Mobile WorldCapital Barcelona

PLIEGO DE PRESCRIPCIONES TÉCNICAS RELATIVAS AL CONTRATO PARA EL SERVICIO DE CISO, SERVICIO DE SOC GESTIONADO Y EL SUMINISTRO DE UNA PLATAFORMA DE SIEM

Exp. A/F202503/S

Índice

PLIEGO DE PRESCRIPCIONES TÉCNICAS

EXP. A/F202503/S

1 OBJETO DEL CONTRATO

La finalidad del presente contrato es planificar, organizar y garantizar la seguridad de todos los activos de información de FUNDACIÓ BARCELONA MOBILE WORLD CAPITAL FOUNDATION (en adelante, "**MWCapital**") y de los sistemas que los apoyan en relación con los niveles de seguridad derivados a partir de la categorización de seguridad de los sistemas de la MWCapital y conforme a los acuerdos de nivel de servicio que se definan para cada caso y actores correspondientes. Al mismo tiempo, establecer un marco para la mejora continua de todos los procesos relacionados con la gestión de la seguridad de la información.

De acuerdo con lo contenido en el informe de necesidad, el objeto del contrato consiste en la contratación de los servicios de externalización de CISO (*Chief Information Security Officer*, "Oficial de Seguridad de la Información", por sus siglas en inglés) para la gestión preceptiva ante incidentes de seguridad y la tecnología asociada, el establecimiento de un SOC (*Security Operacions Center,* "Centro de Operaciones de Seguridad", por sus siglas en inglés), la implantación de un SIEM (*Security Information and Event Management* "Gestión de Eventos e Información de Seguridad", por sus siglas en inglés), así como la dirección para la implantación del sistema de gestión de la seguridad de la información que satisfaga el cumplimiento normativo relativo al Esquema Nacional de Seguridad (ENS), al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales y en cualquier otra norma aplicable.

Por lo tanto, el objetivo de este pliego es establecer las condiciones y el alcance para el servicio de gestión de la seguridad en sistemas heterogéneos (servicios centralizados, comunicaciones, sitio de usuario final, aplicaciones) que integre los diferentes elementos de seguridad e infraestructura para disponer de las mejores capacidades para dar cumplimiento a las obligaciones normativas como entidad público-privada y garantizar y prevenir la seguridad frente a incidentes complejos donde la correlación, coordinación y gestión de las dependencias es un factor crítico que requiere de medios materiales y personales altamente calificados en tecnologías de seguridad y ciberseguridad, así como un servicio de 24x7x365.

MWCapital es plenamente consciente de la relevancia de la protección de seguridad de la información para el correcto desarrollo de sus funciones y como fundamento esencial para la prestación de servicios TIC fiables y de calidad.

2 ALCANCE Y DESCRIPCIÓN DEL SERVICIO

2.1 TERMINOLOGÍA

Se definen los siguientes términos de uso común:

- **Ataque**: Un ataque es uno o varios eventos, provocados por personas no autorizadas, con impacto en la seguridad de la información. Desde la perspectiva de un observador neutral, el ataque puede ser exitoso (una intrusión) o fallido (un intento de ataque o ataque fallido).

- **Incidente**: Evento que atenta contra la confidencialidad, integridad o disponibilidad de la información y los recursos tecnológicos.

- **Intrusión**: Una intrusión es el acceso ilegal o no autorizado a un sistema de información.

- **Seguridad**: En este contexto se entiende por seguridad de las redes y de la información la capacidad de las redes o de los sistemas de información de resistir con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

- **SOC**: Centro de Operaciones de Seguridad (COS), conocido habitualmente como *Security Operations Center* (SOC). Un centro de operaciones de seguridad (SOC) mejora las capacidades de detección, respuesta y prevención de amenazas de una organización mediante la unificación y la coordinación de todas las tecnologías y operaciones de ciberseguridad. Es un equipo interno o subcontratado de profesionales de seguridad de TI dedicados a monitorizar 24x7 toda la infraestructura informática de una organización. Su misión es detectar, analizar y responder a incidentes de seguridad en tiempo real. Esta orquestación de las funciones de ciberseguridad permite al equipo del SOC mantener la vigilancia sobre las

redes, los sistemas y las aplicaciones de la organización y garantiza una posición de defensa proactiva contra las ciber amenazas.

