Pliego de prescripciones técnicas particulares para la contratación de un servicio para el Basque Cybersecurity Centre para la alerta temprana de amenazas y riesgos de ciberseguridad.

Expediente nº: 2021015 Armonizado

Objeto de la contratación: prestación de un servicio para el Basque Cybersecurity Centre para la alerta temprana de amenazas y riesgos de ciberseguridad.

Documento: Pliego de prescripciones técnicas particulares.

Contenido

1. Contexto....3
2. Objeto de la contratación....3
3. Descripción de las actividades a desarrollar....4
3.1. Consideraciones previas....4
3.2. Actividades objeto del contrato....4
3.2.1. Vigilancia Digital....4
3.2.2. Monitorización de activos....5
3.2.3. Detección de fugas de información....5
3.2.4. Análisis....6
3.2.5. Generación de alertas instantáneas....6
3.2.6. Generación de informes de situación....7
4. Metodología y planificación....7
4.1. Seguimiento del servicio....8
4.2. Mejora continua del servicio....8
4.3. Devolución del servicio....8
5. Equipo de trabajo....9

1. CONTEXTO

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca dentro de la Agencia Vasca de Desarrollo Empresarial, (en adelante SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco.

El BCSC, como unidad de SPRI, 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 incluirá 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 impulsará 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 CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabajará 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 área del BCSC de SPRI, precisa contratar un servicio de alerta temprana de ciberamenazas y riesgos.

Los objetivos que se persiguen con la presente contratación son los siguientes:

- Identificación proactiva de ciberamenazas e incidentes de ciberseguridad.
- Alerta temprana a los diferentes públicos objetivos del BCSC.
- Proteger a los diferentes públicos objetivos del BCSC, siendo principalmente empresas y la ciudadanía vasca.

Dicha contratación viene justificada por la imposibilidad de desarrollar el trabajo con medios propios, por la falta de recursos materiales y por la necesidad de realizar trabajos no propios de la SPRI.

3. DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR

3.1. CONSIDERACIONES PREVIAS

En este apartado se describen las características que conforman el objeto del contrato y que el adjudicatario deberá prestar.

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

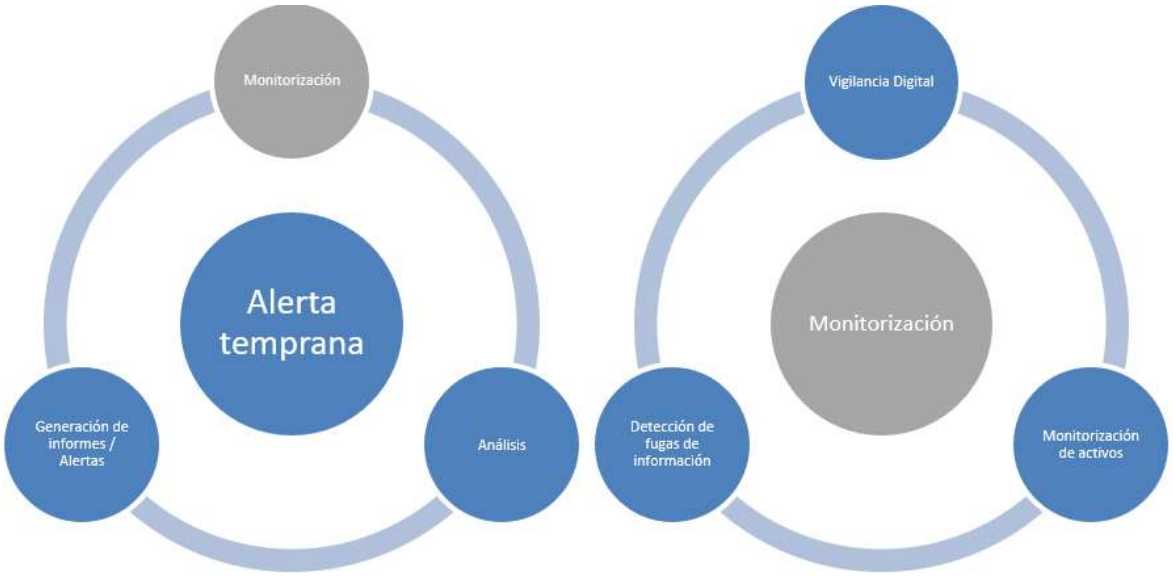
El adjudicatario **deberá aportar el conocimiento, las metodologías y el equipo humano necesario, apoyándose en los recursos técnicos que considere necesarios** (que serán facilitados por el adjudicatario), para asegurar un resultado óptimo en la prestación del servicio. **Se entiende por recurso técnico**, **cualquier tipo de software, hardware o licencia necesaria** para la prestación del servicio en condiciones óptimas.

