Pliego de Prescripciones Técnicas

SERVICIO GESTIONADO DE OPERACIÓN DE CIBERSEGURIDAD DE TMB

Expediente: 15012999

Marzo de 2024
Versión 1.0

Solucions Corporatives
Àrea de Tecnologia

Ernest Costa Lluch
Responsable de Sistemes de Ciberseguretat

Índice de contenidos

1. Introducción

Transports Metropolitans de Barcelona (TMB) es la denominación común de las empresas Ferrocarril Metropolita de Barcelona, SA, Transports de Barcelona, SA, que gestionan la red de metro y bus del Área Metropolitana de Barcelona. También incluye las empresas Projectes i Serveis de Mobilitat, SA que gestiona el teleférico de Montjuïc; Transports Metropolitans de Barcelona, S. L., que gestiona productos tarifarios y otros servicios de transporte, así como la Fundació TMB, que vela por el patrimonio histórico de TMB y promueve los valores del transporte público a través de actividades sociales y culturales.

TMB depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) y OT (Sistemas Operacionales) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos ante daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la Ciberseguridad es garantizar la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de la información, así como la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC y OT deben estar protegidos contra amenazas de rápida evolución. Para garantizar la prestación continua de los servicios y defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios del entorno. Esto supone que, en función de las competencias de cada ámbito, los departamentos deban aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS, operado por Real Decreto 311/2022, de 3 de mayo), realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

2. Objeto

El presente contrato tiene por objeto la contratación de un Servicio de Ciberseguridad Gestionada que dé respuesta a las necesidades del grupo Transports Metropolitans de Barcelona (TMB), de acuerdo con las prescripciones técnicas que se describen en el presente pliego.

2.1. Alcance

El servicio cubre los ámbitos de ciberseguridad en general (IT y OT) de la totalidad de los servicios TIC de TMB. Asimismo, se incluyen tanto aquellas infraestructuras TIC que estén ubicadas en las instalaciones de TMB como aquellas que puedan estar en servicios externos subcontratados basados en Cloud.

Con este objetivo se utilizarán tanto las herramientas propias de TMB descritas en el pliego como herramientas que pueda aportar el adjudicatario.

Incluye una Oficina técnica que gestionará la totalidad del contrato, que se desglosará en los siguientes servicios:

a) Oficina Técnica de Operación de Ciberseguridad
b) Servicio de Operación de Ciberseguridad (SOC)
c) Vigilancia Digital
d) Equipo de Respuesta frente a Incidentes de Seguridad y análisis forense (CSIRT)
e) Administración técnica de plataformas de seguridad

Volumetrías

A efectos de ayudar a dimensionar los recursos necesarios para dar cobertura a los servicios del contrato se debe tener en cuenta que el orden de magnitud de los activos a gestionar es:

- Servidores: 1.000 (Linux/Windows)
- Clientes: 5.000
- Empleados: 9.000

3. Fases de la prestación del servicio

A continuación se describen las fases de la prestación del servicio:

- Fase de Recepción del servicio:

  Se entiende por fase de Recepción del servicio el período que va entre la entrada en vigor del contrato adjudicado al nuevo contratista y la transición de inicio de la asunción del servicio, con el acompañamiento del adjudicatario saliente (si todavía tiene contrato y por TMB).

- Fase de Devolución del servicio:

  Se entiende por devolución del servicio todas aquellas acciones precisas para traspasar en condiciones óptimas todo el servicio sin ninguna merma ni pérdida de funcionalidades al nuevo adjudicatario a la finalización o extinción prematura de este contrato.

3.1. Recepción del servicio

Actualmente TMB ya dispone de un servicio de SOC así como una serie de proyectos en marcha relacionados con ciberseguridad y por tanto el contrato debe prever un tiempo inicial de toma del servicio donde desarrollar las tareas preparatorias necesarias para garantizar una transición ordenada y sin interrupciones del servicio e iniciativas en proceso.

Importante recalcar que actualmente hay una serie de Casos de Uso (CdU) implementados que deberían revisarse en la etapa de recepción del proyecto, para adaptar/mejorar/evolucionar, para que las alertas se envíen al servicio de Monitorización 24x7 correspondiente, así como incorporar todos los CdU que pudieran faltar para las Best Practice que recomiende el proveedor (basado en su experiencia con otros clientes).

Aspectos mínimos a tener en cuenta en la toma del servicio:

- Revisión de los procesos y documentación existente
- Integración de los procesos de notificación de Service Desk
- Análisis/adaptación de casos de uso: biblioteca playbooks, alertas, falsos positivos,…
- Configuración de accesos y provisión de usuarios en los entornos requeridos.
- Identificación de contactos.
- Definición del modelo de gobernanza
- Definición del modelo de informes
- Matriz de escalados
- Definición del modelo de seguimiento de SLA's
- Cuadros de mando iniciales

En aquellos casos en los que no exista documentación previa necesaria para prestar el servicio, el contratista tendrá que planificar y ejecutar su elaboración, de acuerdo con los responsables TMB, y sin coste adicional alguno por TMB.

La dedicación y los recursos usados por el nuevo contratista dedicados al traspaso de conocimientos y asimilación del nuevo entorno y características del servicio serán sin coste adicional alguno por TMB.

El adjudicatario podrá hacer propuestas de nuevos elementos para la gestión y seguimiento del servicio o proponer mejoras en el servicio, y su implantación dependerá de la aprobación por parte de TMB.

3.2. Servicio regular

La fase regular se inicia una vez terminadas todas las tareas de la fase anterior y se extiende hasta la extinción del contrato y antes de la fase de devolución del servicio.

Todas las actividades que, como mínimo, deberá realizar se describen en el apartado 4 de descripción del servicio.

Adicionalmente el adjudicatario deberá presentar propuestas que permitan asegurar la evolución del servicio tanto desde el punto de vista tecnológico, como de gobernanza o incorporación de nuevas funcionalidades y tareas en el servicio.

Los mecanismos de evolución deben incluir información detallada sobre las pautas de activación, los instrumentos de seguimiento, integración de tareas y procedimientos de forma tanto reactiva como proactiva por parte del adjudicatario.

Aparte de los criterios generales, los mecanismos de evolución deben tener en cuenta la incorporación de nuevas funcionalidades que no se hayan previsto inicialmente o que la evolución del mercado y de la demanda hagan que TMB decida incorporarlas (nuevos servicios en la nube, nuevas aplicaciones, nuevos servicios de ciber-inteligencia, etc...).

3.3. Devolución del servicio

El proveedor deberá tener en cuenta que al final del contrato, será necesario realizar un traspaso de conocimiento, documentación, procedimientos, playbooks aplicados, etc, que forman parte del know-how de TMB, y que se deberá trasladar (y facilitar este traslado) al siguiente contrato, en caso de que fuera otro proveedor.

El proceso de offboarding debe contemplar:

- Formalizar fecha de finalización
- Programación del último reporte de servicio
- Desactivación de las integraciones TMB-Proveedor
- Desactivación de los accesos a los sistemas de TMB
- Desactivación de notificaciones

4. Descripción del servicio regular

4.1. Oficina Técnica

El objetivo de este servicio es colaborar con los equipos internos de TMB al supervisar, gestionar y optimizar las operaciones relacionadas con la seguridad de la organización, garantizando la protección de sus infraestructuras, activos y datos. Esta oficina se encargará de implementar y mantener sistemas y procedimientos de seguridad operativa, asegurando una respuesta efectiva frente a incidentes de seguridad y minimizando los riesgos asociados con las amenazas tanto internas como externas.

Con este objetivo en mente, el servicio se dimensionará para que cubra los siguientes aspectos:

- Coordinación, seguimiento y mejora continua del servicio
- Mantenimiento del SIEM
- Thread Hunting
- Gestión de vulnerabilidades
- Auditorías y pentesting
- Consultoría y Proyectos

4.1.1. Coordinación, seguimiento y mejora continua del servicio

Este proceso encargará de liderar, gestionar y controlar la evolución de los distintos servicios para ser más eficientes y eficaces en la ejecución de las tareas responsabilidad de cada ámbito, siempre con visión en el alineamiento de estas acciones con los objetivos de seguridad de TMB.

El servicio deberá mantener constantemente una coordinación de todos los servicios de esta contratación y poder trabajar de forma integrada con cliente.

El objetivo del servicio es ser el principal interlocutor del Servicio de Ciberseguridad Gestionada aportando una visión global de todos los servicios de seguridad contratados por TMB. Gestión de escalados y seguimiento de indicadores/SLAs, entrega de informes semanales y ejecutivos mensuales, etc. controlando la calidad extremo a extremo de acuerdo a los compromisos adquiridos y en general, de impulsar la evolución de los servicios de Seguridad del Cliente a lo largo de la vida del proyecto.

El servicio incluirá un proceso de mejora continua con propuestas escritas de recomendaciones sobre las soluciones y servicios actuales, con cambios y otras mejoras correctivas que potencien la evolución positiva del servicio. Así como posibles ampliaciones que serían recomendables disponer de cara a una futura evolución.

La aplicación de las mejoras será a decisión y criterio de los responsables de TMB. Una vez hayan sido aprobadas, la OT se encargará de coordinar su ejecución.

Se pide pro actividad en el servicio, trabajando de forma cooperativa con el cliente, y no limitándose a la comunicación con las verticales del propio servicio sino, también con otros proveedores para poder mantener una coordinación con ellos, e informando cuando se detecte

alguna carencia por parte del servicio de algún proveedor que en consecuencia pueda influir negativamente con la seguridad de TMB.

La coordinación incluirá la gestión de la bolsa de horas contratadas con el proveedor, proponiendo a cliente, de forma proactiva, la mejor manera de utilizarlas. Se encargará de dar todos los pasos para articular la activación de estas consultorías y proyectos en los servicios definidos en el apartado de “Consultoría y Proyectos bajo demanda”.

