Pliego de Prescripciones Técnicas

Contratación del Servicio de Oficina Ciberseguridad de TMB

Expediente:
15013625

Octubre de 2025
Versión 1.0

Soluciones Corporativas
Área de Tecnología

Índice de contenidos

1. Introducción

Transportes Metropolitanos de Barcelona (TMB) es la denominación común de las empresas Ferrocarril Metropolita de Barcelona, S. A., Transportes de Barcelona, S. A., que gestionan la red de metro y bus del Área Metropolitana de Barcelona. También incluye las empresas Proyectos y Servicios de Movilidad, S. A., que gestiona el teleférico de Montjuïc; Transportes Metropolitans de Barcelona, S. L., que gestiona productos tarifarios y otros servicios de transporte, así como la Fundación TMB, que vela por el patrimonio histórico de TMB y promueve los valores del transporte público a través de actividades sociales y culturales.

La misión de TMB es ofrecer servicios integrales de movilidad, incluyendo metro y autobuses, que:

- Contribuyan a la mejora de la movilidad ciudadana y al desarrollo sostenible.
- Garanticen la prestación de un servicio excelente a la ciudadanía.
- Potencien las políticas de igualdad de oportunidades y responsabilidad social.
- Utilicen de forma eficiente los recursos públicos

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.

La Ciberseguridad se ha consolidado como un elemento esencial para garantizar la protección de la información y la continuidad operativa de los servicios en entornos digitales. Su objetivo es asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos, así como la resiliencia de los sistemas TIC y OT de las amenazas.

En este contexto, la prestación de servicios públicos debe realizarse con plenas garantías de seguridad, tanto para los ciudadanos como para las infraestructuras tecnológicas que los soportan. Esto implica disponer de mecanismos de identificación, prevención, protección y respuesta ante incidentes que puedan comprometer la seguridad de los sistemas de información.

Para abordar estos retos, es imprescindible disponer de un modelo de gobierno de la Ciberseguridad que permita una gestión eficiente, coordinada y alineada con los objetivos estratégicos de la organización. Este modelo debe integrarse en un marco de cumplimiento normativo que incluya las directrices establecidas por las regulaciones nacionales y europeas, como el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD), la Directiva NIS2 y otras normativas sectoriales aplicables.

Asimismo, la Ciberseguridad debe ser concebida como una estrategia dinámica y proactiva, capaz de adaptarse a los cambios del entorno tecnológico y a las nuevas formas de amenaza. Esta estrategia debe contemplar la supervisión continua de la actividad, la detección precoz de vulnerabilidades, la respuesta rápida a los incidentes y la mejora continua de los mecanismos de protección.

Este modelo se mantiene a partir de una Oficina de Ciberseguridad que gestiona las tareas derivadas de la definición del gobierno de la seguridad hasta la gestión de riesgos y supervisión del cumplimiento de las normativas y controles establecidos en el modelo entre otros.

2. Objeto de la licitación

El objeto de la licitación es la contratación de servicios profesionales para la prestación del servicio de Oficina de Ciberseguridad con el objetivo de dar respuesta a las necesidades de TMB en los siguientes ámbitos:

- Gobierno, Riesgo y Cumplimiento (GRC)
- Auditorías
- Cultura y capacitación
- Apoyo y Gestión de la demanda
- Portfolio, programas y proyectos
- Gestión de incidentes de Ciberseguridad

3. Alcance

El alcance de este contrato consiste en el gobierno, apoyo y capacitación en materia de Ciberseguridad, con una visión global y transversal a todo TMB. Esto incluye:

- Tener una visión y gestión global de los procesos de negocio
- Tener una visión y gestión global del riesgo en Ciberseguridad asociados a los procesos de negocio
- Identificar a los responsables de la información, responsables de Seguridad de los diferentes negocios e sistemas (TIC/OT), promover revisiones de cumplimiento
- Promover auditorías de Seguridad
- Tener un marco de cumplimiento de la Ciberseguridad transversal
- Asesorar a TMB en materia de Ciberseguridad
- Tener conocimiento de la gestión de riesgos para entornos TIC y OT
- Tener conocimientos ente la gestión de proyectos y requerimientos de Seguridad en los mismos.

4. Descripción del servicio

4.1. Gobierno Riesgo y Cumplimiento

El grado de complejidad y número de aspectos a tener en cuenta con el fin de definir y garantizar un nivel de seguridad aceptable para la organización, hace necesarios el establecer un modelo y una estructura transversal a todas las empresas que forman parte de TMB en el ámbito de la Ciberseguridad con capacidad para controlar y dar visión conjunta del nivel de seguridad actual y ayudar a tomar todas las decisiones que así lo requieran.

Para llevarlo a cabo se deben dotar de ciertas acciones como un marco de referencia normativo coherente con los diferentes negocios que identifique normas, criterios, políticas para asegurar y controlar el nivel de seguridad de la información.

Dentro de este bloque de Gobierno riesgo y cumplimiento el adjudicatario prestará los siguientes servicios

4.1.1. Gobierno

Este servicio comprende las siguientes tareas.

- **Definición y creación de indicadores e informes**: La definición y creación de indicadores es clave para poder monitorizar el estado de la Ciberseguridad. El adjudicatario definirá de manera conjunta con el área de Ciberseguridad los indicadores clave de rendimiento (KPI). Se espera que el licitador aporte ideas de indicadores. También se definirán los diferentes informes a presentar, contenido y periodicidad. Estos KPIs e informes estarán presentes en cada una de las actividades que se soliciten durante la licitación. Estos informes y KPIs permitirán a la dirección y otros colectivos disponer de una visión clara y actualizada sobre el estado de Ciberseguridad, nivel de cumplimiento, riesgos, evolución etc.

  .
- **Creación del cuadro de mando de Ciberseguridad**: Se desarrollará un cuadro de mando integral que consolide los indicadores definidos, facilitando la toma de decisiones estratégicas y operativas. Este cuadro deberá ser accesible, dinámico y capaz de integrar datos procedentes de diferentes sistemas y herramientas corporativas.

  .
- **Revisión y definición del modelo de relación de gobierno de la Ciberseguridad:** Se revisará el modelo actual de gobernanza y se definirán las relaciones entre los diferentes

actores implicados (unidades de negocio, departamentos técnicos, órganos de dirección), estableciendo roles, responsabilidades y flujos de comunicación claros.

- **Redacción de los diferentes modelos de relación:** Se redactarán los documentos que formalicen los modelos de relación y gobernanza, incluyendo protocolos de coordinación, comités, y mecanismos de supervisión y control.

- **Revisión periódica y actualización de los procedimientos y tareas del gobierno de la Ciberseguridad:** Se garantizará la revisión y actualización periódica de los procedimientos asociados al gobierno de la Ciberseguridad, asegurando su adecuación a la evolución normativa, tecnológica y organizativa.

4.1.2. Riesgo

Este servicio responde al objetivo de gobernar el riesgo de Ciberseguridad corporativo (tanto IT como OT) para dar una visión completa de la gestión de riesgos. Los riesgos de Ciberseguridad aunque se gestionarán y controlarán desde la Oficina de Ciberseguridad se integrarán con el área de riesgos globales de TMB.