El SOC también selecciona, opera y mantiene las tecnologías de ciberseguridad de la organización y analiza continuamente los datos de amenazas para encontrar formas de mejorar la posición de seguridad de la organización.

- **SIEM**: Gestión de Eventos e Información de Seguridad, conocido habitualmente como *System Information and Events Management* (SIEM). Un SIEM es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. Un sistema SIEM combina funciones de un sistema de gestión de información de seguridad, encargado del almacenamiento a largo plazo, el análisis y comunicación de los datos de seguridad, y un sistema de gestión de eventos de seguridad, encargado de la monitorización en tiempo real, correlación de eventos, notificaciones y cuadros de mando de la información de seguridad más significativa de cualquier corporación.

- **SaaS**: El software como servicio o SaaS (Software as a Service) en inglés, ofrece a los usuarios la posibilidad de conectarse a aplicaciones alojadas en un tipo de *cloud computing* (la nube) a través de Internet. También poder operar con ellas sin la necesidad del apoyo de sistemas cliente ad hoc. Al optar por este modelo los empleados de una organización pueden acceder en remoto a la infraestructura para las aplicaciones. El proveedor garantiza la disponibilidad, la seguridad y el buen funcionamiento de las diferentes aplicaciones y datos de nuestra entidad.

2.2 DESCRIPCIÓN DEL SERVICIO

El contrato alcanza todas las tareas, actividades y licencias para:

A. Externalización de CISO (*Chief Information Security Officer*)

MWCapital requiere externalizar la mayor parte de funciones del rol CISO en la organización, prestando este servicio y soporte al CIO de MWCapital y así dirigir, orientar y coordinar la estrategia de seguridad en consonancia con la estrategia y

gestión corporativa, y asumiendo la infraestructura de seguridad existente que permita al equipo TI de MWCapital, centrarse en la toma de decisiones estratégicas y resolutivas sobre la seguridad de la entidad. En particular:

- Entender la misión, los objetivos de MWCapital y los riesgos que afronta la organización y cómo tratarlos.

- Planificar y organizar de la seguridad de los Activos de Información.

- Garantizar que las actividades para implementar el *Roadmap* son planificadas y ejecutadas para satisfacer estos objetivos.

- Generar e implantar políticas de Seguridad de la Información a fin de garantizar la seguridad y privacidad de los datos.

- Dirección para la implantación de un sistema de gestión de seguridad (SIEM) de la información en sistemas heterogéneos (servicios centralizados, comunicaciones, sitio de usuario final, aplicaciones y SaaS). Integración de Elementos de Seguridad e Infraestructura. Correlación, coordinación y gestión de dependencias.

- Aseguramiento del cumplimiento con las regulaciones y estándares aplicables. Proponer las medidas para adecuarse a nuevos marcos normativos que puedan surgir. Promover y supervisar el cumplimiento normativo vigente aplicable de la Seguridad de la Información en MWCapital:

    - Esquema Nacional de Seguridad (ENS)
    - Reglamento General de Protección de Datos (RGPD)
    - Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)

- Gestionar incidentes de seguridad como responsable del equipo de respuesta del SOC.

- Supervisar la administración del control de acceso a la información.

- Supervisar la arquitectura de seguridad de la información de MWCapital.

- Establecer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las TIC.

- Crear el marco para la mejora continua en la gestión de la seguridad de la información.

B. Puesta en marcha y operación de un SOC y una plataforma SIEM (SaaS)

MWCapital requiere un servicio gestionado de SOC (Centro de Operaciones de Seguridad) operado con medios externos por parte de una empresa especializada, que aporte a la vez una herramienta SIEM.

- **Categorización** de seguridad de los sistemas de MWCapital.

- **Monitoreo Continuo.** Vigilancia 24x7 de las redes y sistemas.

- **Detección y prevención de incidentes.** Identificación y análisis de actividades sospechosas.

- **Respuesta a incidentes.** Coordinación y ejecución de acciones de contención, erradicación y recuperación.

- **Gestión de vulnerabilidades.** Identificación y mitigación de vulnerabilidades en los sistemas.

- **Análisis de Inteligencia.** Recolección y análisis de datos de amenazas para mejorar la postura de seguridad.

- **Informes y comunicaciones.** Generación de reportes sobre el estado de la seguridad y comunicación con todos los actores.

