Expediente nº: 2023005 Armonizado

Objeto de la contratación: Servicio de soporte de infraestructuras y seguridad para el Basque CyberSecurity Centre

Documento: Pliego de prescripciones técnicas particulares

ÍNDICE

1. CONTEXTO 3
2. OBJETO DE LA CONTRATACIÓN 3
3. ALCANCE DEL SERVICIO 3
3.1. Consideraciones 3
3.2. Entorno Tecnológico 4
3.3. Actualización tecnológica 5
3.4. Características del servicio 5
4. REQUISITOS DEL SERVICIO 6
4.1. Capacidad de soporte técnico de sistemas e infraestructuras 6
4.1.1. Operación y administración 6
4.1.2. Monitorización 6
4.1.3. Mantenimiento 7
4.2. Capacidad de gestión de incidentes 8
4.2.1. Preparación 8
4.2.2. Detección y análisis 8
4.2.3. Contención, erradicación y recuperación 10
4.2.4. Actividades post-incidente 11
4.3. Capacidad de gestión del riesgo 11
4.3.1. Actualización del Plan de Continuidad 11
4.3.2. Pruebas de continuidad 11
4.4. Capacidad de gestión de vulnerabilidades 11
4.4.1. Análisis de vulnerabilidades 11
4.4.2. Priorización de vulnerabilidades 12
4.4.3. Parcheo y remediación de las vulnerabilidades 12
4.5. Capacidad de soporte técnico experto 12
4.6. Servicios bajo demanda 12
4.6.1. Bolsa de horas 12
4.6.2. Respuesta coordinada ante incidentes críticos 13
5. EQUIPO DE TRABAJO 13
6. ORGANIZACIÓN DEL SERVICIO 14
6.1. Gestión del servicio 14
6.1.1. Herramienta de gestión ITSM 14
6.1.2. Seguimiento del servicio 15
6.1.3. Reporte de actividad 15
6.1.4. Horario y lugar de prestación del servicio 16
6.1.5. Acuerdo de Nivel de Servicio 16
6.2. Plan de transición 18

1. CONTEXTO

El BASQUE CYBERSECURITY CENTRE (en adelante, "**BCSC"**), es una iniciativa que se enmarca dentro de la Agencia Vasca De Desarrollo Empresarial - Enpresen Garapenerako Euskal Agentzia (en adelante "**SPR**I"), ente público de derecho privado 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 Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad abarca 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 Comité Permanente del BCSC.

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 CSIRT, por sus siglas en inglés "Computer Security Incident 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 expediente es la contratación de un servicio de soporte de infraestructuras y seguridad para garantizar la seguridad y el correcto funcionamiento de todos los sistemas y elementos que componen la Infraestructura TIC del BCSC.

3. ALCANCE DEL SERVICIO

3.1. Consideraciones

Actualmente el BCSC dispone de un servicio de soporte técnico para la administración y gestión de sus sistemas e infraestructuras y otro servicio, diferenciado, para la monitorización y operación de su sistema de gestión de eventos e información de seguridad (en adelante "SIEM", *del inglés Security Information and Event Management*) y su plataforma EDR ("Endpoint Detection and Response"). Tanto el SIEM como el EDR forman parte de los sistemas e infraestructuras del BCSC, pero debido a su reciente adquisición todavía no están integrados en el servicio de soporte técnico.

El servicio objeto de la presente licitación tendrá un alcance global, incluyendo todos los sistemas y elementos que componen la infraestructura TIC del BSCS detallados en el apartado 3.2. De este modo, la convergencia de ambos servicios en uno solo facilitará la gestión y agilizará los tiempos de respuesta, lo que a su vez redundará en una mejora de la seguridad de las infraestructuras del BCSC, ya que el tiempo de respuesta ante incidentes de seguridad es un aspecto crítico.

Así mismo, la unificación de ambos servicios favorecerá las sinergias que facilitarán la identificación de acciones de mejora en los sistemas e infraestructuras del BCSC y permitirá una optimización en los costes derivada de la compartición de recursos.

En resumen, la convergencia de los dos actuales servicios permitirá una mayor eficiencia en la gestión del servicio global, que podrá ser prestado con una perspectiva integral.

3.2. Entorno Tecnológico

El alcance del servicio objeto de la contratación incluye todos los sistemas y elementos que componen la Infraestructura TIC del BCSC. En la siguiente tabla se detalla este entorno tecnológico:

Categoría	Tecnología	Detalle
Comunicaciones	- Cisco	- (3) x Switches
Seguridad	- Palo Alto - Fortinet	- (2) x Appliances en HA - (2) x Appliances en HA
Hiperconvergencia	- Nutanix	- (3) x Nodos
Virtualización	- Nutanix Acropolis - VMWare	- - - (2) x Hosts físicos
Almacenamiento	- HPE	- (1) x SAN
Backup	- CommVault	- (1) x Servidor
WiFi	- Aruba	- (3) x Puntos de Acceso
Sistemas Operativos	- Servidores con Sistema Operativo Linux - Servidores con Sistema Operativo Windows	- 60 servidores virtuales - 30 servidores virtuales
Productos Específicos	- Microsoft Active Directory Domain Services - Aruba Clear Pass Policy Manager - Plataforma ProactivaNET	- (2) x DC - (2) Aruba CPPM - (1) sistema
Software	- Herramientas auxiliares y software específico para la gestión de las infraestructuras (FreeIPA, Zabbix, etc.)	- -
SIEM	- Splunk	- (1) sistema
EDR	- Cybereason	- (1) sistema
WAF	- Imperva en modalidad SaaS	- (10) x Dominios

Los ordenadores personales, tanto portátiles como ordenadores de sobremesa, se incluyen parcialmente dentro del alcance del contrato. El alcance para este tipo de dispositivos está limitado a las actividades derivadas de la gestión de incidentes si el incidente de seguridad afecta o tiene su origen en este tipo de dispositivos. Así mismo, los ordenadores personales están incluidos en el alcance de la gestión de vulnerabilidades en fase de análisis y priorización, quedando excluidos de la fase de parcheo y remediación. No son objeto del presente contrato las tareas cotidianas de microinformática. Actualmente disponemos de 25 ordenadores personales, todos ellos dotados con sistema operativo Windows 10.

Por último, también será objeto de este expediente el nuevo equipamiento que pueda adquirirse, así como aquellos sistemas e infraestructuras cuya responsabilidad asuma el BCSC durante la duración del presente contrato.