Esta gestión se aleja de la visión de riesgo únicamente como controles no cumplidos. Esta gestión debe tener una relación estrecha con el resto de áreas operativas y de proyecto de TMB para poder valorar mejor y con más amplitud estos riesgos.

Este servicio incluye las siguientes actividades:

- **Definición del catálogo de amenazas IT/OT:** Elaboración de un catálogo completo de amenazas que afecten a entornos IT y OT teniendo en cuenta las particularidades de los sistemas corporativos e industriales. Este catálogo deberá estar contrastado y validado con los diferentes departamentos de Seguridad y técnico de las diferentes unidades de negocio (Bus, Metro y aTec)

- **Definición de metodologías:** Establecimiento de metodologías para el análisis y gestión de riesgos basadas en estándares reconocidos y adaptadas a las necesidades de la organización. Tanto por IT como en OT. El adjudicatario propondrá una o dos metodologías y será TMB quien aprobará la metodología a aplicar. La metodología debe permitir gestionar los riesgos dentro del marco de requerimientos de la ENS.

- **Ejecución de análisis de riesgos:** Se realizarán evaluaciones periódicas de riesgos sobre sistemas, procesos y activos (mínimo críticos) identificando vulnerabilidad, impactos, probabilidades y asignando responsables de su mitigación. Además, se dará soporte a las diferentes áreas y unidades corporativas cuando no se haya podido realizar un análisis de riesgos ejecutando la tarea específica.

- **Seguimiento de riesgos:** Implantación de un proceso continuo de monitorización y seguimiento de los riesgos identificados, incluyendo su evolución y estado de mitigación.

- **Reporting:** Generación de informes periódicos que reflejen la situación de los riesgos, las acciones de mitigación y las tendencias, para facilitar la toma de decisiones estratégicas, así como la definición e implantación de indicadores del estado del riesgo que deberá estar tanto en la herramienta de GRC como en el QdC Global de Ciberseguridad

- **Identificación y centralización de riesgos de Ciberseguridad (nuevos o existentes)**: Consolidación en un repositorio único de los riesgos detectados, tanto nuevos como existentes, asegurando su trazabilidad y gestión coordinada. Los inputs internos para poder identificar los riesgos son: auditorías, proyectos, seguimiento de proveedores, área de calidad y cumplimiento, áreas de Buen Gobierno, incidentes de Seguridad, indicadores del QdC, excepciones, etc.

4.1.3. Cumplimiento

Este servicio incluye las siguientes tareas necesarias para asegurar el cumplimiento de la normativa aplicable y la correcta gestión de los requisitos legales y regulatorios en materia de Ciberseguridad en cada uno de los negocios y diferentes entidades que conforman TMB.

- **Realización del mapa de trazabilidad Normativa:** Elaboración de un mapa que identifique todas las normativas aplicables a TMB con los procesos, sistemas y controles existentes garantizando la trazabilidad y el seguimiento del cumplimiento. Se debe tener en cuenta toda la normativa aplicable TMB de manera genérica pero también se debe tener en cuenta las Normativas específicas de cada negocio según el sector que aplique

(p.exe: Bus, Metro) tanto por la parte IT como la parte OT. Se partirá de ENS, NIS2 como empresa de sector público pero se debe tener en cuenta otras.
Este mapa de trazabilidad también debe tener un cruce de controles de cada una de las normas con el fin de identificar requisitos comunes a las normas y simplificar el control y la gestión de las evidencias de cada uno.

- **Servicio continuo de revisión de la Normativa aplicable**: El adjudicatario deberá velar por la monitorización y actualización periódica de la normativa vigente, incluyendo cambios legislativos, regulatorios y estándares sectoriales, nuevas normas, leyes derogadas, actualizadas, etc. Con el fin de asegurar la adaptación constante de la organización.
  Cuando se detecte cualquier modificación el adjudicatario será el encargado de actualizar el mapa de trazabilidad normativa con el análisis y los cambios aplicables.

- **Declaración de aplicabilidad:** Redacción y mantenimiento de la declaración de aplicabilidad que defina los controles implementados y justificación de los no aplicables, de acuerdo con las normativas y marcos de referencia.

- **Análisis de impacto:** Realización de análisis de impacto derivados de los cambios normativos, tecnológicos u organizativos, para determinar las implicaciones en procesos y controles

- **Diseño plan de cumplimiento ENS:** Definición del plan estratégico para cumplimiento del Esquema Nacional de Seguridad (ENS), analizando el modelo actual y definiendo el modelo hacia el nivel adecuado según la naturaleza de la organización, incluyendo objetivos, acciones, plazos, responsables, estimaciones, kpis, etc.

- **Ejecución del plan de cumplimiento**: Implementación de las medidas definidas en el plan, coordinando las acciones con las áreas implicadas y asegurando el seguimiento y control de la ejecución.

- **Definición del modelo de relación y colaboración por medidas derivadas del plan de cumplimiento:** Establecer los roles, responsabilidades y canales de comunicación

entre las diferentes áreas para la correcta implementación de las medidas. Todo este modelo quedará reflejado en un documento

- **Apoyo y colaboración con el Delegado de protección de datos (DPD):** El adjudicatario colaborará con el DPD dando apoyo técnico a los requerimientos impuestos por RGPD y la LOPDGDD y otras normas aplicables.

- **Apoyo a diferentes áreas de negocio y departamentos:** Asesoramiento sobre procedimientos, protocolos y acciones derivadas de la normativa aplicable, adaptándolos a las necesidades específicas de cada unidad. Apoyo en la redacción de los procedimientos, protocolos y acciones derivadas, así como supervisión de que se incluyen todos los aspectos requeridos a nivel de cumplimiento.

- **Gestión de excepciones:** Desde la oficina de Ciberseguridad se tendrá control, seguimiento y aprobación sobre las excepciones de Ciberseguridad aplicadas y nuevas que van en contra de una Norma. Se definirá y se implementará un procedimiento con el fin de identificar, documentar y aprobar las excepciones al cumplimiento normativo con un análisis de riesgos asociados. En este procedimiento podrán estar involucrados otras personas de otros departamentos o unidades de negocio. Es responsabilidad de la Oficina de Ciberseguridad (y por tanto del licitador) definir el mecanismo de solicitudes (teniendo en cuenta las herramientas de TMB actuales) y tanto la solicitud como el seguimiento de las medidas compensatorias por la temporalidad de las excepciones aprobadas. El procedimiento también deberá incluir el seguimiento de la excepción, notificaciones al peticionario avisando de la caducidad de la misma y las acciones derivadas una vez se haya caducado y no renovado o no aprobado la renovación además de las dependencias y comunicaciones con otros servicios (por ejemplo: gestión de riesgos) Esta tarea no prevé la compra de una nueva herramienta.

- **Identificación y clasificación de activos globales**: Desde la Oficina de Ciberseguridad se trabajará con otros departamentos y/o áreas de negocio con el fin de tener un inventario global e unificado de activos (tanto IT como OT) con su clasificación para el cumplimiento normativo, asegurando su protección y gestión adecuada.