Así mismo, **el servicio, en toda su extensión, debe ser bilingüe (castellano y euskera)**, por lo que **la totalidad de los contenidos recogidos en las actividades del contrato deberán ser generados en castellano y euskera**. **La oferta debe contemplar este aspecto de manera específica o será excluida.**

Todos los entregables serán generados de acuerdo al manual de identidad corporativa del BCSC y con las correspondientes plantillas, en el caso de que estén previamente definidas, en caso contrario el adjudicatario del servicio realizará una propuesta que será utilizada previa validación por parte del BCSC. Así mismo, los informes se entregarán con maquetación profesional y siguiendo las pautas indicadas por el Centro.

3.2. ACTIVIDADES OBJETO DEL CONTRATO

El adjudicatario del servicio deberá asumir, las siguientes tareas, 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.



3.2.1. VIGILANCIA DIGITAL

En el alcance de la actividad de Vigilancia Digital **se contempla la monitorización continua estimada de 100 objetivos**. Dichos objetivos se establecerán al inicio del servicio y podrán ser conjuntos de empresas en base a ciertos criterios (ejemplo: organismos públicos o clústeres), empresas concretas (ejemplo: Spri), personas, cuentas en redes sociales, páginas web, direcciones IP, amenazas concretas, términos específicos, etc. El BCSC hará una propuesta

inicial de objetivos y el adjudicatario del servicio completará y mantendrá actualizada dicha propuesta en base a su experiencia y conocimiento y de acuerdo a los casos de uso del Centro.

El licitador deberá presentar un listado exhaustivo de fuentes que serán monitorizadas dentro del alcance del servicio, contemplando las siguientes tipologías:

- Fuentes abiertas.
- Fuentes de acceso restringido.
- Fuentes que requieren HUMINT como canales de Telegram o webs en Dark Web (Tor, Freenet, I2P, etc.).

Dicho listado será actualizado a lo largo de la ejecución del servicio y deberá permitir identificar y recolectar información sobre:

- Ciberamenazas que puedan afectar a los diferentes públicos objetivos del BCSC.
- Campañas de malware.
- Fugas de información.
- Incidentes de ciberseguridad.
- Amenazas directas realizadas.
- Posibles fraudes online.
- Noticias falsas que estén teniendo especial repercusión y que puedan tener consecuencias negativas para los públicos objetivos del BCSC.
- Etc.

El licitador deberá presentar y detallar de manera exhaustiva las herramientas que va a utilizar para la prestación del servicio, destacando sus capacidades. Se valorará positivamente que facilite acceso al BCSC a las mismas durante la prestación del servicio.

Las propuestas deberán contemplar un listado exhaustivo de los casos de uso que el licitador es capaz de detectar.

Así mismo, deberá detallar a modo de ejemplo 3 casos de uso concretos, esto es, según el tipo de objetivo (empresas, personas, cuentas en redes sociales, páginas web, direcciones IP, amenazas concretas, términos específicos, etc), qué se va a hacer.

O bien, según lo que se pretenda identificar (ciberamenazas que puedan afectar a los diferentes públicos objetivos del BCSC, campañas de malware, fugas de información, incidentes de ciberseguridad, etc.) qué se va a hacer para detectar estas tipologías.

3.2.2. MONITORIZACIÓN DE ACTIVOS

En el alcance de la actividad de monitorización de activos se contempla la monitorización de la disponibilidad de un listado de hasta 100 dominios. La monitorización permitirá al menos la identificación de caídas prolongadas 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. Se valorará positivamente que facilite acceso al BCSC a las mismas durante la prestación del servicio.

3.2.3. DETECCIÓN DE FUGAS DE INFORMACIÓN

En el alcance de la actividad de detección de fugas de información se contempla la detección de

