia digital e Identificación de amenazas:* | *Detección de campañas de phishing* | *Se deberán detectar como mínimo la cantidad de campañas de phishing indicadas.* | 10 | Mensual | 1% de la facturación mensual. |
| *19* | *Vigilancia digital e Identificación de amenazas:* | *Detección de campañas de smishing* | *Se deberán detectar como mínimo la cantidad de campañas de smishing indicadas.* | 5 | Mensual | 1% de la facturación mensual. |
| *20* | *Vigilancia digital e Identificación de amenazas:* | *Detección de campañas de malware* | *Se deberán detectar como mínimo la cantidad de campañas de malware indicadas.* | 10 | Mensual | 1% de la facturación mensual. |
| *21* | *Vigilancia digital e Identificación de amenazas:* | *Detección de fraudes* | *Se deberán detectar como mínimo la cantidad de fraudes indicados.* | 5 | Mensual | 1% de la facturación mensual. |
| *22* | *Producción de inteligencia y Alerta temprana* | *Generación de alertas previstas (cantidad)* | *Se deberán generar como mínimo la cantidad de alertas previstas indicadas.* | 15 | Mensual | 3% de la facturación mensual. |
| *23* | *Producción de inteligencia y Alerta temprana* | *Generación de alertas previstas (tiempo de notificación)* | *Se deberán difundir las alertas en el plazo máximo indicado.* | 5 horas | Mensual | 3% de la facturación mensual. |
| *24* | *Producción de inteligencia y Alerta temprana* | *Generación de alertas imprevistas (tiempo de notificación)* | *Se deberán difundir las alertas en el plazo máximo indicado.* | 4 horas | Mensual | 3% de la facturación mensual. |
| *25* | *Producción de inteligencia y Alerta temprana* | *Generación de eventos en la plataforma de intercambio de información sobre ciberamenazas (MISP)* | *Se deberán generar como mínimo la cantidad de eventos indicados.* | 30 | Mensual | 3% de la facturación mensual. |
| *26* | *Producción de inteligencia y Alerta temprana* | *Generación y envío de boletines* | *Se deberán generar y enviar los boletines durante el plazo indicado.* | Primera semana de cada mes | Mensual | 3% de la facturación mensual. |
| *27* | *Producción de inteligencia y Alerta temprana* | *Generación de informes de situación* | *Se deberán generar y entregar los informes de situación solicitados durante el plazo indicado.* | Lunes de cada semana | Mensual | 3% de la facturación mensual. |
| *28* | *Producción de inteligencia y Alerta temprana* | *Generación de informes de inteligencia de amenazas y cibercrimen* | *Se deberán generar y entregar los informes de inteligencia de amenazas y cibercrimen solicitados durante el plazo indicado.* | 25 días | Mensual | 3% de la facturación mensual. |

El importe de la penalización a aplicar para cada uno de los códigos será acumulativo tomando como base para el cálculo, el importe correspondiente a la facturación mensual.

Cyberzaintza se reserva la facultad de aplicar el modelo de penalización que a continuación se describe. La cuantía de la penalización será proporcional a la gravedad del incumplimiento y no podrá ser superior al 15% del precio de adjudicación del contrato.

## 5.13 Planes para la gestión adecuada del servicio

El licitador deberá proponer y detallar en su oferta al menos los siguientes planes.

### 5.13.1 Plan de calidad

El licitador deberá proponer un plan de calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan debe contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.

Así mismo, en relación a la información aportada y entregables del servicio se contempla que debe cumplir los siguientes atributos:

- Fiable: Es de suma importancia poder determinar la fiabilidad de los datos aportados por el servicio, por tanto, éste debe proporcionar un nivel de detalle que permita el establecimiento de la misma, para lo cual, que se debe proporcionar al menos la siguiente información y capacidades:
  - La fecha de detección (firstSeen) y la fecha de la última vez que se observó o se tenga referencia (lastSeen) de cada dato proporcionado.
  - Información técnica detallada sobre los datos proporcionados, así como la necesaria para la verificación de la autenticidad de la misma como, por ejemplo: fuente/s de la información, técnicas empleadas para obtener la información, evidencias de los datos obtenidos o relaciones entre los datos. En definitiva, todos los datos que ayuden a contextualizar y validar la fiabilidad de la información entregada.
- Completa (completeness). La información contenida en el servicio debe aportar suficientes detalles como, por ejemplo, aportar evidencias suficientes y de calidad, recomendaciones, etc. para que sea accionable.
- Precisa (accuracy). El servicio debe garantizar a través de algún mecanismo o procedimiento que tiene la capacidad de disminuir los falsos positivos, consiguiendo que la información sea precisa y correcta.
- Relevante (relevance). El servicio debe facilitar el consumo y representación de información relevante para Cyberzaintza.
- Oportuna (timeliness). El servicio debe garantizar que la información se entrega con la velocidad suficiente para asegurar que la misma sigue siendo relevante y actual.

### 5.13.2 Plan de formación

Es responsabilidad del adjudicatario garantizar la formación adecuada del personal del mismo asignado al equipo de trabajo de modo que estén capacitados para correcta prestación de los servicios. Es por ello que deberá proponer un plan formativo que asegure la adecuada prestación del servicio, el cual debe incluir:

- Plan de formación inicial en el uso de las herramientas, que será impartido por los especialistas tanto al personal dedicado al servicio por parte de la entidad adjudicataria, como al equipo de Cyberzaintza involucrado en las tareas que son objeto del contrato.
- Plan de formación continua para el personal dedicado al servicio, el cual contemple diferentes acciones formativas generales a lo largo de la prestación del servicio que vayan alineadas con la actividad que desarrollan. Se estima como mínimo un taller mensual para todo el equipo de

trabajo con una duración estimada de 2 horas que será impartido por alguno de los especialistas del adjudicatario del servicio y que será grabado para ponerlo a disposición permanente del equipo asignado al servicio por si hay rotación. Así mismo, cada uno de los perfiles dedicado al servicio deberá contar con un plan formación específico que incluya formación en ELK, en Python, en MITRE ATT&CK Defender (MAD), etc. con el propósito de obtener certificaciones que demuestren la consolidación de lo aprendido. Se deberán presentar anualmente evidencias de al menos 12 acciones de formación generales y 4 acciones de formación individuales, estas últimas con una estimación total de al menos 80 horas de formación externa.

Se establece la necesidad de que al menos 2 componentes del equipo dedicado estén permanentemente certificados en la siguiente certificación:

- Elastic Certified Engineer

En el caso de que al inicio del contrato el adjudicatario no incluya 2 componentes del equipo de trabajo con dicha certificación, tendrán un plazo máximo de 1 año para certificarse.

Así mismo, se establece la necesidad de que al menos 3 componentes del equipo dedicado estén certificados de manera permanente en alguna de las siguientes certificaciones:

- ATT&CK Cyber Threat Intelligence Certification
- Certified Threat Intelligence Analyst (CTIA)

En el caso de que al inicio del contrato el adjudicatario no cumpla requisito, tendrá un plazo máximo de 1 año para hacerlo.

Los gastos correspondientes al proceso de formación y los derivados del mismo correrán a cargo del adjudicatario. El incumplimiento de este punto será objeto de penalización.

Sin perjuicio de lo anterior, durante la vigencia del contrato, y ante la identificación de una deficiencia o necesidad estratégica, Cyberzaintza podrá solicitar a la adjudicataria del servicio adaptar/certificar a un determinado número de recursos en tecnologías existentes. La adaptación/certificación, nivel de la misma, número de recursos afectados y plazo máximo de obtención se establecerán de mutuo acuerdo entre Cyberzaintza y la adjudicataria siendo, en todo caso, responsabilidad y obligación de la adjudicataria la adaptación/certificación de los recursos sin coste asociado para Cyberzaintza.

### 5.13.3 Plan de sustitución

Se solicita la inclusión de un plan de sustitución en el caso de que haya variaciones en la plantilla que presta el servicio.

Cyberzaintza se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación, y durante el curso de los trabajos, cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto con respecto a sí misma, como con respecto al personal que proponga para la prestación de los servicios.

No obstante, la designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de Cyberzaintza, y en este caso, el adjudicatario se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por Cyberzaintza de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

La empresa adjudicataria se compromete a adoptar las medidas necesarias orientadas a prevenir la rotación y, en cualquier caso, a minimizar el impacto que pueda ocasionar en Cyberzaintza y en el propio servicio.

Cualquier cambio en los integrantes del equipo de trabajo deberá ser conocido y aprobados por Cyberzaintza.

## Línea de servicio de seguridad ofensiva

# 6 Lote 3: "Servicio para la gestión proactiva de la superficie de exposición"

## 6.1 Objeto

Este lote tiene por objeto la contratación de un servicio de monitorización de la superficie de exposición, el cual permita identificar potenciales riesgos de manera temprana y ofrezca soluciones para corregirlos.

## 6.2 Alcance

El alcance del contrato contempla las siguientes actividades:

- Servicio de EASM que incluya los requisitos que se describen en el apartado correspondiente.
- Configuración inicial de la plataforma.
- Integración con el modelo de inteligencia de Cyberzaintza.
- Explotación activa de la información.
- Equipo de trabajo asociado al servicio.
- Formación asociada al servicio prestado en base, principalmente, al uso, administración y configuración del mismo.
- Soporte asociado durante toda la prestación del servicio.

La empresa adjudicataria deberá suministrar las licencias de la herramienta EASM, junto con el soporte de fabricante asociado.

El soporte de fabricante debe incluir, sin coste adicional, el acceso a las actualizaciones de parches, alertas de seguridad, y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.

## 6.3 Requisitos

La solución deberá aportar, al menos, las siguientes funcionalidades o requisitos:

- REQ01: La solución deberá ser multi-tenant, permitiendo la configuración independiente de las organizaciones configuradas.
- REQ02: Los servidores deberán estar ubicados en la UE.
- REQ03: La solución deberá permitir agrupar a las organizaciones en base a diferentes criterios como por ejemplo categoría, importancia, sector, etc. y visualizar la información de cada una de ellas de manera individual.
- REQ04: Multiusuario y roles de acceso: La solución deberá permitir la gestión de múltiples usuarios, sin limitación, y definir roles con acceso granular personalizables,

asegurando acceso granular a funciones y datos sensibles y garantizando que sólo el personal autorizado pueda realizar acciones críticas.

- REQ05: Cobertura completa de la superficie de exposición: La solución debe ser capaz de identificar y mapear todas las áreas de exposición a amenazas accesibles desde internet, incluyendo activos en nubes privadas, públicas e híbridas. Para el entorno on-premise, podrá integrarse con herramientas internas de escaneo para mejorar la visibilidad.
- REQ06: El descubrimiento de activos se podrá realizar mediante dominios registrados, rangos de direcciones IP públicas y análisis de huellas digitales de la organización, complementando con cualquier otra información de activos de la organización (direcciones IP no asignadas públicamente a la organización, por ejemplo), que podrá ser configurada manualmente.
- REQ07: Se utilizarán técnicas no invasivas para la detección e identificación de activos expuestos.
- REQ08: La solución debe analizar e identificar al menos los siguientes factores de riesgo, aportando por cada uno de ellos información detallada:
  - Configuraciones de correo: SPF, DKIM, DMARC, DNSSEC, etc.
  - Certificados inseguros, caducados, etc.
  - Sistemas vulnerables: tecnología y versiones de productos, bases de datos expuestas, git expuestos, etc.
  - Servicios expuestos: RDP, FTP, Telnet, SMB, SSH, etc.
  - Infecciones.
  - Reputación de direccionamiento IP y dominios.
- REQ09: La solución ofrecerá una puntuación global para cada organización configurada, así como una puntuación individual para cada uno de los factores de riesgo.
- REQ10: Detección continua: La solución deberá realizar una monitorización continua y automática con una frecuencia mínima de detección de 48 horas o menor para identificar cambios en la superficie de exposición.
- REQ11: Capacidad de priorización de riesgos: La solución deberá ofrecer información para priorizar los riesgos basándose en su impacto, probabilidad de explotación y contexto de la organización, incluyendo fuentes externas de inteligencia de amenazas.
- REQ12: Integración con sistemas de seguridad existentes: La solución deberá integrarse con herramientas de gestión de vulnerabilidades y SIEM mediante conectores nativos o APIs para correlación de datos, pudiendo realizarse consultas ilimitadas.
- REQ13: Alertas y notificaciones en tiempo real: La solución deberá permitir la configuración de envío de alertas personalizadas según el manual de identidad de marca de Cyberzaintza, debiendo ser independientes e individualizadas en base a diferentes criterios como, por ejemplo, que puntuación descienda un porcentaje determinado, que la puntuación individual de alguno de los ámbitos a evaluar varíe, etc.
- REQ14: Visualización y mapas interactivos: La solución debe proporcionar un mapa visual y dinámico e interactivo de la infraestructura que permita a los administradores identificar fácilmente los puntos de exposición y proporcionar una vista visual interactiva con representación gráfica de relaciones entre activos expuestos y riesgos asociados.
- REQ15: Cumplimiento normativo: La solución deberá ofrecer capacidades que faciliten la identificación de riesgos que puedan afectar al cumplimiento de normativas como ENS, ISO 27001 y RGPD.
- REQ16: Capacidades de auditoría y reporte: La solución deberá permitir generar informes personalizables con el diseño de Cyberzaintza, que incluyan evidencias de

identificación de activos, puntuaciones, análisis de riesgos y medidas correctivas recomendadas.

