Pliego de Prescripciones Técnicas para la contratación de un servicio de gestión de la línea de asesoramiento y respuesta frente a incidentes de ciberseguridad del BCSC.

Expediente nº: 2023026 Armonizado

Objeto de la contratación: prestación de un servicio de gestión de la línea de asesoramiento y respuesta frente a incidentes de ciberseguridad.

Documento: Pliego de Prescripciones Técnicas

1. Contexto

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en SPRI-Agencia Vasca de Desarrollo Empresarial (en adelante SPRI), dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team” y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. Objeto de la contratación

El objeto del contrato corresponde a un servicio de asesoramiento y respuesta frente a incidentes de ciberseguridad que ofrece el Centro Vasco de Ciberseguridad (BCSC, en adelante) a sus diferentes públicos objetivos a través de los canales establecidos para ello. Los públicos objetivos del centro son en la actualidad: entidades, tanto privadas como públicas, y ciudadanía.

3. Requisitos técnicos

3.1 Consideraciones

A continuación, se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por el BCSC, cubriendo los aspectos de tareas a realizar y resultados esperados.

Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario) pudiendo los licitadores ampliarlos en sus ofertas.

El licitador deberá aportar y describir los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

4. Descripción de las tareas a realizar

4.1 Asesoramiento y respuesta a incidentes

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

- **Buzones de correo**: un buzón que es la vía principal de entrada de los incidentes de ciberseguridad (incidencias@bcsc.eus).
- **Atención telefónica**: a través del teléfono 900 104 891.
- **Búsqueda proactiva**: la actividad se detalla en el apartado 3.2.2 Búsqueda proactiva de potenciales amenazas y riesgos.

Una vez se reciben los incidentes, en el caso de los emails, se procesarán de manera automática en la herramienta de ticketing, la cual deberá enviar 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 BCSC, 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 lo escalará internamente a un equipo técnico de nivel 2 con mayor experiencia, y finalmente si es necesario, se solicitará asesoramiento al equipo técnico del BCSC.

A continuación, se indican las tipologías de incidentes gestionados en 2022:

Tipología	Porcentaje
Fraude	55,63%
Contenido abusivo	16,83%
Intrusión	11,26%
Intento de intrusión	4,66%
Programa malicioso	3,41%
Sistemas vulnerables	2,27%
Disponibilidad	1,25%
Compromiso de la información	1,25%
Obtención de información	0,68%
Otros	2,73%

De cara a una mejora continua del servicio, **el adjudicatario del servicio revisará periódicamente y actualizará la base de datos de conocimiento del servicio tanto con la operativa del servicio, así como los procedimientos a seguir dependiendo del tipo de incidente recibido (playbooks), el procedimiento de escalado, procedimiento de activación del protocolo de emergencia, las plantillas con las respuestas una vez consensuadas, etc**. **El BCSC le facilitará acceso a la misma.**

Tal y como se indica en la operativa del servicio, se contemplan **2 niveles de operación**:

- Tareas a realizar por el nivel 1:
  - Atender los canales habilitados por el BCSC 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.
- Cerrar los incidentes en la herramienta de ticketing una vez hayan sido resueltos.

- Tareas a realizar por el 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 al BCSC en el caso de que no saber cómo dar una respuesta adecuada.
  - Prestar apoyo al equipo que realiza las tareas de búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad.
  - Mantener un alto grado de coordinación con el BCSC.
- Por encima de los niveles 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.
  - 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.
  - Prestar apoyo al equipo que realiza las tareas de búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad.
  - Ser interlocutor entre el BCSC y los equipos técnicos de niveles 1 y 2.

Ocasionalmente, integrantes del equipo que realice las tareas de asesoramiento y respuesta a incidentes participarán en iniciativas del BCSC 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.

El número de incidentes que podrían registrarse a lo largo de un mes y ser objeto del

contrato, se fija un valor aproximado de 200, con las siguientes consideraciones:

- El valor que se indica es el mínimo que el BCSC 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.