El **SIEM,** dentro del plan estratégico de seguridad corporativa, debe cumplir con los siguientes requerimientos mínimos:

- Herramienta SIEM líder en el mercado debido a la criticidad de la seguridad corporativa. Se considera líder si aparece como tal en los últimos 3 cuadrantes de Gartner de SIEM.

- Herramienta SIEM tipo SaaS, optimizando así el soporte, actualizaciones y mantenimiento, facilitando la implementación y escalabilidad.

- SaaS y licenciamiento propiedad de MWCapital, garantizando así la independencia entre servicios de Partners y la herramienta SIEM. Permiten, así, dar continuidad a todas las tareas evolutivas y casos de uso implementados sin ningún tipo de migración a nuevas plataformas SIEM.

- Herramienta SIEM catalogada como Calificada en ENS nivel ALTO dentro del Catálogo de seguridad de las TIC del CCN-CERT (aprobado por Real Decreto 3/2010).

- Herramienta SIEM licenciada con capacidad de ingesta mínima de 20GB/día de Logs.

En definitiva, el alcance del contrato es toda la Infraestructura Tecnológica de MWCapital, al cual se puede acceder conforme lo establecido siguiendo las instrucciones establecidas en el **Anexo I y Anexo II**.

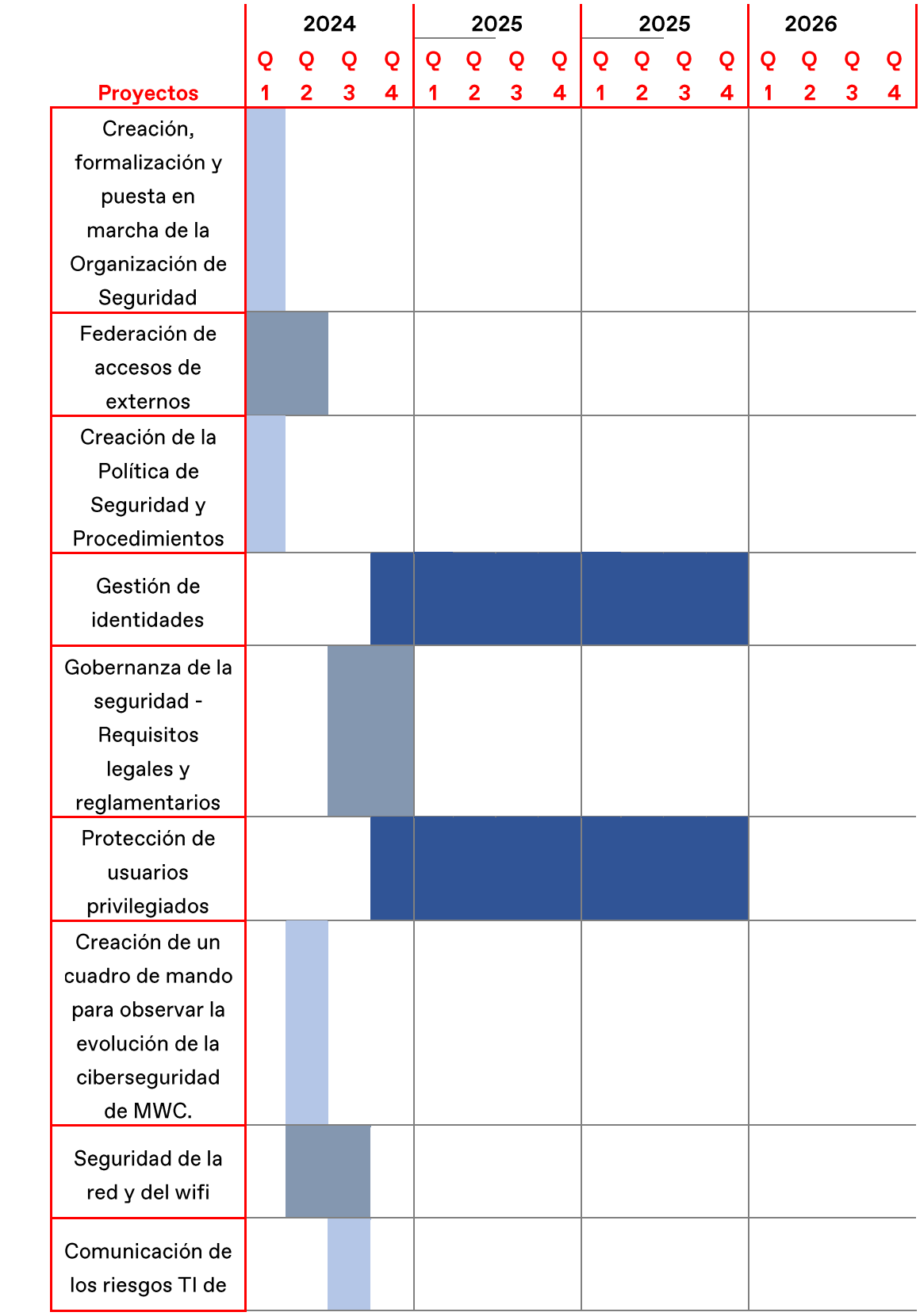
2.3 PLAN DIRECTOR (ROADMAP)