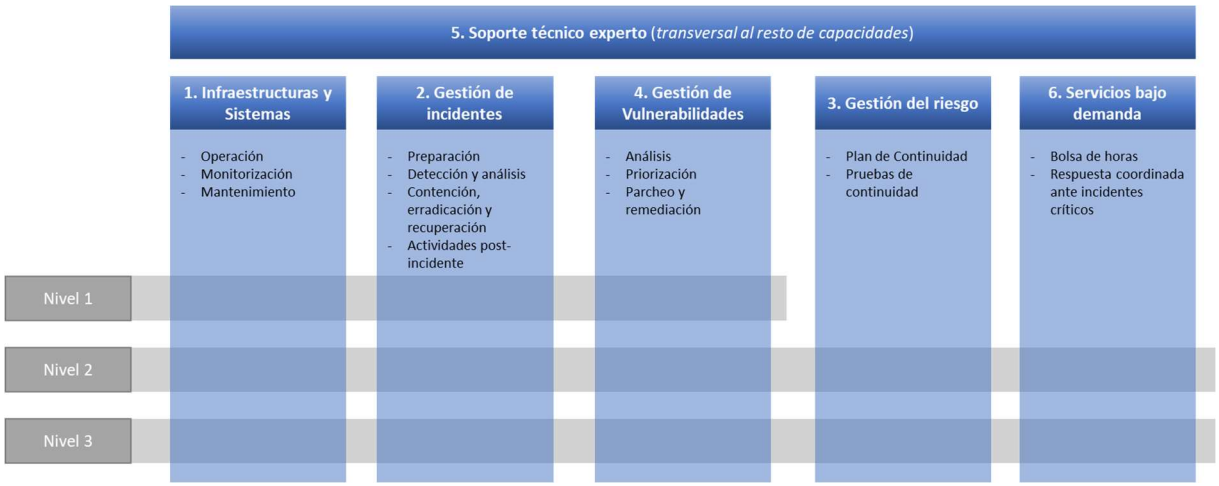
3.3. Actualización tecnológica

En el transcurso de la ejecución del contrato el servicio deberá recepcionar las nuevas tecnologías que vayan surgiendo a lo largo de su vigencia, fijándose para cada una los plazos en los que se deberán asumir.

Adicionalmente la empresa adjudicataria deberá formar y, si procediera, certificar durante ese plazo a un mínimo de los técnicos adscritos al servicio.

3.4. Características del servicio

La empresa que resulte adjudicataria del contrato deberá prestar el servicio de soporte de infraestructuras y seguridad de todos los sistemas e infraestructuras del BCSC. En la siguiente figura se recogen las capacidades demandadas, desarrolladas posteriormente a lo largo del presente pliego de prescripciones técnicas:



Capacidades del servicio

A continuación, se detalla el alcance del contrato, cuyo contenido se complementa con los requerimientos descritos en el apartado 4.

- **1. Capacidad de soporte técnico de los sistemas e infraestructuras** del BCSC, incluyendo:
    - La operación, gestión, administración y monitorización de todos los sistemas e infraestructuras del BCSC, así como la generación y actualización de la documentación técnica correspondiente.
    - El mantenimientos correctivo, preventivo y evolutivo de acuerdo con los niveles de servicio descritos en el pliego de prescripciones técnicas.
    - Los escalados a fabricantes utilizando los contratos de mantenimiento existentes.
- **2. Capacidad de gestión de incidentes** de seguridad, incluyendo:
    - Las tareas de preparación para responder adecuadamente ante cualquier incidente de seguridad.
    - Las operaciones de seguridad para la monitorización de los eventos, así como el análisis, identificación, detección y alerta temprana de incidentes de seguridad. Incluyendo la explotación activa de las herramientas específicas de seguridad.
    - Las tareas de contención, erradicación y recuperación ante incidentes de seguridad.
    - La identificación de las lecciones aprendidas después de un incidente.
- **3. Capacidad de gestión del riesgo**, incluyendo:
    - La revisión y actualización anual del Plan de Continuidad para los servicios TIC.
    - La actualización de los planes de recuperación y la realización de las pruebas de continuidad correspondientes.

- **4. Capacidad de gestión de vulnerabilidades**, incluyendo:
    - La realización de escaneos periódicos sobre todos los elementos y sistemas que componen la infraestructura del BCSC.
    - El análisis y priorización de las vulnerabilidades identificadas.
    - El parcheo y la remediación de las vulnerabilidades.
- **5. Capacidad de soporte técnico experto**, incluyendo:
    - El apoyo técnico y la coordinación con todos los grupos y equipos involucrados en el contrato.
- **6. Servicios bajo demanda**, incluyendo:
    - Una bolsa de horas para actividades que tengan relación directa con el contrato y no estén incluidas en su alcance.
    - La respuesta coordinada ante incidentes de seguridad críticos.

4. REQUISITOS DEL SERVICIO

4.1. Capacidad de soporte técnico de sistemas e infraestructuras (en adelante, "**Servicio 1**")

4.1.1. Operación y administración

La propuesta para la capacidad de soporte técnico deberá contemplar la operación, gestión y administración de la infraestructura del BCSC detallada en el apartado 3.2. Se realizarán todas las tareas solicitadas por el BCSC en este ámbito, así como todas aquellas que el adjudicatario considere necesarias para el correcto funcionamiento de los sistemas, incluyendo el tratamiento y seguimiento de los tickets generados desde otras capacidades objeto de este contrato.

Sin ánimo de ser exhaustivos, las tareas de operación y administración pueden implicar acciones como desplegar nuevos servidores virtuales, realizar y restaurar backups, gestionar cuentas de usuarios, bastionar los sistemas, gestionar los activos o cambiar la configuración, actualizar y parchear sistemas y otros elementos que componen la infraestructura del BCSC, etc.

Así mismo, el adjudicatario deberá mantener actualizada la documentación existente y generar los nuevos documentos (p. Ej., Topología de interconexión, configuraciones, diagramas de red, diagrama de flujo de datos, mapas del sistema, etc.) que se consideren necesarios para mantener debidamente documentados los sistemas e infraestructuras objeto del servicio. Dentro del servicio se incluirá al menos una actividad de actualización anual de toda la documentación técnica generada y existente que haga referencia a los sistemas que componen la infraestructura.

Desde la operación se apoyarán y se dará soporte a todas las actividades derivadas de la gestión de incidentes, gestión del riesgo y gestión de vulnerabilidades. Igualmente se colaborará con el soporte técnico experto en aquellas tareas que así lo requieran.

La operación será realizada de forma peticionada por el BCSC o consensuada entre ambas partes cuando el adjudicatario lo proponga de forma proactiva. Todas las tareas realizadas, tanto las solicitadas por parte del BCSC como aquellas propuestas proactivamente por el adjudicatario, deberán quedar debidamente documentadas y registradas en las herramientas de gestión ITSM del BCSC.