- REQ17: Los informes se podrán generar tanto en euskera como en castellano.
- REQ18: Capacidad de escalabilidad: La solución debe ser capaz de adaptarse a infraestructuras que crecen o cambian rápidamente, asegurando su eficacia sin importar el tamaño de la organización.
- REQ19: Protección contra riesgos de subdominios huérfanos y activos abandonados: La solución deberá detectar y alertar sobre activos huérfanos o subdominios abandonados que puedan ser utilizados para ataques de secuestro de subdominio.
- REQ20: Evaluación de exposición de puertos y servicios: La plataforma deberá identificar y alertar sobre puertos y servicios expuestos, proporcionando contexto sobre su riesgo y recomendaciones de mitigación.
- REQ21: Visibilidad sobre tecnologías y frameworks utilizados: La solución deberá identificar tecnologías y frameworks utilizados en los activos expuestos, alertando sobre versiones obsoletas o vulnerables.
- REQ22: Capacidades de respuesta ante incidentes: La solución deberá facilitar la remediación por lo que deberá proporcionar guías de respuesta ante incidentes y recomendaciones de mitigación para cada tipo de vulnerabilidad identificada.
- REQ23: Detección de riesgos en certificados SSL/TLS y configuraciones inseguras: La solución deberá identificar certificados SSL/TLS caducados o configuraciones inseguras que puedan comprometer la seguridad de la comunicación cifrada.
- REQ24: Detección de configuraciones inseguras de correo: SPF, DKIM, DMARC, DNSSEC, etc.
- REQ25: Funcionalidad de búsqueda histórica y comparativa de exposiciones: La plataforma deberá permitir la consulta de exposiciones históricas y comparativas para evaluar cambios en la superficie de ataque a lo largo del tiempo.
- REQ26: Integración con frameworks de seguridad como MITRE ATT&CK: Para facilitar la alineación con estándares de ciberseguridad y la priorización de amenazas mediante la identificación de tácticas y técnicas utilizadas por actores de amenazas, la solución deberá mapear las amenazas detectadas con el framework MITRE ATT&CK.
- REQ27: La solución deberá mantener una base de datos actualizada de ataques recientes con potencial impacto a las entidades bajo el ámbito de actuación de Cyberzaintza.
- REQ28: Permitirá la configuración de al menos 150 entidades para las cuales se podrá acceder de manera permanente a la totalidad de la información
- REQ29: Se contempla la configuración de al menos 1.000 entidades para las cuales se podrá acceder únicamente a la puntuación general.
- REQ30: Se podrán configurar activos ilimitados, sin restricción, en cada una de las entidades. A modo de ejemplo, se establece la configuración de la entidad correspondiente al TLD .EUS con un total de 17.000 dominios y un incremento anual de entorno al 10%.

El licitador deberá indicar de manera expresa si solución propuesta cubre una serie de **requisitos obligatorios**, para lo cual deberá completar la tabla detallada contenida en la pestaña titulada "Requisitos" del archivo Excel Anexo II – PCT_Requisitos Técnicos_Lote3.xlsx correspondiente a los requerimientos solicitados en el Lote 3 del presente expediente. Así mismo, podrá especificar funcionalidades adicionales de la solución.

Para garantizar el cumplimiento de los requisitos designados como Req.XX, el licitador deberá proporcionar las evidencias pertinentes, consistentes en:

- Capturas de pantalla que acrediten la funcionalidad requerida.
- Breve descripción del contenido de cada captura, explicando su relación con el requisito evaluado. Esta información se incluirá en un anexo específico, en el que cada evidencia

estará numerada según el orden exacto de los requisitos Req.XX establecidos en la documentación del procedimiento.

El incumplimiento de las condiciones formales de presentación establecidas en este documento podrá afectar a la valoración de la oferta pudiendo llegar a la exclusión de esta.

Cyberzaintza se reserva el derecho a solicitar una prueba de las capacidades técnicas de cualquiera de las soluciones propuestas por el licitador propuesto como adjudicatario, coincidiendo con la fase de acreditación de requisitos previos.

En caso de que así sea requerido:

- Los costes para la realización de esas pruebas serán íntegramente asumidos por el propuesto como adjudicatario que, además, deberá facilitar el soporte que sea solicitado por Cyberzaintza para la realización de dicha prueba.
- El periodo de prueba no podrá superar los 30 días naturales y deberá realizarse en los 45 días siguientes a la publicación de la propuesta de adjudicación de la Mesa de Contratación.
- En caso de que el resultado de la prueba no sea satisfactorio porque se evidencie que la solución no cumple con los requisitos establecidos en este PCT, el licitador será descartado como posible adjudicatario por incumplimiento del PCT.

## 6.4 Metodología

Las empresas licitadoras deberán incluir en su oferta una descripción detallada de la metodología de prestación del servicio, que permita valorar la capacidad técnica, la organización, los procedimientos y los recursos propuestos para garantizar la adecuada ejecución del contrato.

Dicha metodología debe incluir reuniones de seguimiento del contrato:

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista se reunirá con la dirección técnica del proyecto de Cyberzaintza, si esta lo considera necesario para la adecuada prestación del servicio, con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato.

Cyberzaintza podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento y la correcta ejecución del objeto del contrato. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

En dicha reunión se revisarán al menos los siguientes puntos:

- Trabajos realizados en el periodo anterior.
- Trabajos planificados para el siguiente periodo.
- Seguimiento económico del contrato.
- Incidencias surgidas y áreas de mejora.

## 6.5 Planificación

Los licitantes deberán realizar una **propuesta de planificación** que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas.

En la planificación se debe incluir una fase de devolución del servicio:

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, a prestar apoyo, y realizar la transferencia del conocimiento, documentación técnica y administrativa necesaria para el traspaso del servicio, etc. al siguiente adjudicatario del contrato, en caso de que éste sea distinto al adjudicatario del presente pliego.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de Cyberzaintza cuando se produzca la finalización del contrato.

Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por Cyberzaintza con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

La fase de devolución concluirá con la celebración de la reunión de cierre del proyecto, donde se tratarán al menos los siguientes puntos:

- Memoria final de actividad.
- Documentación técnica y administrativa.
- Actas de todas las reuniones de seguimiento.
- Revisión de lecciones aprendidas y mejoras incluidas en la memora final del contrato. Esta información podrá ser solicitada como adelanto en cualquier momento durante la ejecución del contrato.
- Certificado acreditativo de borrado de la información utilizada en la provisión del servicio.
- Cierre del contrato.

## Línea de servicio de respuesta a incidentes (CSIRT)

# 7 Lote 4: “Servicios de despliegue y ejecución de una capacidad de preparación y respuesta a incidentes de ciberseguridad”

## 7.1 Objeto

El objeto del expediente es la contratación de un servicio de despliegue y ejecución de una capacidad de preparación y respuesta a incidentes de ciberseguridad que permita una coordinación eficiente, así como unificar y elevar el nivel de madurez.

## 7.2 Requisitos

- El servicio se prestará en su totalidad en formato bilingüe: tanto en euskera como en castellano.
- Los materiales se generarán siguiendo las pautas del manual de identidad de marca de la Agencia.
- El adjudicatario asumirá los gastos derivados de los desplazamientos, dietas y otros costos asociados a la disposición de medios necesarios para estos y, en general, para la ejecución del proyecto en las condiciones de presencialidad indicadas.

## 7.3 Alcance

En este apartado se describe el alcance de los servicios solicitados a través de este expediente, no siendo el listado que aparece a continuación una relación exhaustiva de las características del

servicio contratado, sino las actividades generales demandadas por Cyberzaintza, cubriendo los aspectos de tareas a realizar y los resultados esperados.

| Preparación | Respuesta a incidentes |
|---|---|
| • Definición de una metodología de respuesta a incidentes.<br>• Planificación, despliegue y mantenimiento de una capacidad de respuesta a incidentes.<br>• «Incident readiness assessment»: consultoría para la elaboración y validación de planes de respuesta a incidentes de ciberseguridad y gestión de crisis.<br>• Desarrollo y mantenimiento de un protocolo a nivel de Gobierno para la gestión de crisis para incidentes de alto impacto en Euskadi<br>• Organización y ejecución de ciberejercicios. | • Gestión de la línea de asesoramiento.<br>• Activación del protocolo de alerta.<br>• Análisis de incidentes.<br>• Respuesta activa.<br>• Gestión de crisis. |

A continuación, se describen las tareas generales que se ejecutarán dentro del contrato. **Para cada una de las tareas referidas a continuación, el licitador deberá presentar y detallar de manera exhaustiva las herramientas / plataformas que utilizará para la prestación del servicio, destacando sus funcionalidades y limitaciones de manera explícita.** El adjudicatario del servicio facilitará acceso permanente e ininterrumpido a Cyberzaintza durante la prestación del mismo.

## 7.4 Preparación

### 7.4.1 Definición de una metodología de respuesta a incidentes

Los licitadores deberán presentar una propuesta de metodología basada en estándares y buenas prácticas de aplicación en el ámbito de prestación de servicio de Cyberzaintza que contemple todas las fases de la respuesta a incidentes de ciberseguridad, definiendo claramente los roles, las responsabilidades, las tareas, procedimientos, herramientas, etc. El adjudicatario del servicio deberá formalizar toda la parte documental.

### 7.4.2 Planificación, despliegue, mantenimiento y evolución de una capacidad de respuesta a incidentes

Se solicita una bolsa de horas para la planificación, despliegue, mantenimiento y evolución de una capacidad de respuesta a incidentes, quedando incluidas tareas tales como el asesoramiento, consultoría, desarrollo de procedimientos, soporte en el despliegue de herramientas que contribuyan al objeto del servicio, automatización, etc.

Los licitadores deberán presentar una propuesta de infraestructura de adquisición remota y análisis de evidencias, detallando todos los aspectos relacionados tanto el hardware como con el software, posible separación entre entornos, etc. El adjudicatario del servicio desplegará dicha

infraestructura, una vez consensuada con Cyberzaintza, desarrollando todas las automatizaciones, scripts, etc. necesarios y aportando el software necesario.

Así mismo, se desarrollarán a lo largo del servicio documentación técnica como playbooks de coordinación y de respuesta, procedimientos operativos, checklist, etc. que contribuyan a que las entidades de Euskadi sean más resilientes frente a los ciberataques. Toda la documentación se elaborará de acuerdo a estándares y normativa aplicable a los diferentes públicos de Cyberzaintza. Los licitadores deberán presentar una propuesta de documentación inicial a elaborar previa a la prestación formal del servicio, que contemple al menos playbooks, procedimientos operativos, instrucciones técnicas, etc.

En este sentido, se contempla una bolsa de 1200 horas anuales, que podrán ejecutarse según necesidad para cubrir las tareas descritas y facturadas según trabajos realizados. De no consumirse, las horas se podrán utilizar en el resto de los servicios en caso necesario, aplicando el precio de adjudicación de cada una de las bolsas.

#### 7.4.3 «Incident readiness assessment»: consultoría para la preparación para la respuesta a incidentes de ciberseguridad y gestión de crisis.

Se solicita una bolsa de horas para el acompañamiento a las instituciones públicas en la elaboración de planes de respuesta a incidentes de ciberseguridad y de gestión de crisis «forensic readiness». El equipo asignado al servicio se reunirá con entidades públicas de Euskadi, de manera remota o presencial según necesidad, y les guiará y asesorará en la elaboración de planes que contribuyan a elevar su nivel de preparación y resiliencia frente a amenazas en el ámbito de la ciberseguridad, asegurando que en el caso de sufrir un incidente se disponga de la información necesaria para responder de manera adecuada. Se contempla el desarrollo de planes de respuesta a incidentes (IRP), planes de continuidad (BCP), planes de recuperación ante desastre (DRP), etc., todos ellos alineados con normativa y estándares aplicables.

Así mismo, se revisará y validará los planes de aquellas entidades que ya dispongan de ellos y así lo soliciten.

El adjudicatario deberá disponer de medios para recibir las peticiones de este tipo de actuaciones ya que el horario es 8x5. En este sentido, se contempla una bolsa de 1700 horas anuales, que podrán ejecutarse según necesidad para cubrir las tareas descritas y facturadas según trabajos realizados. De no consumirse, las horas se podrán utilizar en el resto de los servicios en caso necesario, aplicando el precio de adjudicación de cada una de las bolsas.