Se detallan a continuación otras tareas que serán cubiertas por el servicio de la OT:

- Responsabilidad frente al Cliente de la provisión y explotación de los servicios de seguridad que tenga contratados. Intervenir en todos los proyectos de seguridad nuevos que se contraten y responsabilidad en la planificación y seguimiento global de su implantación.
- Gestión externa e interna, de escalados de averías para todos los servicios de seguridad. Coordinación interna con los responsables de otros servicios del proveedor desde un punto de vista técnico.
- Interlocución principal, tanto frente a TMB como internamente al proveedor para la gestión de escalados y coordinaciones de incidencias de alto impacto relacionadas con las infraestructuras de seguridad.
- Implantación del modelo de gobierno y atención con TMB, así como la aplicación de las metodologías actualizadas que conduzcan a la práctica de una cultura de seguridad informática.
- Gestión de cambios y gestión de la configuración en el modelo/alcance de prestación del Servicio.
- Visión extremo a extremo de la calidad del servicio de seguridad prestado al Cliente, seguimiento y control de los indicadores/SLA, reporting al Cliente y organización interna.
- Definición y ejecución de procedimientos de actuación para garantizar la correcta provisión y explotación de los servicios, apoyándose en el resto de figuras/unidades dedicadas a la atención del Cliente.
- Definición y liderazgo de Planes de Mejora Continua de la prestación del servicio y de todas las plataformas gestionadas por el servicio. Identificación de problemas tanto de seguridad como dentro del servicio, siendo responsable de su gestión.
- Asesoramiento sobre la constante evolución tecnológica y cómo ésta puede beneficiar o aumentar los niveles de seguridad existentes en TMB.
- Compartir los conocimientos sobre las mejores prácticas seguidas para garantizar la continuidad del negocio, la confidencialidad de la información y su integridad.
- Disponibilidad Proveedor las 24 horas del día y los 365 días del año para poder atender cualquier situación crítica o grave sobre alguno de los servicios de seguridad prestados por el proveedor que el cliente considere que requiera su atención o conocimiento. En caso de sustitución por vacaciones/bajas, etc. de las personas asignadas a la OT, se comunicará a TMB y se realizará el traspaso con la antelación de que lo requiera el cambio.

- Seguimiento de los incidentes relevantes con afectación al servicio y creación del correspondiente informe de incidente post mortem.

4.1.2. Mantenimiento del SIEM

El servicio que se solicita incluye el desarrollo, puesta a punto y mejora continua de los paneles del SIEM de TMB, actualmente implementados sobre una plataforma Splunk onpremise, mediante la incorporación de las fuentes de datos y procedimientos de actuación (playbooks) que se consideren necesarios para mejorar la detección y gestión de las alertas.

El SIEM de TMB que actualmente está basado en una plataforma SPLUNK onpremise donde se ingestan a diario unos 200Gb de diversas fuentes: Firewalls, Antispam, Backup, Eventos de directorio activo, IRM (SealPath), Antimaware (antivirus y application control), herramienta de gestión de vulnerabilidades, O365, CASB,.... y dónde hay configuradas más de 80 alertas con su playbook asociado.

El proveedor deberá operar la solución del SIEM de Splunk, propiedad de TMB. No obstante si durante la duración del contrato, TMB decidiera migrar a otro, la Oficina Técnica debería adaptarse a esta nueva tecnología y colaborar en migrar los Casos de Uso (CdU) existentes en la actual plataforma y evolucionarla.

El proveedor deberá contemplar que a lo largo del contrato, la volumetría de ingesta, la cantidad de fuentes o incluso los productos, pueden variar. A título de ejemplo, se está trabajando en cambiar las fuentes de Antivirus/EDR y CASB.

Requerimientos solicitados:

La gestión de la solución debe contemplar:

- **Capa de Recolección de Datos**, con capacidad de recolección de fuentes de datos multi-entorno (On-premise, cloud o híbrido), bajo diferentes formatos y vías de recolección. El servicio debe contemplar la incorporación de todas las fuentes de datos, ya sean de IT como de OT, que sean susceptibles de aportar información de calidad al SIEM, para un buen gobierno de seguridad.
- **Gestión de alertas del SIEM**, creación y mantenimiento de casos de uso (IT y OT) que se consideren necesarios, tanto por parte del proveedor y su experiencia en el servicio (adaptando su catálogo estándar de casos de uso) como por parte de TMB que quiera implementar casos de uso concretos por necesidades. Aplicando los ajustes necesarios de excepciones.
- **Definición de procedimientos**, de forma que cada alerta disponga del correspondiente procedimiento operativo documentado que esté acordado con TMB, que contenga el Playbook con el árbol de decisión hasta la resolución final. Tienen que quedar claros los pasos concretos hasta la resolución de cada CdU independientemente de si lo realizará el SOC o si se abordará con recursos propios de TMB. TMB proveerá un repositorio sharepoint donde dejar de forma ordenada toda la documentación generada en el transcurso del servicio.

- **Capa de Orquestación y Automatización** que permite aplicar automatizaciones. Siempre que sea posible y con los servicios disponibles del cliente (con SOAR u otras soluciones complementarias, e. Ansible), se tratarán de automatizar todos los CdU que sea posible para mejorar la velocidad de respuesta y la dependencia de trabajos manuales.
- **Capa de Inteligencia de Amenazas** (IOC) con fuentes abiertas, propias y de terceros que permiten mejorar el ratio de detección y disponer de capacidades adicionales de enriquecimiento y automatización mediante un TIP (Threat Intelligence Platfom) del proveedor.
- El proveedor deberá proporcionar un **amplio catálogo de casos de uso propios** en continua evolución con una base de conocimiento elaborada sobre la base de más. Este catálogo deberá estar mapeado y alineado con el framework de MITRE.

4.1.3. Threat Hunting

El Servicio de Threat Hunting realizará búsquedas iterativas y proactivas en los sistemas y redes de TMB, con el objetivo de identificar amenazas avanzadas que pueden haber evadido los controles de seguridad ya establecidos. Es una medida de seguridad preventiva y proactiva, capaz de proporcionar detección amenazas antes de que tengan un impacto en el negocio, y no gira en torno a herramientas específicas.

El Servicio de Búsqueda de Amenazas sigue un enfoque de hipótesis. El objetivo de estas hipótesis es detectar posibles atacantes que operen entre las fases de reconocimiento y exfiltración del marco MITRE ATT&CK. capaz de evadir los controles de seguridad existentes en un entorno concreto de forma específica".

El equipo de Threat hunting generará distintas consultas para cada hipótesis, que se ejecutarán sobre la infraestructura de TMB siguiendo los procedimientos aprobados por el Servicio de Theat Hunting Los resultados de estas consultas serán analizados por el equipo y, en su caso. suficientes pruebas, se notificarán como alertas. Las alertas se definen como "la evidencia de actividad maliciosa que no ha sido detectada". previamente por otras herramientas o equipos".

TMB será informado de las hipótesis que se van a analizar y de los resultados de estos análisis.

Entregables

El servicio de búsqueda de amenazas proporciona los siguientes mecanismos de seguimiento y generación de informes:

- Informe de búsqueda de amenazas: informe mensual estándar basado en la ejecución del servicio y que contiene investigación de amenazas, alertas y recomendaciones.
- Notificaciones de alerta: hallazgos relevantes que deben notificarse lo antes posible, sin esperar al informe mensual.

4.1.4. Gestión de vulnerabilidades

El servicio debe cubrir el seguimiento de la publicación de vulnerabilidades aplicables a las tecnologías que utiliza TMB. Gestionando los riesgos detectados, y realizando un seguimiento de las acciones necesarias hasta conseguir mitigarlos o minimizarlos.

Como fuentes de información dispondrá de la herramienta propia de TMB de Gestión de Vulnerabilidades, así como newsletters públicas y/o fuentes internas del proveedor.

Como fuentes de información se contemplarán comunicaciones externas (CERTS, alertas tempranas, fabricantes, cero days, etc…), comunicaciones internas de la operación de seguridad de TMB (incidentes de seguridad reportados, notificaciones del personal TMB, detectadas por el propio servicio de ciberseguridad, derivadas de las auditorías de seguridad o de los propios escaneos de vulnerabilidades, etc…) y de otras vulnerabilidades detectadas por organismos externos a TMB.

La resolución si es necesario realizarla a través de recursos externos al proveedor (ya sea con recursos de TMB o contratos a empresas de terceros), hará el seguimiento y realizará las solicitudes que haya que realizar con la plataforma de ticketing oportuna en cada caso.

También supervisará el estado de la operación de la herramienta de Gestión de Vulnerabilidades que será operada por terceros, pero deberá llevar la vigilancia/control de la correcta ejecución, dando a conocer a TMB si se detecta algún mal funcionamiento/ejecución de la gestión de vulnerabilidades.

4.1.5. Auditorías y Pentesting

El objetivo de este servicio es facilitar una visión clara de la vulnerabilidad de TMB y los riesgos potenciales a los que se encuentran expuestos sus sistemas de información, a partir de ahí proveer de una serie de medidas correctivas y preventivas, así como recomendaciones adicionales de seguridad proactiva, que permitan garantizar un adecuado nivel de seguridad.

El resultado final debe ayudar a TMB en su esfuerzo por mejorar la postura de seguridad y conocer los riesgos reales que afectan a la exposición de la empresa, presentando informes con los riesgos que necesitan ser remediados y una orientación para hacerlo .

Los informes deben identificar claramente las mejoras que deben abordarse, con priorización, y proporcionar el acompañamiento para realizar todos los ajustes necesarios, que deben gestionarse desde la Oficina técnica que será quien coordinará la aplicación de las acciones correctivas a realizar.

El servicio contemplará la ejecución de al menos 4 simulacros por cuatrimestre (12 ejecuciones al año) así como la posibilidad de realizar ejecuciones a petición de TMB (que se gestionarán con la bolsa de horas de la oficina técnica).