De esta forma la capacidad que se debe asegurar (número de incidentes mensuales mínimos comprometidos) es de **250 incidentes**, siendo en todo caso y tal y como se ha señalado, un número estimativo, teniendo el adjudicatario que atender todo incidente que sobrepase esa cantidad. 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 grabar conversaciones para su posterior revisión, reproducir locuciones pregrabadas, envío de mensajes de texto y realizar encuestas para evaluar la satisfacción del servicio, así como una plataforma para registrar las incidencias que el adjudicatario integrará con el buzón de correo, y que a su vez permitirá la importación de la base de datos actual; tarea que será realizada nada más iniciar el servicio. Así mismo, la plataforma permitirá exportar la información ya que a lo largo del servicio ésta se migrará a la herramienta de gestión de incidentes que el BCSC estipule.

El servicio se ofrecerá en formato 24x7 y en formato bilingüe: euskera y castellano, cumpliendo el acuerdo de nivel de servicio especificado en el apartado 5 Acuerdo de nivel de servicio. Todos los documentos del servicio se elaborarán de acuerdo con el manual de identidad corporativa del BCSC y bajo su propia marca.

4.2 Activación del protocolo de emergencia / alertas

El equipo técnico aportado por el adjudicatario del servicio para realizar las tareas descritas en el apartado 4.1 Asesoramiento y respuesta a incidentes, a petición del BCSC, activará el protocolo de emergencia / alertas para dar respuesta a situaciones que así lo requieran. En este sentido, se enviarán mensajes de texto o llamará, según corresponda, a los puntos de contacto especificados por el BCSC 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. El servicio se ofrecerá en el mismo formato 24x7 que el servicio 4.1 Asesoramiento y respuesta a incidentes.

4.3 Búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad

El servicio, que será ofrecido en formato 8x5, contempla la realización de tareas destinadas a la identificación proactiva de posibles incidentes de ciberseguridad en base a la identificación de amenazas que estén teniendo o pudieran tener un impacto

significativo en el ámbito de Euskadi, así como la identificación de riesgos que pudieran derivar en incidentes de ciberseguridad que afectasen a los diferentes públicos del BCSC. En ese sentido, se contempla realizar las siguientes tareas:

- **Automatización y Orquestación:** conlleva la mejora continua del modelo de inteligencia del BCSC con el objetivo de mejorar constantemente las capacidades de detección proactiva y reactiva de incidentes.
  - Tareas:
    - Administración de servidores Linux.
    - Mantenimiento de ELK.
    - Contribuir a la evolución del modelo de inteligencia: análisis, diseño e implementación de casos de uso, así como la actualización de los mismos, propuesta de mejoras, etc.
    - Mantenimiento y desarrollo de cuadros de mando en Kibana con indicadores referentes al estado de la ciberseguridad en Euskadi.
    - Despliegue, configuración y mantenimiento de herramientas de monitorización, análisis, etc.
    - Interactuar con multitud de APIs de diferentes servicios tales como Shodan, Zoomeye, Phishtank, MISP, OTX, etc.
    - Desarrollo de scripts a medida.
    - Diseño de interfaces.
    - Elaboración y actualización de documentación técnica como casos de uso y procedimientos de actuación.
    - Apoyo a los diferentes servicios que ofrece el CERT del BCSC.
- **Identificación proactiva y alerta temprana:** conlleva la explotación continua del modelo de inteligencia del BCSC con el objetivo de identificar proactivamente incidentes de ciberseguridad, así como riesgos que puedan derivar en potenciales incidentes, los cuales, serán remitidos al equipo técnico aportado por el adjudicatario del servicio para realizar las tareas descritas en el apartado 4.1 Asesoramiento y respuesta a incidentes para que tomen las medidas oportunas de cara a realizar la correspondiente mitigación o solución.
  - Tareas:
    - Interactuar con las herramientas correspondientes al modelo de inteligencia del BCSC para explotar la información de cara a identificar los incidentes.
    - Análisis, elaboración, publicación y difusión de:
      - comunicados de avisos y alertas.
      - boletines de seguridad.
      - informes sobre incidentes de ciberseguridad sufridos por terceros.