Los licitadores deberán presentar a modo de ejemplo una propuesta de metodología que incluya los factores a evaluar de cara a determinar si una entidad está preparada o no para responder a incidentes.

#### 7.4.4 Desarrollo y mantenimiento de un protocolo a nivel de Gobierno para la gestión de crisis para incidentes de alto impacto en Euskadi

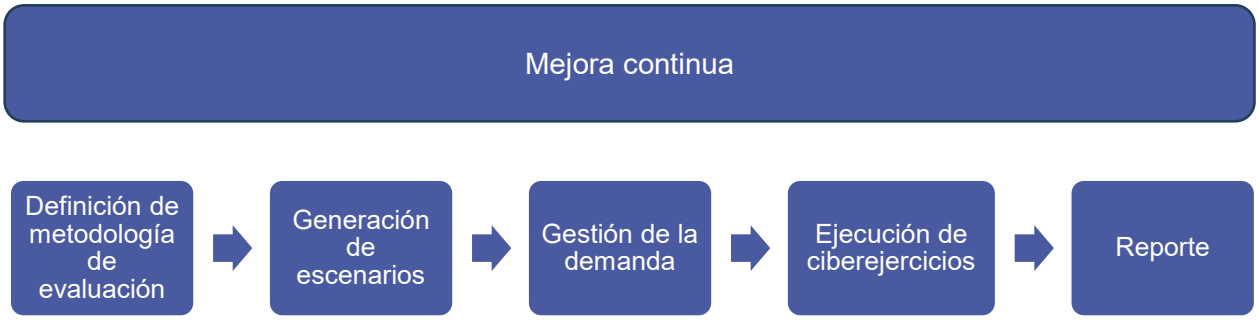
El adjudicatario desarrollará un protocolo para la respuesta a incidentes con alto impacto en Euskadi y cuya materialización derive en una potencial crisis.

En primer lugar, se identificarán aquellas tipologías de incidentes con potencial afección masiva y se priorizarán por potencial impacto.

Un vez identificadas y priorizadas, desarrollará y mantendrá actualizada toda la operativa necesaria, lo que incluye la elaboración documental de todas las fases de la gestión de la crisis. Esto incluye la identificación y mantenimiento de puntos de contacto de todos los interlocutores, la definición de flujos, procedimientos generales, procedimientos técnicos, plantillas, etc., alineados en todo momento con el marco legislativo aplicable.

### 7.4.5 Organización y ejecución de ciberejercicios.

Dentro de la tarea se contemplan las siguientes actividades:




#### 7.4.5.1 Definición de una metodología de evaluación.

Los licitadores deberán proponer una metodología que permita evaluar de manera común y objetiva a las entidades participantes en los ciberejercicios.

Dicha metodología, que deberá ir alineada con los estándares de ciberseguridad de aplicación a los públicos objetivos del servicio, deberá así mismo detallar diferentes ámbitos de evaluación, ponderando cada uno de ellos, de modo que finalmente se obtenga tanto una puntuación general, así como individual por cada uno de los apartados, y recomendaciones concretas que permitan a las entidades participantes la mejora de su nivel de resiliencia.

De igual modo, deberán realizar un planteamiento de entregables que incluya formularios y documentación adicional para la recogida de evidencias de las entidades participantes, para la presentación de resultados, incluyendo métricas, etc.

#### 7.4.5.2 Generación de escenarios

Se contemplan dos tipos de ciberejercicios:

1. Table-top o debate, para perfiles estratégicos. Usados habitualmente para poner a prueba el funcionamiento de los comités de crisis, los protocolos internos de actuación, etc. A partir de un guion previamente elaborado por el adjudicatario, se realizará una simulación de acciones ante una audiencia que deberá tomar decisiones al respecto. Dependiendo de estas decisiones, así como de valores determinados de forma aleatoria, el ciberejercicio tomará un curso u otro, siguiendo el proceso hasta llegar a su finalización.
2. Escenario real o simulacro, para perfiles técnicos. Se realizan acciones reales sobre una audiencia o un sistema o conjunto de sistemas, con objeto de evaluar su nivel de seguridad. El objetivo puede incluir tanto recursos tecnológicos como organizativos o humanos. Ejemplos típicos de este tipo de ejercicio son el envío de correos o mensajes de texto con eventos o inyecciones que requieren la toma de decisiones y la ejecución de tareas internas dentro de la organización en diferentes ámbitos como el operacional, el legal, el financiero, etc. Incluyen el desarrollo de evidencias como capturas de tráfico de red, volcados de memoria, exportaciones de registro, cuentas en redes sociales, publicaciones, diseño de noticias ficticias, etc.

Cyberzaintza cuenta en la actualidad con varios escenarios diferentes desarrollados, algunos de los cuales están disponibles en su página web:

- https://www.ciberseguridad.eus/servicios-administracion-publica/ciberejercicios
- https://www.ciberseguridad.eus/empresa-segura/exercise-in-a-box

Los licitadores deberán proponer 4 escenarios realistas relacionados con la respuesta a incidentes de ciberseguridad y la gestión de crisis para desarrollar de manera anual, siendo 3 de ellos de tipo table-top y 1 de ellos de tipo escenario real. Dichos escenarios serán los que se ejecutarán de manera regular y continuada durante la vigencia del contrato, en sesiones bajo demanda. Así mismo, actualizará los escenarios existentes, según necesidad.

Los materiales seguirán el formato de los ya existentes, es decir, mantendrán la siguiente estructura por cada uno de los escenarios, si bien se valorarán propuestas de mejora:

- Ficha explicativa del ciberejercicio.
- Guía de coordinación.
- Documento para los participantes.
- Documento para apuntar observaciones.
- Presentación que se utilizarán para la ejecución del ciberejercicio.
- Evidencias e infraestructura a desplegar.

Se generarán en bilingüe, tanto euskera como castellano, siguiendo el manual de identidad corporativa de Cyberzaintza y las plantillas que provea a la entidad adjudicataria del servicio. Así mismo, el adjudicatario configurará los ciberejercicios en la plataforma utilizada por Cyberzaintza.

**Los licitadores presentarán un ejemplo completo de escenario de cada tipo, es decir, una presentación con los correspondientes contenidos desarrollados, teniendo en consideración la estructura, la calidad de los materiales, los mensajes fuerza, la adaptación de los mensajes al público objetivo, la infraestructura, las evidencias, etc.** En el caso de las evidencias y la infraestructura bastará con que detallen el contenido a generar.

#### 7.4.5.3 Gestión de la demanda

La entidad adjudicataria será la responsable de gestionar las solicitudes, lo que incluye:

- Cyberzaintza facilitará al adjudicatario del servicio acceso a la plataforma a través del cual se gestionarán todas las solicitudes. El contratista enviará al solicitante una ficha de solicitud de sesión de ciberejercicio que deberá ser cumplimentada, en la que se contemple la recogida de datos del solicitante, información de contacto incluida, las características generales del servicio, la política de privacidad, el idioma en el que sea que se preste el servicio, etc. Por cada solicitud se debe rellenar una ficha, y se mantendrá un histórico de solicitudes.

  Atendiendo al alcance de los ciberejercicios se contemplan los siguientes tipos que serán ejecutados por el adjudicatario del servicio:

| Tipo | Público objetivo | Alcance | Activación | Materiales a utilizar | Modo de ejecución | Duración |
|---|---|---|---|---|---|---|
| Ejercicios table-top | Perfiles estratégicos y Perfiles técnicos | Individual | A petición de los diferentes públicos objetivos contemplados dentro del alcance del contrato | Los generados por el adjudicatario. | Presencial | De 150 a 240 minutos. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Colectivo | A petición de Cyberzaintza | Se generarán nuevos materiales adhoc. | | |
| Ejercicios de escenario real | Perfiles técnicos | Colectivo | A petición de Cyberzaintza | Se generarán nuevos materiales adhoc. | Online | De 1 a 7 días, con dedicación variable. |

- Las solicitudes se gestionarán diariamente de modo que no quede ninguna pendiente para el siguiente día, salvo que entre fuera del horario de prestación de servicio establecido.
- El adjudicatario del servicio gestionará las solicitudes y coordinará la realización de los ciberejercicios, solventando cualquier inconveniente que pudiera surgir.
- El adjudicatario del servicio pondrá un número de teléfono a disposición del servicio para facilitar la resolución de dudas por parte de los solicitantes en caso necesario.
- El destinatario del servicio proporcionará los medios necesarios para la realización de los ciberejercicios de manera presencial, y el adjudicatario para la realización online.
- Se prevé la ejecución de al menos 44 ejercicios table-top individuales de manera anual.
- Se prevé la ejecución de al menos 8 ejercicios table-top colectivo de manera anual.
- Se prevé la ejecución de al menos 4 ejercicios de escenario real de manera anual.

#### 7.4.5.4 Ejecución de ciberejercicios

Una vez concretadas la fecha y modo de ejecución:

- El adjudicatario del servicio confirmará con el solicitante vía telefónica las sesiones 24 horas antes de la fecha de ejecución.
- El adjudicatario del servicio ejecutará el ciberejercicio, acudiendo al lugar acordado en caso necesario. A cada ciberejercicio acudirán un coordinador. La ejecución estará enfocada a fomentar la participación, al aprendizaje a partir de situaciones similares, etc.

#### 7.4.5.5 Reporte

Con posterioridad a la realización del ciberejercicio, el adjudicatario elaborará un informe a modo de reporte que será entregado a la/s entidad/es participante/s y que incluirá:

- Objetivo.
- Tipo de ejercicio realizado.
- Escenario ejecutado.
- Dinámica.
- Participantes.
- Conclusiones, lo que incluirá diferentes métricas como.
  - Nivel de participación.
  - Tiempo en toma de decisiones.
  - Idoneidad de las decisiones tomadas.
  - Efectividad de las decisiones tomadas.
  - Efectividad en la comunicación.

- Idoneidad de los procedimientos internos.
- Etc.

- Recomendaciones.

En el caso de los ciberejercicios de alcance colectivo generará así mismo un informe general.

Los informes de reporte se entregarán en un plazo máximo de 14 días laborables. De cara a agilizar los tiempos de entrega y homogeneizar la información, el adjudicatario preparará las plantillas correspondientes siguiendo el manual de identidad corporativa de Cyberzaintza y automatizará todos los procesos en la medida de lo posible.

Los entregables serán tanto en formato «human readable» como «machine readable».

El reporte no se considerará válido hasta que Cyberzaintza lo valide, debiendo el adjudicatario del servicio aplicar los cambios que le sean requeridos.

Así mismo, el adjudicatario del servicio se encargará de trasladar al solicitante de la jornada la correspondiente encuesta de valoración y su posterior recogida. Dicha encuesta será preparada por el adjudicatario del servicio y deberá contar con la validación de Cyberzaintza.

## 7.5 Respuesta a incidentes

### 7.5.1 Gestión de la línea de asesoramiento

La tarea consiste en la gestión de la línea de asesoramiento frente a incidentes de ciberseguridad que ofrece Cyberzaintza a sus diferentes públicos objetivos a través de los canales establecidos para ello. Los públicos objetivos del centro son en la actualidad: sector público, empresa privada y ciudadanía, todos ellos de la CAPV.

En la actualidad existen los siguientes canales habilitados para el reporte de incidentes, los cuales serán atendidos por el adjudicatario del servicio:

- **Buzón de correo**: un buzón que es la vía principal de entrada de los incidentes de ciberseguridad (incidencias@cyberzaintza.eus).
- **Atención telefónica**: a través del teléfono 900 104 891.

Una vez se reciben los incidentes, en el caso de los emails, se procesarán de manera automática en la herramienta de ticketing, la cual enviará una respuesta automática e inmediata a los remitentes indicándoles el identificador asignado a las mismas a modo de acuse de recibo. En el caso de llamadas, el equipo técnico de nivel 1 los registrará en la herramienta, y en ambos casos, los analizará, categorizará en base a la taxonomía utilizada por el Cyberzaintza, recogida en la guía CCN-STIC 817, y ofrecerá asesoramiento con las pautas de actuación más apropiadas de cara a ayudar a la persona o entidad que lo haya reportado. Así mismo, realizará las tareas de notificación y coordinación necesarias para mitigar / desmantelar la amenaza en los casos en los que corresponda y, finalmente, realizará un seguimiento para evaluar el nivel de efectividad de las mismas.

En caso de ser necesario un análisis más especializado o no saber la manera de proceder, el equipo técnico de nivel 1 completará toda la información del caso y lo escalará internamente a un equipo técnico de nivel 2 con mayor experiencia, y finalmente si es necesario, se solicitará asesoramiento al equipo técnico de Cyberzaintza, que actuará como nivel 3.