4.1.2. Monitorización

La propuesta para la capacidad de soporte técnico también deberá incluir la monitorización continuada de todos los sistemas y elementos que componen la infraestructura del BCSC y que están detallados en el apartado 3.2.

El objetivo de la monitorización será la detección temprana de incidencias en cualquier elemento de la infraestructura, de modo que ésta pueda ser atendida y quede resuelta de la forma más efectiva y en el menor tiempo posible. Cuando se detecte una posible incidencia, el adjudicatario generará el ticket correspondiente en la herramienta de gestión ITSM del BCSC.

El adjudicatario proporcionará y mantendrá actualizado un dashboard del estado de salud de la infraestructura de forma que sea posible consultarlo por parte del BCSC.

Actualmente el BCSC dispone de un sistema de monitorización basado en la herramienta Zabbix. La empresa adjudicataria deberá utilizar y mantener dicho sistema, sin perjuicio de que también pueda integrar su propia herramienta de monitorización previo consenso y aprobación por parte del BCSC. La herramienta deberá monitorizar el estado general de todos los sistemas y elementos que componen la infraestructura objeto del contrato, sus consumos, paradas, fallos, disponibilidad de los servicios, etc., y se integrará con la herramienta de gestión ITSM del BCSC para la apertura automática de incidencias.

4.1.3. Mantenimiento

La empresa adjudicataria deberá mantener todos los sistemas y elementos que componen la infraestructura del BCSC y que están detallados en el apartado 3.2.

Se incluirán todas las actividades derivadas de la realización de los mantenimientos correctivos, preventivos y evolutivos, así como el escalado a fabricante, que deberán quedar debidamente documentadas y registradas en la herramienta ITSM del BCSC.

El servicio incluirá la documentación y/o actualización de la documentación con aquellas tareas recurrentes que sean necesarias para efectuar los mantenimientos.

Mantenimiento correctivo

La propuesta deberá incluir el mantenimiento correctivo cuyo objetivo será la solución de deficiencias en cualquiera de los equipos incluidos en el contrato, entendiendo deficiencia como algo que debería funcionar o estar correcto y que no lo está.

El mantenimiento correctivo deberá incluir la realización de todas las tareas necesarias para la resolución de las incidencias e incidentes, tratando siempre de restaurar el servicio en el menor tiempo posible, minimizando el impacto y adoptando las medidas necesarias para prevenir la repetición de estas.

En aquellos casos en los que se determine que la responsabilidad de resolver la incidencia excede el alcance del contrato la empresa adjudicataria realizará el escalado a la tercera parte correspondiente. Los escalados estarán claramente definidos y procedimentados por parte del BCSC para evitar cualquier tipo de confusión. El escalado consistirá en comunicar la incidencia a través de los canales definidos en el procedimiento.

Mantenimiento preventivo

El licitador deberá incluir en su propuesta el mantenimiento preventivo cuyo objetivo será garantizar el buen funcionamiento y fiabilidad de los equipos incluidos en contrato y detectar posibles focos de problemas que puedan surgir en el futuro.

El adjudicatario deberá realizar dos informes anuales en los que reflejará el estado actual del equipamiento objeto del contrato y realizará una propuesta orientada a mejorar el rendimiento y/o disponibilidad de la infraestructura.

El informe incluirá el análisis de los siguientes aspectos como mínimo: revisión hardware, versiones software, fechas de fin de vida (tanto software como hardware), existencia de bugs y/o vulnerabilidades, configuraciones realizadas, estado y consumo de licencias y rendimiento de los equipos, así como del conjunto de la infraestructura.

Tras la recepción de los informes el BCSC analizará los resultados y estudiará la conveniencia de llevar a cabo las acciones propuestas. Si la decisión es favorable a la ejecución de alguna de las propuestas, y su ejecución no supone la modificación de las licencias ni la adquisición de nuevos componentes, dicha ejecución será realizada por el adjudicatario, sin que ello conlleve coste alguno.

Mantenimiento evolutivo

El licitador deberá incluir una propuesta de mantenimiento evolutivo para realizar las modificaciones necesarias en la infraestructura con el objeto de aumentar o mejorar las funcionalidades del sistema, ya sea por las necesidades del BCSC o por otras causas como pueden ser, por ejemplo, cambios normativos, fin de soporte de versiones, etc.

El BCSC analizará las propuestas y la conveniencia de llevar a cabo las acciones propuestas. Si la decisión es favorable a la ejecución de alguna de las propuestas, y su ejecución no supone la modificación de las licencias ni la adquisición de nuevos componentes, dicha ejecución será

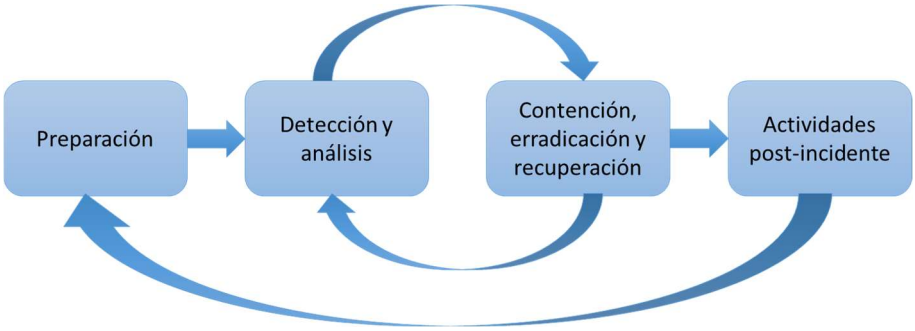
realizada por el adjudicatario, sin que ello conlleve coste alguno.

Escalado a fabricante

Cada uno de los sistemas y elementos que componen la infraestructura del BCSC dispone de un contrato de mantenimiento con el correspondiente fabricante. Cuando sea necesario, la empresa adjudicataria será la responsable de realizar los escalados a fabricante a través de las herramientas disponibles en cada caso.

4.2. Capacidad de gestión de incidentes (en adelante, "**Servicio 2**")

La capacidad de gestión de incidentes cubrirá todo el ciclo de vida de la respuesta ante incidentes de acuerdo con las siguientes fases:



Gestión de incidentes

4.2.1. Preparación

El servicio incluirá la preparación de todos los procedimientos de respuesta, incluyendo la revisión y actualización del Plan de Respuesta ante Incidentes. Adicionalmente, como guía de referencia sobre las acciones a llevar a cabo, se diseñarán los Playbooks correspondientes.

Se deberá implementar un catálogo de capacidades y de tareas asociadas a partir del análisis de las herramientas disponibles en el BCSC, a fin de hacer una explotación optima de las mismas y de identificar gaps a la hora de dar respuesta a los posibles incidentes que puedan surgir.