- **Apoyo y consultoría:** A partir de cualquier tarea derivada de cumplimiento, apoyo y consultoría especializada para atender necesidades puntuales relacionadas con las tareas de la Oficina de Ciberseguridad

- **Mejora continua de metodología, cuerpo normativo:** Revisión y evolución constante de la metodología de cumplimiento, actualizaciones e integraciones. Se espera por parte del adjudicatario pro actividad en la evolución del servicio aportando ideas, mejoras, automatizaciones, etc de las tareas que se desarrollarán en toda la Oficina de Ciberseguridad.

4.1.4. Herramienta de Gobierno riesgo y cumplimiento

Actualmente TMB no dispone de ninguna herramienta de GRC. El adjudicatario será el encargado de proporcionar una para llevar el servicio. Será el encargado de todo el ciclo de vida de la misma (diseño, implantación, explotación y mantenimiento de la misma). Una vez implantada será la herramienta principal del servicio para hacer seguimiento y control.

El adjudicatario deberá llevar a cabo el mantenimiento de la misma por lo tanto deberá:

- Establecer mecanismos necesarios para automatizar la interoperabilidad de esta herramienta con otros sistemas corporativos de los que se alimenta y con aquellos a los que servirá de fuente de actualización de la información
- Evaluación constante del estado de la herramienta
- Proponer evoluciones y mejoras
- Velar por el estado de vulnerabilidades de la misma y actualizaciones
- La gestión de los usuarios deberá integrarse con la herramienta de gestión de accesos e identidad de TMB.

El adjudicatario documentará toda la metodología, implantación, procedimientos, guías y otros documentos necesarios relacionados con la puesta en marcha de la herramienta, la configuración, interconexión de la herramienta con otros sistemas de información con los que se deba intercambiar información.

4.2. Auditorías

Este servicio tiene como objetivo verificar el nivel de cumplimiento, eficacia y adecuación de los controles de Ciberseguridad implantados, así como identificar oportunidades de mejora para reforzar la postura de Ciberseguridad de la organización. Estas actividades ayudarán a la Organización a priorizar las resoluciones de los incumplimientos que se detecten. Aunque este servicio se realizará desde la Oficina de Ciberseguridad deberá estar alineado y coordinado con el área de Calidad de TMB. Las actividades incluidas son:

- **Diseño de un plan anual de auditorías:** Elaboración de un plan estratégico que defina el calendario, alcance y objetivos de las auditorías a realizar durante el año, priorizando áreas críticas y sistemas críticos

- **Ejecución del plan de auditorías:** Realización de las auditorías programadas según el plan anual, aplicando metodologías reconocidas y asegurando la cobertura de los requisitos normativos y de seguridad.

- **Auditorías puntuales:** Ejecución de auditorías específicas respuesta a incidentes, cambios significativos, requerimientos internos o necesidad detectada. El tipo de auditoría puede ser tanto de cumplimiento Normativo, como de vulnerabilidades, etc.)

- **Auditorías parciales:** Revisión focalizada en procesos, sistemas o controles determinados, para validar su correcta implementación y eficacia.

- **Apoyo a auditorías externas hacia TMB:** Coordinación y asistencia en auditorías realizadas por terceros, facilitando la información necesaria y asegurando la correcta gestión de las evidencias.

- **Seguimiento y control sobre las mejoras identificadas en las revisiones** Centralización y seguimiento de las acciones correctivas derivadas de las auditorías, asegurando su implantación y verificación en los plazos establecidos.

Todas las actividades serán medidas y algunas generarán informes a pactar con el adjudicatario, tal y como indica el punto 4.1.1 de la licitación.

4.3. Cultura y capacitación

Las personas son la primera línea de defensa ante las amenazas digitales, más allá de la tecnología y son el principal vector de ataque.

En una organización tan grande y con perfiles operativos tan diferentes es esencial establecer una cultura de Ciberseguridad sólida y transversal.

La capacitación y la concienciación permite reducir este riesgo, asegurando que cada persona entienda su papel en la protección de los activos corporativos y disponga de las competencias necesarias para actuar de manera segura.

Este servicio incluye las siguientes tareas:

- **Análisis de los perfiles actuales de la compañía:** Identificación y clasificación de los perfiles profesionales existentes, teniendo la cuenta el papel que desempeñan en la compañía, su interacción con sistemas IT y OT responsabilidades, conocimiento, etc. con el fin de tener diferentes perfiles a los que poder desarrollar contenido a medida de sus necesidades.

- **Definición de un plan de formación:** Diseño de un plan formativo específico para cada perfil detectado, asegurando que las competencias adquiridas respondan a las necesidades operativas y estratégicas de la organización

- **Diseño de un plan de concienciación transversal:** Creación de un programa global de concienciación orientado a toda la organización, con campañas, materiales divulgativos, acciones periódicas para reforzar la cultura de la seguridad. Este plan debe ser original y dinámico.

- **Ciber ejercicios:** Planificación y ejecución de Cibersimulacros (ejemplo: ejercicio de respuesta a incidentes, pruebas de phising, crisis simuladas, etc) con el fin de evaluar la preparación y capacidad de la reacción de los equipos. Para cada ciber ejercicio se hará una evaluación y se medirá si la respuesta ha sido adecuada, si se han detectados gaps

a los procedimientos, etc. (el contenido del informe se definirá con el adjudicatario durante la prestación del servicio)

Todas las actividades serán medidas y algunas generarán informes a pactar con el adjudicatario, tal y como indica el punto 4.1.1 de la licitación.

4.4. Apoyo y gestión de la demanda

En una organización como TMB la gestión eficiente de la demanda y el control de los proveedores son elementos importantes para garantizar la seguridad y cumplimiento normativo. Directivas como NIS2 y el Esquema Nacional de Seguridad (ENS) que son de aplicación a TMB establecen obligaciones específicas para entidades del sector público, incluyendo la necesidad de supervisar a los proveedores y terceros que acceden a sistemas o datos de TMB. Este control es esencial para reducir riesgos derivados de la cadena de suministro y asegurar que las medidas de Ciberseguridad se aplican de manera homogénea.

El servicio de Apoyo y Gestión de la demanda tiene como objetivo centralizar, priorizar y dar respuesta a las necesidades relacionadas con la Ciberseguridad. Las actividades incluidas son:

- **Ciberseguridad en las licitaciones:** Esta actividad incluye el análisis de las medidas actuales que se incluyen tanto de carácter técnico como requisitos de cumplimiento a los proveedores referente a ENS. El adjudicatario hará este análisis actual y propondrá mejoras sobre esta documentación. El adjudicatario participará en cada una de las licitaciones actuales prescribiendo los requerimientos necesarios en base al objeto licitado y validando en fases posteriores a la definición de requerimientos que la documentación aportada por ganador de la licitación es la correcta. Además interactuará con otras áreas internas con el fin de automatizar este proceso.