Para determinar el detalle del alcance que pueda dar cumplimiento al objeto del contrato, MWCapital ha realizado un primer análisis de ciberseguridad y ha establecido un Plan Director dividido en proyectos, con objetivos y actividades diferenciadas, para su ejecución a lo largo de un calendario plurianual.

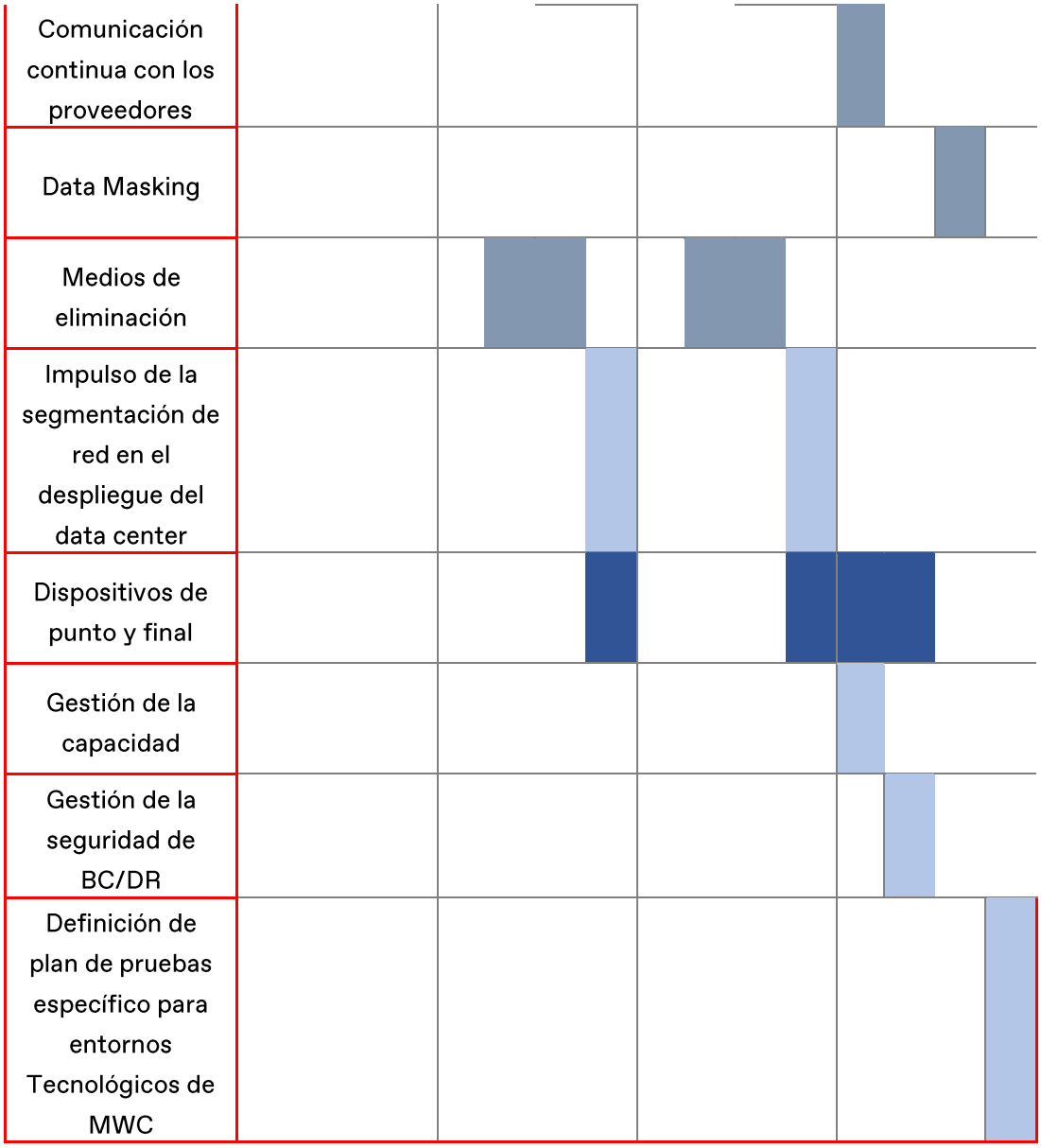
Este "Plan Director" ya se encuentra en ejecución y el contratista deberá acomodarse al plan ya iniciado al inicio del contrato. En este sentido, una de las primeras tareas del contratista en base las tareas de *onboarding* es analizar, revisar y modificar, si cabe, el Plan Director.