Dentro del alcance del contrato, la empresa adjudicataria deberá definir un procedimiento particular para la identificación y tratamiento de incidentes críticos, que deberá validarse por el BCSC. Se entiende por incidente crítico aquel que identifica una situación de alto riesgo para la seguridad de los servicios y/o del negocio del BCSC.

Todas las guías y planes definidos deberán ser aprobados por el BCSC y se probarán con periodicidad anual. El objetivo de las pruebas será verificar las capacidades de respuesta y analizar el funcionamiento de los workflow de respuesta implementados. Dichas pruebas podrán incluir una parte práctica cuyo objetivo será verificar que las medidas de seguridad y las capacidades de detección implementadas se comportan según lo esperado.

4.2.2. Detección y análisis

La empresa adjudicataria realizará la explotación de las tecnologías SIEM y EDR. Actualmente el BCSC dispone de un SIEM, del fabricante Splunk, que integra las fuentes de logs de todos los sistemas y componentes de la infraestructura TIC del BCSC y de una plataforma EDR, del fabricante Cybereason, que también está integrada en el SIEM.

El objetivo principal del servicio será la monitorización de eventos de seguridad, identificación, detección, alerta temprana y respuesta ante incidentes, apoyándose principalmente en las tecnologías SIEM y EDR desplegadas.

La empresa adjudicataria deberá establecer los mecanismos de control y ejecutar las actividades asociadas que sean necesarias para asegurar el correcto funcionamiento de los agentes en los elementos cubiertos tanto por el SIEM como por el EDR, identificando aquellos que no estén debidamente cubiertos por estas herramientas, no cuenten con el software o políticas actualizadas, etc.

Plataforma SIEM

Se realizará la monitorización y correlación de los eventos generados en el SIEM, identificando y analizando los posibles incidentes de seguridad para determinar su alcance, evaluar su impacto y

proponer medidas correctivas o de remediación. La empresa adjudicataria realizará todas las comprobaciones necesarias para la catalogación de incidentes de seguridad o falsos positivos. Todos los incidentes deberán quedar debidamente documentados y registrados en la herramienta de gestión ITSM del BCSC.

La empresa adjudicataria consensuará con el BCSC una metodología de trabajo para la correcta explotación del SIEM. Dicha metodología deberá permitir, al menos:

- Aportar mediante la configuración de dashboards una visión del estado de fuentes, eventos y salud de la propia plataforma, así como de la información del resto de herramientas del ecosistema TI del BCSC que cuenten con capacidades de integración directa.
- Realizar la correcta integración de nuevas fuentes de eventos y su correspondiente mapeo de eventos que permita implementar con garantías los casos de uso.
- Realizar las búsquedas necesarias que complementen las labores de Treat Hunting o de investigaciones ante incidentes, documentándolas y generando una base de conocimiento que ayude a los analistas en su trabajo.
- Establecer los mecanismos de control y ejecutar las actividades asociadas que sean necesarias para asegurar el correcto funcionamiento de los agentes en los elementos cubiertos por el SIEM, identificando aquellos que no estén debidamente cubiertos por esta herramienta, no cuenten con el software actualizadas, etc…

Plataforma EDR

A través de la explotación de la plataforma EDR se realizará la detección y el análisis de todas las actividades sospechosas y comportamientos anómalos en los endpoints. Para ello la empresa adjudicataria consensuará con el BCSC una metodología de trabajo que analice todas las alertas y eventos que vayan apareciendo en la plataforma de forma que, al menos:

- Se descarten las no relevantes, las detectadas por error o que sean motivadas por actividades necesarias para el normal funcionamiento del BCSC, ajustando la plataforma o proponiendo acciones concretas para que la aparición de estas no se repita, quedando además todo ello registrado.
- Se configure la herramienta y defina un mecanismo para el correcto tratamiento de aquellas que requieran de acciones inmediatas por ser especialmente relevantes bien por su nivel de criticidad o por su naturaleza.
- Se identifiquen y analicen actividades sospechosas o comportamientos anómalos en los endpoints, en caso de endpoints comprometidos la empresa adjudicataria deberá registrar el incidente en la herramienta de gestión ITSM del BCSC y activar las capacidades de gestión de incidentes.
- Configurar un dashboard que aporte una visión del estado de la plataforma, de las actividades identificadas y realizadas, del estado de salud de los agentes y equipos (Reportando – Aislados – Etc.).

Adicionalmente, la empresa deberá realizar las pruebas necesarias (al menos con periodicidad anual) que aseguren el correcto funcionamiento del procedimiento para la ejecución de un DFIR a través del EDR con recopilación y análisis de evidencias ante un incidente de seguridad.

Casos de uso

En lo relativo a los casos de uso, el servicio incluirá tanto la adaptación de los casos de uso existentes como la definición de nuevos casos de uso, cuyo origen podrán ser solicitudes realizadas por el BCSC para cubrir casos concretos que se necesiten o propuestas proactivas de la empresa adjudicataria basadas en su propia experiencia. La empresa adjudicataria deberá proponer un plan de análisis de las capacidades actuales y tras ello definir una hoja de ruta de implementación de nuevos casos de uso que las mejoren.

Actualmente el BCSC utiliza el framework MagMa para la gestión y definición de casos de uso, apoyándose y mapeando con ATT&CK de MITRE para completar el mapa de capacidades del BCSC. El adjudicatario deberá asumir esta metodología de trabajo inicialmente, pudiendo proponer a futuro mejoras e incluso su sustitución por otra, ejecutando el correspondiente plan de transición que deberá tener el mínimo impacto sobre la operativa y capacidades existentes en ese momento.

Se deberá presentar una metodología que asegure la correcta implementación de los casos de uso de acuerdo con lo indicado en el párrafo anterior, dicha metodología debe cubrir todo el ciclo de vida del caso de uso y asegurar al menos:

- Cumplimiento de los requisitos de la nomenclatura establecida.
- Correcta implementación del caso de uso sobre la herramienta incluyendo las actividades de integración de nuevas fuentes o eventos en caso de ser necesarios.
- Verificación del correcto funcionamiento del caso de uso, indicando y documentando las pruebas para replicar la amenaza. (Prueba de concepto).
- Ajuste de los umbrales y filtros para evitar alertas excesivas o falsos positivos.
- Ajuste del caso de uso para que la información aportada sea lo más completa y accesible en las fases de análisis.
- Documentación del caso en los correspondientes documentos de control del servicio, incluyendo fase del desarrollo (Pre-Pro), viabilidad de la implementación del caso, etc….
- Definición del workflow de respuesta y sus tareas asociadas, con la correspondiente validación por parte del BCSC.
- Verificación de que el caso de uso es correctamente, comunicado, registrado y atendido en las diferentes herramientas de ticketing y por los grupos implicados.