- informes en base a la información del modelo de inteligencia.

- Caracterización de amenazas y ataques mediante el framework de Mitre ATT&CK.
- Elaboración de inteligencia accionable para prevenir, detectar y responder a incidentes: reglas de yara, snort, sigma, etc.
- Alimentar las herramientas de compartición de información sobre amenazas.
- Elaboración y actualización de documentación técnica y procedimientos de actuación.
- Apoyo a los diferentes servicios que ofrece el CERT del BCSC.

4.4 Generación de materiales que contribuyan a prevenir y reaccionar frente a incidentes de ciberseguridad

En base a las tareas indicadas anteriormente, el adjudicatario del servicio propondrá, investigará y realizará informes técnicos de amenazas, familias de malware, vulnerabilidades, etc. de cara a realizar la alerta temprana de las mismas. Los informes se desarrollarán tanto en euskera como en castellano y siguiendo el manual de identidad corporativa del BCSC.

Se contempla la elaboración de 2 tipos de informes:

- *Sencillos*: normalmente, corresponden al análisis de vulnerabilidades o amenazas desde una perspectiva global. Se elaborarán de manera proactiva y bajo demanda, y su elaboración se estima en una dedicación de 3 o 4 horas. Se contempla la elaboración estimada de 35 informes anuales de este tipo.
- Complejos: corresponde al análisis de familias de malware, actores maliciosos, etc., con una perspectiva detallada sobre su ámbito de afección, vector de entrada, comportamiento, propagación, medidas de mitigación etc. Su elaboración será reactiva, bajo demanda del BCSC, y se contempla la elaboración estimada de 14 informes anuales de este tipo, siendo la periodicidad mensual y contemplando 2 adicionales fuera de ciclo para situaciones excepcionales.

Una vez validados, el adjudicatario publicará dichos informes en la web del BCSC. Es posible consultar ejemplos de informes de ambos tipos en la página web del centro.

5. Acuerdo de nivel de servicio

El licitador se comprometerá a garantizar que los servicios 4.1 Asesoramiento y respuesta a incidentes y 4.2 Activación del protocolo de emergencia / alertas serán prestados de acuerdo a un modelo 24x7 con los niveles mínimos que se detallan a continuación.

Código	Descripción	Valor objetivo	Porcentaje de cumplimiento mínimo
1	Tiempo de respuesta. No se trata de la respuesta inicial de asignación del identificador del caso y acuse de recibo, la cual debe ser automática, si no en la que se ofrece el asesoramiento inicial.	2 horas	95%
2	Activación de protocolo de emergencia y contacto con todas las personas identificadas en el escalado.	30 minutos	100%

El licitador se compromete a realizar el seguimiento de la calidad con la que se presta la tarea 4.1 Asesoramiento y respuesta a incidentes, para lo cual reportará con periodicidad mensual los correspondientes indicadores de calidad del servicio que obtendrá a partir del recuento de fallos cometidos de acuerdo a la siguiente tabla:

Nivel	Tipos
Bajo	Errores con afectación únicamente a nivel interno y fácilmente subsanables. Categorización incorrecta del incidente. Incidente sin campos completados. El error tiene escaso o nulo impacto. Escalado no justificado.
Medio	Errores de gestión cuyas consecuencias no se circunscriben al ámbito interno, sino que tienen afectación hacia terceros. Peticiones al BCSC de información ya proporcionada o disponible en la base de datos de conocimiento. Envío de recomendaciones redundantes o no aplicables o sin relación con la consulta. Envío de respuesta con plantilla por defecto sin eliminar los comentarios que contiene o sin actualizar la información. Errores ortográficos o gramaticales en la respuesta.
Alto	Envío de información confidencial a destinatarios incorrectos. Solicitud de baja de sistemas legítimos. Errores de gestión con consecuencias externas y capacidad de

	provocar daños importantes a terceros. Envío de solicitudes o recomendaciones completamente erróneas. Queja justificada por una mala gestión. Comunicaciones de falsos positivos a organizaciones representativas.