El proveedor deberá proporcionar las herramientas **Simulación de Infracciones y Ataque (BAS)** necesarias para poder realizar las autorías/pentesting de TMB. Estas herramientas deberían estar basadas y presentar los resultados según el marco MITRE ATT&CK.

Todos los módulos de la herramienta escogida por el proveedor, serán administrados en **modalidad servicio** (TMB no dispondrá de licenciamiento ni soporte de la solución que proporcione el proveedor) y por tanto incluirá servicios profesionales tanto para la implantación y mantenimiento como para la explotación de la herramienta.

El servicio debe incluir las capacidades para actuar de forma homogénea y coordinada por:

- Probar todas las fases de un ataque, desde la preexplotación hasta la postexplotación, la persistencia y el mantenimiento del acceso.
- Realizar pruebas de forma continua, periódica y bajo demanda.
- Realizar pruebas seguras sin interferir en la operativa de TMB.
- Probar controles de seguridad tanto perimetrales como internos.
- Actualización continua para ofrecer simulaciones que también incluyan amenazas detectadas "in-the-wild".
- Proporcionar informes exhaustivos y concluyentes que incluyan recomendaciones de mitigación.

4.1.6. Funcionamiento del servicio

El servicio dispondrá de un perfil Analista de Seguridad dedicado al servicio BAS (Breach and Attack Simulation) que, coordinado con la oficina técnica y contando si es necesario con el apoyo de otros expertos del proveedor:

- Recomendará las simulaciones que mejor se adapten a la postura y madurez de seguridad del TMB.
- Definirá claramente el alcance de los simulacros en relación con el activo (red, aplicación, etc.) y los objetivos.
- Planificará las pruebas con un enfoque estructurado con una metodología organizada en diversas etapas: previa a la intervención (alcance, planificación), intervención (ejecución de las pruebas) y posterior a la intervención (apoyo a la remediación, presentación de informes, re -testing).
- El analista de seguridad deberá tener relación directa y soporte por el fabricante de la herramienta.

Ciclo de Vida

Se estructurará cada simulacro en cuatro fases principales que se desarrollará y repetirán de forma cíclica y en las que interactúan un conjunto definido de personas, tecnología y procesos:

1. **Planificación.** En una fase inicial se acordará y planificará con TMB el alcance, las franjas horarias y las posibles restricciones. En base a esta información, se provisionará el servicio para que esté listo y el equipo técnico pueda ejecutar las pruebas de seguridad.
2. **Ejecución de las pruebas**. Las pruebas de seguridad son ejecutadas en base a la planificación acordada. Después de realizar la evaluación, se genera una puntuación que refleja la magnitud de las potenciales amenazas para los sistemas o recursos objetivo, con una evaluación comparativa específica del sector.

3. **Comunicación de resultados.** En esta fase se generarán los informes y entregables del resultado de los simulacros, donde se indicarán las medidas de mitigación para cada una de las brechas de seguridad encontradas. También en esta fase, el analista de seguridad asignado realizará reuniones con el equipo de seguridad de TMB para explicar los findings y los informes entregados.
4. **Re-Test.** Se realizará una repetición de las pruebas para validar si los pasos de remediación propuestos por los expertos han sido ejecutados y han sido efectivos.

Entregables

Los informes de las pruebas presentarán el desempeño realizado por el servicio incluido en esta propuesta.

Después de cada simulacro, se entregarán un informe técnico y otro ejecutivo cuyo contenido puede variar dependiendo del tipo de simulacro o vector de ataque utilizado, pero que básicamente incluirán la siguiente información:

- Descripción: Incluye la motivación de TMB para llevar a cabo la prueba.
- Alcance: Contiene los activos objetivo dentro del alcance y el calendario de pruebas.
- Conclusiones: Información general que transmite los hallazgos detallados en una valoración resumida.
- Recomendaciones generales: En base a los resultados de las pruebas, ofrece recomendaciones generales que resumen las medidas a adoptar.
- Listas priorizadas de todas las brechas de seguridad y riesgos encontrados sobre los activos testados, ordenados por grado de severidad e impacto.

4.1.7. Módulos de la Herramienta (BAS)

A continuación se mencionan diferentes módulos que deberá poder cubrir la herramienta con la realización de simulaciones que proporcionen la postura de seguridad en distintos ámbitos:

Desafío de los Controles de DLP

Las filtraciones de datos crean un enorme impacto financiero en la reputación de las empresas víctima. Las soluciones de DLP están diseñadas para proteger contra la filtración de datos. Las organizaciones dependen casi por completo de la implantación, metodología y configuración de la DLP para proteger sus valiosos datos.

El módulo de exfiltración de datos está diseñado para evaluar en qué medida las soluciones y controles de DLP impiden la extracción de información crítica desde el exterior de la organización. La plataforma pone a prueba los flujos de salida de datos (como información de identificación personal, médica, financiera y confidencial empresarial) para validar que estos activos de información permanecen en su interior.

El vector empaqueta los datos en distintos tipos de archivos, incluyendo imágenes y archivos, e intenta exfiltrarlos utilizando múltiples métodos de exfiltración.

Pruebas de Endpoint Security

El módulo de evaluación Endpoint Security permite probar y optimizar la eficacia de la seguridad de los endpoints. Este vector desafía las medidas de seguridad de los endpoints contra un conjunto completo de ataques que simulan el comportamiento malicioso de ransomware, gusanos, troyanos y otros tipos de malware.

Las pruebas permiten crear escenarios de ataque personalizados utilizando cientos de mandos en toda la Kill-Chain de los ciberataques, mapeados en el marco MITRE ATT&CK.

Movimiento lateral (Hopper)

El módulo de protección de la red interna o vector de movimiento lateral desafía a las políticas de segmentación y configuración de la red interna contra diferentes técnicas y métodos utilizados por los atacantes para propagarse dentro de la red y controlar sistemas adicionales.

El vector simula a un adversario que tiene el control de un solo equipo de trabajo e intenta moverse lateralmente dentro de la organización. El resultado de la evaluación es una visualización de todos los endpoints que la evaluación ha podido llegar con una descripción detallada de los métodos utilizados para cada salto.

La evaluación identifica los puntos débiles de la infraestructura, los errores de configuración de la red y las contraseñas no seguras, proporcionando orientación para su corrección.

Protección de Web Gateway

Este módulo desafía los controles que protegen a los empleados tanto del acceso como de la descarga de malware alojado en sitios web maliciosos y comprometidos.

El vector prueba la protección de entrada contra miles de diferentes archivos maliciosos y exploits simulados, y la protección de salida contra información compuesta por miles de URL que se actualizan a diario.

Seguridad del correo electrónico

Permite probar y optimizar la postura de ciberseguridad del correo electrónico de la compañía. Este vector desafía a las medidas de seguridad del correo electrónico contra un amplio conjunto de ataques mediante el envío de correos electrónicos con archivos adjuntos que contienen ransomware, gusanos, troyanos o enlaces a sitios web maliciosos.

La simulación revela los correos electrónicos maliciosos, tipos de archivos y archivos incrustados que podrían llegar a la bandeja de entrada de los empleados.

Seguridad del WAF

Permite probar y optimizar las medidas de seguridad web. Este vector identifica en primer lugar todos los formularios y otros medios de importación de datos disponibles en el dominio de seguridad de infraestructura técnica y, a continuación, desafía al WAF contra miles de ataques, incluyendo los principales payloads de OWASP, inyección de comandos y ataques de inyección de archivos para evaluar la integridad de la configuración del WAF y sus capacidades de bloqueo.

4.1.8. Consultoria y Proyectos bajo demanda

Este servicio se consumirá en formato de bolsa de horas, permitiendo así abordar rápidamente las necesidades emergentes y proporcionar soluciones inmediatas dentro del proceso de mejora continua de la ciberseguridad.

Éstas podrán provenir de TMB o bien de propuestas que vengan de la Oficina Técnica.

Para llevar a cabo este servicio se contará con recursos de perfiles técnicos del ámbito de la seguridad como: Consultores, Proyectistas, Compliance, Vigilancia digital, Auditores/pentesting, concienciación, etc

Metodología de trabajo

- Presentación de la propuesta de servicio de consultoría/proyecto
- Valoración del esfuerzo en horas
- Definición de la documentación de la propuesta y de entregables
- Aprobación de TMB
- Ejecución
- Entrega de entregables y cierre

A modo de ejemplo, a continuación se muestra una relación de posibles actividades:

1. Análisis de riesgos
2. Evaluación de la madurez de seguridad de proveedores.
3. Procedimientos de desarrollo seguro de software.
4. Revisión sobre el cumplimiento normativo de la Directiva NIS2.
5. Revisión sobre el cumplimiento de la Ley de Protección de Infraestructuras Críticas (LPIC).
6. Plan de formación y concienciación en Ciberseguridad.
7. Acompañamiento a la certificación ISO 27001.
8. Estado de salud del Directorio Activo
9. Elaboración del plan de adecuación al ENS y su implementación.
10. Consultas en el ámbito de Compliance (p.e. protección de datos personales).
11. Modelo de gobierno de la Ciberseguridad según ISA/IEC 62443.
12. Revisión sobre el Plan de Continuidad de Negocio.
13. Procedimiento de Gestión de Incidentes.
14. Análisis de Impacto (BIA)
15. Simulación de phishing

4.2. Monitorización/Operación 24x7

La misión principal del Centro de Operaciones de Seguridad (SOC) será proteger la información y sistemas de TMB contra las amenazas cibernéticas en modalidad 24x7x365. Para ello el servicio tendrá como principal cometido la monitorización y análisis continuo de la actividad de

la red, los sistemas y las aplicaciones de TMB en busca de actividades sospechosas o anomalías para detectar y dar respuesta a los posibles incidentes de seguridad.