Los incidentes de ciertas tipologías o pertenecientes a públicos objetivo concretos de la Agencia, como por ejemplo entidades públicas y empresas que pertenezcan a alguna iniciativa estratégica de Cyberzaintza, serán gestionados directamente por nivel 2 sin intervención de nivel 1.

A continuación, de un total de 1.265 incidentes gestionados en 2024, se indican las tipologías:

| Tipología | Porcentaje |
|---|---|
| Fraude | 55,53% |
| Contenido abusivo | 3,33% |
| Intrusión | 12,36% |
| Intento de intrusión | 1,14% |
| Programa malicioso | 15,28% |
| Sistemas vulnerables | 2,11% |
| Disponibilidad | 3,33% |
| Compromiso de la información | 0,65% |
| Obtención de información | 0,73% |
| Otros | 5,53% |

Se contemplan 3 niveles de operación por parte del adjudicatario:

- Tareas a realizar por el equipo de asesoramiento de nivel 0:
  - Se considera estratégico hacer un esfuerzo en automatización, IA y en cualquier otra tecnología/herramienta que permita reducir hasta eliminar la carga de trabajo de poco valor añadido que se realice: identificación, clasificación, solicitud de información adicional, contextualización, escalado, etc. y limitar así los posibles errores humanos.
  - El equipo asignado a nivel 0 deberá liderar proactivamente todas las tareas de automatización, siendo el responsable de las automatizaciones en el conjunto de herramientas utilizadas en el alcance de la actividad y cooperando con otros posibles grupos de soporte de otros entornos sobre los que se realicen las automatizaciones.
  - **La tarea principal será eliminar la necesidad de un Nivel 1 en el servicio, sustituyéndolo por automatización, y reducir la carga para el resto de los niveles.** Para ello configurará debidamente el sistema de respuesta de voz interactiva (IRV) de la plataforma que aporte el proveedor y realizará las automatizaciones, integraciones y desarrollos necesarios, aportando así mismo para ello las herramientas necesarias, por ejemplo, de orquestación, IA, etc. **El plazo objetivo de sustitución de nivel 1 es de 1 año.** En este sentido, se contempla una bolsa de 650 horas anuales, que podrán ejecutarse según necesidad para cubrir las tareas descritas y facturadas según trabajos realizados. De no consumirse, las horas se podrán utilizar en el resto de los servicios en caso necesario, aplicando el precio de adjudicación de cada una de las bolsas. Los licitadores deberán presentar en su oferta una propuesta de cómo llevar a cabo la tarea.
- Tareas a realizar por el equipo de asesoramiento de nivel 1:
  - Atender los canales habilitados por Cyberzaintza para el servicio.
  - Registrar los incidentes en la herramienta de ticketing en base a su correspondiente categorización.
  - Analizar los incidentes y preparar una respuesta acorde utilizando como apoyo la base de datos de conocimiento. El objetivo de dicha respuesta será el de asesorar en la prevención y respuesta relativas a ciberseguridad.

- Realizar las comprobaciones e investigaciones necesarias para la mitigación / resolución de los incidentes.
- Realizar las notificaciones oportunas para mitigar / neutralizar la amenaza.
- Realizar el seguimiento de los incidentes.
- Escalar los incidentes a nivel 2 en el caso de que no saber cómo dar una respuesta adecuada.
- Mantener un alto grado de coordinación con el nivel 2.
- Seguimiento de los incidentes.
- Cerrar los incidentes en la herramienta de ticketing una vez hayan sido resueltos.
- Contribuir a la creación y mantenimiento actualizado de una base de datos de contactos técnicos en el ámbito de la ciberseguridad de los organismos públicos, para lo cual deberán realizar las llamadas oportunas solicitando la información necesaria.
- Contribuirán a la difusión de los servicios de la Agencia, para lo cual facilitarán información a los contactos técnicos de las organizaciones, en los casos en los que así se requiera.

- Tareas a realizar por el equipo de asesoramiento de nivel 2:
  - Asesorar y resolver los incidentes escalados por el nivel 1.
  - Mantener un alto grado de coordinación con el nivel 1.
  - Revisar la gestión de las incidencias por parte de nivel 1 y evaluar la calidad de las mismas y aspectos de mejora.
  - Formar a nivel 1 cuando sea necesario de cara a mantener un nivel alto de excelencia en la prestación del servicio.
  - Escalar los incidentes a Cyberzaintza en el caso de que no saber cómo dar una respuesta adecuada.
  - Generación y mantenimiento de playbooks.
  - Actualización de la base de datos de conocimiento: procedimientos (escalado, emergencia, etc.), plantillas, etc.
  - Mantener un alto grado de coordinación con Cyberzaintza.
- Por encima de los niveles 0, 1 y 2 se contempla la figura del coordinador técnico del servicio, la cual realizará las siguientes tareas:
  - Evaluar de manera continua y desde un punto de vista técnico la calidad y utilidad del servicio prestado, para lo cual revisará la totalidad de los incidentes gestionados.
  - Proponer acciones correctivas y de mejora del servicio, así como realizar un seguimiento de las mismas.
  - Mantener actualizada la base de datos de conocimiento, lo que contempla el desarrollo de procedimientos, playbooks, plantillas, etc.
  - Coordinación entre los niveles 1 y 2 que permita una prestación de servicio eficaz y coordinada de cara al cliente interno y externo.
  - Ser interlocutor entre Cyberzaintza y los equipos técnicos de niveles 0, 1 y 2.

Ocasionalmente, integrantes del equipo que realice las tareas de asesoramiento y respuesta a incidentes participarán en iniciativas de Cyberzaintza cuyo objeto contribuya a la mejora del servicio, como es puede ser el caso de role plays, ciberejercicios, etc. Se contempla un máximo de 3 actividades anuales.

Con respecto al número de incidentes que podrían registrarse a lo largo de un mes y ser objeto del contrato, se fija un valor aproximado de 1.000, con las siguientes consideraciones:

- El valor que se indica es el mínimo que Cyberzaintza requiere para poder participar en el presente pliego, sin perjuicio de la obligación del adjudicatario de atender todo incidente que se produzca.
- El número de solicitudes realmente gestionadas cada mes no tendrá impacto en la facturación.

- En caso de que a lo largo de un mes se supere el número de solicitudes aproximadas, se valorará flexibilizar los acuerdos de nivel de servicio una vez analizado el contexto.

Los oferentes que comprometan un número inferior serán excluidos de la licitación por ser este requisito mínimo esencial del Pliego. Se estima que de manera anual hay un incremento del número de eventos de al menos un 25%.

El contratista deberá gestionar la transferencia del número actual para lo cual deberá de disponer de una infraestructura, desde la que se atenderán las llamadas del teléfono de contacto, con la capacidad de respuesta de voz interactiva (IVR), grabar conversaciones para su posterior revisión, reproducir locuciones pregrabadas, envío de mensajes de texto y realizar encuestas para evaluar la satisfacción del servicio. La plataforma para registrar las incidencias (Freshdesk) será provista por Cyberzaintza, que facilitará acceso al equipo de trabajo asignado al servicio.

**El servicio se ofrecerá de manera ininterrumpida en horario 24x7, en formato bilingüe: euskera y castellano y cumpliendo el acuerdo de nivel de servicio especificado en el apartado niveles de servicio. Todos los documentos del servicio se elaborarán de acuerdo con el manual de identidad corporativa del Cyberzaintza y bajo su propia marca.**

### 7.5.2 Activación del protocolo de emergencia

El equipo técnico aportado por el adjudicatario del servicio para realizar las tareas descritas en el apartado anterior, a petición de Cyberzaintza, activará el protocolo de emergencia para dar respuesta a situaciones que así lo requieran. En este sentido, se enviarán mensajes de texto y/o llamará, según corresponda, a los puntos de contacto especificados por Cyberzaintza para alertarles de la activación de dicho protocolo y se realizarán cuantas notificaciones sean oportunas para dar respuesta a esta situación. Se deberá indicar la plataforma a utilizar, así como las funcionalidades principales de la misma. La tarea se ofrecerá en el mismo formato que el de asesoramiento.

### 7.5.3 Análisis de incidentes de ciberseguridad

Se analizarán incidentes con impacto o potencial impacto en Euskadi de modo que se identifiquen mecanismos para mitigar el riesgo de que suceda o vuelva a suceder.

Ejemplos de tipologías de incidentes que se analizarán:

- Incidentes de ciberseguridad de entidades públicas y privadas de Euskadi.
- Incidentes de ciberseguridad de entidades estatales que pudieran reproducirse en el ámbito de Euskadi.
- Incidentes globales con impacto en Euskadi.
- Etc.

Los análisis tendrán como resultado informes que contemplarán al menos la siguiente información:

- Resumen ejecutivo.
- Descripción del incidente.
- Análisis detallado del modus operandi (Mitre Attack (en formato gráfico y JSON) y Diamond Model).
- Listado de IOC.
- Recomendaciones.
- Reglas de yara, snort, sigma, siems, etc.

Todos los documentos del servicio se elaborarán en euskera y castellano de acuerdo con el manual de identidad corporativa del Cyberzaintza y bajo su propia marca.

### 7.5.4 Respuesta activa a incidentes de ciberseguridad

Se solicita asistencia adicional que cubra casos de emergencia o necesidades relacionadas con incidentes o problemas como ataques de seguridad, brechas de datos, problemas de red críticos, incidentes de malware o virus, problemas de acceso no autorizado, etc. en administración pública o entidades designadas como estratégicas por parte de Cyberzaintza. El adjudicatario deberá disponer de medios para recibir las peticiones de este tipo de actuaciones ya que el horario en el que se debe prestar es 24x7.

En este sentido, se contempla una bolsa de 750 horas anuales, que podrán ejecutarse según necesidad y facturadas según trabajos realizados. De no consumirse, las horas se podrán utilizar en caso necesario cuando se consuman las otras bolsas de horas, aplicando el precio de adjudicación de cada una de las bolsas.

Los licitadores deberán presentar a modo de ejemplo una propuesta de playbook para responder a un incidente de ransomware. Así mismo, deberán presentar el ejemplo de un informe de gestión de un incidente en el que se refleje la estructura detallada.

Dentro de esta tarea se engloba cualquier tipo de actividad derivada de la respuesta a incidentes de ciberseguridad:

- Desplazarse, si así lo determina Cyberzaintza, a las instalaciones de la entidad afectada, dentro de la Comunidad Autónoma del País Vasco.
- Despliegue y mantenimiento de entornos de adquisición y análisis de evidencias.
- Adquisición y análisis de evidencias como, por ejemplo: volcados de memoria, capturas de red, malware, registros, logs, etc.
- Propuesta de medidas: técnicas, operativas y organizativas.
- Asesoramiento en la respuesta en los distintos ámbitos: técnico, jurídico, comunicativo, etc.
- Coordinación con las diferentes áreas de las entidades involucradas en la gestión de los incidentes.
- Despliegue de medidas para la protección de los diferentes públicos objetivos de Cyberzaintza.
- Documentación de todo lo relacionado con el incidente y reporte.
- Identificación de medidas para evitar que vuelva a suceder o que suceda a otras entidades.
- Presentación del reporte.
- Etc.

En casos de gravedad extrema se requerirá el despliegue de una capacidad de gestión de crisis.

## 7.6 Metodología y planificación

Los licitantes deberán realizar una **propuesta de metodología y de plan de trabajo** que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas. Así mismo deberá incluir:

### 7.6.1 Fase inicial

Contempla la configuración, formación y puesta en marcha del servicio. Se debe contemplar un periodo inicial de configuración de las plataformas y los entornos, de formación específica al equipo de trabajo, de revisión y actualización de la operativa actual, playbooks, plantillas, etc. y cuya duración máxima será de 4 semanas.

### 7.6.2 Descripción y detalle de cada una de las tareas recogidas dentro del servicio.

### 7.6.3 Seguimiento del Servicio

Con periodicidad mensual el contratista entregará un informe de seguimiento del servicio y se realizará una reunión con el objetivo de evaluar el desempeño del mismo e identificar puntos de mejora. El contratista realizará una propuesta de informe que tendrá que superar un proceso de validación por parte Cyberzaintza. En dicha propuesta incluirá las métricas especificadas en el apartado Acuerdo de nivel de servicio.

### 7.6.4 Fase de devolución y cierre del proyecto:

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, a prestar apoyo, y realizar la transferencia del conocimiento, documentación técnica y administrativa necesaria para el traspaso del servicio, etc. al siguiente adjudicatario del contrato, en caso de que éste sea distinto al adjudicatario del presente pliego.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de Cyberzaintza cuando se produzca la finalización del contrato.

Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por Cyberzaintza con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

La fase de devolución concluirá con la celebración de la reunión de cierre del proyecto, donde se tratarán al menos los siguientes puntos:

- Memoria final de actividad.
- Documentación técnica y administrativa.
- Actas de todas las reuniones de seguimiento.
- Revisión de lecciones aprendidas y mejoras incluidas en la memora final del contrato. Esta información podrá ser solicitada como adelanto en cualquier momento durante la ejecución del contrato.
- Certificado acreditativo de borrado de la información utilizada en la provisión del servicio.
- Cierre del contrato.

## 7.7 Planes para la gestión adecuada del servicio

El licitador deberá proponer y detallar en su oferta al menos los siguientes planes.

### 7.7.1 Plan de calidad

El licitador deberá proponer un plan de calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan debe contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.

### 7.7.2 Plan de formación

Es responsabilidad del adjudicatario garantizar la formación adecuada del personal del mismo asignado al equipo de trabajo de modo que estén capacitados para correcta prestación de los servicios. Es por ello que deberá proponer un plan formativo que asegure la adecuada prestación del servicio, el cual debe incluir:

- Plan de formación inicial en el uso de las herramientas, que será impartido por los especialistas tanto al personal dedicado al servicio por parte de la entidad adjudicataria, como al equipo de Cyberzaintza involucrado en las tareas que son objeto del contrato. En relación al uso de la herramienta de ticketing, todo el equipo asignado al contrato realizará la formación gratuita específica de Freshdesk de Fresworks Academy, debiendo presentar el correspondiente certificado de superación.
- Plan de formación continua para el personal dedicado al servicio, el cual contemple diferentes acciones formativas generales a lo largo de la prestación del servicio que vayan alineadas con la actividad que desarrollan. Se estima como mínimo un taller mensual para todo el equipo de trabajo con una duración estimada de 2 horas que será impartido por alguno de los especialistas del adjudicatario del servicio y que será grabado para ponerlo a disposición permanente del equipo asignado al servicio por si hay rotación. Así mismo, cada uno de los perfiles dedicado al servicio deberá contar con un plan formación específico que incluya formación en respuesta a incidentes de ciberseguridad, etc. con el propósito de obtener certificaciones que demuestren la consolidación de lo aprendido. Se deberán presentar anualmente evidencias de al menos 12 acciones de formación generales y 4 acciones de formación individuales, estas últimas con una estimación total de al menos 80 horas de formación externa.

  Se establece la necesidad de que al menos 1 de los componentes del equipo dedicado estén permanente certificados en la siguiente certificación:

- Certified Incident Handler (ECIH)

  En el caso de que al inicio del contrato el adjudicatario no incluya ningún componente del equipo de trabajo con dicha certificación, tendrá un plazo máximo de 1 año para certificarse.

  Los gastos correspondientes al proceso de formación y los derivados del mismo correrán a cargo del adjudicatario. El incumplimiento de este punto será objeto de penalización.

  Sin perjuicio de lo anterior, durante la vigencia del contrato, y ante la identificación de una deficiencia o necesidad estratégica, Cyberzaintza podrá solicitar a la adjudicataria del servicio adaptar/certificar a un determinado número de recursos en tecnologías existentes. La adaptación/certificación, nivel de la misma, número de recursos afectados y plazo máximo de obtención se establecerán de mutuo acuerdo entre Cyberzaintza y la adjudicataria siendo, en todo caso, responsabilidad y obligación de la adjudicataria la adaptación/certificación de los recursos sin coste asociado para Cyberzaintza.

### 7.7.3 Plan de sustitución

Se solicita la inclusión de un plan de sustitución en el caso de que haya variaciones en la plantilla que presta el servicio.

Cyberzaintza se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación, y durante el curso de los trabajos, cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto con respecto a sí misma, como con respecto al personal que proponga para la prestación de los servicios.

No obstante, la designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de Cyberzaintza, y en este caso, el adjudicatario se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por Cyberzaintza de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

La empresa adjudicataria se compromete a adoptar las medidas necesarias orientadas a prevenir la rotación y, en cualquier caso, a minimizar el impacto que pueda ocasionar en Cyberzaintza y en el propio servicio.

Cualquier cambio en los integrantes del equipo de trabajo deberá ser conocido y aprobados por Cyberzaintza.

## 7.8 Niveles de servicio

El desarrollo del Servicio y su calidad deberá gobernarse de acuerdo a unos Acuerdos de Nivel de Servicio (ANS) que sirvan para medir el grado de calidad del mismo, un Plan de Calidad que desarrolle las estrategias y procedimientos implantados para la consecución de los ANS y unas reuniones periódicas que permitan evaluar la marcha del Plan de Calidad, el grado de cumplimiento de los ANS y permitir la toma de decisiones necesarias para mitigar desviaciones y mejorar continuamente la calidad del servicio.

Los niveles de servicio ofertados deberán cumplir, como mínimo, los indicados en este pliego. Adicionalmente el licitador podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados por la adjudicataria y Cyberzaintza. En cualquier caso, si a criterio de Cyberzaintza fuera necesario para mejorar el servicio que presta a sus clientes, durante estas revisiones los ANS podrán ser actualizados, añadidos o retirados. El incumplimiento de dichos niveles será penalizado según lo dictado en el pliego de condiciones particulares.

El licitador se comprometerá a garantizar que las tareas requeridas serán prestadas con los niveles mínimos que se detallan a continuación.

| CÓDIGO | PROCESO | INDICADOR DE SERVICIO | DESCRIPCIÓN | VALOR OBJETIVO | PERIODO DE CÓMPUTO | PENALIZACIÓN |
|---|---|---|---|---|---|---|
| *1* | *Definición de una metodología de respuesta a incidentes* | *Formalización documental para la correcta prestación del servicio.* | Elaboración de toda la lógica de prestación del servicio, así como la documentación necesaria. | <1 mes | Mensual | 5% de la facturación mensual, hasta que se realice. |
| *2* | *Definición de una metodología de respuesta a incidentes* | *Definición de una metodología de evaluación de la preparación para la respuesta a incidentes* | Elaboración de toda la lógica para evaluar el nivel de preparación de las entidades a las que prestar servicio frente a la respuesta a incidentes | < 1 mes | Mensual | 5% de la facturación mensual, hasta que se realice. |

| | | | | | | |
|---|---|---|---|---|---|---|
| *3* | *Planificación, despliegue, mantenimiento y evolución de una capacidad de respuesta a incidentes* | *Despliegue de entorno de adquisición y análisis de evidencias.* | Como parte de la capacidad de respuesta a incidentes, se establece la necesidad del despliegue de un entorno de adquisición y análisis de evidencias. | <2 meses | Mensual | 5% de la facturación mensual, hasta que se realice. |
| *4* | *Organización y ejecución de ciberejercicios* | *Generación de escenarios* | Los escenarios solicitados deberán estar disponibles en su totalidad dentro del plazo establecido. | <1 mes | Mensual | 3% de la facturación mensual, hasta que se realice. |
| *5* | *Gestión de la línea de asesoramiento* | *Automatizaciones para reemplazar a N1 (hasta automatizar todo lo viable).* | Se deberán identificar y realizar automatizaciones para eliminar la necesidad de N1 y para limitar la carga de trabajo del resto de niveles y evitar fallos humanos en la gestión de tickets. | <1 año | Anual | 10% de la facturación mensual, hasta que se realice. |
| *6* | *Gestión de la línea de asesoramiento* | *Tiempo entre registro de incidente de prioridad alta y escalado, en caso necesario.* | Existen una serie de criterios que determinan la prioridad de los incidentes, como por ejemplo la tipología o la entidad remitente. En estos casos, cuando sea necesario escalarlo a otro nivel, deberá realizar en el plazo máximo establecido con el fin de agilizar su gestión. | <1 hora | Mensual | 5% de la facturación mensual. |
| *7* | *Gestión de la línea de asesoramiento* | *Tiempo de respuesta inicial.* | *No se trata de la respuesta inicial de asignación del identificador del caso y acuse de recibo, la cual es automática, si no en la que se ofrece el asesoramiento inicial.* | 2 horas | Mensual | 2% de la facturación mensual. |
| *8* | *Gestión de la línea de asesoramiento* | *Encuesta de valoración negativa.* | En el caso de que se reciba una encuesta de valoración negativa en la prestación del servicio, se analizará con el objetivo de identificar dicha prestación se ha realizado bajo los parámetros de calidad establecidos. En el caso de que no sea así, conllevará penalización. | 0 | Mensual | 5% de la facturación mensual. |
| *9* | *Gestión de la línea de asesoramiento* | *Errores de nivel bajo* | Se contempla como errores de nivel bajo:<br>▪ Incidentes sin campos completados. Incidentes con campos mal completados.<br>▪ Errores con afectación únicamente a nivel interno y fácilmente subsanables.<br>▪ El error tiene escaso o nulo impacto.<br>▪ Escalado a N2 no justificado. | <10 | Mensual | 2% de la facturación mensual. |
| *10* | *Gestión de la línea de asesoramiento* | *Errores de nivel medio* | Se contempla como errores de nivel medio:<br>▪ Errores de formato en la respuesta.<br>▪ No responder adecuadamente a lo solicitado.<br>▪ Errores de gestión cuyas consecuencias no se circunscriben al ámbito interno, sino que tienen afectación hacia terceros. | <5 | Mensual | 5% de la facturación mensual. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | ▪ Peticiones a Cyberzaintza de información ya proporcionada o disponible en la base de datos de conocimiento.<br>▪ Envío de recomendaciones redundantes.<br>▪ Envío de respuesta con plantilla por defecto sin eliminar los comentarios que contiene o sin actualizar la información.<br>▪ Escalado a N3 no justificado. | | | |
| *11* | *Gestión de la línea de asesoramiento* | *Errores de nivel alto* | Se contempla como errores de nivel alto:<br>▪ Respuesta al solicitante con el mero fin de romper el SLA.<br>▪ Errores ortográficos o gramaticales en la respuesta.<br>▪ Envío de información confidencial a destinatarios incorrectos.<br>▪ Solicitud de baja de sistemas legítimos o que nada tienen que ver con el incidente analizado.<br>▪ Errores de gestión con consecuencias externas y capacidad de provocar daños importantes a terceros.<br>▪ Envío de solicitudes o recomendaciones2completamente erróneas.<br>▪ Queja justificada por una mala gestión. | 0 | Mensual | 10% de la facturación mensual. |
| *12* | *Activación de protocolo de emergencia* | *Activación de protocolo de emergencia* | Cuando así lo solicite Cyberzaintza, se activará el protocolo de emergencia y se ejecutarán todas las tareas recogidas en el mismo. Dicha activación y ejecución de las tareas deberá realizarse en el plazo máximo establecido. | 30 minutos | Cada vez que se solicite | 5% de la facturación mensual. |
| *13* | *Respuesta activa a incidentes de ciberseguridad* | *Activación de la respuesta activa a incidentes de ciberseguridad.* | Confirmación de la activación de respuesta activa a incidentes de ciberseguridad. | 30 minutos | Cada vez que se solicite | 5% de la facturación mensual. |
| *14* | *Respuesta activa a incidentes de ciberseguridad* | *Inicio de actividades de respuesta activa.* | Confirmación del inicio de actividades de respuesta activa a incidentes de ciberseguridad. | 2 horas | Cada vez que se solicite | 5% de la facturación mensual. |
| *15* | *Gestión adecuada del servicio* | *Sustitución de integrante del equipo de trabajo a petición de Cyberzaintza* | *Cyberzaintza podrá solicitar en cualquier momento la sustitución de cualquier integrante del equipo de trabajo asociado al servicio, en caso de que determine que no disponga de la experiencia o no realice las tareas con el nivel de calidad adecuado, debiendo ser reemplazo por el adjudicatario del servicio teniendo como límite el tiempo máximo establecido.* | 30 días | Cada vez que se solicite | 5% de la facturación mensual hasta que se solucione. |
| *16* | *Gestión adecuada del servicio* | *Reposición de integrante del equipo de trabajo en el caso de que se vaya de la* | *En el caso de que un integrante del equipo de trabajo asociado al servicio abandone la entidad adjudicataria, ésta deberá reponerlo teniendo como límite el tiempo máximo establecido, asumiendo así mismo su personal* | 30 días | Cada vez que se solicite | 5% de la facturación mensual hasta que se solucione. |