- **Seguridad en los proveedores:** Verificación y seguimiento del cumplimiento de requisitos de seguridad por parte de los proveedores durante todo el ciclo de vida de la contratación. Esta actividad puede incluir tanto auditorías al proveedor como validaciones que los certificados de cumplimiento siguen vigentes.

- **Atención al buzón de correo genérico:** Existe una cuenta de correo genérica de Ciberseguridad. El adjudicatario hará la gestión y respuesta de las consultas, comunicaciones, peticiones solicitadas a través del buzón. Este buzón no es la entrada

de incidentes de Ciberseguridad o peticiones de seguridad de los usuarios, ya que hay otros mecanismos y órganos para estas gestiones más técnicas.

- **Registro y clasificación de nuevas peticiones:** Registro de las nuevas solicitudes, peticiones, consultas con su clasificación por tipología, priorización, y otros campos.

- **Resolución de consultas:** Atención y resolución de las diferentes dudas planteadas por las diferentes áreas de la organización.

- **Apoyo a la evolución de la gestión de la demanda y peticiones de apoyo:** Se espera que el adjudicatario realice mejora continua sobre los procesos actuales de la gestión de la solicitada, adaptándolos a nuevas necesidades y requisitos normativos. Además de participar de cualquier evolutivo y automatización de las mismas.

4.5. Portfolio, programas y proyectos

La gestión de programas y proyectos es un pilar fundamental para garantizar que las iniciativas de Ciberseguridad se ejecuten de manera ordenada, eficiente y alineada con los objetivos estratégicos de la organización. En una organización como TMB con alta complejidad operativa, es esencial disponer de un marco que asegure la integración de la seguridad en todas las fases del ciclo de vida de los proyectos, desde el diseño hasta el cierre. Este servicio permite coordinar esfuerzos, priorizar acciones y asegurar que los proyectos cumplan con los requisitos normativos y las mejores prácticas.

Las actividades incluidas son:

- **Tener un programa de proyectos de Seguridad:** Crear y actualizar un programa global que agrupe todos los proyectos de Seguridad en curso y planificados.

- **Apoyo a la edición del procedimiento de gestión de proyectos:** Asistencia en la definición y mejora de los procedimientos corporativos para la gestión de proyectos, incorporando requisitos de Seguridad.

- **Realización de formularios o checklist de control en las diferentes fases:** Creación de herramientas de control tanto al inicio del proyecto como una parte de seguimiento y

al cierre del mismo para verificar que los requisitos de Seguridad quedan bien definidos como validados su ejecución y antes de entrar en servicio.

- **Apoyo a la realización de los procedimientos internos de la Oficina de Ciberseguridad dentro del ciclo de vida de los proyectos:** Revisión de la documentación actual y redacción de los procedimientos y protocolos internos de la Oficina de Ciberseguridad para la ejecución de estas tareas

- **Registro de nuevos proyectos:** Alta y clasificación de proyectos, asegurando la trazabilidad y el seguimiento

- **Participación en los diferentes programas y proyectos:** Presencia en los diferentes proyectos y programas en comités, reuniones, grupos de trabajo con el fin de garantizar la incorporación de la seguridad en el ciclo de vida de los proyectos.

- **Seguimiento de cada proyecto:** Monitorización periódica del estado, riesgos y desviaciones de los proyectos

- **Gestión de proyectos PM:** Participación activa como responsable de proyecto (PM) en aquellas iniciativas de Ciberseguridad que, por su **estrategia, complejidad, criticidad o impacto directo en la organización**, requieran una gestión dedicada y coordinada. La Oficina de Ciberseguridad asumirá la dirección operativa del proyecto, incluyendo la **planificación, seguimiento, coordinación de equipos, gestión de riesgos y reporting**, asegurando la alineación con los objetivos estratégicos de TMB y la correcta integración de la seguridad en todas las fases del ciclo de vida del proyecto.

- **Definición y redacción del modelo de relación con riesgos y excepciones:** Establecer los protocolos de comunicación y gestión entre los diferentes proyectos, y la gestión de riesgos de Ciberseguridad y excepciones de Ciberseguridad para garantizar el correcto aviso y registro de detección a raíz de la ejecución de un proyecto

- **Apoyo en la definición del Plan Director de Seguridad (PDS):** Apoyo en la elaboración del PDS, alineado con los objetivos estratégicos de seguridad.

- **Seguridad en el diseño (arquitecto):** Incorporación de criterios de Ciberseguridad en la fase de diseño e implantación actuando como consultor. Proponiendo soluciones adecuadas, valorando soluciones planteadas, etc. Esta figura tendrá relación con otros arquitectos de la compañía. Se espera que este arquitecto haga revisiones fuera de proyectos y detecte arquitecturas mejorables, arquitecturas que van en contra de la normativa y se planteen soluciones y apoyo a la implantación.

4.6. Gestión de incidentes de seguridad

La gestión de los incidentes de seguridad se gestiona desde el SOC (que no depende funcionalmente de la Oficina de Ciberseguridad).

La normativa aplicable tanto nacional como europea, obliga a notificar incidentes de seguridad relativos a la Ciberseguridad. Desde el servicio se realizarán las siguientes tareas:

- **Revisión protocolos y procedimientos**: Se revisará el modelo actual de notificación y de coordinación con el SOC con el fin de validar e implementar los mecanismos y procesos con el fin de realizar las notificaciones de incidentes de Seguridad
- **Apoyo a la orquestación de los incidentes de Seguridad graves**: Coordinación interna y externa en casos de Ciber incidentes de seguridad que quedan fuera del alcance del SOC
- **Training ciber incidentes**: Sesiones sobre ciber incidentes, con el fin de explicar a las personas involucradas su rol y responsabilidad Y acciones ante un incidente de seguridad

Además, se realizarán revisiones periódicas e informes sobre los incidentes. El detalle de los informes y los KPIs se definirán con el adjudicatario al inicio del contrato.

5. Modelo de prestación del servicio

El modelo de prestación describe cómo se organizará y se ejecutará el servicio de la Oficina de Ciberseguridad. Se definen los mecanismos operativos, la disponibilidad, los perfiles profesionales implicados y la coordinación con el equipo interno de TMB, con el objetivo de garantizar una prestación eficiente, segura y alineada con las necesidades de la organización.

5.1. Tipología de servicio

El servicio objeto de esta licitación se prestará de manera **continuada**, con el objetivo de dar apoyo especializado en materia de Ciberseguridad a la organización. La oficina externa actuará como extensión del equipo interno de TMB, contribuyendo a la gestión proactiva de todas las tareas descritas en la descripción del servicio.

5.2. Modalidad de prestación

La prestación del servicio se llevará a cabo en **modalidad híbrida**, combinando la presencia física y el trabajo remoto según las necesidades operativas.

Se prevé la figura de un/a **responsable del servicio**, que estará presencialmente en las instalaciones de TMB **tres días por semana**, y el resto en modalidad remota. Esta figura actuará como interlocutor/a principal con la organización y facilitará la coordinación entre el equipo externo e interno. Por defecto el responsable del servicio estará ubicado en la oficina Corporativa de Zona Franca

El equipo técnico trabajará principalmente en remoto.