Las funciones clave del SOC incluyen:

- **Investigación de posibles incidentes**: analizar las alertas para determinar si son ataques reales o falsos positivos.
- **Elección y priorización de incidentes**: Evaluar y priorizar los incidentes para optimizar recursos y minimizar riesgos.
- **Coordinación de respuesta y resolución de incidentes**: Contando con recursos técnicos propios del SOC u orquestando a los diversos actores involucrados y herramientas disponibles.

El centro de operaciones de seguridad (SOC) será coordinado por la oficina técnica y contará como mínimo con los siguientes recursos:

- Servicio de operación: **Equipo 24x7** responsable del 1er. Nivel encargado de la recepción, diagnóstico y coordinación de la respuesta y resolución de las alertas.
- Técnicos 2º y 3er. Nivel **(8x5 + guardias)** especialistas en las plataformas de seguridad de TMB (punto 3.5 de este documento).

Requerimientos solicitados:

La lista mínima de tareas a ofrecer es:

- El contratista dispondrá de un centro operativo (SOC) en modo 24x7x365 que pertenezca a la “Red nacional de SOC” donde se recibirán, notificarán, gestionarán y escalarán las alertas e incidentes de ciberseguridad. Este centro deberá estar redundado con un centro de contingencia que permita la continuidad del servicio en caso de grave incidencia en su centro de operaciones.
- Monitorización 24x7x365 de las alertas y eventos generados y recibidos en la plataforma SIEM de TMB. El contratista asumirá la integración de las alertas con sus sistemas.
- Monitorización 24x7x365 de las alertas y eventos generados por el EDR de TMB, utilizando las capacidades EDR para realizar investigaciones sobre las alertas accediendo a la consola EDR (es decir, la interfaz de usuario dentro de la plataforma correspondiente).
- Monitorización 24x7x365 de las alertas y eventos generados por otros canales que no son el SIEM y que se consideren necesarios: CASB,...
- TMB podrá también abrir un ticket mediante correo a una dirección de correo electrónico o llamada telefónica al equipo de Nivel 1.
- El Servicio sólo llevará a cabo las acciones de respuesta, siempre que hayan sido previamente aprobadas por TMB y estén documentadas en los playbooks del Servicio.
- Las alertas serán registradas en una plataforma de tiqueting que permita realizar su seguimiento.
- Gestión de las alertas en 24x7: procedimientos de registro, diagnosis, clasificación, resolución/mitigación por parte de nivel 1 y en caso necesario escalado a nivel 2.

- El adjudicatario se integrará con los diferentes organismos oficiales en los que TMB esté sujeto por ley (RGPD) o con lo que se consideren oportunos para la cooperación a la gestión y detección de incidentes (foro CSIRT.es, Red Nacional de SOC's , Agencia de Ciberseguridad de Cataluña, CCN-CNI). Y si el servicio lo requiere, se realizará la ingesta de los sistemas de registro y notificación de incidentes corporativos.

4.2.1. Cuadro de mandos del servicio de operación

El proveedor generará un Dashboard/Cuadro de mando dentro de la plataforma SIEM de TMB (actualmente Splunk), que facilite el seguimiento de las operaciones de seguridad y el Estado de la Ciberseguridad en TMB.

Deberá proporcionar una visión mensual de la prestación del servicio, con las actividades ejecutadas, acciones planificadas, puntos bloqueantes o que requieran atención, así como un resumen de las incidencias gestionadas, volumetrías asociadas a los servicios y próximos pasos y propuestas de mejora de servicio.

Se acordará el contenido de los cuadros de mando facilitando la siguiente lista como ejemplo:

- **Estado general de la Ciberseguridad**
  - Filtros por tiempo, estado, tipos de ticket y prioridad
  - Mapa interactivo de geolocalización de IPs públicas correspondientes a ataques
  - Categoría de tickets, subcategoría de tickets, prioridad de tickets
  - Tipo de ataque detectado y Tabla detallada de todos los tickets.
- **SLAs**
  - Tiempo medio de vida de notificación de un incidente de Seguridad
  - Número de tickets medidos para el cálculo del SLA
  - Porcentaje de cumplimiento
  - Evolución del cumplimiento de SLA de los tickets en el tiempo
  - Número de tickets que incumplen de criticidad baja y % del total
- **Volumen**
  - Filtros por tiempo, estado, tipos de tickets y prioridad
  - Distribución de tipos de tickets en el período
  - Número de incidentes gestionados
  - Día de máximo número de incidentes gestionados y cantidad
  - Número de peticiones gestionadas
  - Mapa de calor de atención de tickets
- **Productividad**
  - Filtros por tiempo, estado, tipos de ticket y prioridad
  - Distribución de todos los tickets gestionados en el tiempo según la tipología
  - Número de incidentes de seguridad gestionados
  - Número de incidentes de seguridad con impacto gestionados
  - Tipología de todos los tickets gestionados

- **Métricas y KPI avanzados** detalle de las de operaciones y seguridad para el seguimiento del servicio, así como del estado de la seguridad corporativa. Estas métricas deben poder revisarse en cualquier momento en tiempo real con Dashboards personalizados, así como un cuadro de mando del estado de la postura de seguridad para la visión de un CISO. Así como poder generar un informe en cualquier momento de la postura de seguridad actual.

4.3. Administración técnica de las plataformas

Se incluyen en este módulo los servicios de administración técnica para las plataformas de seguridad de TMB: Antivirus/EDR, Antispam y SSE/CASB de TMB.

Estos servicios incluirán de forma genérica las siguientes tareas:

Mantenimiento Correctivo

- Resolución de incidencias y fallos técnicos.
- Intervención urgente en caso de problemas críticos que afecten a la operatividad de la plataforma.
- Registro y seguimiento de todas las incidencias hasta su resolución.

Mantenimiento Preventivo

- Revisión periódica del estado de la plataforma.
- Aplicación de actualizaciones de seguridad y parches.
- Realización de pruebas de rendimiento y ajustes necesarios para garantizar la estabilidad del sistema.
- Análisis y prevención de posibles fallos futuros.

Mantenimiento Evolutivo

- Implementación de mejoras y nuevas funcionalidades.
- Configuración de la plataforma conforme a las nuevas necesidades de TMB.
- Gestión de accesos: usuarios y roles
- Integración con otros sistemas y plataformas según se requiera.
- Formación y capacitación al personal interno sobre nuevas funcionalidades.

Otros

- Generación de informes: Crear informes regulares de actividad, incluyendo estadísticas, tendencias y análisis de seguridad.
- Reuniones de Revisión: Realizar reuniones periódicas para revisar los informes y platear posibles mejoras en el sistema.
- Capacitación del Personal: Formar al personal sobre el uso de las diferentes plataformas y las mejores prácticas para su uso.
- Asistencia Técnica: Proporcionar soporte técnico continuo para resolver problemas y responder a preguntas.

- Documentación: Mantener una documentación detallada y actualizada del sistema y sus configuraciones.
- Asegurar el Cumplimiento: Garantizar que las distintas plataformas cumplan con las normativas y leyes vigentes sobre protección de datos y privacidad.
- Escalabilidad: Asegurar que el sistema pueda escalar según el crecimiento y necesidades de TMB.
- Resiliencia y Redundancia: Implementar medidas para asegurar la alta disponibilidad y la continuidad del servicio en caso de fallos.

4.3.1. Administración EDR

El proveedor deberá gestionar la solución EDR de TMB, que actualmente se basa en la solución que se Trellix (con Endpoint Security, EDR y Application Control).

Si en algún momento, TMB cambia de producto EDR (para la totalidad o parte del parque gestionado por Trellix, deberá realizar la administración de la/s plataforma/s que cubran todo este parque de equipos.

En el caso particular de equipos Legacy que se cubren con Application Control, en caso de no poder gestionarse con una nueva herramienta EDR, tendrán que seguir cubriéndose con este producto (que tendrá licenciado TMB) hasta que desaparezcan estos equipos Legacy . Este parque de equipos Legacy es actualmente de menos de 1000 clientes.

Además de las tareas de administración técnica que se han establecido como genéricas, la plataforma EDR incluirá tareas específicas de operación de la herramienta, como son:

- La administración de las políticas propias del EDR respecto a la detección y contención de alertas e incidencias.
- La administración de las políticas propias del antivirus y la configuración de políticas adhoc por perfiles que le puedan ser solicitadas.
- La gestión de los IOCs relacionados con el EDR, tanto en lista blanca como en lista negra.
- Gestionar las vulnerabilidades de los dispositivos bajo control del EDR y realizará los informes de vulnerabilidades relacionados, tal y como se describe en el apartado 4.1.4 de este documento.
- Apoyo a la integración del agente EDR en los nuevos equipos en los que deban ser instalados.
- Comprobar y testear aleatoriamente, con periodicidad semanal, que las sondas y agentes del EDR funcionan correctamente y generan alertas que terminan ingestadas en el SIEM.

4.3.2. Administración Antispam

El servicio de gestión y administración técnica de la plataforma antispam debe incluir diversas tareas esenciales para garantizar que el sistema funcione de forma óptima, protegiendo eficazmente contra correos electrónicos no deseados y potencialmente peligrosos.

Además de las tareas de administración técnica que se han establecido como genéricas, la plataforma antispam incluirá tareas específicas más importantes que deben considerarse:

- Alertas y Notificaciones: Configurar alertas automáticas para incidentes de spam y actividades sospechosas.
- Actualización de Filtros y Reglas: Actualizar regularmente los filtros y reglas de detección de spam basados en las últimas amenazas y patrones de spam.
- Ajustes de Configuración: Ajustar la configuración del sistema para optimizar la detección y filtrado de spam sin afectar a la entrega de correos legítimos.
- Integraciones: Integrar la plataforma antispam con otros sistemas y herramientas de TMB.
- Listas Blancas y Negras: Gestionar listas blancas (whitelists) y listas negras (blacklists) de remitente.
- Revisiones Periódicas: Revisar y actualizar periódicamente estas listas para mantener su efectividad.