A continuación, el Plan Director en ejecución. Los proyectos de cada dominio parten de un nivel de madurez determinado y tiene como objetivo un nivel de madurez superior.

Para conocer en detalle estos grados de madurez y los dominios del Plan Director se deben seguir las instrucciones establecidas en el **Anexo I y Anexo II**.


2024
2025
2025
2026
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4
Proyectos
Creación, formalización y puesta en marcha de la Organización de Seguridad
Federación de accesos de externos
Creación de la Política de Seguridad y Procedimientos
Gestión de identidades
Gobernanza de la seguridad - Requisitos legales y reglamentarios
Protección de usuarios privilegiados
Creación de un cuadro de mando para observar la evolución de la ciberseguridad de MWC.
Seguridad de la red y del wifi
Comunicación de los riesgos TI de


forma periódica al negocio
Prevención de fuga de la información
Proceso de actualización del marco normativo
Diligencia en acuerdos con terceros
Incrementar medidas de seguridad para proveedores
Inventario y automatización de activos de sistemas
Analizar la idoneidad de establecer un modelo de clasificación y etiquetado de los sistemas de información
Gestión de Incidentes de seguridad
Campaña de concienciación/formación en terceros.
Gestión de copias de seguridad



2.4 ETAPAS DEL CONTRATO

Este contrato establece dos (2) etapas para su ejecución, una primera etapa de on*boarding* y una segunda de ejecución del Plan Director:

2.4.1 Etapa 1: *Onboarding*

La **etapa de *onboarding*** es crucial para establecer un entendimiento mutuo y una colaboración efectiva entre MWCapital y el contratista. Esta fase inicial asegura que todos los aspectos relacionados con la seguridad de la información se alineen con

los objetivos estratégicos y operativos de MWCapital, garantizando una transición fluida y estableciendo una base sólida para la ejecución del contrato. El contratista liderará y ejecutará cada uno de los pasos del *onboarding*, y generará los entregables detallados.

La duración de la etapa de *onboarding* será de un máximo de tres (3) meses a contar desde el día siguiente a la formalización del contrato.

a) Objetivos de la Etapa de *Onboarding*:

- Facilitar la integración del equipo del contratista con el entorno de MWCapital.
- Revisar y alinear el Plan Director de ciberseguridad con las necesidades actuales.
- Establecer canales de comunicación eficientes y claros.
- Evaluar las infraestructuras y recursos de seguridad actuales.
- Definir roles y responsabilidades claras para todas las partes involucradas.

b) Pasos de la Etapa de *Onboarding*:

1. Reunión inicial (kick—off)

- **Objetivo**: Iniciar formalmente la colaboración y establecer expectativas claras.

- **Actividades**:
  - Presentación de equipos y revisión de objetivos del contrato.
  - Discusión sobre la cultura organizacional de MWCapital.
  - Revisión del cronograma y metodología de trabajo.
  - Definición de expectativas y métricas de éxito.
  - Presentación de riesgos identificados y recomendaciones de mejora.

- **Entregables**:
  - **Informe de Reunión de Inicio**: Documento que resume los objetivos acordados, el cronograma, la metodología a seguir, riesgos.

2. **Definición de Roles y Responsabilidades**

   - **Objetivo**: Clarificar las funciones de cada miembro del equipo y las expectativas del proyecto.