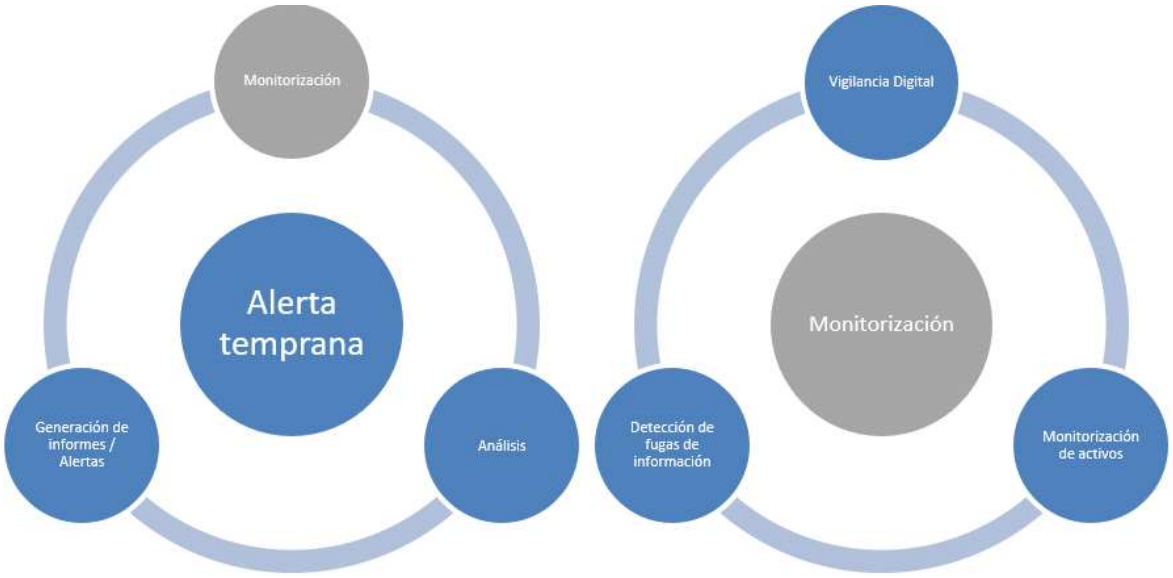
fugas de información que afecten a un listado de hasta 100 dominios. Esto es, supongamos que se produce una fuga de información en la que aparecen listados una serie de emails pertenecientes al dominio monitorizado. El adjudicatario del servicio deberá tener la capacidad de detectar este tipo de fugas.

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 del BCSC.

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. Se valorará positivamente que facilite acceso al BCSC a las mismas durante la prestación del servicio.

3.2.4. ANÁLISIS

Toda la información obtenida en las actividades de 0



Vigilancia Digital, 3.2.2 Monitorización de activos y 3.2.3 Detección de fugas de información será analizada en detalle por el equipo de trabajo asignado al servicio por parte del licitador, evaluando el riesgo, impacto potencial, criticidad, etc. de cara a alertar en caso de que sea necesario.

3.2.5. GENERACIÓN DE ALERTAS INSTANTÁNEAS

En el caso de que sea necesario, el equipo de trabajo asignado al servicio generará alertas instantáneas. **El licitador deberá proponer una estructura de alerta y presentará 3 ejemplos diferentes lo más detallados posibles.** Dichas alertas tendrán 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.

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

- Uno de los objetivos a monitorizar sufre un incidente de ciberseguridad y esta información se hace pública.

- Uno de los objetivos a monitorizar sufre un ataque de denegación de servicio.
- La web de alguno de los objetivos a monitorizar sufre un defacement.
- Información confidencial de unos los objetivos a monitorizar, la cual es accesible de manera pública.
- Uno de los objetivos a monitorizar sufre una amenaza directa en redes sociales.

3.2.6. GENERACIÓN DE INFORMES DE SITUACIÓN

De manera puntual, **el BCSC podrá solicitar informes de situación que contemplen un marco temporal concreto** de la totalidad o parte de los objetivos a monitorizar para ver la evolución o el estado. Dicha información se obtendrá a partir de las actividades de 0



Vigilancia Digital, 3.2.2 Monitorización de activos y 3.2.3 Detección de fugas de información y podrá ser completada con información obtenida a partir del modelo de inteligencia del BCSC.

Un ejemplo de informe de estas características puede ser obtener toda la información de los últimos 3 meses de los objetivos a monitorizar que estén relacionados con el ámbito sanitario. **Se estima la generación anual de 6 informes de esta tipología**.

Todos los informes deberán ser generados a doble columna en euskera y castellano y estar profesionalmente maquetados de acuerdo con el manual de identidad corporativa del BCSC.

El licitador deberá proponer una estructura de informe y presentará 1 ejemplo lo más detallado posible, teniendo en cuenta que será distribuido tanto a un público técnico como no técnico. Dichos informes tendrán como mínimo la siguiente información:

- Cuadro de mando que refleje de manera clara la situación.
- Resumen ejecutivo que contemple el análisis del cuadro de mando y las conclusiones.
- Tareas realizadas con indicadores tanto cuantitativos como cualitativos.

Se estima así mismo el envío de un email semanal en el día y hora convenidos, el cual incluirá un resumen ejecutivo con lo sucedido esa semana, junto con la información más relevante relacionada con los objetivos a monitorizar. El BCSC aportará la plantilla que deberá ser utilizada.