Como consecuencia de dicha evaluación se contempla la prestación del servicio de acuerdo a los siguientes niveles mínimos:

Código	Descripción	Porcentaje de cumplimiento objetivo	Porcentaje de cumplimiento mínimo
3	Fallos de nivel bajo	90%	75%
4	Fallos de nivel medio	90%	75%
5	Fallos de nivel alto	100%	95%

El licitador se comprometerá a garantizar que el servicio 4.4 Generación de materiales que contribuyan a prevenir y reaccionar frente a incidentes de ciberseguridad será prestado con los niveles mínimos que se detallan a continuación.

Código	Descripción	Valor objetivo	Porcentaje de cumplimiento mínimo
6	Elaboración y entrega de informes sencillos	3 horas	90%
7	Elaboración y entrega de informes complejos	21 días	100%

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

SPRI 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 10% del precio de adjudicación del contrato:

- Código 1:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 80%: Penalización 1% de la facturación mensual.
  - Cumplimiento < 70%: Penalización 3% de la facturación mensual.
  - El primer incumplimiento de este indicador no conllevará penalización, se registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.

- Mínimo de instancias de este tipo necesarias para activar la penalización: 10 solicitudes.

- Código 2:
  - 100% > Cumplimiento: Penalización 10% de la facturación mensual por cada solicitud no atendida en el plazo marcado.
  - Mínimo de instancias de este tipo necesarias para activar la penalización: 1 solicitud.
- Código 3:
  - Cumplimiento >= 75%: Sin penalización.
  - 75% > Cumplimiento >= 70%: Penalización 1% de la facturación mensual.
  - Cumplimiento < 70%: Penalización 3% de la facturación mensual.
  - El primer incumplimiento de este indicador no conllevará penalización, se registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.
  - Mínimo de instancias de este tipo necesarias para activar la penalización: 10 fallos.
- Código 4:
  - Cumplimiento >= 75%: Sin penalización.
  - 75% > Cumplimiento >= 70%: Penalización 1% de la facturación mensual.
  - Cumplimiento < 70%: Penalización 3% de la facturación mensual.
  - El primer incumplimiento de este indicador no conllevará penalización, se registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.
  - Mínimo de instancias de este tipo necesarias para activar la penalización: 10 fallos.
- Código 5:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 90%: Penalización 2% de la facturación mensual.
  - Cumplimiento < 90%: Penalización 5% de la facturación mensual.
  - Mínimo de instancias de este tipo necesarias para activar la penalización: 1 fallo.
- Código 6:
  - Cumplimiento < 90%: Penalización 1% de la facturación mensual por cada solicitud no atendida en el plazo marcado.
  - Mínimo de instancias de este tipo necesarias para activar la penalización: 3 solicitudes.
- Código 7:
  - Cumplimiento < 100%: Penalización 1% de la facturación mensual por cada solicitud no atendida en el plazo marcado.

- Mínimo de instancias de este tipo necesarias para activar la penalización: 3 solicitudes.

El primer incumplimiento de los códigos 1, 3, 6 y 7 no conllevará penalización, si no que registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.

En relación a los códigos 2, 4 y 5 en caso de mantenerse o reiterarse la defectuosa ejecución del contrato tras el tercer apercibimiento escrito, el órgano de contratación podrá proceder a la resolución del contrato.

6. Comunicación de incidencias

Debido a la naturaleza sensible del servicio y de los datos a los que se tiene acceso, el caso de que el adjudicatario detecte un incidente de ciberseguridad con potencial impacto o afectación en la prestación de servicios objeto del contrato, deberá notificar inmediatamente la incidencia a la persona del BCSC designada como responsable del contrato.