Inteligencia y Threat Hunting.

El servicio también deberá contemplar la integración con los feeds de inteligencia propios de la empresa adjudicataria, así como de aquellos procedentes de otras fuentes externas.

El servicio incluirá actividades proactivas de Threat Hunting, para la búsqueda proactiva de amenazas y comportamientos anómalos con la explotación de la telemetría e información obtenida de las fuentes, tanto sobre el EDR como sobre el SIEM. Estas actividades podrán tener su origen tanto en solicitudes del BCSC para cubrir casos concretos como en propuestas proactivas por parte de la empresa adjudicataria en base a su experiencia y, sobre todo, a su información de inteligencia disponible.

Se debe realizar una propuesta metodológica de trabajo por parte de la empresa adjudicataria que englobe las áreas anteriormente citadas y que describa el enfoque que tiene para cubrir este servicio en el BCSC.

4.2.3. Contención, erradicación y recuperación

El servicio incluirá la ejecución de las medidas propuestas, así como cualquier otra actuación correctiva necesaria para la contención, erradicación y recuperación en caso de incidentes. Dichas acciones podrán realizarse sobre cualquiera de los sistemas y elementos identificados en el apartado 3.2.

El objetivo de la fase de contención será limitar el daño y prevenir un impacto mayor. Para ello la empresa adjudicataria realizará todas las actividades necesarias para que el incidente no se propague y no genere más daños a la información o a la propia infraestructura.

Una vez contenido el incidente, durante la fase de erradicación la empresa adjudicataria deberá realizar todas las tareas necesarias para eliminar los componentes que causaron el incidente. Así mismo, se identificarán todos los hosts afectados y se procederá también a su erradicación con el objetivo de evitar que algún componente del incidente permanezca y pueda desencadenar futuros incidentes.

Finalmente, durante la fase de recuperación, la empresa adjudicataria realizará todas las tareas necesarias para restablecer el funcionamiento normal de los sistemas. Incluyendo las pruebas y tareas de verificación para validar que los sistemas se encuentran finalmente 100% operativos. Sin ánimo de ser exhaustivos, las tareas de recuperación pueden implicar acciones como restaurar sistemas a partir de copias de seguridad limpias, reconstruir sistemas desde cero, reemplazar los archivos comprometidos por versiones limpias, instalar parches, cambiar contraseñas o reforzar la seguridad del perímetro de la red (por ejemplo, conjuntos de reglas de cortafuegos, listas de control de acceso al router, etc.).

Todos los incidentes deberán quedar debidamente documentados y registrados en la herramienta de gestión ITSM del BCSC.

4.2.4. Actividades post-incidente

La empresa adjudicataria realizará un análisis posterior al cierre de cada uno de los incidentes de seguridad gestionados. El objetivo del análisis post-incidente será aprender de lo sucedido y limitar las posibilidades de que el incidente vuelva a producirse. Las lecciones aprendidas serán debidamente documentadas y puestas en común con el BCSC.

Este análisis también servirá para identificar formas de mejorar tanto las medidas de seguridad como la propia capacidad de gestión de incidentes. La empresa adjudicataria deberá aplicar las mejoras de seguridad identificadas, previa validación por parte del BCSC, siempre y cuando su ejecución no suponga la modificación de las licencias ni la adquisición de nuevos componentes.

4.3. Capacidad de gestión del riesgo (en adelante, "**Servicio 3**")

La empresa adjudicataria deberá realizar la asistencia técnica en materia de gestión de riesgos, con el objetivo de gestionar aquellos riesgos que podrían impactar en la continuidad de los servicios TIC del BCSC. Anualmente elaborará el cronograma y planificará las actividades a desarrollar, así como los entregables a presentar durante esa anualidad. La propuesta deberá ser validada por el BCSC e incluirá al menos las siguientes actividades:

4.3.1. Actualización del Plan de Continuidad

Actualmente se dispone de un Plan de Continuidad para los servicios TIC. Dicho plan se deberá revisar y actualizar con una periodicidad anual. Esta tarea incluirá la identificación de los nuevos servicios/procesos críticos TIC que se hayan puesto en marcha, así como la actualización de los existentes. Así mismo se actualizarán tanto el Análisis de Impacto en el Negocio (BIA), como el Análisis de Riesgos (AR), y se revisarán las estrategias de continuidad, actualizando las estrategias ya implantadas e identificando nuevas estrategias que permitan cumplir con los requisitos de continuidad.

4.3.2. Pruebas de continuidad

La empresa adjudicataria deberá revisar el Plan de Recuperación, incluyendo la actualización de los procedimientos de contingencia existentes, así como la definición de los nuevos procedimientos que sean necesarios para responder y recuperar los servicios TIC.

Así mismo, se revisarán y actualizarán los Planes de Pruebas existentes, cuyo objetivo es detallar las actividades de recuperación, y se generarán nuevos planes que sean necesarios en caso de ser necesario.

Finalmente, con el objetivo de validar los Planes de Pruebas, la empresa adjudicataria organizará y participará activamente en un simulacro anual.

4.4. Capacidad de gestión de vulnerabilidades (en adelante, "**Servicio 4**")

La capacidad de gestión de vulnerabilidades cubrirá por completo el ciclo de vida de las vulnerabilidades de todos los elementos y sistemas que componen la infraestructura del BCSC.

4.4.1. Análisis de vulnerabilidades

La empresa adjudicataria deberá realizar un análisis de vulnerabilidades de todos los elementos y sistemas que componen la infraestructura del BCSC. La periodicidad de los escaneos se consensuará con el BCSC y será, al menos, mensual. Sin perjuicio de que puedan solicitarse escaneos bajo demanda en determinadas circunstancias.

Para la realización de los escaneos la empresa adjudicataria deberá utilizar una plataforma de gestión de vulnerabilidades capaz de realizar el análisis de la postura de seguridad de los sistemas de BCSC. Del mismo modo, deberá ser capaz de analizar sistemas desde la red interna del BCSC y desde Internet. La plataforma deberá analizar tanto vulnerabilidades genéricas de sistemas como específicas de entorno web.

La solución de gestión de vulnerabilidades deberá contemplar la existencia de alguna sonda en la nube para analizar el direccionamiento expuesto a Internet, y deberá permitir desplegar sondas en distintas zonas de red para analizar el direccionamiento de dichas zonas de red, así como optimizar el tráfico generado durante los análisis. El personal del BCSC deberá tener acceso a la consola de administración de la herramienta, con posibilidad de hacer uso de esta, si fuera preciso.

En cualquier caso, la gestión y administración de la herramienta será realizado en su totalidad por el personal de la empresa adjudicataria.