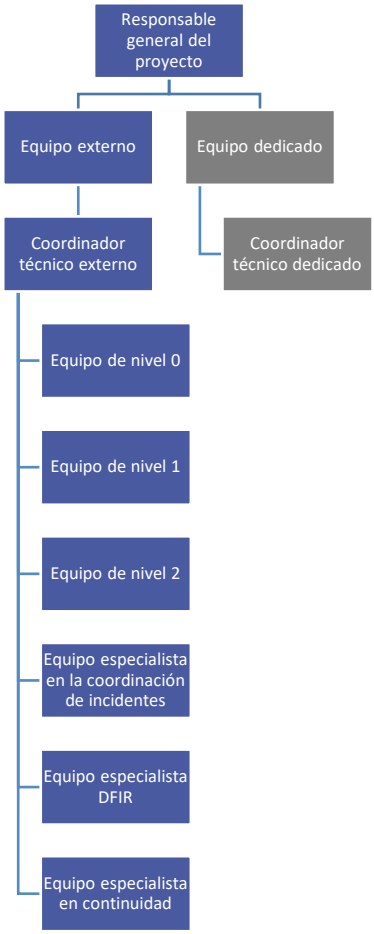
| | | | | | | |
|---|---|---|---|---|---|---|
| | | *entidad adjudicataria.* | *interno la ejecución de tareas que venía realizando en Cyberzaintza.* | | | |
| *17* | *Gestión adecuada del servicio* | Plan de formación | El adjudicatario del servicio deberá proponer y ejecutar un plan de formación de acuerdo a los requisitos establecidos por Cyberzaintza. | 100% del equipo asignado al contrato. | Anualmente | 5% de la facturación mensual hasta que se solucione. |
| *18* | *Gestión adecuada del servicio* | *Certificación técnica* | *Personal del equipo dedicado con certificación correspondiente en vigor de acuerdo con el Plan de formación.* | Mínimo 1 para las certificaciones indicadas en la sección del Plan de formación. | 12 meses a partir del inicio del contrato | 5% de la facturación mensual hasta que se solucione. |
| *19* | *Gestión adecuada del servicio* | Plan de formación | El equipo de trabajo asignado al contrato deberá realizar la formación de uso de la herramienta, | < 14 días | Primer mes | 5% de la facturación mensual hasta que se solucione. |
| *20* | *Gestión adecuada del servicio* | *Devolución del servicio* | Deberán cumplirse las condiciones establecidas relativas a la devolución del servicio. | - | Finalización del contrato | No se procederá a realizar el pago de la última factura mensual del servicio hasta que se cumplan las condiciones establecidas |

El importe de la penalización a aplicar para cada uno de los códigos será acumulativo tomando como base para el cálculo, el importe correspondiente a la facturación mensual.

Cyberzaintza se reserva la facultad de aplicar el modelo de penalización que a continuación se describe. La cuantía de la penalización será proporcional a la gravedad del incumplimiento y no podrá ser superior al 15% del precio de adjudicación del contrato.

## 7.9 Organización y equipo de trabajo

El equipo de trabajo encargado de construir la capacidad de DFIR y ejecutar las tareas especificadas en el ámbito de este contrato deberá respetar el siguiente organigrama:




La empresa adjudicataria asignará al proyecto, de forma continuada, un equipo humano que se encargará de las labores descritas dentro del alcance del presente contrato. El equipo de trabajo estará compuesto por personal adecuado y con experiencia en las tareas objeto del servicio. En este sentido, los oferentes deberán **detallar el equipo de trabajo** disponible para la ejecución del contrato indicando para cada recurso el perfil y grupo operativo al que se asocia, así como su **experiencia en actividades similares** para asegurar la correcta prestación del servicio.

Se deberán indicar los **roles y responsabilidades del equipo de trabajo propuesto para las distintas tareas**.

Las condiciones y aptitudes exigibles al personal asignado para la ejecución de este proyecto son las siguientes:

- Responsable general del proyecto: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del pliego y se encargará de la relación profesional entre el proveedor y Cyberzaintza.

  Dicho rol deberá cumplir los siguientes requisitos:

  - Tener una buena capacidad de planificación.
  - Habilidades de comunicación efectiva.
  - Conocimientos sólidos en metodologías de gestión de proyectos.
  - Habilidad de resolución de problemas.
  - Buena orientación a los resultados.

  Tendrá las siguientes funciones:

- Controlar los Procesos de Gestión ITIL y establecer los indicadores de control de gestión y los informes de gestión.
- Mantener y actualizar con Cyberzaintza los Acuerdos de Niveles de Servicio (ANS).
- Coordinar las funciones del servicio y la correcta ejecución de los procesos de gestión.
- Mejora continua del servicio.

Debe presentar experiencia contrastable de al menos 5 años en tareas similares y es imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.

- **Coordinador técnico externo:** designación de una persona que evaluará la calidad del servicio en términos técnicos, realizando una revisión diaria completa de los incidentes gestionados y proponiendo aspectos de mejora, además de servir de enlace técnico con los niveles 0, 1 y 2. Se debe indicar las capacidades y experiencia, debiendo contar con al menos 3 años de experiencia en la gestión de un servicio de estas características, en la gestión de incidentes de ciberseguridad y siendo imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.
- **Coordinador técnico dedicado:** perfil altamente cualificado en materia de seguridad y especializado en respuesta a incidentes.

  Tendrá las siguientes funciones:

  - Seguimiento de las actividades realizadas.
  - Elaboración de documentación (playbooks, procedimientos, guías, etc.).
  - Planificación y ejecución de dinámicas para responder a incidentes de ciberseguridad.
  - Análisis de incidentes de ciberseguridad.
  - Respuesta activa a incidentes de ciberseguridad.
  - Coordinación de diferentes áreas en la respuesta a incidentes.
  - Gestión del conocimiento interno.
  - Apoyo a los diferentes servicios que presta la dirección de operaciones de Cyberzaintza.

  Se debe indicar las capacidades y experiencia, debiendo contar con al menos 3 años de experiencia en la gestión de un servicio de estas características, en la gestión de incidentes de ciberseguridad y siendo imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.
- **Técnicos de nivel 0**: personal con experiencia en sistemas, comunicaciones y automatización. Deberá contar con al menos 3 años de experiencia en el objeto del contrato.
- **Técnicos de nivel 1:** personal bilingüe (euskera y castellano), y con competencia básica en inglés, con experiencia en tareas relacionadas con la atención a usuarios y experiencia en las tareas descritas en el apartado de gestión de la línea de asesoramiento, siendo imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar los perfiles asignados al servicio, así como su correspondiente experiencia en el objeto del contrato. Deberán contar con al menos 2 años de experiencia en el objeto del contrato. Se establece un mínimo de 10 perfiles, de los cuales al menos 5 deben contar al menos con acreditación B2.

- **Técnicos de nivel 2:** personal con amplia experiencia en todas las tareas descritas en el alcance del contrato. Se debe indicar los perfiles asignados al servicio, así como su correspondiente experiencia en tareas que son objeto del contrato. Deberán contar con al menos 3 años de experiencia en el objeto del contrato. Se establece un mínimo de 4 perfiles, de los cuales al menos 2 deben contar al menos con acreditación B2.
- **Técnicos especialistas en la coordinación de incidentes (Incident handler):** perfil con experiencia en coordinar la gestión de incidentes de ciberseguridad, siendo imprescindible por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Deberá contar con al menos 3 años de experiencia en el objeto del contrato y competencia idiomática fluida de euskera.
- **Técnicos especialistas en DFIR (incidente responders):** perfiles especializados en la respuesta a incidentes de ciberseguridad, que cuenten con conocimientos globales y transversales de seguridad que le permita ejecutar con solvencia las tareas establecidas dentro del alcance del contrato, como por ejemplo adquisición y análisis de evidencias, generación de inteligencia, análisis de malware, generación de informes, etc. Se incluyen así mismo otro tipo de perfiles relacionados con la respuesta a incidentes como, por ejemplo, consultores de GRC, jurídico, de comunicación, de gestión de crisis, etc. Darán apoyo al gestor de incidentes o incident handler. Los licitadores deberán contemplar esta casuística y presentar experiencia contrastable en las tareas recogidas, siendo imprescindible por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar los perfiles asignados al servicio, así como su correspondiente experiencia en el objeto del contrato. Deberán contar con al menos 3 años de experiencia en el objeto del contrato.

Para la actividad 7.4.3 Incident readiness assessment se deberá incluir un equipo de consultores especialistas en continuidad y con experiencia en las tareas descritas en el apartado, siendo imprescindible por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Deberán contar con al menos 3 años de experiencia en el objeto del contrato y competencia idiomática fluida de euskera.

Para la actividad 7.4.4 Organización y ejecución de ciberejercicios, se deberán contemplar de manera específica los siguientes roles:

- Designación de personas con rol **facilitador** que gestionen las solicitudes de ciberejercicios. Deberán tener la suficiente capacitación técnica y experiencia en coordinación y gestión de actividades de la naturaleza objeto del contrato, siendo exigible al menos 3 años. Así mismo, al menos 2 personas del equipo asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.
- Designación de personas con rol de **coordinador de los ciberejercicios** que deberán tener la suficiente capacitación técnica y experiencia impartición de jornadas de la naturaleza objeto del contrato, siendo exigible al menos 3 años y es imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia. Así mismo, al menos 2 personas del equipo asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.

### 7.9.1 Dimensionamiento y dedicación

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad establecida en la siguiente tabla para cada uno de los roles, cumpliendo para ello con la dedicación indicada durante la ejecución del contrato:

| | % Dedicación | Año 1 | Año 2 | Año 3 | Año 4 | Año 5 | Total contrato |
|---|---|---|---|---|---|---|---|
| **Responsable del servicio** | La necesaria para realizar el seguimiento del servicio. | | | | | | |
| **Coordinador técnico externo** | La necesaria para realizar el seguimiento del servicio. | | | | | | |
| **Técnicos de nivel 0** | **Según necesidades del servicio.** | | | | | | |
| **Técnicos de nivel 1** | | | | | | | |
| **Técnicos de nivel 2** | | | | | | | |
| **Técnicos especialistas en DFIR** | **Bajo demanda.** | | | | | | |
| **Coordinador técnico interno** | **100%** | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | 1.700 horas | **8.500 horas** |

Para la organización y ejecución de ciberejercicios:

| | |
|---|---|
| **Facilitador** | **Bajo demanda.** |
| **Coordinador de ciberejercicio** | |

### 7.9.2 Modelo de prestación del servicio

Debido a la naturaleza sensible de la información que se va a gestionar dentro del alcance del contrato, el acceso a los sistemas y la necesidad de coordinación con otras áreas de Cyberzaintza, se hace necesario que el equipo realice la actividad en los siguientes términos:

- Las reuniones mensuales de seguimiento se llevarán a cabo exclusivamente de manera presencial en las oficinas de Cyberzaintza y será necesaria la asistencia del Responsable general del proyecto.
- Los roles que corresponden al equipo dedicado prestarán el servicio en las instalaciones del adjudicatario, con la realización de actividades de manera presencial en las instalaciones de Cyberzaintza al menos dos días a la semana. Los días específicos para trabajar físicamente en la oficina serán acordados con el responsable del servicio, y en caso de desacuerdo, la Agencia determinará los días correspondientes. Además, puede haber ocasiones en las que la Agencia solicite una presencia física más frecuente debido a la importancia crítica de las tareas a realizar o por necesidades puntuales.

## 7.10 Horario del servicio

Las actividades de apartado 7.4 Preparación se prestarán en formato 8x5.

En situaciones de crisis Cyberzaintza podrá solicitar la extensión de la disponibilidad del servicio a un horario 24x7, así como la activación de perfiles adicionales dentro del marco de este contrato, tal y como se describe en el apartado Respuesta activa a incidentes de ciberseguridad.

Dado que la extensión de la jornada puede exceder de las horas/jornadas que cada individuo deba cumplir de acuerdo con sus condiciones laborales, se elaborará un plan que deberá ser aprobado por Cyberzaintza para cubrir el horario habitual en toda su extensión.

El adjudicatario tomará las medidas que fueran precisas para asegurar que tiene suficiente personal localizable y puede atender cualquier incidencia dentro del periodo de atención y con el tiempo de respuesta requerido en el contrato.

Las actividades de apartado 7.5 Respuesta a incidentes se prestarán en formato 24x7.

### 7.11 Equipamiento y software para el equipo de trabajo

El adjudicatario del servicio proveerá y mantendrá todo el equipamiento necesario para la prestación del servicio, lo que incluye para cada uno de los integrantes nominales dedicados al servicio:

- Portátil con las características suficientes para la prestación del servicio. Cyberzaintza requerirá la instalación de diferentes agentes de ciberseguridad.
- 2 monitores.
- Elevador para el portátil.
- Teléfono móvil.
- Licencia de Office 365 de tipo E3.

En el caso de evolución del tratamiento de la identidad por parte de Cyberzaintza, el adjudicatario deberá adaptarse a los nuevos requisitos.

El equipo asignado al servicio cumplirá la política y directrices de seguridad de Cyberzaintza.