4.3.3. Administración CASB/SSE

El servicio de gestión y administración técnica de la plataforma CASB (Cloud Access Security Broker) tiene como objetivo que la plataforma CASB funcione de forma efectiva, protegiendo a la empresa contra amenazas y garantizando la seguridad y cumplimiento normativo en el uso de servicios en la nube .

Además de las tareas de administración técnica que se han establecido como genéricas, la plataforma CASB incluirá tareas específicas, las más importantes a considerar:

- Monitorización en tiempo real: Supervisar la actividad de los usuarios y los dispositivos en aplicaciones en la nube para detectar comportamientos anómalos y posibles amenazas.
- Alertas y Notificaciones: Configurar alertas automáticas para incidentes de seguridad, accesos no autorizados y actividades sospechosas.
- Configuración: Configurar la plataforma CASB para la integración con las aplicaciones y servicios en la nube utilizados por la empresa.
- Definición de Políticas: Establecer y mantener políticas de seguridad para el acceso y uso de las aplicaciones en la nube.
- Ajustes de Políticas: Ajustar las políticas basadas en los resultados de la monitorización y nuevas necesidades.
- Revisiones Periódicas: Realizar revisiones periódicas del sistema para asegurarse de que funciona correctamente y detectar posibles vulnerabilidades.
- Mejoras y Nuevas Funcionalidades: Implementar mejoras y nuevas funcionalidades en la plataforma CASB.
- Integraciones: Integrar la plataforma CASB con otros sistemas de seguridad y herramientas de gestión de la empresa.

- Control de Accesos: Gestionar y controlar los accesos de los usuarios a las aplicaciones y servicios en la nube según las políticas establecidas.
- Auditoría de Accesos: Realizar auditorías periódicas de los accesos para asegurarse de que sólo los usuarios autorizados tengan acceso a la información sensible.

El proveedor tiene como misión proporcionar una solución integral y prospectiva de seguridad que proteja, garantice, posibilite y mejore el negocio actual y futuro del cliente. El Servicio Security Edge del proveedor debe contar y aprovecharse de las sinergias del Security Operation Center (SOC) del proveedor.

El Servicio Security Edge gestionado por el proveedor debe estar destinado a proporcionar seguridad al perímetro del negocio, donde la nube y el trabajo desde cualquier lugar y dispositivo han supuesto una transformación radical, permitiendo al cliente tanto delegar la gestión de la protección de la navegación web y el acceso a sus aplicaciones corporativas, así como la gestión de incidentes de seguridad en un equipo experto (SOC), permitiendo hacer foco en aquellas tareas de mayor valor para el núcleo de su negocio.

Se debe realizar un acompañamiento en la evolución en cuanto a la aplicación de políticas (DLP, Navegación, etc) y de Concienciación/educación del usuario para que haya una madurez en cuanto al uso que hacen los usuarios de las plataformas SaaS. Mediante las Best Practices y la experiencia del proveedor con otros clientes, se propondrá la mejor manera de ir evolucionando hacia el mejor control de la seguridad de los clientes mediante las diferentes funcionalidades de CASB inline, CASB API, Security Gateway, etc.

Se realizará un seguimiento periódico del estado de salud y de reporte del comportamiento de los usuarios, y una estrategia de mejora continua.

4.3.4. Administración herramienta gestión vulnerabilidades

El objetivo de la Gestión de vulnerabilidades es identificar vulnerabilidades o debilidades de seguridad conocidas o potenciales en las redes y sistemas de información de TMB frente a ataques externos e internos y aplicar los ajustes o configuraciones que permitan corregirlas.

En este ámbito, lo que se solicita concretamente al adjudicatario de este servicio es la administración técnica de la plataforma con responsabilidad sobre las tareas genéricas que se han establecido para globalmente este capítulo.

Habrá otros proveedores que serán usuarios de la plataforma y que la utilizarán para realizar el análisis y remediación de las vulnerabilidades detectadas.

En todo caso, si será responsable de este servicio dar respuesta a consultas técnicas o peticiones de soporte o de configuración que estos otros actores le soliciten.

4.3.5. Administración Herramientas CCN-CERT

Se solicita la gestión de las herramientas de CCN-CERT, así como la conveniencia de utilizarlas o sustituirlas por otros servicios que disponga el cliente.

Actualmente se dispone de microCLAUDIA y CLARA, que son de uso gratuito proporcionados por el CCN-CERT, pero que requieren un servicio de gestión que deberá proporcionar el proveedor de la licitación y en su caso, el escalado de incidencias/bugs con CCN - CERT y quizás fabricantes de terceros.

También es posible la necesidad de gestión de otro tipo de servicios que CCN-CERT pueda recomendar como LUCIA, que es una herramienta para la gestión de incidentes de seguridad (Listado Unificado de Coordinación de Incidentes y Amenazas).

Está desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

4.4. Equipo de Respuesta frente a Incidencias de Seguridad y análisis forense (CSIRT)

El equipo que ofrecerá el servicio en base a los siguientes recursos:

- 20 jornadas anuales (8x5) + 5 jornadas anuales (fuera 8x5), de especialistas para gestión de incidentes de impacto, investigación, análisis forense u otras tareas especializadas a petición de TMB.

La metodología requerida deberá ser aprobada por el CCN-CERT, de acuerdo con el Esquema Nacional de Seguridad (ENS) y que está referenciada en las guías CCN-STIC-403 y CCN-STIC-817.

Este servicio debe cubrir como mínimo:

- Posible activación desde el servicio de Monitorización del SIEM y/o de la operación EDR, así como a petición de TMB o de la Oficina Técnica.
- Capacidades de investigación y análisis forense:
  - Evaluación inicial y de evidencias preliminares.
  - Extracción y recolección de evidencias sobre sistemas comprometidos
  - Contextualizar la amenaza, evaluar el nivel de compromiso, posibles movimientos laterales, escalada de privilegios, etc.
- Respuesta y remediación
  - Coordinación durante el incidente con el equipo de Seguridad TIC de TMB.
  - Apoyo sobre la ejecución de la contención para minimizar el impacto.
  - Apoyo a la erradicación, recuperación del servicio
  - Monitorización y control post incidente
- Análisis de malware (código malicioso)
  - Identificar el comportamiento de los artefactos
  - Identificar los IOC aplicables a la infraestructura de seguridad de TMB para detección y bloqueo posteriores
  - Identificar sus mecanismos de propagación

- Informes técnicos del incidente
  - Informe de detalle de toda la investigación de gestión del incidente y del posible análisis del malware (malware)
- Lecciones aprendidas y propuestas de mejora

4.5. Vigilancia Digital

Se solicita el servicio de Vigilancia Digital para proteger el negocio, marca y reputación contra los riesgos que surgen de la transformación digital.

El servicio debe presentar un enfoque holístico que cubra tanto la web abierta como la deep y la dark web, proporcionando información accionable sobre amenazas que permita reducir los ataques exitosos disminuyendo la superficie de ataque y ayudar a detectar posibles brechas de seguridad y acelerar la recuperación.

TMB deberá disponer de acceso al MISP (Plataforma de Inteligencia de Amenazas) dentro del servicio de Threat Intelligence para acceder a los IOC. Así que se podrán consumir estos indicadores automáticamente sin coste adicional para TMB.

Esta plataforma deberá ser accedida por servicios de automatización, por ejemplo si es vía Web, a través de una API que permita consultar las detecciones, a fin de poder automatizar las acciones a realizar. Por tanto, que no exclusivamente se pueda acceder a los contenidos de la plataforma a través del acceso manual. La idea es poder automatizar un procedimiento en cuanto a la plataforma aparezca un contenido detectado por la Inteligencia de Amenazas.

El servicio de Vigilancia Digital, incluirá la suscripción a una newsletter de seguridad del propio servicio (que incluya información sobre Vulnerabilidades, Malware, organizaciones criminales activas,...) sin coste adicional por TMB.

El servicio de Vigilancia digital se prestará sobre los siguientes ámbitos:

- Reputación y marca
  - Uso no autorizado de marca
  - Dominios sospechosos
  - Counterfeit
- Fraude online
  - Apps móviles sospechosas
- Disrupción del negocio
  - Robo de credenciales

Reputación y marca

Uso no autorizado de marca

Se identificarán aquellos sitios web y contenidos en redes sociales u otras plataformas, que pretendan suplantar o aprovecharse de la imagen y reputación del cliente para confundir al usuario final mediante el uso de su marca, logo o imagen.

Para ello se monitorizarán redes sociales, canales relacionados con el sector del cliente y blogs en busca de usos no autorizados de sus marcas.

Dominios sospechosos

Se detectarán aquellos nuevos registros de dominios que contengan en su nombre palabras clave directamente relacionadas con el cliente. Este módulo se complementa además con capacidades de typosquatting basadas en algoritmos de similitud y proximidad:

- Similitud: reemplazando ciertos caracteres por otros similares o deformando las palabras para que sean visualmente iguales.
- Proximidad: eliminando o reemplazando sólo ciertos caracteres.

Además, se proporcionará siempre que esté disponible, la información de registro (WHOIS) asociada a los dominios sospechosos identificados. Para ello se consultarán las bases de datos de los dominios de alto nivel (TLD, incluyendo ccTLD y gTLD), tomando como referencia los dominios registrados por el cliente.

Counterfeit

Se identificarán canales de comercialización no autorizados en los que se encuentren disponibles productos del cliente, falsificaciones de éstos, réplicas, productos de segunda mano o que simulen ser un canal oficial de distribución.

Para ello se monitorizarán redes sociales, plataformas de venta/compraventa online, canales relacionados con el sector del cliente, canales de distribución no oficiales, publicidad, blogs y foros relacionados con su sector.