   - **Actividades**:
     - Establecer roles y responsabilidades específicas para cada parte involucrada.
     - Asignar los recursos humanos y tecnológicos necesarios para la ejecución del plan.

   - **Entregables**:
     - **Documento de Roles y Responsabilidades**: Organigrama y descripción detallada de roles.

3. **Establecimiento de Canales de Comunicación**

   - **Objetivo**: Garantizar una comunicación eficiente entre MWCapital y el contratista.

   - **Actividades**:
     - Definir protocolos de comunicación para incidentes, reportes, y reuniones regulares.
     - Selección de herramientas de comunicación y colaboración.

   - **Entregables**:
     - **Protocolo de Comunicación**: Descripción de los canales y protocolos de comunicación establecidos.

4. **Evaluación de Infraestructura y Sistemas**

   - **Objetivo**: Obtener un conocimiento profundo de las infraestructuras de TI y sistemas de seguridad actuales.

   - **Actividades**:
     - Realizar un inventario completo de todos los activos de TI, sistemas de seguridad, y aplicaciones.
     - Análisis de riesgos para identificar vulnerabilidades y puntos críticos.

- **Entregables**:
    - **Inventario de Infraestructura y Sistemas**: Detalle de todos los activos y sistemas de MWCapital (Formato: Documento Excel o base de datos).
    - **Informe de Evaluación de Riesgos**: Informe que identifica vulnerabilidades y recomienda medidas de mitigación.

5. **Revisión del Plan Director de Ciberseguridad**

- **Objetivo**: Evaluar el Plan Director existente y ajustar según sea necesario.

- **Actividades**:

    - Análisis detallado del estado actual del Plan Director.
    - Identificación de áreas críticas y alineación con objetivos estratégicos.
    - Propuesta de ajustes o modificaciones para mejorar la eficacia del plan.

- **Entregables**:

    - **Informe de Evaluación del Plan Director**: Análisis del Plan Director y Plan Director ajustado, modificado.

2.4.2 Etapa 2: *Ejecución del Plan Director*

La **etapa de ejecución del Plan Director** implica la implementación de todas las medidas, políticas, procedimientos y acciones necesarias para garantizar la seguridad de la información dentro de MWCapital.

El Plan Director está diseñado para establecer un entorno de seguridad robusto, que proteja la integridad, confidencialidad y disponibilidad de los datos y sistemas de MWCapital, alineándose con los estándares internacionales y normativas aplicables.

a) Objetivos de la Etapa de Ejecución:

- **Implementación de un modelo de gobierno de seguridad** que dirija y mantenga un entorno seguro.

- **Formalización y aplicación de políticas de seguridad** que sean consistentes con las necesidades de la organización.

- **Gestión de terceros** y proveedores para garantizar la seguridad de las interacciones externas.

- **Cumplimiento normativo** a través de la creación de un cuadro de mando y gestión de requisitos legales.

- **Gestión de la información y tecnología**, incluyendo la automatización de activos y la protección de datos.

- **Pruebas** de sistemas para asegurar la incorporación segura de nuevos activos, dispositivos o funcionalidades.

- **Hacking ético.** La realización por parte del contratista de mínimo 2 acciones de intrusión o ataque controladas siguiendo las mejores prácticas de la industria y la metodología OWASP, identificando, explotando y documentando vulnerabilidades en los sistemas objeto del contrato y a petición de MWCapital, que determinará en el momento de solicitar la acción, los sistemas objetivo y la preferencia de la tipología de ataques. Estas acciones incluirán técnicas avanzadas para evaluar la resiliencia de los sistemas ante amenazas reales, garantizando en todo momento la confidencialidad, integridad y disponibilidad de la información.
  Adicionalmente, el contratista generará un informe técnico detallado que incluirá la descripción de las vulnerabilidades detectadas, su nivel de criticidad, evidencia del impacto y las medidas de mitigación recomendadas, alineándose con normativas como el Esquema Nacional de Seguridad (ENS), ISO 27001 y el Reglamento General de Protección de Datos (RGPD).