## Línea de servicio de concienciación

# 8 Lote 5: “Servicio de campañas de phishing”

### 8.1 Objeto

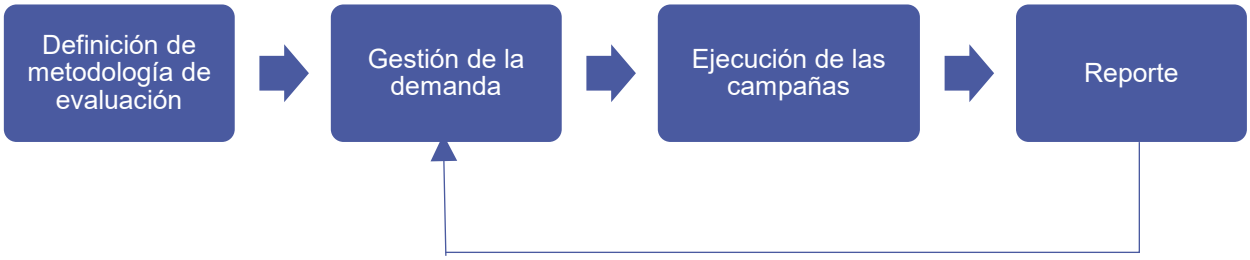
El objeto del expediente es la contratación de un servicio de ejecución de campañas de phishing para Cyberzaintza y sus públicos objetivo. Los públicos objetivo del servicio son principalmente entidades del sector público vasco, así como entidades privadas que formen parte de alguna iniciativa dentro del alcance de las entidades estratégicas para Cyberzaintza.

### 8.2 Requisitos

- El servicio se prestará en su totalidad en formato bilingüe: tanto en euskera como en castellano.
- El servicio se prestará en horario laboral de 09:00 a 18:00 de lunes a viernes.
- Los materiales se generarán siguiendo las pautas del manual de identidad de marca de la Agencia.

### 8.3 Alcance

Se solicita la presentación de una oferta en respuesta a este pliego para la adquisición de los servicios según las necesidades que se detallan a continuación.




### 8.3.1 Definición de una metodología de evaluación

Los licitadores deberán proponer una metodología que permita evaluar de manera común y objetiva a las entidades participantes en las campañas de phishing.

Dicha metodología, que deberá ir alineada con los estándares de ciberseguridad de aplicación a los públicos objetivos del servicio, deberá así mismo detallar diferentes ámbitos de evaluación, ponderando cada uno de ellos, de modo que finalmente se obtenga tanto una puntuación general, así como individual por cada uno de los apartados, y recomendaciones concretas que permitan a las entidades participantes la mejora de su nivel de resiliencia.

De igual modo, deberán realizar un planteamiento de entregables que incluya formularios y documentación adicional para la recogida de evidencias de las entidades participantes, para la explicación de la metodología para la presentación de resultados, incluyendo métricas, etc.

### 8.3.2 Gestión de la demanda

La entidad adjudicataria será la responsable de gestionar las solicitudes, lo que incluye:

Cyberzaintza facilitará al adjudicatario del servicio acceso a una plataforma a través de la cual se gestionarán todas las solicitudes. El contratista enviará al solicitante una ficha de solicitud online de campaña de phishing que deberá ser cumplimentada, en la que se contemple la recogida de datos de la entidad solicitante, información de contacto incluida, las características generales del servicio, la política de privacidad, etc. Por cada solicitud se debe rellenar una ficha, y se mantendrá un histórico de solicitudes.

Atendiendo al alcance de las campañas de phishing se contemplan los siguientes tipos:

| Tipo | Alcance | Activación | Modo de ejecución | Resultados | Duración |
|---|---|---|---|---|---|
| Campaña simple | Individual | Bajo demanda. A través de Cyberzaintza a petición de los diferentes públicos objetivos contemplados dentro del alcance del contrato. | Online | One shot | De 2 a 3 semanas. |

| | | | | | |
|---|---|---|---|---|---|
| Campaña compleja | Colectivo | A petición de Cyberzaintza, con la previsión especificada más adelante. | Online | Continuos | 3 meses. |

- Las solicitudes se gestionarán diariamente de modo que no quede ninguna pendiente para el siguiente día, salvo que entre fuera del horario de prestación de servicio establecido.
- El adjudicatario del servicio gestionará las solicitudes y coordinará la realización de las campañas de phishing, solventando cualquier inconveniente que pudiera surgir.
- El adjudicatario del servicio pondrá un número de teléfono a disposición del servicio para facilitar la resolución de dudas por parte de los solicitantes en caso necesario.
- Se prevé la ejecución de al menos 12 campañas simples de manera anual.
- Se prevé la ejecución continua de 4 campañas complejas de manera anual con una duración cada una de 3 meses y con varias simulaciones cada una de ellas. Así mismo, se prevé 2 campañas complejas adicionales para iniciativas puntuales con alcance colectivo.
- Las simulaciones de las campañas serán personalizadas en cada caso utilizando para ello diferentes pretextos con el objetivo de aumentar la efectividad de las mismas.

### 8.3.3 Ejecución de las campañas

Una vez acordada la realización de la campaña, el adjudicatario realizará todas las tareas de preparación como, por ejemplo:

- Reuniones para concretar el alcance.
- Registro de dominios necesarios.
- Definición y modelado de los correos multi-idioma.
- Obtención del listado de objetivos.
- Configuración de los ataques.
- Solicitud a la entidad o entidades participantes de exclusión de las direcciones desde las que se va a remitir la campaña.
- Selección de diferentes simulaciones de ataque.
- Ejecución.
- Resolución de dudas.

### 8.3.4 Reporte

Una vez finalizada la campaña, el adjudicatario elaborará un informe que será entregado a la/s entidad/es participante/s y que incluirá:

- Objetivo.
- Descripción y detalle de la campaña realizada.
- Resultados.
- Comparación con la media.
- Recomendaciones.

Se entregarán en un plazo máximo de 14 días laborables.

En el caso de las campañas complejas elaborará tanto un informe individual por cada participante, como un informe general de la campaña.

El entregable será siguiendo el manual de identidad corporativa de Cyberzaintza y tanto en formato «human readable» como «machine readable».

## 8.4 Metodología y planificación

Los licitantes deberán realizar una **propuesta de metodología y de plan de trabajo** que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas. Así mismo deberá incluir:

### 8.4.1 Seguimiento

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista se reunirá con la dirección técnica del proyecto de Cyberzaintza, si esta lo considera necesario para la adecuada prestación del servicio, con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato.

Cyberzaintza podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento y la correcta ejecución del objeto del contrato. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

En dicha reunión se revisarán al menos los siguientes puntos:

- Trabajos realizados en el periodo anterior.
- Trabajos planificados para el siguiente periodo.
- Seguimiento económico del contrato.
- Incidencias surgidas y áreas de mejora.

### 8.4.2 Cierre y devolución del servicio

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, a prestar apoyo, y realizar la transferencia del conocimiento, documentación técnica y administrativa necesaria para el traspaso del servicio, etc. al siguiente adjudicatario del contrato, en caso de que éste sea distinto al adjudicatario del presente pliego.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de Cyberzaintza cuando se produzca la finalización del contrato.

Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por Cyberzaintza con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

La fase de devolución concluirá con la celebración de la reunión de cierre del proyecto, donde se tratarán al menos los siguientes puntos:

- Memoria final de actividad.
- Documentación técnica y administrativa.
- Actas de todas las reuniones de seguimiento.

- Revisión de lecciones aprendidas y mejoras incluidas en la memora final del contrato. Esta información podrá ser solicitada como adelanto en cualquier momento durante la ejecución del contrato.
- Certificado acreditativo de borrado de la información utilizada en la provisión del servicio.
- Cierre del contrato.

## 8.5 Planes para la gestión adecuada del servicio

El licitador deberá proponer y detallar en su oferta al menos los siguientes planes.

### 8.5.1 Plan de calidad

El licitador deberá proponer un plan de calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan debe contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.

### 8.5.2 Plan de sustitución

Se solicita la inclusión de un plan de sustitución en el caso de que haya variaciones en la plantilla que presta el servicio.

Cyberzaintza se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación, y durante el curso de los trabajos, cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto con respecto a sí misma, como con respecto al personal que proponga para la prestación de los servicios.

No obstante, la designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de Cyberzaintza, y en este caso, el adjudicatario se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por Cyberzaintza de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

La empresa adjudicataria se compromete a adoptar las medidas necesarias orientadas a prevenir la rotación y, en cualquier caso, a minimizar el impacto que pueda ocasionar en Cyberzaintza y en el propio servicio.

Cualquier cambio en los integrantes del equipo de trabajo deberá ser conocido y aprobados por Cyberzaintza.

## 8.6 Requisitos de la solución propuesta

El contratista deberá aportar las herramientas y entornos necesarios para asegurar el resultado óptimo del proyecto, información que deberá ser incluida en la oferta presentada.

El contratista deberá disponer de una plataforma para la ejecución de los trabajos que incluya al menos los siguientes requisitos:

- Disponibilidad continua durante la duración del contrato.
- Solución multi-tenant que permita configurar de manera segmentada hasta 100 entidades y hasta 5.000 destinatarios, que podrán ir variando.

- Permitirá realizar campañas ilimitadas tanto individuales como colectivas.
- Permitirá realizar campañas multi-idioma: castellano y euskera.
- Permitirá el análisis de la infraestructura del cliente desde una perspectiva de ciberseguridad, en lo que se refiere al correo electrónico.
- Permitirá la selección de diferentes simulaciones de ataque como por ejemplo emails con urls, con adjuntos, simulación de ransomware, smishing, etc.
- Permitirá configurar múltiples plantillas y la generación y personalización de nuevas.
- Permitirá evaluar la efectividad de los envíos tanto de manera individual por cada una de las entidades participantes, como agregada para el caso de las campañas complejas.
- Dispondrá de dashboards configurables con métricas e indicadores.
- Dispondrá de API REST con acceso ilimitado para su integración con otras herramientas.
- Deberá incluir módulos formativos de ciberseguridad.
- Permitirá la generación de informes personalizados tanto individuales por cada una de las entidades participantes, como agregados.

El licitador deberá indicar de manera expresa si la solución propuesta cubre una serie de **requisitos obligatorios**, para lo cual deberá completar la tabla detallada contenida en la pestaña titulada "Requisitos" del archivo Excel Anexo II – PCT_Requisitos Técnicos_Lote5.xlsx correspondiente a los requerimientos solicitados en el Lote 5 del presente expediente.

Para garantizar el cumplimiento de los requisitos designados como Req.XX, el licitador deberá proporcionar las evidencias pertinentes, consistentes en:

- Capturas de pantalla que acrediten la funcionalidad requerida.
- Breve descripción del contenido de cada captura, explicando su relación con el requisito evaluado. Esta información se incluirá en un anexo específico, en el que cada evidencia estará numerada según el orden exacto de los requisitos Req.XX establecidos en la documentación del procedimiento.

El incumplimiento de las condiciones formales de presentación establecidas en este documento podrá afectar a la valoración de la oferta pudiendo llegar a la exclusión de esta.

Cyberzaintza se reserva el derecho a solicitar una prueba de las capacidades técnicas de cualquiera de las soluciones propuestas por el licitador propuesto como adjudicatario, coincidiendo con la fase de acreditación de requisitos previos.

En caso de que así sea requerido:

- Los costes para la realización de esas pruebas serán íntegramente asumidos por el propuesto como adjudicatario que, además, deberá facilitar el soporte que sea solicitado por Cyberzaintza para la realización de dicha prueba.
- El periodo de prueba no podrá superar los 30 días naturales y deberá realizarse en los 45 días siguientes a la publicación de la propuesta de adjudicación de la Mesa de Contratación.
- En caso de que el resultado de la prueba no sea satisfactorio porque se evidencie que la solución no cumple con los requisitos establecidos en este PCT, el licitador será descartado como posible adjudicatario por incumplimiento del PCT.

## 8.7 Organización y equipo de trabajo

Para la adecuada ejecución del proyecto el contratista debe tener capacidad suficiente para aportar como mínimo los siguientes perfiles con la dedicación correspondiente:

- Responsable general del proyecto: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del pliego y se encargará de la relación profesional entre el proveedor y Cyberzaintza.

  Dicho rol deberá cumplir los siguientes requisitos:

- Tener una buena capacidad de planificación.
- Habilidades de comunicación efectiva.
- Conocimientos sólidos en metodologías de gestión de proyectos.
- Habilidad de resolución de problemas.
- Buena orientación a los resultados.

Tendrá las siguientes funciones:

- Controlar los Procesos de Gestión ITIL y establecer los indicadores de control de gestión y los informes de gestión.
- Mantener y actualizar con Cyberzaintza los Acuerdos de Niveles de Servicio (ANS).
- Coordinar las funciones del servicio y la correcta ejecución de los procesos de gestión.
- Mejora continua del servicio.

Debe presentar experiencia contrastable de al menos 5 años en tareas similares y es imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.