Así mismo, BCSC podrá requerir a la contratista que le dote información detallada sobre el incidente en cuestión; la cual será debidamente gestionada y siguiendo una política «need to know» y en el caso de requerir difusión controlada, se solicitará autorización previa para ello.

7. Metodología y plan de trabajo

El licitador deberá realizar una propuesta que incluya **tanto la metodología como el plan de trabajo y cronograma, reflejando los hitos más relevantes del servicio con sus respectivas fechas, y herramientas que se utilizarán para la prestación del servicio**.

La metodología deberá contemplar obligatoriamente los siguientes aspectos:

- **Operativa general para la prestación del servicio, incluyendo además lo siguiente:**
  - **Fase inicial:** contempla la configuración, formación y puesta en marcha del servicio. Se debe contemplar un periodo inicial de configuración de la plataforma de llamadas y de la herramienta de ticketing, 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.
  - **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 del BCSC. En dicha propuesta incluirá las métricas especificadas en el apartado 5. Acuerdo de nivel de servicio.

- **Fase de devolución y cierre del proyecto:** al finalizar el proyecto, el contratista deberá presentar una Memoria Final, que sirva a modo de informe justificativo del alcance efectivo de los trabajos realizados, y que incluya aspectos tales como el detalle de entregables, recursos consumidos, objetivos e hitos conseguidos y propuesta de recomendaciones de actividades y objetivos a alcanzar en el servicio en los siguientes meses. Así mismo, deberá entregar toda la información de la herramienta de ticketing sobre los incidentes gestionados, así como toda la que se haya elaborado dentro del alcance del servicio, y garantizar el borrado de todos los ficheros que pudieran existir en sus equipos informáticos con cualquier dato de carácter personal.

- **Descripción y detalle de cada una de las tareas recogidas dentro del servicio.**
- **Garantizar el cumplimiento del acuerdo de nivel de servicio.**
- **Mejora continua del servicio:**
  - Se solicita un **plan de contingencia** que asegure un servicio mínimo en caso de fallo de sus comunicaciones de voz y datos y de sus sistemas informáticos principales, o sustitución de personal**.** Cualquier incidencia relevante que afecte a la prestación del Servicio deberá ser informada de forma inmediata al BCSC, y deberá quedar recogida en los correspondientes informes mensuales de reporte de actividad del servicio.
  - Se solicita un **plan de mejora continua** que contemple una serie de medidas que contribuyan a evaluar periódicamente la calidad del servicio con el objetivo de alcanzar un nivel de excelencia, pudiendo ser estas, por ejemplo: realización de llamadas de prueba, análisis y evaluación aleatoria de los incidentes gestionados tanto vía email como telefónica, etc.
  - Así mismo, se solicita la inclusión de un **plan de formación** continua para el equipo que presta el servicio, el cual contemple diferentes acciones formativas **tanto al inicio como a lo largo de la prestación del servicio** que vayan alineadas con la actividad que desarrollan. Dicho plan debe centrarse especialmente tanto en el equipo de nivel 1 que realiza la actividad 4.1 Asesoramiento y respuesta a incidentes, así como en el equipo que realiza la actividad 4.3 Búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad, **siendo especialmente relevante este último para lo cual se deberán presentar anualmente evidencias de al menos 4 acciones formativas, no contando para ello formaciones internas**.
  - Finalmente, se solicita la inclusión de un **plan de sustitución** en el caso de que haya variaciones en la plantilla que presta el servicio, siendo especialmente relevante en el caso del equipo que realiza la actividad 3.2.3 Búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad.