La duración de la etapa de Ejecución del Plan Director comprende desde el fin del *onboarding* hasta la finalización plazo de ejecución del contrato. A continuación, se enumeran los proyectos derivados del Plan Director:

b) Pasos de la Etapa de Ejecución del Plan Director:

Paso 1: Establecimiento del Modelo de Gobierno

P1: Creación, formalización y puesta en marcha de la Organización de Seguridad

Paso 2: Implementación de Políticas y Procedimientos de Seguridad

- P2: Creación de la Política de Seguridad y Procedimientos
- P3: Proceso de Actualización del Marco Normativo

Paso 3: Gestión de Terceros y Proveedores

- P4: Incrementar Medidas de Seguridad para Proveedores
- P5: Federación de Accesos de Externos
- P6: Diligencia en Acuerdos con Terceros
- P7: Campaña de Concienciación/Formación en Terceros
- P8: Comunicación Continua con los Proveedores

Paso 4: Cumplimiento Normativo

- P9: Creación de un Cuadro de Mando para Ciberseguridad
- P10: Gobernanza de la Seguridad - Requisitos Legales y Reglamentarios

Paso 5: Gestión de la Información y Tecnología

- P11: Inventario y Automatización de Activos de Sistemas
- P12: Data Masking
- P13: Gestión de Copias de Seguridad
- P14: Modelo de Clasificación y Etiquetado de Sistemas de Información
- P15: Medios de Eliminación
- P16: Protección de Usuarios Privilegiados

Paso 6: Gestión de la Tecnología

- P17: Segmentación de Red en el Data Center
- P18: Protección de Dispositivos de Punto Final
- P19: Gestión de la Capacidad

Paso 7: Desarrollo y Pruebas

- P20: Definición de Plan de Pruebas para Entornos Tecnológicos

Paso 8: Web y Redes

- P21: Seguridad de la Red y del WiFi
- P22: Capacidades de Monitorización Pasiva en Redes de Control

Paso 9: Prevención de Incidentes

- P23: Comunicación de Riesgos TI al Negocio
- P24: Prevención de Fuga de Información

Paso 10: Procedimiento de Incidencias

P25: Gestión de la Seguridad de BC/DR

P26: Gestión de Incidentes de Seguridad

Paso 11: Seguridad en RRHH

P27: Gestión de Identidades

Para más detalle consultar el Plan Director, al cual se puede tener acceso siguiendo las instrucciones establecidas en el **Anexo I y Anexo II**.

También forma parte del alcance la generación de todos los entregables previstos en la metodología y la organización.

3 ORGANIZACIÓN

La metodología de gestión de las actividades del contrato está basada en el marco de gestión y trabajo Scrum, tanto en sus roles como en su única fase (el *sprint*) y las reuniones estándar que contiene. Este marco se implementará para permitir un ciclo de retroalimentación continuo y mejoras iterativas. Cada *sprint* ira seguido de una revisión y una oportunidad para hacer ajustes basados en la retroalimentación.

Los roles del equipo Scrum se repartirán entre la Dirección de Innovación de MWCapital y el contratista de la siguiente manera:

Dirección de Innovación de MWCapital:

- Product Owner.
- Scrum Master.
- Enlaces.

Contratista:

- Proxy Product Owner.
- Equipo SOC.
- Responsable del contrato que será el interlocutor único entre el contratista y MWCapital para todos los temas relacionados con la gestión y ejecución del contrato.

Los interlocutores de MWCapital serán el Product Owner, el Proxy Product Owner, el Scrum Master y los enlaces, y facilitarán la información necesaria y el acceso a

los interlocutores oportunos para garantizar la productividad del equipo y su correcta toma de decisiones informadas.

Con carácter general, MWCapital velará, mediante las figuras del Product Owner y Scrum Master, el cumplimiento de los plazos acordados, así como la calidad y la adecuación de los servicios objeto de este contrato y su ejecución según la metodología y los estándares ágiles Scrum.

Igualmente, MWCapital proporcionará enlaces para las diferentes disciplinas del proyecto que sean necesarias.

Estos interlocutores tendrán la responsabilidad de validar las partes del sistema que estén bajo su responsabilidad y según la metodología SCRUM, aportando requisitos y facilitando el trabajo dentro de sus áreas. Es posible que algunos de estos interlocutores pertenezcan a otros proveedores de MWCapital que presten servicios relacionados con las diferentes disciplinas que rodean el proyecto. Esto no debe comportar ningún problema ni entorpecer la ejecución del contrato. MWCapital reforzará la idea de equipo multidisciplinario sin importar la pertenencia a uno u otro proveedor.