Tanto el responsable del servicio como el equipo técnico deberán tener **la posibilidad de desplazarse a otras instalaciones de TMB** para la realización de tareas específicas que requieran presencia física. Estos desplazamientos serán **planificados previamente** y no generarán **ningún coste adicional** para TMB.

La dirección de la oficina Corporativa es:

TMB Oficinas Corporativas – Edificio Zona Franca II
Dirección: Calle 60, 21-23 Sector A 08040 Barcelona

5.3. Disponibilidad del servicio

El adjudicatario deberá cubrir el servicio de lunes a viernes de 08:00 AM a 16:00 PM, incluido el periodo vacacional donde se mantendrá operativo el servicio. Si se tendrán en cuenta el calendario de fiestas de Cataluña y municipio.

Sin perjuicio del horario ordinario del servicio, en caso de incidente grave de ciberseguridad, emergencia operativa o situación excepcional que pueda afectar a la continuidad del servicio, la seguridad de la información o los sistemas corporativos, el adjudicatario deberá estar disponible para prestar apoyo fuera del horario establecido, de manera puntual y extraordinaria, a requerimiento de TMB.

5.4. Equipo de trabajo

El adjudicatario propondrá un equipo de trabajo adecuado para la ejecución de los servicios.

Es necesario que los licitadores detallen en sus propuestas cuál es la organización que proponen para el servicio, teniendo en cuenta que deberán dotar al personal necesario para asegurar las funciones que son objeto de este contacto descritas en el apartado 4 de la licitación.

La empresa adjudicataria deberá proponer un **equipo de trabajo adecuado** para la prestación del servicio, **asegurando su continuidad y estabilidad** durante toda la vigencia del contrato. En su propuesta, deberá detallar los **recursos asignados**, incluyendo los **perfiles profesionales**, las **funciones asociadas** y las **certificaciones técnicas correspondientes**. No obstante, TMB establece como mínimos obligatorios los perfiles que se describen a continuación, considerándolos **imprescindibles** para el correcto desarrollo del servicio.

A continuación, se detallan los diferentes roles necesarios con el fin de llevar a cabo las funciones descritas anteriormente. El listado de responsabilidades es una aproximación de mínimos, pero no están especificadas todas las tareas previamente descritas. Se espera que en las ofertas presentadas se planteen una propuesta con el detalle de los perfiles y tareas que se deben acometer dentro de la Oficina de Ciberseguridad donde incluya todas las tareas a realizar repartidas en los diferentes perfiles. Las tareas aquí mencionadas son las que principalmente serán objeto de revisión en el seguimiento del contrato.

Se espera un equipo dedicado para cada perfil. TMB controlará que así sea y cualquier cambio pasará por los requerimientos de notificación detallados más abajo:

PERFIL	DESCRPIPCIÓN
Responsable del servicio	**RESPONSABILIDADES MÍNIMAS**
	Interlocutor único ante TMB. Responsable de garantizar que la prestación del servicio es correcta. Coordinador global que realizará principalmente las siguientes funciones: • Garantizar la ejecución del servicio tal y como se especifica en el pliego • Coordinar y supervisar el equipo a su cargo y comunicar a TMB posibles cambios con los motivos, garantizando los requerimientos mencionados sobre el cambio de personal • Gestión de la planificación de las tareas • Gestión de los riesgos detectados durante el servicio, así como el plan de mitigación de los mismos • Seguimiento de la calidad del servicio • Detectar oportunidades de mejora • Elaboración de los informes de servicio y justificación de cumplimiento de ANS • Garantizar la implementación del Cuadro de Mando del servicio • Proponer e implementar mejoras en la gestión del servicio (previamente aceptadas por TMB) • Participación en los comités del servicio • Elaboración de informes y kpis
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los 5 últimos años gestión de servicios de Ciberseguridad Acreditar 3 años de experiencia en gestión de oficinas de Ciberseguridad (de los últimos 5 años) Acreditar experiencia en entornos públicos o grandes organizaciones que combinen sector IT y OT Acreditar conocimiento y experiencia en gobernanza de la Ciberseguridad Acreditar conocimiento y experiencia en normativas (ENS, ISO 27001) Acreditar conocimientos en gestión de proyectos
	TITULACIONES
	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN

	Dedicación completa con presencialidad en oficinas de TMB 3 días por semana – 1 FTE (Full Time Equivalente)

PERFIL	DESCRPIPCIÓN
Consultor GRC	**RESPONSABILIDADES MÍNIMAS**
	Especialista en estándar y normativas de seguridad, elaboración de cuerpos normativos de seguridad , gestión de riesgos de seguridad de la información y herramientas GRC así como cumplimiento técnico de la legalidad • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación y seguimiento del marco normativo corporativo • Apoyo, análisis, elaboración de informes y asesoramiento del cumplimiento técnico de leyes aplicables a TMB • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación y seguimiento de gestión de riesgos (metodologías, análisis y seguimiento) • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación y seguimiento de gestión de excepciones (metodologías, análisis y seguimiento) • Control y seguimiento, soporte, asesoramiento de los niveles de cumplimiento de proveedores de TMB • Elaboración cuadros de mando • Elaboración de informes y kpis
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los últimos 5 años, 3 años de experiencia en servicios de consultoría de GRC Acreditar participación (preferentemente liderazgo) en más de un proyecto del ámbito de elaboración de normativas y mapas de trazabilidad normativa Acreditar participación en elaboración de análisis de riesgos en los sectores IT y OT Acreditar conocimiento en normativas de sector IT y OT Acreditar conocimiento en metodologías de gestión de riesgos Acreditar el conocimiento del uso y explotación de herramientas de GRC, ya sea en proyectos donde ha implantado la herramienta en un cliente o como servicio haciendo uso de las mismas.
	TITULACIONES

	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN
	Dedicación 2 FTE (Full Time Equivalente)

PERFIL	DESCRPIPCIÓN
Auditor	**RESPONSABILIDADES MÍNIMAS**
	Especialistas en realizar auditorías de diferentes ámbitos. • Cumplimiento: Protección de datos, Esquema Nacional de Ciberseguridad (ENS), sistemas de gestión de seguridad de la información (SGSI), NIS2, auditorías sector OT • Técnicas: Pentest, análisis de vulnerabilidades, análisis de aplicaciones, análisis de aplicaciones móviles, análisis de código (estático y dinámico) Principales tareas a realizar: • Definición y aprobación del Plan Anual de auditorías • Ejecución de auditorías internas de cumplimiento • Ejecución de auditorías técnicas • Apoyar en la ejecución de auditorías externas de cumplimiento • Apoyo a las diferentes áreas de negocio, departamentos sobre las mejoras surgidas • Gestión del seguimiento de las correcciones • Elaboración de informes y kpis • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación y seguimiento de auditorías de ENS • Auditorías y control de proveedores
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los 5 últimos años, 3 años de experiencia en auditorías de cumplimiento (ISO27001, ENS) Acreditar durante los 3 últimos años la participación en más de un proyecto de auditorías técnicas Acreditar durante los 3 últimos años la participación en más de un proyecto de análisis de riesgos IT y OT
	TITULACIONES