Fraude online

Apps móviles sospechosas

Se detectará la publicación de aplicaciones móviles sospechosas relacionadas con el cliente o la suplantación de las aplicaciones oficiales facilitadas por él, con el posible objetivo de confundir a sus usuarios para obtener credenciales, datos personales o infectarlas con algún tipo de malware.

Para ello se monitorizarán los mercados móviles oficiales (Apple Store, Google Play), así como mercados móviles alternativos, identificando aquellas aplicaciones móviles con referencias al nombre del cliente o a su marca.

Disrupción de negocio

Robo de credenciales

Se identificarán credenciales que se hayan visto comprometidas, ya sea en un escape o en un robo, y correspondan con permisos de acceso a sistemas, instalaciones y procesos relacionados con el cliente.

Para ello se monitorizarán fuentes públicas, como plataformas de compartición de información (pastebin), e información recogida por botnets (crime servers). Así como sitios de la Deep y Dark Web, en caso de haber contratado este ámbito de monitorización.

Para los robos, se proporcionará además la información de contexto disponible: nombre de usuario, contraseña (en caso de ser de servicios de terceros o de pertenecer a colaboradores o clientes se mostrará ofuscada), url del servicio afectado, tipo de usuario afectado, ubicación del servicio afectado, organización del servicio afectado, fecha de compromiso, dominio del usuario comprometido, host del servicio afectado, puerto del servicio afectado, tipo de botnet asociada , evidencia.

El servicio no incluye la verificación de la validez o vigencia de credenciales.

Consumo de las acciones de Takedown por la respuesta a amenazas

El objetivo prioritario en la resolución de amenazas, y al que están enfocadas todas las capacidades de respuesta del Servicio, es la gestión del cierre del sitio que aloja la amenaza (y/o los sitios intermedios que dan acceso al fraude, como proxy, dns, etc.), mientras se mitiga paralelamente su potencial impacto. Para ello se analizará el tipo de información publicada y la naturaleza del daño (derechos de autor, propiedad intelectual...), y, en base al medio de difusión y legislación aplicable, se procederá a realizar las gestiones pertinentes en nombre del cliente. En este punto debe tenerse en cuenta que las capacidades de respuesta se aplican únicamente sobre aquellas fuentes del servicio que son públicas.

Para gestionar estas acciones, el proveedor necesitará contar con los documentos que acrediten el registro de las marcas del cliente en los países en los que esté disponible, datos de contacto de la persona o departamento en cliente para la gestión de casos que requieran firma de Digital Millennium Copyright Act (DMCA) y una autorización expresa que autorice el servicio Digital Risk Protection del proveedor a actuar en su nombre. No contar con estos documentos podrá demorar o incluso imposibilitar la correcta resolución del caso.

En algunos casos es posible que sea necesario que el cliente gestione directamente ciertas acciones, fundamentalmente cuestiones de índole legal. En tal caso, la tarea del proveedor se limitaría a aportar las evidencias o información disponible. Las labores de asesoramiento legal al cliente se encuentran fuera del alcance del servicio.

Siempre que el servicio inicie las gestiones de cierre de un caso, este caso se descontará de la bolsa contratada. En determinadas circunstancias, es posible que el proveedor realice todas las acciones a su alcance y no se llegue a un nivel de resolución adecuado. Cuando se dé esta situación, o pasados un máximo de 60 días desde el inicio de las gestiones, el proveedor cerrará el caso. Para esta serie de casos, el proveedor proporcionará al cliente las evidencias recolectadas durante el proceso de gestión del caso en cuestión.

El cierre de una amenaza viene definido mediante la agrupación de los diferentes recursos maliciosos (URL, direcciones IP, cuentas de correo, etc.) en unidades denominadas casos, según los siguientes criterios:

Para las amenazas de Phishing y pharming y Malware, esta agrupación se lleva a cabo mediante la aplicación de una serie de reglas o criterios:

- Para un mismo instante de tiempo, todos los recursos online de un mismo dominio o dirección IP se agrupan dentro de un único caso (ej. http://fraude1.dominioX.com; http://fraude2.dominioX .com; etc.).

- Del mismo modo, dentro de un mismo caso sólo pueden existir URLs de un mismo dominio (ej. fraude.com) o dirección IP (ej. http://123.123.123.123/fraude).
- Si el fraude está alojado en un solo sitio, pero es accesible desde múltiples nombres de dominio o direcciones IP, todos estos recursos serán tratados como un único caso.
- Si una amenaza incluye recursos maliciosos en diferentes dominios alojados en sitios diferentes (diferentes ISPs, empresas de hosting, etc.) se tratarán como casos separados dentro de la misma amenaza.
- En caso de que, posterior a la resolución de un caso, reaparezcan URLs (las mismas u otras nuevas) pertenecientes al mismo dominio o dirección IP ya tratada, se reabrirá de nuevo el caso (sin coste asociado), siempre que no se haya cumplido el período de garantía (48 horas). Por el contrario, en caso de que el período de garantía hubiera expirado, se abrirá un nuevo caso (caso hijo), el cual será relacionado al con el caso anterior (caso padre) y se contabilizará como un nuevo caso.
- Los elementos asociados a un caso que no formen parte intrínseca del recurso malicioso principal (y por tanto su cierre no conduzca a la resolución final del fraude en cuestión) serán gestionados como relaciones del caso, y no serán contabilizados como caso. En este sentido, el criterio que va a definir cada resolución dependerá directamente de la naturaleza del fraude. A modo de ejemplo, podríamos mencionar los siguientes escenarios:
  - Una web redirectora en una página de phishing será generalmente tratada como relación de un caso (web de phishing)
  - Una cuenta de correo podrá ser gestionada como relación (ej. correo electrónico conteniendo la URL de la web de phishing) o como caso en sí mismo (ej. estafa de carta nigeriana).

  Para el resto de amenazas, cada recurso malicioso (perfil social, aplicación móvil, etc.) se corresponderá con un caso.

Peticiones bajo demanda

El proveedor debe disponer de todos los módulos, aunque TMB, inicialmente partirá de los módulos indicados, pudiendo utilizarse los indicados, de la bolsa de horas dedicadas para proyectos de la Oficina Técnica:

- Reputación y marca
  - Contenido ofensivo (A demanda)
  - Seguimiento de identidad digital (A demanda)
- Fraude online
  - Phishing y Pharming (A demanda)
  - Software malicioso (A demanda)
  - Carding (A demanda)
- Disrupción del negocio
  - Exposición de información (A demanda)
  - Hacktivismo (A demanda)
  - Activismo (A demanda)

- Vulneración de mecanismos de seguridad (A demanda)

4.5.1. Alcance

- 8 Marcas
- 17 dominios externos
- 4 dominios internos
- 4 dominios de correo
- 14 IPs de servicios público
- 300 IPs públicas
- 2 Productos Web (venta y Att cliente)
- 15 Perfiles de Redes Sociales
- 4 Aplicaciones móviles
- 50 Acciones de takedown
- 10 jornadas de analista de Seguridad para búsquedas en Dark Web u otras peticiones relacionadas en el ámbito de Vigilancia digital a petición de TMB.

5. Acuerdos de nivel de servicio (SLA)

Monitorización/Operación 24x7

En la siguiente tabla se muestran los SLA por el servicio:

TIEMPO DE RESPUESTA

Prioridad	Periodo de Notificación	Nivel de soporte
Crítica	30 minutos (*)	24/7
Alto	1h (*)	24/7
Media	4h (*)	24/7
Baja	NBD (*)	24/7

(*) la métrica objetivo hace referencia a la **primera acción de respuesta**, no a que el incidente se haya gestionado por completo dentro de este período de tiempo.

Clasificación de las prioridades:

Prioridad	Descripción
Crítica	TMB ha confirmado que la red está siendo atacada de forma sostenida, y/o que se ha producido un brote de virus a gran escala (o que afecte a activos críticos), y/o ha identificado una brecha a gran escala, que afectará de forma inminente a la reputación o al negocio del Cliente (incluida una violación del trabajo confidencial, Registros de Salud u otros datos controlados)
Alta	La infraestructura de TMB está bajo un ataque sostenido y/o varios sistemas se ven afectados por un virus, y/o se ha identificado una violación a gran escala que no incluye un impacto inmediato en la reputación comercial del cliente (trabajo no confidencial, información personal identificativa común como correo electrónico y nombre de usuario), y/o se informa de un ataque inmediato contra el cliente en los medios de comunicación
Media	Un solo servidor (no crítico) se ve comprometido por malware o las credenciales de un solo usuario están expuestas a través de malware o piratería
Baja	El sistema de un solo usuario está comprometido por malware, No es un ataque de impacto.