La solución de gestión de vulnerabilidades propuesta deberá permitir descubrir los activos existentes en las redes a analizar y realizar un seguimiento continuo del estado de la seguridad de dichos activos, otorgando una visión detallada de la situación de cada uno de esos activos, así como una visión global que abarque a todos.

4.4.2. Priorización de vulnerabilidades

La empresa adjudicataria realizará un análisis de los resultados obtenidos y un primer triaje descartando falsos positivos. Así mismo, las vulnerabilidades identificadas deberán priorizarse no solo en términos de su valoración CVSS, sino también en base al nivel de riesgo asociado a cada una de ellas. El nivel de riesgo se cuantificará en base a indicadores de amenaza e información de inteligencia.

Adicionalmente la empresa adjudicataria aportará un análisis experto que vaya más allá de lo que aporten las herramientas, debiendo contar con conocimientos específicos, para poder revisar manualmente entornos en caso necesario y velará porque no se escalen falsos positivos.

En caso de la aparición de una vulnerabilidad especialmente crítica para los sistemas del BCSC el servicio deberá comunicarla dentro en un plazo inferior a 24h y comenzar con su seguimiento y atención prioritaria. Informando de manera continua y periódica de las medidas de mitigación y/o remediación que se vayan identificando y colaborando en determinar si pueden ser aplicadas o no en el entorno del BCSC y su impacto. En caso de que fuese viable su implementación, deberá aportar el conocimiento necesario y colaborar en dicha actividad. Esta casuística está enfocada a eventos tipo 0-Day, o vulnerabilidades explotadas de forma especialmente activa por algún motivo.

4.4.3. Parcheo y remediación de las vulnerabilidades

El BCSC analizará los resultados presentados por la empresa adjudicataria y estudiará la conveniencia de llevar a cabo las acciones de parcheo y/o remediaciones propuestas. Si la decisión es favorable a la ejecución de alguna de las propuestas, y su ejecución no supone la modificación de las licencias ni la adquisición de nuevos componentes, dicha ejecución será realizada por el adjudicatario, sin que ello conlleve coste alguno.

Una vez completadas estas tareas la empresa adjudicataria validará las acciones de remediación y/o mitigación comprobando que han sido correctamente implementadas mediante la verificación de las vulnerabilidades, ya sea de forma manual, escaneo recurrente, o bajo demanda.

Todas las acciones de parcheo y/o remediación deberán quedar debidamente documentadas y registradas en la herramienta de gestión ITSM del BCSC.

4.5. Capacidad de soporte técnico experto (en adelante, "**Servicio 5**")

La capacidad de soporte técnico experto deberá ser prestada por un ingeniero/a con dedicación completa al contrato.

Será el interlocutor principal y responsable de la calidad del servicio en términos técnicos. Coordinando todos los equipos para proveer un servicio integral y apoyando en todas aquellas tareas técnicas que por su naturaleza o complejidad así lo requieran. Adicionalmente, estará abierto a las necesidades del BCSC para la resolución de consultas y la realización de las actividades que les sean encomendadas.

El soporte técnico experto estará involucrado en las actividades diarias del BCSC y participará activamente en las tareas de operación y administración de los sistemas e infraestructuras. Con objeto de facilitar esta última tarea la prestación de esta capacidad se realizará desde las dependencias del BCSC diariamente.

4.6. Servicios bajo demanda

A continuación, se detallan los servicios cuyo consumo se realizará bajo demanda del BCSC:

4.6.1. Bolsa de horas (en adelante, "**Servicio 6")**

El servicio incluirá una **bolsa de horas de 200 horas** para la realización de actividades que tenga relación directa con el contrato, pero queden fuera del alcance inicial del mismo. A continuación, se expone, a modo de ejemplo, una relación enunciativa y no limitativa de tareas que podrían

solicitarse:

- Participación en iniciativas del BCSC cuyo objeto contribuya a la mejora del servicio, como es puede ser el caso de role plays, ciberejercicios, etc.
- Automatización y optimización de tareas repetitivas como: la instalación de agentes, actualización de parámetros de configuración, comprobaciones periódicas, etc.
- Realización actividades tipo test de intrusión y pen-testing.
- Actividades relacionadas con la revisión en profundidad de políticas de las herramientas de seguridad, de red, del directorio activo, etc.
- Participación en pruebas de concepto de productos y valoración de cara a su posible implantación en el BCSC.
- …

4.6.2. Respuesta coordinada ante incidentes críticos (en adelante, "**Servicio 7**")

En caso de identificarse un incidente crítico, además de las tareas especificadas apartado 4.2. sobre la gestión de incidentes, la empresa adjudicataria proveerá un servicio especializado de análisis forense digital y respuesta ante incidentes. Este servicio especializado de respuesta ante incidentes críticos deberá incluir al menos:

- Análisis forense de los eventos, para determinar orígenes del ataque, medios utilizados y objetivos.
- Definición de las medidas de contención a aplicar, planes para la recuperación de los sistemas y preservación de evidencias.
- Implementación de las medidas de contención y recuperación indicadas.
- Servicios de asesoría y asistencia legal inicial, durante las tareas asociadas a la respuesta ante incidentes, como apoyo en la ejecución de medidas legales en caso de incidentes graves de seguridad o acciones derivadas de obligaciones normativas y/o regulatorias.
- Documentación e informe del incidente desde su identificación, impacto, a las medidas para su resolución y ajustes propuestos sobre el global del servicio.

El servicio especializado en caso incidente crítico se prestará a demanda, de forma remota o in-situ, según el impacto del incidente en cuestión y las necesidades de recuperación de sistemas que se determinen.

5. EQUIPO DE TRABAJO

La propuesta deberá incluir el detalle del equipo de trabajo propuesto que al menos deberá contemplar los siguientes roles y responsabilidades:

- Responsable del Servicio

  Persona encargada de ejercer las facultades de responsable del Servicio en lo referente al servicio contratado, siendo el interlocutor y responsabilizándose frente al BCSC de las personas que prestan el servicio.

- Soporte técnico experto

  Ingeniero/a con elevados conocimientos técnicos y capacidad de gestión que será el enlace con todos los grupos y equipo de trabajo implicados en el contrato. Así mismo, estará involucrado en las tareas del día a día del BCSC.

- Nivel 1

  Equipo de personas que prestarán la atención de primera línea, podrán responsabilizarse de aquellas tareas que requieran un menor grado de especialización.

- Nivel 2

  Especialistas en cada una de las tecnologías y servicios objeto del contrato para el escalado

de tickets que no puedan ser resueltos en primera instancia por el nivel 1.