	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN
	1,5 FTE (Equivalente a tiempo completo)

PERFIL	DESCRPIPCIÓN
Gestor de proyectos programas y portfolio	**RESPONSABILIDADES MÍNIMAS**
	Especialista en la gestión de proyectos realizando como mínimo las siguientes tareas: • Creación y coordinación de portfolios, programas y proyectos de Ciberseguridad • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación y seguimiento de procedimiento de gestión de proyectos y otras metodologías y modelos de relación • Apoyo, desarrollo, elaboración, control, mantenimiento, modificación de herramientas de control de proyectos • Gestión de proyectos (PM) de algunos proyectos estratégicos • Apoyo en la definición del Plan Director de Seguridad (PDS) • Elaboración de informes y kpis
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los 5 últimos años, 3 años de experiencia en gestión de proyectos de seguridad Experiencia en gestión de proyectos complejos Experiencia en gestión de proyectos en entornos mixtos (IT y OT) Acreditar conocimiento en metodologías de gestión de proyectos, programas y portfolio Experiencia en participación la definición de Plan Director de Seguridad en los últimos 3 años
	TITULACIONES
	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN

	1,5 FTE (Equivalente a tiempo completo)

PERFIL	DESCRPIPCIÓN
Técnico senior especialista en seguridad	**RESPONSABILIDADES MÍNIMAS**
	Apoyo técnico en la seguridad y gestión de la demanda • Revisión de requerimientos técnicos de validación de medidas de Seguridad • Apoyo a las licitaciones y validaciones proveedores • Persona de enlace con diferentes áreas de la compañía y diferentes áreas de negocio de carácter técnico • Apoyo en la gestión de incidentes de seguridad
	CONOCIMIENTOS Y EXPERIENCIA
	Experiencia en gestión de incidentes en infraestructuras críticas Experiencia en coordinación IT/OT Acreditar conocimiento ISA/IEC 62443 Habilidad para actuar como enlace entre las áreas técnicas y de negocio, facilitando la traducción bidireccional de requisitos y soluciones, especialmente en entornos híbridos IT/OT y en organizaciones del sector público.
	TITULACIONES
	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN
	0,5 FTE (Equivalente a tiempo completo)

PERFIL	DESCRPIPCIÓN
Arquitecto de seguridad	**RESPONSABILIDADES MÍNIMAS**
	Especialista en la integración de la seguridad en los diseños de los proyectos. Principales tareas: • Participación en los proyectos con el fin de analizar, dar apoyo, diseñar, soluciones seguras alineadas con la normativas vigentes y buenas prácticas • Análisis de las arquitecturas actuales con el fin de detectar mejoras. Diseñando propuestas de solución más segura • Apoyo y coordinación con el área de arquitectura de sistemas abiertos e industriales con el fin de analizar, definir soluciones • Elaboración de informes, metodologías, estándares y kpis • Apoyo elaboración de planes de mejora de riesgos
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los 5 últimos años, 3 años de experiencia en análisis y definición de arquitecturas seguras IT Acreditar durante los 5 últimos años, 3 años de experiencia en análisis y definición de arquitecturas seguras OT Acreditar participación en proyectos de seguridad de cloud Acreditar conocimiento ISA/IEC 62443 Acreditar conocimiento en normativas y buenas prácticas
	TITULACIONES
	Titulación universitaria en ingeniería informática, telecomunicaciones o similar
	DEDICACIÓN
	0,5 FTE (Equivalente a tiempo completo)

PERFIL	DESCRPIPCIÓN
Formación y capacitación	**RESPONSABILIDADES MÍNIMAS**
	Especialista en formación y capacitación de grandes organizaciones: • Análisis y definición de los perfiles de la compañía • Definición de planes de formación y concienciación adaptada a cada perfil • Diseño de un plan de formación y concienciación transversal • Planificación y ejecución de Cibersimulacros • Realización de informes con los resultados y análisis de los cibersimulacros • Propuestas de mejoras respecto a los gaps detectados • Elaboración de informes y KPIs
	CONOCIMIENTOS Y EXPERIENCIA
	Acreditar durante los 5 últimos años, 3 años de experiencia en análisis y definición de planes de formación y capacitación Acreditar conocimiento en formación y cultura de Ciberseguridad para grandes empresas Acreditar conocimiento en formación y cultura de Ciberseguridad en entornos OT e IT Haber participado en definición y coordinación de ejercicios de Cibersimulacros para empresas con más de 5000 empleados Haber participado en definición y coordinación de ejercicios de Cibersimulacros en empresas con activos OT Acreditar conocimientos en awareness & training
	TITULACIONES
	Grado o titulación universitaria en Pedagogía, Psicología, comunicación, formación de personas adultas o ingeniería informática, telecomunicaciones o similar con especialización en formación
	DEDICACIÓN
	0,5 FTE (Equivalente a tiempo completo)

Adicionalmente el adjudicatario designará un único **responsable de la cuenta** que será el último responsable del de la licitación. 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.

TMB podrá solicitar en cualquier momento al adjudicatario el listado de personas que forman parte del equipo del proyecto

TMB se reserva el derecho de verificar las capacidades del personal asignado o que participa puntualmente en la Oficina de Ciberseguridad y rechazarlo en caso de que no cumpla con los requisitos exigidos o con el rendimiento esperado. Los gastos que se deriven como consecuencia de los cambios en el equipo irán a cargo del adjudicatario.

La empresa adjudicataria deberá mantener el equipo de trabajo adscrito al contrato durante toda la vigencia del mismo. En caso de que se tenga que producir la sustitución de algún miembro del equipo, que no sea por causas de fuerza mayor, el adjudicatario lo comunicará a TMB y la sustitución deberá hacerse por un perfil que como mínimo tenga las mismas características profesionales y técnicas que las exigidas en este apartado.; en caso contrario este hecho será susceptible de penalización.

Además, en caso de sustituir a algún miembro del equipo de trabajo, se exigirá que:

- En caso de sustitución de un miembro del equipo, se exige un periodo de coexistencia mínimo de 15 días entre la persona que causa baja y la persona que se incorpora, con el objetivo de garantizar la transferencia de conocimiento. Esta condición no será exigible cuando la baja se produzca sin preaviso por causas de fuerza mayor, despido inmediato, enfermedad súbita u otras circunstancias que hagan imposible la coexistencia.
- Una formación de TMB y del servicio a desarrollar (a cargo del adjudicatario)

5.5. Mecanismos de comunicación y coordinación

Para garantizar una gestión eficiente y alineada con las necesidades de TMB, el adjudicatario deberá designar a un/a **interlocutor/a único/a** como responsable de la coordinación general del servicio. Esta figura actuará como punto de contacto principal con TMB, gestionando la planificación, el seguimiento y la resolución de las actuaciones derivadas del servicio.