Respuesta delante de incidencias de Seguridad y análisis forense (CSIRT)

En la siguiente tabla se muestran los SLA por el servicio:

TIEMPO DE RESPUESTA

Prioridad	Periodo de Notificación	Nivel de soporte
Crítica	1 h	24/7
Media	4h	24/7
Baja	8 h	24/7

Clasificación de las prioridades:

Prioridad	Descripción
Crítica	Incidentes que tienen un impacto considerable (afectación a la confidencialidad, disponibilidad y la integridad) a información considerada crítica para la actividad de TMB y/o sistemas TIC críticos. El incidente con capacidad de afectación a gran cantidad de información valiosa y causó la degradación de servicios vitales de TMB. Estos incidentes pueden ser típicamente, malware destructivo, denegación de servicios, compromiso de sistemas, incidentes de hacking y violaciones de políticas que afecten a sistemas críticos o información crítica por TMB.
Media	Un solo servidor (no crítico) se ve comprometido por malware o las credenciales de un solo usuario están expuestas a través de malware o piratería
Baja	Incidentes de seguridad en sistemas no críticos para TMB

Penalizaciones aplicables al servicio regular (TABLA 5.1)

Ámbito	Descripción ANS	Cálculo	Periodicidad del cálculo	Umbral de cumplimiento	Tipo
Monitorización	Tiempo máximo de respuesta por incidencias Críticas y Altas	Tiempo objetivo transcurrido entre que se detecta/notifica hasta que se genera una respuesta del servicio	Se evaluará el cálculo mensualmente	Críticas >60 minutos (previsto 30m) Altas >2h (previsto 1h) Media >8h (previsto 4h	Muy grave Grave Leve
Respuesta delante de incidencias de Seguridad y análisis forense (CSIRT)	Tiempo máximo de respuesta por incidencias Críticas y Altas	Tiempo objetivo transcurrido entre que se notifica al CSIRT hasta que se genera una respuesta del servicio	Se evaluará el cálculo mensualmente	Crítica >2h (previsto 1h) Media >8h (previsto 4h) Baja >NBD (24h) (previsto 8h)	Muy grave Grave Leve
Oficina Técnica	Actividades del servicio de Pentesting ejecutadas	Diferencia entre el número de escaneos previstos y el número de escaneos realizados	Se evaluará el cálculo mensualmente	Inferior a lo establecido (4 simulacros x cuatrimestre)	Leve
Oficina Técnica	Notificación inmediata de detecciones con riesgo crítico, muy alto y alto hacia el responsable del servicio según procedimiento	Diferencia entre vulnerabilidades presentes en los informes y notificaciones efectuadas	Se evaluará el cálculo mensualmente	Inmediato al tener confirmación de la detección	Leve

Ámbito	Descripción ANS	Cálculo	Periodicidad del cálculo	Umbral de cumplimiento	Tipo
Monitorización	Tiempo máximo de entrega de informes de cierre en caso de incidencias críticas	Días transcurridos desde la fecha fijada para su entrega	Se evaluará el cálculo mensualmente	2 días laborables	Muy leve
Oficina Técnica	Tiempo de respuesta a la petición bajo demanda	Días transcurridos entre la demanda y la respuesta recibida del contratista	Se evaluará el cálculo mensualmente	5 días laborables	Muy leve
Oficina Técnica	Informe resumen del Comité Estratégico de seguimiento del servicio	Presentación del informe 2 días laborables posteriores a la reunión	Se evaluará el cálculo mensualmente	10 días laborables posteriores a la fecha establecida de entrega (2 días después de la reunión)	Muy leve
Oficina Técnica	Informe resumen del Comité Táctico mensual de seguimiento del servicio	Presentación del informe 2 días laborables posteriores a la reunión	Se evaluará el cálculo mensualmente	10 días laborables posteriores a la fecha establecida de entrega (2 días después de la reunión)	Muy leve
Oficina Técnica	Revisión del correcto funcionamiento de las plataformas de seguridad (si no se incluye en el comité táctico)	Presentación del informe 2 días laborables posteriores a la reunión	Se evaluará el cálculo mensualmente	10 días laborables posteriores a la fecha establecida de entrega (2 días después de la reunión)	Muy leve

6. Confidencialidad

La empresa colaboradora debe aceptar la Política de Seguridad Tecnológica y de la Información de TMB. El adjudicatario se compromete a no difundir y guardar el más absoluto secreto de toda la información a la que tenga acceso en cumplimiento del servicio actual ya la que sólo el personal autorizado por TMB. El adjudicatario será responsable de las violaciones del deber de secreto que puedan producirse por el personal bajo su cargo.

Se le obliga a aplicar las medidas necesarias para garantizar la eficacia de los principios de mínimo privilegio y necesidad de conocer por parte del personal que participe en el desarrollo del servicio.

Una vez finalizado el presente servicio, se compromete a destruir con las garantías de seguridad suficientes o devolver toda la información facilitada por TMB, así como cualquier otro producto obtenido como resultado del presente contrato.

La empresa colaboradora debe aceptar el compromiso de confidencialidad respecto a los datos a los que tendrá acceso y que son propiedad de TMB.

Los permisos de acceso a los sistemas y aplicación, en caso necesario, tendrán el nivel necesario para el trabajo a realizar y asignados a usuarios personales. En caso de precisarse del acceso con un usuario con privilegios elevados en el sistema se llevará a cabo a través de la herramienta que dispone TMB para este fin, de forma que queden trazadas las acciones que se realicen.

Cumplimiento de la ley Orgánica de Protección de Datos de Carácter Personal

La adjudicataria se compromete a cumplir cuántas obligaciones le son exigibles en materia de protección de datos personales tanto por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas por el respecto al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("RGPD") como por la ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos de Carácter Personal así como todas las demás normas legales o reglamentarias incidan, desarrollen o sustituyan las anteriores en este ámbito.

7. Modelo de relación

Estará basado en la figura del interlocutor/coordinador único entre el adjudicatario y el TMB.

Este interlocutor es fundamental para acompañar y apoyar el establecimiento de las políticas, buenas prácticas y controles de seguridad en el ámbito del servicio.

7.1. Gobernanza y reporting

El gobierno del servicio de ciberseguridad gestionada debe cumplir:

- Gestión centralizada a nivel transversal y de todos los subservicios.
- Generación la capa de reporting a diferentes niveles, táctico y operativo.
- Garantía de la implementación de un Cuadro de mando (Dashboard) integral con todos los indicadores identificados de los distintos subservicios.

7.2. Modelo organizativo del equipo de trabajo

El presente servicio objeto de licitación debe permitir cierta autosuficiencia a la hora de contactar, gestionar y resolver cualquier tipo de incidencias o tareas de proyectos que impliquen proveedores externos, sin que la interlocución dependa exclusivamente de los responsables de TMB.

Para dar respuesta a las necesidades planteadas por TMB, se pide tener un modelo de relación basado en 3 niveles, con el objetivo de:

- Garantizar el seguimiento y buen gobierno del servicio.
- Maximizar su alineamiento a las necesidades estratégicas y operativas de TMB mientras dure la prestación del servicio.

Así pues, este modelo organizativo se basa en el establecimiento de una relación entre el adjudicatario y TMB a tres niveles y comités:

- Nivel estratégico / Comité estratégico.
- Nivel táctico / Comité táctico.
- Nivel operativo / Comité operativo.

7.2.1. Nivel estratégico

Se define a nivel estratégico un comité ejecutivo que se reunirá de forma ordinaria dos veces al año con el fin de mantener un punto de contacto a alto nivel para asegurar el buen funcionamiento del servicio contratado. A este nivel, se propone que por parte del adjudicatario asista como mínimo la persona responsable de cuenta, el/la coordinadora del servicio, y por parte de TMB la persona responsable de la Dirección de Operaciones de TMB, así como el CISO y personas

responsables de seguridad IT y OT, así como la persona responsable de la gestión del servicio en TMB.

Los/las asistentes a este comité tendrán capacidad decisoria sobre los compromisos del mismo y en aquellos aspectos que puedan originar la modificación del servicio.

7.2.2. Nivel táctico

Se proponen reuniones mensuales para poder realizar un seguimiento del servicio y poder poner en común los puntos que se consideren necesarios exponer. Por parte del adjudicatario, asistirá el coordinador del servicio y, si fuera necesario, uno o varios especialistas de servicio que puedan aportar información relevante del servicio.

Por parte de TMB asistirá el responsable del servicio y, si fuera necesario, los técnicos especialistas.

La finalidad de estas reuniones mensuales será exponer:

- El estado del servicio.
- Las principales incidencias que hayan surgido o estén en activo.
- La situación de los proyectos y tareas en curso.
- Revisión del calendario previsto.

7.2.3. Nivel operativo

Se propone una reunión semanal de revisión técnica tipo "clínico" para poder resolver los temas más urgentes que pueda haber y realizar seguimiento técnico de los proyectos y tareas. Por parte del proveedor adjudicatario asistirá el coordinador o los especialistas involucrados si quiere delegarlo y por parte de TMB asistirán el responsable del servicio y los técnicos especialistas de seguridad necesarios.

El objetivo básico será tratar las problemáticas específicas que afecten al servicio prestado

7.2.4. Funciones y actividades de los niveles del modelo organizativo

Nivel estratégico / Comité estratégico:

- Seguimiento y control de la ejecución del contrato.
- Seguimiento y evaluación del servicio prestado. Analizará las necesidades del servicio y podrá decidir ampliaciones o reducciones del mismo. Validar el alcance general, objetivos y resultados esperados.
- Validación de la planificación de las tareas previstas a realizar.
- Verificación del cumplimiento de las especificaciones solicitadas.
- Propuestas de modificaciones/ampliaciones de Acuerdos de Nivel de Servicio (ANS).
- Seguimiento económico del contrato.
- Resolución de conflictos.
- Entregables mínimos esperados:

- Antes de la convocatoria:
  - Asistentes convocados.
  - Orden del día.
  - Documentación auxiliar.
  - Informes necesarios de los temas a tratar.
- Después de la reunión:
  - Acta con los acuerdos alcanzados y la toma de decisiones.
  - Convocatoria para la siguiente reunión: fecha, hora y lugar.

Nivel táctico / Comité táctico:

- Validación de las tareas de control de la explotación e implantación de los servicios.
- Revisión de informes mensuales de los diferentes servicios.
- Verificación del cumplimiento de los acuerdos de servicio establecidos.
- Aprobación de proyectos de mejoras.
- Seguimiento de la realización de mejoras y evolución del servicio regular.
- Verificación del desempeño de los ANS.
- Resolución de conflictos.
- Análisis y priorización de tareas.
- Validación de los procedimientos de mejora por parte de los Responsables de Seguridad.
- Análisis y control de la ocupación de los perfiles asignados por la consecución del servicio (informe semanal y acumulado mensual).
- Entregables mínimos esperados:
  - Antes de la convocatoria:
    - Asistentes convocados.
    - Orden del día.
    - Informe seguimiento del servicio
    - Documentación auxiliar.
    - Informes necesarios de los temas a tratar.
  - Después de la reunión:
    - Acta con los acuerdos alcanzados y la toma de decisiones.
    - Convocatoria para la siguiente reunión: fecha, hora y lugar.