- Designación de personas con rol facilitador que gestionen las solicitudes de campañas de phishing. Deberán tener la suficiente capacitación técnica y experiencia en coordinación y gestión de campañas de la naturaleza objeto del contrato, siendo exigible al menos 3 años. Así mismo, todas las personas asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera.
- Designación de personas con rol de técnicos en ciberseguridad que generen las evidencias, desplieguen, mantengan y operen la infraestructura necesaria, etc. Así mismo, generarán el informe final con las conclusiones, siendo exigible al menos 2 años de experiencia.

## Oficina técnica para la gestión de todos los servicios

# 9 Lote 6: “Oficina técnica para gestión de las iniciativas del Departamento de Operaciones”

## 9.1 Objeto

Este lote tiene por objeto la contratación de un servicio de Oficina técnica para la gestión de los servicios e iniciativas del Departamento de Operaciones de Cyberzaintza con el fin de asegurar su correcta ejecución y contribuyendo a elevar el nivel de madurez de los mismos.

## 9.2 Requisitos

- El servicio se prestará en su totalidad en formato bilingüe: tanto en euskera como en castellano.
- El servicio se prestará en horario laboral de 09:00 a 18:00 de lunes a viernes.
- Cyberzaintza sigue el modelo de buenas prácticas de ITIL para la definición y provisión de los procesos y servicios que presta. Es por ello que los trabajos que se deriven de este proyecto deberán estar adecuados a la norma ISO 20000-1:2018.
- Los materiales se generarán siguiendo las pautas del manual de identidad de marca de la Agencia.
- El adjudicatario asumirá los gastos derivados de los desplazamientos, dietas y otros costos asociados a la disposición de medios necesarios para estos y, en general, para la ejecución del proyecto en las condiciones de presencialidad indicadas. A efectos de realizar la propuesta, se estiman 5 desplazamientos mensuales fuera de las instalaciones de Cyberzaintza. No

obstante, es importante señalar que esta cifra no es vinculante y puede cambiar según las necesidades y circunstancias específicas de la Agencia.

## 9.3 Alcance

En este apartado se describe el alcance de los servicios solicitados del presente lote a través de este expediente, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por Cyberzaintza, cubriendo los aspectos de tareas a realizar y los resultados esperados.

- Seguimiento y supervisión de los servicios e iniciativas, con el objetivo de que se presten de manera eficaz y eficiente.
- Seguimiento y supervisión de los contratos y proyectos, evaluando el grado de avance de planificaciones, ejecución presupuestaria, etc.
- Gestión y organización documental:
  - Documentación y mantenimiento de las líneas de servicio.
  - Documentación y mantenimiento del catálogo de servicios, lo que incluirá la realización de un conjunto de documentos (pptx, infografías, vídeos o lo que se considere necesario) para mostrar y ofrecer los servicios prestados desde el Departamento a nuestros clientes actuales y a posibles clientes.
  - Modelado de nuevos servicios.
  - Documentación, mantenimiento y optimización de los procedimientos y procesos sobre los que se soportan los servicios, siguiendo las pautas de estándares internacionales.
  - Preparación de materiales para las reuniones y documentación de actas.
- Participación en comités y reuniones de seguimiento.
- Despliegue y mantenimiento de todas las herramientas necesarias para la ejecución de los trabajos.
- Definición, recolección y mantenimiento de indicadores, métricas e hitos del Departamento.
- Creación de cuadros de mando y de informes automáticos para el seguimiento del trabajo realizado en el Departamento.
- Gobierno y seguimiento centralizado de Planes de Mejora de los servicios apoyándose en el cuadro de indicadores.
- Apoyo a la dirección técnica de operaciones en el ofrecimiento de sus servicios a los clientes de una forma óptima.
- Captación de nuevos clientes para el Departamento.
- Elaboración y mantenimiento de un modelo de costes y tarifas para los servicios prestados.
- Dinamización de las diferentes comunidades de ciberseguridad impulsadas por Cyberzaintza: Cyberzaintza coordina varias iniciativas enfocadas a fomentar la colaboración interinstitucional tanto en ámbito público como privado, y así contribuir a la generación de relaciones de confianza y del intercambio de información correspondiente a buenas prácticas, casos de éxito, etc. Dentro del alcance de esa actividad se incluyen las siguientes tareas:
  - Preparación de todos los materiales necesarios para la dinamización de las comunidades: convocatorias de reunión, recopilación de información, elaboración de presentaciones, elaboración de actas, etc.
  - Promover la participación de los miembros de las comunidades en actividades formales o informales, así como en los grupos de trabajo.
  - Asistencia presencial o remota, según necesidad, a las reuniones de las comunidades.
  - Identificación de buenas prácticas y generación de materiales para que sean compartidas en las diferentes comunidades como, por ejemplo: políticas de seguridad, políticas de gestión de proveedores, políticas de intercambio de información, procedimientos de respuesta a incidentes, pilotos con tecnología concreta, etc.

- Elaboración de encuestas cuyas conclusiones sean posteriormente compartidas entre los participantes.
- Velar por que las comunidades refuercen, compartan y difundan conocimientos especializados en materia de ciberseguridad entre todos los miembros de las mismas.
- Registrar todas las actividades realizadas en el ámbito de las comunidades.
- Ejercer de punto de contacto y resolución ante las posibles dudas que puedan recibirse de miembros de las comunidades y que se reciban a través de diferentes medios (email, teléfono, RRSS, etc.).

- Identificación de fondos europeos en el ámbito de la ciberseguridad a los que podría optar la Agencia.
- Soporte a la dirección de operaciones y otras áreas que la persona responsable del servicio designe.

El servicio, asumirá además tareas del día a día en la gestión propia de los Servicios, complementándose con la actividad propia del personal de Cyberzaintza, acorde a las capacidades y necesidades que en cada momento se tengan.

## 9.4 Incompatibilidades

Se establecen incompatibilidades en la adjudicación simultánea de algunos de los lotes a un mismo adjudicatario ya que existen, relaciones de control y/o supervisión de unos sobre otros. Son incompatibles entre sí por su objeto el lote 6 respecto al grupo de lotes 1 a 5, por lo que no se aceptarán propuestas para el lote 6 que hayan presentado oferta en alguno de los lotes 1 a 5.

## 9.5 Metodología y planificación

Los licitantes deberán realizar una **propuesta de metodología y de plan de trabajo** que incluya un cronograma con los hitos más relevantes para la puesta en marcha y ejecución del servicio con sus respectivas fechas. Así mismo deberá incluir:

### 9.5.1 Seguimiento

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista se reunirá con la dirección técnica del proyecto de Cyberzaintza, si esta lo considera necesario para la adecuada prestación del servicio, con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato.

Cyberzaintza podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento y la correcta ejecución del objeto del contrato. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

En dicha reunión se revisarán al menos los siguientes puntos:

- Trabajos realizados en el periodo anterior.
- Trabajos planificados para el siguiente periodo.
- Seguimiento económico del contrato.
- Incidencias surgidas y áreas de mejora.

### 9.5.2 Cierre y devolución del servicio

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, a prestar apoyo, y realizar la transferencia del conocimiento, documentación técnica y administrativa necesaria para el traspaso del servicio, etc. al siguiente adjudicatario del contrato, en caso de que éste sea distinto al adjudicatario del presente pliego.

Por lo tanto, el adjudicatario deberá considerar como parte del alcance de los servicios solicitados, la ejecución de todas las tareas que sean necesarias para garantizar la continuidad del servicio por parte de Cyberzaintza cuando se produzca la finalización del contrato.

Por último, el adjudicatario deberá garantizar el borrado de información sensible en los sistemas propios del adjudicatario que no pasen a ser explotados por Cyberzaintza con la transferencia del servicio, certificando mediante documento escrito la ejecución de dichos trabajos.

En caso de que el adjudicatario no garantice la entrega del servicio en las condiciones establecidas en el presente pliego, no se procederá con la última factura del servicio.

El licitador deberá describir en su propuesta técnica (Plan de transferencia del Servicio) el alcance, plazos y procedimiento propuesto para realizar de forma efectiva la transferencia del servicio con la finalización del contrato, sin pérdidas de datos ni configuración, y sin interrupción del servicio, y garantizando las mismas capacidades operativas y funcionales de los sistemas actuales.

La fase de devolución concluirá con la celebración de la reunión de cierre del proyecto, donde se tratarán al menos los siguientes puntos:

- Memoria final de actividad.
- Documentación técnica y administrativa.
- Actas de todas las reuniones de seguimiento.
- Revisión de lecciones aprendidas y mejoras incluidas en la memora final del contrato. Esta información podrá ser solicitada como adelanto en cualquier momento durante la ejecución del contrato.
- Certificado acreditativo de borrado de la información utilizada en la provisión del servicio.
- Cierre del contrato.

## 9.6 Planes para la gestión adecuada del servicio

El licitador deberá proponer y detallar en su oferta al menos los siguientes planes.

### 9.6.1 Plan de calidad

El licitador deberá proponer un plan de calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan debe contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.

### 9.6.2 Plan de sustitución

Se solicita la inclusión de un plan de sustitución en el caso de que haya variaciones en la plantilla que presta el servicio.

Cyberzaintza se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación, y durante el curso de los trabajos, cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto con respecto a sí misma, como con respecto al personal que proponga para la prestación de los servicios.

No obstante, la designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de Cyberzaintza, y en este caso, el adjudicatario se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por Cyberzaintza de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

La empresa adjudicataria se compromete a adoptar las medidas necesarias orientadas a prevenir la rotación y, en cualquier caso, a minimizar el impacto que pueda ocasionar en Cyberzaintza y en el propio servicio.

Cualquier cambio en los integrantes del equipo de trabajo deberá ser conocido y aprobados por Cyberzaintza.

## 9.7 Herramientas

Se deben especificar las herramientas que se van a utilizar en la prestación del servicio, así como sus funcionalidades.

## 9.8 Organización y equipo de trabajo

El licitador deberá detallar el equipo de trabajo disponible para la ejecución del contrato indicando para cada recurso el perfil y grupo operativo al que se asocia, así como su experiencia en actividades similares para asegurar la correcta prestación del servicio. Los perfiles previstos para la ejecución del contrato son los siguientes:

- Responsable general del proyecto: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del pliego y se encargará de la relación profesional entre el proveedor y Cyberzaintza.

  Dicho rol deberá cumplir los siguientes requisitos:

  - Tener una buena capacidad de planificación.
  - Habilidades de comunicación efectiva.
  - Conocimientos sólidos en metodologías de gestión de proyectos.
  - Habilidad de resolución de problemas.
  - Buena orientación a los resultados.

  Tendrá las siguientes funciones:

  - Controlar los Procesos de Gestión ITIL y establecer los indicadores de control de gestión y los informes de gestión.
  - Mantener y actualizar con Cyberzaintza los Acuerdos de Niveles de Servicio (ANS).
  - Coordinar las funciones del servicio y la correcta ejecución de los procesos de gestión.
  - Mejora continua del servicio.

  Debe presentar experiencia contrastable de al menos 5 años en tareas similares y es imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.

  Designación de un conjunto de especialistas en las tareas contempladas dentro del alcance del contrato, que incluya los roles de consultores y gestores de procesos, de servicios y de costes. Se debe indicar las capacidades y experiencia, debiendo contar con al menos 5 años de experiencia y siendo imprescindible, por razones de disponibilidad y agilidad en la prestación del servicio, que la actividad se realice desde un centro de trabajo situado en un radio no superior a 120 km de Vitoria-Gasteiz. Se debe indicar las capacidades y experiencia.

- Consultor de ciberseguridad: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del Pliego. Debe presentar experiencia contrastable de al menos 3 años en tareas similares. Así mismo, todas las personas asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese

respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.

- Consultor / gestor de procesos: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del Pliego. Debe presentar experiencia contrastable de al menos 4 años en tareas similares. Así mismo, todas las personas asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.
- Consultor / gestor de servicios: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del Pliego. Debe presentar experiencia contrastable de al menos 4 años en tareas similares. Así mismo, todas las personas asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.
- Consultor / gestor de costes: deberá disponer de un perfil adecuado al nivel de exigencia técnica requerido en las condiciones del Pliego. Debe presentar experiencia contrastable de al menos 4 años en tareas similares. Así mismo, todas las personas asignadas a este rol tendrán conocimiento acreditado o contrastable tanto en castellano como en euskera. A ese respecto, se incorporará a la oferta certificación acreditativa de nivel B2 o equivalente de euskera.

### 9.8.1 Dimensionamiento y dedicación

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad establecida a continuación para cada uno de los roles, cumpliendo para ello con la dedicación indicada durante la ejecución del contrato:

- Consultor de ciberseguridad: 1.000 horas anuales.
- Consultor / gestor de procesos: 300 horas anuales.
- Consultor / gestor de servicios: 500 horas anuales.
- Consultor / gestor de costes: 200 horas anuales.

La dedicación mínima estimada del personal asignado al servicio será de 2.000 horas anuales.