No obstante, TMB podrá contactar directamente con otros miembros del equipo de la oficina externa de Ciberseguridad para la gestión operativa de tareas específicas, con el objetivo de facilitar una respuesta más ágil y eficiente. En todo caso, el/la responsable designado/a por el adjudicatario **será informado/a de todas las interacciones** para garantizar la trazabilidad y la coherencia en la prestación del servicio.

Durante la fase inicial del servicio, se definirá **la periodicidad de las reuniones de seguimiento**, así como **la constitución de diversos comités**, con funciones diferenciadas:

- Un comité estratégico, orientado a la revisión global del servicio, alineación con los objetivos de TMB y propuestas de mejora.
- Uno o más comités operativos, centrados en el seguimiento de las actividades técnicas, gestión de incidencias y coordinación funcional.

Estos comités estarán formados por representantes de TMB y el adjudicatario, y su composición y dinámica de trabajo se formalizarán al inicio de la prestación.

La responsabilidad de generar las actas resultantes de estos comités será del adjudicatario

5.6. Metodología del contrato

El adjudicatario definirá un Plan de Contrato que describa cómo llevará a cabo los servicios contratados. El servicio se desplegará en las siguientes fases:

5.6.1. Fase de implatación:

Objetivo: Poner en marcha el servicio de manera ordenada, segura y coordinada

Tareas mínimas principales:

- Reunión inicial Kick-off con TMB
- Validación del plan de calidad
- Definición del plan de contrato
- Definición del plan de trabajo/servicio
- Revisión y definición de la gestión de la demanda
- Definición de los diferentes comités con la periodicidad
- Asignación del equipo y validación de TMB
- Configuraciones de acceso a los sistemas y herramientas
- Transferencia de conocimiento inicial
- Establecer canales de comunicación y protocolos de escalamiento

Duración: Esta fase no puede durar más de 3 meses del kick-off

Resultado esperado: Servicio operativo con todos los mecanismos de gestión y seguimiento activo

En los casos en que no haya documentación previa necesaria para prestar el servicio, el adjudicatario deberá planificar y ejecutar su elaboración, de acuerdo con los responsables de TMB y sin ningún coste adicional por TMB.

5.6.2. Fase ejecución del servicio

Objetivo: Desarrollar el servicio según los requerimientos técnicos y operativos establecidos

Tareas mínimas principales:

- Prestación continuada del servicio de la Oficina de Ciberseguridad acuerdo el plan de trabajo y las tareas definidas en el pliego
- Participación en comités
- Creación de Cuadro de Mando

- Elaboración de informes periódicos
- Evaluación de los KPIs, ANS y propuestas de mejora
- Revisión post-implantación (entre los tres y seis meses) para ajustar el servicio

Duración: Durante la vigencia del contrato (con prórrogas si aplica)

Resultado esperado: Servicio estable, trazable y alineado con los objetivos de TMB

En los casos en que no haya documentación previa necesaria para prestar el servicio, el adjudicatario deberá planificar y ejecutar su elaboración, de acuerdo con los responsables de TMB y sin ningún coste adicional por TMB.

Se espera que el adjudicatario realice propuestas de mejora en el servicio y su implantación dependerá de la aprobación por parte de TMB

5.6.3. Fase devolución del servicio

Objetivo: Finalizar el contrato garantizando la continuidad operativa y la conservación del conocimiento.

Tareas mínimas principales:

- Elaboración del plan de devolución del servicio, consensuado con TMB
- Transferencia de conocimiento acumulado a TMB y al nuevo adjudicatario, si procede
- Entrega de documentación final
- Cierre de acceso a los sistemas y revocación de credenciales
- Apoyo activo en el proceso de transición hacia el nuevo adjudicatario, facilitando la comprensión de los servicios prestados, los sistemas utilizados y las casuísticas operativas
- Participación, si se cae, en reuniones de traspaso con TMB y el nuevo adjudicatario
- Revisión conjunta del servicio prestado
- Clausura de los comités y valoración final

Duración: Durante la vigencia del contrato. Se definirá conjuntamente con TMB si se inicia 2 meses antes de la fecha de vencimiento en función de las necesidades operativas, garantizando la transferencia completa de conocimiento. Esta fase se realizará en paralelo a la fase de ejecución del servicio sin coste adicional.

Resultado esperado: Cierre ordenado del servicio con toda la información transferida y sistemas protegidos

Plan de devolución:

El adjudicatario será el responsable de elaborar el Plan de devolución del contrato sobre el conocimiento del conjunto de iniciativas, tareas que se han ejecutado dentro del servicio además de las que están en curso o próximamente a iniciarse.

El Plan debe incluir todas las actividades, traspaso de documentación, procedimientos, customizaciones realizadas, etc que forman parte del conocimiento de TMB y que deberán trasladarse a TMB y al nuevo adjudicatario.

El plan debe cumplir como mínimo los siguientes principios y contenidos:

- Transferencia de conocimiento a TMB y al nuevo proveedor incluyendo procedimientos, , configuraciones, casuísticas operativas, metodologías para cada una de las actividades con las particularidades de cada tarea/servicio y lecciones aprendidas
- Entregables generados y documentación generada durante la vigencia del contrato en las últimas versiones. Incluyen informes técnicos, manuales de uso, inventarios, históricos de actuaciones, etc.
- Debe contemplar las tareas mínimas descritas en la fase de devolución de servicio
- Apoyo en la validación del traspaso con disponibilidad para consultas durante el periodo de transición
- Informe de cierre de servicio

Este plan deberá ser validado por TMB antes de su ejecución y formará parte de los entregables finales del contrato.

5.7. Gestión de la demanda

Actualmente TMB dispone de un buzón de correo genérico con el fin de atender las peticiones tal y como se detalla en el apartado 4.4 Apoyo y gestión de la demanda del presente documento. Durante la fase de implantación se revisará el procedimiento actual y se definirá su evolución de manera junta entre TMB y el adjudicatario. El adjudicatario deberá proponer un procedimiento flexible y escalable para la recepción, clasificación, priorización y seguimiento de las peticiones de servicio incluyendo:

- Tipología de demandas (consultas, incidencias, actuaciones planificadas).
- Canal de comunicación (ticketing, correo, etc.).
- Tiempos de respuesta orientativos según criticidad
- Protocolos de escalamiento.

Este procedimiento deberá ser validado por TMB y revisado periódicamente.

5.8. Gobernanza del servicio

La gobernanza del servicio se basará en mecanismos de seguimiento y control correspondientes al Plan de calidad que se validará al inicio de la prestación. El proveedor deberá participar en comités de seguimiento con TMB, con una composición y periodicidad que se determinarán durante la fase de implantación.

Los comités podrán ser:

- Estratégicos: para revisar la evolución global del servicio y propuestas de mejora.
- Operativos: para hacer seguimiento de las actuaciones técnicas e indicadores de servicio.

Se establecerán también indicadores de calidad (KPI) y mecanismos de revisión desde SLA /ANS que serán parte del sistema de control de servicio y que se revisarán en el momento de implantación del servicio.