4. METODOLOGÍA Y PLANIFICACIÓN

El proveedor deberá prestar el servicio de acuerdo con las pautas establecidas por el BCSC y aprovechando todo el conocimiento previo obtenido durante la ejecución previa del servicio. La operativa asociada podría evolucionar, por lo que la manera de trabajar al inicio del contrato podrá ser modificada a lo largo de la vigencia del contrato con el objetivo de que el servicio se preste con mayor calidad, sin que ello suponga propiamente una modificación del contrato en el sentido regulado en los artículos 203 y ss, de la vigente Ley de Contratos del Sector Público.

Los licitadores deberán proponer de manera clara la metodología a seguir durante el desarrollo del servicio, cumpliendo los objetivos fijados en el presente Pliego de Prescripciones Técnicas.

En la metodología, **los licitadores deberán detallar la operativa de trabajo, el modelo de relación con el BCSC, los roles y responsabilidades, la forma en la que abordará cada una de las actividades reflejadas en el apartado 3.2 Actividades objeto del contrato y las herramientas que va a utilizar para la prestación del servicio**. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

En relación al listado de entregables solicitados en las distintas tareas que son objeto del contrato se presenta la siguiente tabla para clarificar el alcance del servicio:

Entregable	Periodicidad
Alertas instantáneas	Las que sean oportunas.
Email de estado	Semanal
Informe de estado	Bajo demanda. Estimado 6.

4.1. SEGUIMIENTO DEL SERVICIO

Se llevarán a cabo reuniones ordinarias de seguimiento y control entre el responsable del servicio por parte del adjudicatario y la persona designada por el BCSC. En estas reuniones se revisará la planificación, priorización y la evolución de los trabajos asignados, así como las especificaciones de cada uno de los objetivos y la validación de las tareas realizadas.

Independientemente de los expresado con anterioridad, el adjudicatario del servicio podrá ser reclamado y citado por la persona asignada por el BCSC, o la persona en quien delegue, en cualquier momento para la realización de reuniones que se convoquen por medio de procedimiento urgente.

Anualmente, el contratista deberá presentar una Memoria de actividad, 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.

4.2. MEJORA CONTINUA DEL SERVICIO

El licitador podrá proponer una serie de medidas que contribuyan a alcanzar y mantener el nivel de excelencia del servicio.

4.3. DEVOLUCIÓN DEL SERVICIO

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 que contribuyan a la mejora de la prestación del servicio.

5. 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 3.2 Actividades objeto del contrato. El equipo de trabajo estará compuesto por personal adecuado y con experiencia en las materias objeto del servicio, y atenderá las necesidades del servicio acorde a la jornada laboral del BCSC, es decir, de lunes a viernes de 8.00 a 18.00.

EL BCSC requiere que un equipo especializado lleve a cabo la operación del servicio y a través del seguimiento y la revisión, garantice su calidad. Los oferentes deberán acreditar las capacidades técnicas y requisitos mínimos que se detallan a continuación:

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

- Designación de una persona que ejerza como Coordinador General del servicio con conocimiento y experiencia suficiente en labores de esta naturaleza, quien ejercerá la interlocución con la persona delegada por el BCSC de SPRI.

  Requisitos mínimos. Para el ejercicio de las funciones de Coordinador General, será imprescindible reunir los siguientes requisitos:

  - Experiencia profesional: experiencia acreditada en trabajos de consultoría en materia de ciberseguridad de al menos cinco años (5).
  - Habilidades: conocimientos demostrables, mediante formación o experiencia previa en la materia, en herramientas de generación y presentación de información para hacer más eficiente la comunicación, así como en la redacción de informes ejecutivos y asesoría a alta dirección.
  - Certificaciones: se valorará disponer de certificaciones de ciberseguridad.

- Asignación al servicio un pool de analistas con experiencia en las tareas objeto del contrato.

  Requisitos mínimos. Para el ejercicio de las funciones de Técnico / Analista, será imprescindible reunir los siguientes requisitos:

  - Experiencia profesional: experiencia acreditada en las actividades que son objeto del contrato de al menos dos años (2).
  - Habilidades: conocimientos demostrables, mediante formación o experiencia previa en análisis de ciberamenazas, vigilancia digital, herramientas de monitorización, etc.
  - Certificaciones: se valorará disponer de certificaciones de ciberseguridad.

- Asignación al servicio de recursos / servicio especializado en traducciones a euskera, justificándolo con la documentación acreditativa pertinente.
- Asignación al servicio de recursos / servicio especializado en diseño y maquetación de entregables.

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

El personal asignado al contrato dependerá exclusivamente de la empresa adjudicataria. En ningún supuesto podrá considerarse con relación laboral, contractual, funcionarial o de naturaleza alguna respecto del Gobierno Vasco, SPRI, y/o sociedades participadas por los mismos, tanto durante la vigencia del contrato como al término de este.