8. Equipo de trabajo

La empresa adjudicataria asignará al proyecto, de forma continuada, un equipo humano que se encargará de las labores descritas en el apartado de 4 Descripción de las tareas a realizar. 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 del proyecto:** designación de una persona que ejerza como responsable general del proyecto con conocimiento y experiencia suficiente en labores de esta naturaleza, 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, y quien realizará principalmente las siguientes tareas:
  - Ejercer de interlocutor con la persona asignada por el BCSC.
  - Elaborar informes de seguimiento.
  - Elaborar actas de seguimiento del servicio.
  - Informar de incumplimientos en los SLA.
  - Notificar de cualquier incidencia que afecte a la correcta prestación del servicio.
  - Velar por la mejora continua y calidad del servicio.

  Se debe indicar las capacidades y experiencia.
- **Coordinador técnico del servicio**: designación de una persona que evaluará la calidad del servicio en términos técnicos, proponiendo aspectos de mejora y sirviendo de enlace técnico con los niveles 1 y 2. Se debe indicar las capacidades y experiencia, debiendo contar con al menos 3 años de experiencia en 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.
- **Equipo de nivel 1 de respuesta a incidentes:** 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 3.2.1 Asesoramiento y respuesta a incidentes, 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.

- **Equipo de nivel 2 de respuesta a incidentes:** Personal con amplia experiencia en las tareas descritas en el apartado 3.2.1 Asesoramiento y respuesta a incidentes. Se debe indicar los perfiles asignados al servicio, así como su correspondiente experiencia en tareas que son objeto del contrato.
- **Equipo encargado de la búsqueda proactiva de amenazas y riesgos**: El adjudicatario del servicio destinará en exclusividad a 2 recursos para la realización de las tareas especificadas en el apartado 4.3 Búsqueda proactiva de potenciales amenazas y riesgos. Se debe indicar las capacidades y experiencia de ambos.
  - Un perfil con dedicación exclusiva a las tareas de automatización y orquestación, el cual contará con al menos 2 años de experiencia administrando ELK, utilización de APIs, diseño de interfaces, bases de datos, etc. y experiencia en administración de servidores Linux, programación en Bash y Python, node.js y tecnologías similares.
  - Dos perfiles con dedicación exclusiva a las tareas descritas en la identificación proactiva y alerta temprana con al menos 2 años de experiencia en la explotación de información de modelos de inteligencia de amenazas de ciberseguridad, desarrollo de inteligencia accionable como reglas de yara, snort y sigma, caracterización de amenazas mediante mitre att&ck, análisis de amenazas y elaboración de contenido de alerta temprana como avisos, alertas e informes, elaboración de playbooks, etc.

Junto con la información anterior se deberá entregar la tabla del Anexo EquipoTrabajo.xlsx.

IMPORTANTE: Únicamente se indicarán las certificaciones del responsable de proyecto, y exclusivamente aquellas relacionadas con la gestión de proyectos.

El centro de trabajo de las personas que realicen las tareas descritas en los apartados 4.1 Asesoramiento y respuesta a incidentes, 4.2 Activación del protocolo de emergencia / alertas y 4.4 Generación de materiales que contribuyan a prevenir y reaccionar frente a incidentes de ciberseguridad será las oficinas e instalaciones de la empresa adjudicataria de este, manteniendo una conexión remota VPN con la infraestructura informática del BCSC necesaria para desempeñar los trabajos, y a través de la cual se registrarán las solicitudes y su detalle.

El centro de trabajo de las personas que realicen las tareas descritas en el apartado 4.3 “Búsqueda proactiva de potenciales amenazas y riesgos que puedan derivar en incidentes de ciberseguridad”, podrá ser, en caso de que así lo decida la entidad contratante, las propias oficinas e instalaciones del BCSC, dada la naturaleza sensible de la información con la que se debe trabajar. Por todo ello, el equipo de trabajo propuesto deberá estar dimensionado, preparado y contar con los recursos precisos, para ejecutar el contrato en las citadas instalaciones de BCSC con total normalidad.

El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y

consecuentemente valorado.

Los trabajos desarrollados por el equipo del proyecto serán supervisados directamente por el personal del BCSC que podrá pedir las explicaciones e informaciones que considere oportunas al objeto de verificar el correcto desarrollo de los trabajos contratados.