- Nivel 3

  Expertos en cada una de las tecnologías y servicios objeto del contrato para el escalado de tickets que no puedan ser resueltos por el nivel 2. Se responsabilizarán de aquellas actividades que requieran un mayor grado de especialización, así como de aquellas peticiones de servicio, incidencias o incidentes que tengan una mayor complejidad.

Para cada una de las personas que componga el equipo de trabajo, excepto aquellas con rol de Nivel 1, se deberá indicar en qué roles participa, así como su dedicación y centro de trabajo desde donde prestará el servicio.

Las características del equipo de trabajo se justificarán mediante la utilización de la tabla correspondiente, según se indica en el pliego de cláusulas administrativas. Para el rol de Nivel 1 se incluirá una única fila que englobe todo el conocimiento y experiencia de los miembros que forman parte de ese equipo, es decir, **no será necesario incluir el desglose individual de cada uno de los miembros con rol de Nivel 1.**

NO DEBERÁ DETALLARSE NI DEDUCIRSE SI EL EQUIPO DE TRABAJO PROPUESTO ESTAR EN POSESIÓN DE ALGUNA DE LAS CERTIFICACIONES DETALLADAS EN LA CLÁUSULA 22.2.2 DE LAS CONDICIONES ESPECÍFICAS DEL PLIEGO ADMINISTRATIVO, DADO QUE ESTAS SERÁN OBJETO DE VALORACIÓN COMO CRITERIO EVALUABLE A TRAVÉS DE FÓRMULA.

El licitador se compromete, en caso de ser adjudicatario, a mantener el equipo, según lo establecido en el documento de Equipo de Trabajo, 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 BCSC, con la antelación necesaria en función de la criticidad del servicio, y en cualquier caso al menos 15 días naturales previos a la realización del cambio de recurso. En todo caso el sustituto o sustitutos tendrán un perfil igual o superior al ofertado, o recurso a sustituir.

BCSC 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.

6. ORGANIZACIÓN DEL SERVICIO

6.1. Gestión del servicio

6.1.1. Herramienta de gestión ITSM

El BCSC dispone de su propia herramienta de gestión ITSM. La gestión del servicio objeto del contrato se realizará exclusivamente con dicha herramienta. La empresa adjudicataria deberá asumir y adecuarse a ésta, para ello se le proporcionará un usuario de acceso a la misma con el que podrá desarrollar su trabajo. Adicionalmente, la herramienta también dispone de una API REST, para su integración con plataformas externas, que se pondrá a disposición de la empresa adjudicataria.

Se permitirá explotar la herramienta ITSM del BCSC mediante integraciones con la herramienta ITSM de la empresa adjudicataria. Cualquier coste derivado de dicha integración deberá ser asumido por la empresa adjudicataria y no podrá ser repercutido al servicio.

Cualquier acción realizada en el marco del proyecto por el adjudicatario, independientemente de su naturaleza, deberá quedar debidamente documentada y registrada en la herramienta ITSM del BCSC. Así mismo, los indicadores del servicio, incluyendo aquellos empleados en el cálculo del cumplimiento del Acuerdo de Nivel de Servicio establecido, se obtendrán de esta herramienta.

Del mismo modo, la apertura de cualquier incidencia, incidente o petición de servicio por parte del BCSC se realizará exclusivamente desde la herramienta del BCSC. Adicionalmente, la empresa adjudicataria pondrá a disposición del servicio un número de teléfono, operativo 24x7, para la atención de tickets de máxima prioridad.

6.1.2. Seguimiento del servicio

El adjudicatario realizará un seguimiento continuado del estado de las incidencias, incidentes y peticiones de servicio con objeto de identificar posibles incumplimientos en el nivel de servicio establecido. Cualquier desviación importante en este sentido deberá ser inmediatamente notificada a la persona designada por el BCSC para su tratamiento con el responsable del servicio. Del mismo modo, si el BCSC identificase desviaciones importantes en el nivel de cumplimiento del SLA este hecho se pondrá en conocimiento del responsable del servicio para su análisis.

Para asegurar la calidad del servicio la empresa adjudicataria realizará reuniones de seguimiento de manera periódica, su contenido concreto se acordará con el BCSC, siendo su objetivo y periodicidad mínima los detallados a continuación:

- Seguimiento técnico semanal, para la revisión de las actividades abordadas durante la semana.
- Seguimiento ejecutivo mensual, para el análisis en detalle de la actividad del periodo.
- Seguimiento estratégico semestral, para hacer un seguimiento del proyecto a nivel estratégico.
- Seguimientos técnicos específicos, para realizar el seguimiento de tareas específicas que requieran de una dedicación mayor. Su periodicidad podrá variar en función de las necesidades y del grado de madurez de los servicios asociados.

6.1.3. Reporte de actividad

El modelo de reporting permitirá verificar de forma continuada el estado del servicio y deberá contemplar como mínimo los aspectos detallados a continuación:

Informe mensual

La empresa adjudicataria realizará un informe de seguimiento mensual donde se detallarán las incidencias, incidentes y peticiones de servicios del periodo. El objetivo de dicho informe será asegurar la calidad final del servicio realizado y su contenido detallado se acordará entre la empresa adjudicataria y la persona designada por el BCSC.

El informe incluirá un resumen ejecutivo a alto nivel de los principales sucesos del periodo que servirá de cuadro de mando, permitiendo conocer el estado general del servicio, en lo relativo a la volumetría y evolución del servicio.

Adicionalmente, en el informe se incluirán anexos en los que se detallarán las actividades específicas correspondientes a las siguientes capacidades del servicio:

Soporte técnico de sistemas. Se incluirá el detalle de las incidentes y peticiones de servicios atendidas durante el mes, incluyendo su identificación, priorización, descripción, activos afectados, resolución, etc.

Gestión de incidentes. Se reflejarán todas las acciones relativas a la gestión de incidentes, con detalle de su identificación, priorización, descripción, activos afectados, nivel de riesgo si aplica, criticidad, etc. Aportando además evidencias, referencias documentales y recomendaciones para aquellas especialmente relevantes. Así mismo el informe incluirá un resumen ejecutivo a alto nivel de los principales hallazgos.

Gestión de vulnerabilidades. Se detallarán los resultados del análisis de las vulnerabilidades incluyendo las vulnerabilidades encontradas con detalle de su identificación, priorización, descripción de la vulnerabilidad, activos afectados, nivel de riesgo, valoración CVSS si existe, evidencias, referencias documentales, planes de mitigación y recomendaciones.

Mantenimiento preventivo

Los informes correspondientes a los mantenimientos preventivos se presentarán siguiendo las indicaciones detalladas en el apartado 4.1.3. del pliego de prescripciones técnicas.

Gestión del riesgo

La documentación y entregables correspondiente a la de gestión del riesgo se presentarán de acuerdo con lo descrito en el apartado 4.3. del pliego de prescripciones técnicas.