Nivel operativo / Comité operativo:

- Seguimiento rutinario.
- Propuestas de mejora y cambios.
- En caso de identificarse riesgos o cambios significativos en la evolución del servicio se convocan las reuniones operativas para tratar el tema en cuestión.
- En caso de evidenciar un riesgo elevado, se procederá a convocar al Comité Estratégico o al Comité Táctico según se considere.
- Análisis de incidencias detectadas de los operadores que implican solicitar una reunión operativa.

- Análisis de peticiones que impliquen un control detallado debido a un impacto técnico, económico, de ejecución, etc.
- El comité podrá ser convocado por iniciativa tanto de TMB como del adjudicatario. El comité se constituirá en un máximo de 24 horas desde el momento de la convocatoria.
- Entregables mínimos esperados:
    - Antes de la convocatoria:
        - Asistentes convocados
        - Orden del día
        - Documentación auxiliar
        - Informes necesarios de los temas a tratar
    - Después de la reunión:
        - Acta con los acuerdos alcanzados y la toma de decisiones.
        - Convocatoria para la siguiente reunión: fecha, hora y lugar

8. Prestación del servicio

8.1. Horario

El adjudicatario tendrá que cubrir los horarios de lunes a viernes entre las 08:00 AM y las 14:00 PM, incluido el período vacacional donde se mantendrá operativo el servicio.

El adjudicatario cubrirá fuera del horario laboral definido la recepción y resolución de incidentes de nivel crítico alto.

Este horario no aplicará por los servicios requeridos 24x7x365 especificados en los servicios regulares.

8.2. Localización física

La prestación del servicio objeto de esta contratación debe cumplir con los siguientes ítems:

Salvo la presencia del Service Manager (que será de al menos 3 días en presencial), la ejecución de las tareas se llevará a cabo principalmente de forma remota.

Sin embargo, si TMB lo considera, por la naturaleza de la invención o incidencia, puede pedir realizar las tareas de forma presencial. En este caso, de no indicar otra cosa, se harán en la oficina de TMB situada en la siguiente dirección:

Centro de Apoyo Tecnológico - C/Josep Estivill, 47 - 08027, Barcelona

No se admitirán cargos que no estén incluidos en el precio de la oferta referentes a desplazamientos, dietas, ni alojamiento.

La solicitud de los servicios se realizará, en los casos en que no se trate de incidencia, con un período de antelación, a convenir entre las partes, nunca superior a una semana natural.

El servicio dispondrá de un referente que será el interlocutor con el responsable del servicio de TMB y se dispondrá de los recursos necesarios para finalizar las tareas en las fechas acordadas.

Se presentará una planificación de los trabajos a realizar para acordar con TMB la duración del trabajo en caso de que se trate de tareas que permitan esta planificación.

TMB facilitará que el adjudicatario realice las tareas y reuniones de forma virtual utilizando

herramientas de videoconferencia, herramientas colaborativas o conectividad segura.

A petición de TMB, algunas reuniones o actuaciones serán de obligada presencialidad, entre otras pueden ser:

- Las reuniones de nivel estratégico, táctico y operacional.
- Las incidencias de seguridad de nivel alto.
- Las tareas que requieran la realización de entrevistas o recogida de evidencias físicas.
- Y todas aquellas tareas en las que no sea posible el uso de la virtualidad para la realización de las mismas.

9. Recursos del contrato

Los recursos necesarios para cubrir los servicios que se piden serían cuantificados en dedicación:

Oficina técnica de Operación de Seguridad

- Service Manager 1 FTE 8x5 dedicación exclusiva a TMB con una presencialidad mínima de 3 días a la semana en TMB
- Equipo de analistas de seguridad 2 FTE
- Consultoría y proyectos: bolsa de horas: 80 Jornadas anuales

Servicio de Operación de Seguridad

- Servicio Nivel 1,2,3: 24X7X365

Administración Técnica de plataformas de seguridad

- Equipo de analistas de Seguridad Técnicos especialistas: 1 FTE 8x5

Equipo de Respuesta frente a Incidencias de Seguridad y análisis forense (CSIRT)

- 20 jornadas anuales (8x5) + 5 jornadas anuales (fuera 8x5), de especialistas para gestión de incidentes de impacto, investigación, análisis forense u otras tareas especializadas a petición de TMB.

Vigilancia Digital

- Servicios de vigilancia segundo alcance definido en el pliego
- Servicios de remediación: 50 Acciones de takedown anuales

NOTA: siempre que se indique horario 8x5 es en horario de oficina de TMB.

Recordar que al alcance de la licitación se incluye que el proveedor deberá proporcionar una herramienta **Simulación de Infracciones y Ataque (BAS)** para poder realizar las autorías/pentesting de TMB (a modo de ejemplo, Cymulate, Pentera, etc). Incluyendo los posibles módulos adicionales de escenarios avanzados que sean necesarios para prestar el servicio de forma adecuada y completa.

A continuación se detallan los tipos de perfiles que el adjudicatario deberá asignar al servicio, con sus responsabilidades:

- Responsable de cuenta.
- Service Manager (Coordinador del servicio de seguridad).
- Analistas de Seguridad / Especialistas.
- Consultores de seguridad de la información.

9.1. Responsable de Cuenta

El adjudicatario designará un único responsable de cuenta que será el referente para todos los contratos que tenga con TMB, siendo el último responsable de los de la prestación de los servicios.

Esta figura se mantendrá durante toda la vida del contrato en la gestión comercial, durante la ejecución del servicio y hasta la devolución del mismo, y será el interlocutor y responsable en caso de que se produzcan cambios en el alcance o coste de los servicios que impliquen una modificación contractual.

9.2. Service Manager

Será el interlocutor único frente a TMB y será el responsable de garantizar que la prestación del servicio es correcta. Es decir, garantizará el servicio asegurando la optimización del mismo y, por tanto, minimizando los posibles riesgos.

Deberá realizar principalmente las siguientes funciones:

- Garantizar la ejecución del servicio, tal y como se especifica en este pliego, asegurando todos y cada uno de los tiempos de respuesta pedidos y que TMB pueda requerir.
- Coordinar y supervisar de forma periódica el equipo a su cargo, comunicando en su caso los posibles cambios en éste, así como sus causas.
- Gestión de los riesgos detectados así como la presentación del plan de mitigación de los mismos.
- Detectar oportunidades de mejora.
- Elaboración de los informes de servicio y justificación del cumplimiento de los ANS.
- Garantizar la implementación del Dasboard/Cuadro de mando del servicio.
- Proponer e incorporar, si son aceptadas, mejoras en la gestión global del servicio.

En cuanto al recurso asignado, TMB tendrá la potestad de pedir cambio siempre y cuándo, y de forma justificada, éste no preste el servicio de forma satisfactoria por TMB.

El adjudicatario se compromete a mantener al coordinador durante la vigencia del contrato, pudiendo sustituirlo sólo por causas justificadas. En este caso, la persona que le sustituya deberá cumplir con la solvencia requerida, siendo TMB quien validará que el perfil se ajuste a la solvencia.

Por otra parte, el adjudicatario tendrá que solicitar por escrito cualquier cambio en el perfil y con una antelación suficiente que garantice un correcto traspaso de conocimientos para evitar afectaciones en el servicio. El cambio sólo podrá hacerse si previamente se ha validado por TMB el cumplimiento de los requisitos de solvencia anteriormente mencionados.

9.3. Analistas de Seguridad / Especialistas

Los especialistas serán los técnicos asignados al servicio por el adjudicatario que llevarán a cabo las tareas y actuaciones que requieran una especialización técnica para poder garantizar un resultado satisfactorio.

El equipo del adjudicatario que prestará el servicio en TMB contará con trabajadores que tengan perfiles de especialistas al menos en los siguientes ámbitos:

- Técnico especialista en hacking ético y pentesting.
- Analista de seguridad.
- Auditor en seguridad de la información y continuidad de negocio.
- Técnico especialista en seguridad de la respuesta a incidentes de seguridad de la Información.
- Profesional certificado en seguridad de la información en entornos cloud.
- Técnico administrador de plataformas tecnológicas (SIEM).
- Técnico especialista en informática forense e investigación interna

Tanto el coordinador del servicio como los perfiles especialistas asignados al servicio tendrán que cumplir los requerimientos expresados en el apartado de solvencia técnica del PCP.

9.4. Consultores en seguridad de la información

El perfil de consultores en seguridad de la información o consultores en ciberseguridad son quienes prestarán el servicio basado en bolsa de horas/Jornadas.

Estos perfiles deben cumplir las siguientes capacidades o competencias:

- Conocimiento profundo en las mejores prácticas de seguridad de la información y las tendencias actuales en ciberseguridad.
- Capacidad para evaluar riesgos y definir estrategias de mitigación.
- Conocimiento de las regulaciones de seguridad de la información relevantes como RGPD.
- Capacidad para traducir problemas técnicos en términos de comprensibles por las personas no técnicas.
- Habilidad para analizar situaciones complejas de seguridad y encontrar soluciones efectivas.
- Capacidad para crear informes de ejecutivos claros y concisos que resuman hallazgos o recomendaciones de seguridad de forma comprensible por la alta dirección u otros stakeholders.
- Habilidad para presentar datos técnicos y métricos de seguridad de forma visualmente atractiva mediante gráficos y tablas.
- Experiencia en la redacción de informes de evaluación de riesgos y documentación técnica que apoye la toma de decisiones informadas en seguridad de la información.
- Capacidad para gestionar una crisis en caso de incidente grave de seguridad.

- Compromiso con el aprendizaje constante y la actualización de conocimientos, dado que la ciberseguridad es un campo en constante evolución.