5.9. Integración con el equipo interno

El servicio deberá prestarse de manera coordinada con la Responsable de la Oficina de Ciberseguridad de TMB y el CISO facilitando la colaboración y la transferencia de conocimiento.

Aunque la relación principal será entre la responsable de la Oficina de Ciberseguridad de TMB con el responsable del servicio durante la vigencia del contrato y dada la naturaleza de la misma se deberá participar en reuniones internas, grupos de trabajo con otras unidades de negocio, áreas, etc.

Este modelo podría requerir desplazamiento a reuniones en otras ubicaciones de TMB fuera de la oficina de corporativa tal y como se detalla en el apartado 5.2 Modalidad de prestación.

Este modelo de relación se formalizará durante la fase de implantación.

6. Requerimientos del servicio

6.1. Requerimientos técnicos

TMB no proporcionará los equipos informáticos (PCs, portátiles u otros dispositivos) necesarios para la prestación del servicio. Por lo tanto, el licitador deberá disponer de los **medios técnicos propios adecuados** para garantizar el correcto desarrollo de las tareas asignadas, incluyendo la conexión segura a los sistemas de TMB cuando sea necesario.

La conexión con TMB se detallará con el adjudicatario

El adjudicatario debe tener conocimiento y experiencia demostrable en el uso de herramientas de GRC.

El adjudicatario debe tener capacidad para trabajar en entornos híbridos (cloud y on-premise)

6.2. Acuerdos Nivel servicio (ANS)

Los niveles de servicio y plazos exigibles para atender la demanda de las nuevas peticiones de la Oficina de Ciberseguridad (ya sea a través del buzón genérico o de los mecanismos que se implanten durante la vigencia del contrato son los siguientes:

- **Tiempo de registro de nuevas solicitudes**: Es el tiempo transcurrido entre que entra la petición por cualquiera de los canales y se registra, clasifica y prioriza. **8h laborables**
- **Tiempo de resolución:** Es el tiempo transcurrido desde que la petición se registra hasta que se da por cerrada o correctamente derivada al afectado o responsable: **32h laborables**
    - Todas aquellas peticiones que se clasifiquen como **urgentes** se deberá dar respuesta en **8h laborable**

Será la responsable de la Oficina de Ciberseguridad quien determinará si la petición es urgente

Penalizaciones aplicables

Ámbito	Descripción ANS	Cálculo	Atribuciones del cálculo	Umbral de cumplimiento
Informes	Entrega de informes periódicos dentro del plazo pactado (5 primeros días del mes)	% de informes entregados fuera de plazo	Mensual	Crítica: <95% Alta: 95–97% Media: 97–99% Baja: ≥99%
Peticiones urgentes	Tiempo de respuesta a peticiones urgentes	% de peticiones urgentes resueltas en ≤8h laborables	Mensual	Crítica: <90% Alta: 90–95% Media: 95–98% Baja: ≥98%

Presencialidad	Presencia del responsable 3 días/semana	Días de presencia efectiva vs. días requeridos	Mensual	Crítica: <80% Alta: 80–90% Media: 90–95% Baja: ≥95%
Sustitución de personal	Sustitución sin preaviso ni perfil equivalente	Casos detectados vs. total cambios	Por caso	Crítica: Cualquier sustitución sin validación
Incorrecta dedicación del personal	Detección de rotación del personal asignado a cada perfil sin preaviso o autorización por el tipo de tarea	Casos detectados vs personas asignadas	Por caso	Crítica: Cualquier sustitución sin validación
Cuadro de mando	Actualización mensual del QdC	% de meses con actualización completa	Trimestral	Crítica: <90% Alta: 90–95% Media: 95–98% Baja: ≥98%
Gestión de la demanda	Tiempo de registro y resolución de peticiones	% de peticiones registradas en ≤8h y resueltas en ≤32h	Mensual	Crítica: <85% Alta: 85–90% Media: 90–95% Baja: ≥95%
Comités	Redacción y entrega de actas de los comités en el plazo acordado	% de actas entregadas dentro del plazo	Mensual	Crítica: <90% Alta: 90–95% Media: 95–98% Baja: ≥98%
Escalado de temas críticos	Escalado de temas urgentes/críticos a TMB en tiempo adecuado	% de casos escalados en ≤4h (laborables o temas críticos fuera de horas)	Mensual	Crítica: <90% Alta: 90–95% Media: 95–98% Baja: ≥98%
Auditorías	Resultados de auditorías externas o internas sobre	Número de incidencias críticas o altas detectadas	Por auditoría	Crítica: ≥1 incidencia críticaAlta: ≥2

	el cumplimiento del contrato			incidencias altas
Dedicación de recursos	Verificación de que la dedicación de los recursos es la pactada	Horas reales dedicadas vs. horas comprometidas	Mensual	Crítica: <85% Alta: 85–90% Media: 90–95% Baja: ≥95%

6.3. Requerimientos organizativos

Toda la documentación, comunicaciones e informes derivados del servicio deberán redactarse en catalán, y si procede, también en castellano, según las indicaciones de TMB.

La empresa adjudicataria deberá presentar un **plan de calidad** que defina los mecanismos de control, seguimiento y mejora continua aplicables a la prestación del servicio. Este plan deberá incluir cómo se garantiza el cumplimiento de los requerimientos técnicos y organizativos, la gestión de las incidencias, la trazabilidad de las actuaciones, y los procedimientos de auditoría interna.

Asimismo, se deberán establecer indicadores de calidad (KPI) que permitan a TMB evaluar el rendimiento del servicio, así como propuestas de revisión periódica para asegurar la adaptación a las necesidades cambiantes de la organización.

El plan de calidad formará parte de la documentación a entregar en la propuesta técnica y será revisado y validado por TMB durante la fase de implantación del servicio.

TMB se reserva el derecho de auditar al adjudicatario para garantizar que se está cumpliendo con las condiciones de la licitación

7. Requerimientos medioambientales

Criterio	Descripción
Impresión de informes - documentos de trabajo y/o documentos finales	En caso de que sea necesaria la impresión de cualquier documento de trabajo, se deberá: • Acordar con TMB la impresión o no del mismo. • Priorizar: ○ Reducir lo máximo posible el número de impresiones, ajustándolas a las necesidades ○ "Utilizar papel 100% reciclado (excepto por planos no imprimibles en DINA4 o DINA3). ○ Imprimir los documentos a doble cara y en blanco y negro (el color sólo se utilizará en casos en los que no se pueda interpretar en blanco y negro)
EMBALAJES -no primarios Material reciclado	En el caso de que la licitación incluya la entrega de productos o materiales, y estos se suministren con embalajes no primarios, estos deberán estar fabricados íntegramente con materiales reciclados. (1) embalaje adicional al del propio material para la distribución final del producto)
Derrame y vertido de líquido	En el caso de utilización de líquidos se deberán tomar las medidas que sean necesarias durante la realización del servicio por qué en ningún caso haya ningún tipo de vertido o derrame de líquido directo al medio ambiente. Al mismo tiempo si el servicio implica el uso y/o manipulación de productos líquidos peligrosos se deberá disponer de medios de contención y absorción ante el posibles derramamientos.