6.1.4. Horario y lugar de prestación del servicio

La capacidad de soporte técnico experto, descrito en el apartado 4.5., se prestará desde las dependencias del BCSC diariamente. En ese caso, los miembros del equipo desplazado a las oficinas de BCSC contarán con identificación que les acredite como personal de la Contratista y SPRI podrá requerir a la Contratista, en cualquier momento, justificación sobre el alta en Seguridad Social de este personal, que utilizará su propio material y equipos, salvo que por necesidad del servicio deba utilizar material de BCSC. El resto de las capacidades objeto del presente contrato se prestarán de forma habitual en las dependencias del adjudicatario, sin perjuicio de que haya ciertas situaciones en las que el BCSC pueda requerir la presencia de uno o varios de los miembros del equipo de trabajo en sus dependencias. Estas situaciones pueden venir derivadas de la criticidad de los trabajos a realizar o de una necesidad puntual del BCSC.

De manera específica las siguientes actividades se realizarán de forma presencial en las oficinas del BCSC y requerirán la participación del responsable del servicio, del soporte técnico experto y de los técnicos de nivel 2/3 involucrados en cada caso: reuniones de seguimiento mensuales, simulacros para verificar los planes de contingencia, intervenciones que por su alcance o impacto el BCSC considere conveniente realizar in-situ, ciberejercicios y otras situaciones análogas.

Los principales miembros del equipo que componen la capacidad de soporte técnico de sistemas e infraestructuras de nivel 2/3, deberán prestar el servicio desde una oficina técnica, situada a una distancia no superior a 150 Kms de las oficinas en las que se encuentra el BCSC (Parque Tecnológico de Miñano – 015010 Vitoria-Gasteiz - Araba), ubicación lo suficientemente cercana al BCSC para garantizar, ante cualquier eventualidad que pueda surgir, una presencia en las dependencias del BCSC en un plazo adecuado y en cualquier caso, no superior a una hora y media.

El servicio se prestará en horario continuado 24x7. No obstante algunos de los SLA se calcularán en horario continuado 24x7 y otros en horario laboral de acuerdo con lo detallado en el apartado 6.1.5.

A efectos de cálculo de los SLA en horario laboral se considerará el siguiente horario:

- Jornada partida (octubre a mayo):
    - Lunes a jueves: de 8:00 a 18:00
    - Viernes: de 8:00 a 15:00
- Jornada intensiva (junio a septiembre):
    - Lunes a viernes: de 8:00 a 15:00

6.1.5. Acuerdo de Nivel de Servicio

La empresa licitadora deberá proponer un modelo de acuerdo de nivel de servicio que garantice la prestación de los servicios contratados dentro de unos límites aceptables, comprometiéndose al menos a garantizar que los servicios serán prestados de acuerdo con los niveles mínimos que se detallan a continuación:

SLA para incidencias e incidentes

Prioridad	Descripción	Tiempo de respuesta	Tiempo de resolución/contención
Crítica	Pérdida o degradación de un servicio crítico	< 1 hora	< 3 horas (**horario 24x7**)
Alta	Pérdida de un servicio que no tiene consideración de crítico	< 2 hora	< 6 horas (horario laboral)
Media	Degradación de un servicio que impide trabajar adecuadamente	< 3 horas	< 12 horas (horario laboral)
Baja	Sin pérdida de servicio	< 6 horas	< 24 horas (horario laboral)

SLA para peticiones de servicio

Prioridad	Descripción	Tiempo de respuesta	Tiempo de resolución
Crítica	Peticiones urgentes o cuya no aplicación impide la puesta en marcha de una funcionalidad prioritaria	< 2 horas	< 8 horas (**horario 24x7**)
Alta	Petición cuya no aplicación impide la puesta en marcha de una nueva funcionalidad	< 3 horas	< 16 horas (horario laboral)
Media	Petición que permite el funcionamiento habitual del servicio	< 4 horas	< 24 horas (horario laboral)
Baja	Petición cuyo aplazamiento no afecta al funcionamiento habitual del servicio	< 8 horas	< 48 horas (horario laboral)

SLA para la gestión del riesgo

Por las características específicas de las actividades enmarcadas dentro de la gestión del riesgo el SLA aplicable para esas actividades será el siguiente:

Prioridad	Descripción	Retraso
Alta	Documentación y entregables presentados con la calidad suficiente sin retrasos respectos de las fechas previstas en el cronograma y en la planificación anual.	< 1 semana

Penalidades

En caso de incumplimiento, la penalización a aplicar será acumulativa tomando como base para el cálculo de los porcentajes una duodécima parte del precio de adjudicación. El primer incumplimiento de las incidencias o incidentes de prioridad media y baja no conllevará penalización y se registrará un apercibimiento que activará el modelo de penalizaciones en los sucesivos meses.

El modelo de penalización será el siguiente:

- Tickets de Prioridad Crítica:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 80%: Penalización 3%.
  - Cumplimiento < 80%: Penalización 5%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Crítica del mes.
- Tickets de Prioridad Alta:
  - Cumplimiento >= 95%: Sin penalización.
  - 95% > Cumplimiento >= 75%: Penalización 3%.
  - Cumplimiento < 75%: Penalización 5%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Alta del mes.
- Tickets de Prioridad Media:
  - Cumplimiento >= 90%: Sin penalización.
  - 90% > Cumplimiento >= 75%: Penalización 1%.
  - Cumplimiento <75%: Penalización 3%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Media del mes.
- Tickets de Prioridad Baja:
  - Cumplimiento >= 80%: Sin penalización.
  - 80% > Cumplimiento >= 70%: Penalización 1%.
  - Cumplimiento <70%: Penalización 3%.
  - Los porcentajes hacen referencia al total de tickets de Prioridad Baja del mes.

Se entenderá por ticket cualquier incidencia, incidente o petición de servicio. A pesar de que las fórmulas aplicables son las mismas, los indicadores se calcularán por separado para las incidencias, incidentes y las peticiones de servicio.

6.2. Plan de transición

La empresa licitadora deberá detallar en su oferta de forma clara y concisa su propuesta tanto de plan de transición de entrada al servicio como de salida al finalizar el contrato. Ninguna de estas fases de transición del servicio podrá suponer coste adicional alguno para el BCSC.

Los planes de transición propuestos deberán contemplar los siguientes requisitos:

- Se establece un período de devolución del servicio a realizar en el último mes de vigencia del contrato, para la eventualidad de que a la finalización se produjera un cambio de adjudicatario.
- La transición de entrada a este expediente, en su caso, deberá llevarse a cabo en las dos semanas iniciales de prestación efectiva del servicio.