Con carácter general, la interlocución de los roles de MWCapital asignados al contrato (Product Owner y Scrum Master) será indistintamente con todos los miembros del equipo. Es necesario que esta organización incluya la figura del Responsable de contrato del proveedor, que será el interlocutor único entre el contratista y MWCapital para todos los temas relacionados con la gestión y ejecución del contrato. Las funciones y responsabilidades del Responsable de contrato del contratista están detalladas en el apartado 4.1. *Funciones y requisitos por perfil* de este pliego.

La organización del contrato deberá ajustarse a los requisitos mínimos que se especifican en los siguientes apartados.

3.1 COMITÉ DE DIRECCIÓN

Sus funciones son las de supervisar la marcha del contrato y la toma de decisiones que afectan al objetivo y alcance del mismo. El Responsable de contrato del contratista asistirá a las reuniones de este Comité siempre que sea requerido por cualquiera de sus miembros.

Resultado de todas las reuniones: se redactará un acta con los temas tratados y los acuerdos tomados. El Responsable de contrato del contratista será el encargado de la elaboración de la documentación de seguimiento del contrato necesaria para tal fin y también de levantar el acta de las reuniones. Esta acta se hará llegar en la mayor brevedad posible a todos los destinatarios que el Comité de Dirección considere oportuno.

Se reúne normalmente cada 4 o 6 sprints, aunque se podrá convocar con carácter extraordinario siempre que se considere necesario. Forman parte:

- Dirección de Innovación de MWCapital o en quien delegue.
- Product Owner.
- Proxy Product Owner.
- Scrum Master.
- Responsable de contrato del contratista (según requerimientos).

3.2 EVENTOS DE SEGUIMIENTO

El día a día del proyecto lo gestionan los roles del Equipo Scrum (Product Owner, Proxy Product Owner, Enlaces y el Equipo). Los diferentes eventos sirven para gestionar el estado del desarrollo al resto de actores de MWCapital, así como apoyar al Product Owner en la toma de decisiones para definir los siguientes sprints.

A continuación, se describen los diferentes eventos de seguimiento:

3.3 PLANIFICACIÓN DEL SPRINT (SPRINT PLANNING)

La Planificación del Sprint es la reunión inicial donde el equipo Scrum determina qué ítems del Backlog se harán durante esta iteración. Esta reunión tiene dos (2) objetivos principales:

- Determinar qué se hará: se seleccionan los ítems más prioritarios desde el punto de vista de negocio y técnico, de manera colaborativa entre todo el equipo Scrum.
- Determinar cómo se hará: el Equipo analiza técnicamente cómo se harán los ítems, p.e. haciendo un diseño de alto nivel y desglosando las tareas técnicas.

Es muy importante que los ítems estén previamente analizados (estado ready) para que esta reunión sea eficiente y se generen pocas dudas que puedan causar problemas dentro del Sprint.

Aspectos básicos de la Planificación del Sprint:

- Asistentes: Product Owner, Proxy Product Owner, Enlaces, el Equipo y el Scrum Master.
- Entradas: Backlog de producto y metas de negocio del Product Owner.
- Salidas: Backlog de sprint y meta del sprint.

3.4 SCRUM DIARIO (REUNIÓN DIARIA)

El Scrum diario es una reunión que se realiza todos los días para que el Equipo de desarrollo haga seguimiento del Sprint, se coordine y decida acciones correctivas en caso de que sea necesario. Participarán el Scrum Master de MWCapital y el equipo de desarrollo con participación puntual de los diferentes enlaces.

El formato habitual de la reunión consiste en los miembros del Equipo utilizando estas preguntas para coordinarse y tomar decisiones:

- ¿Qué he hecho desde la última reunión para cumplir la meta del Sprint?
- ¿Qué haré hoy para cumplir la meta del Sprint?
- ¿Qué riesgos o problemas veo para que el equipo cumpla la meta del Sprint?

Aspectos básicos:

- Equipo, enlaces (opcional) y Scrum Master (opcional).
- Duración máxima: 15 minutos.
- Entradas: Backlog de sprint y meta del sprint.
- Salidas: Backlog de sprint y decisiones.

Dadas las particularidades de este contrato, al principio de su ejecución el Comité de Dirección determinará la necesidad y la frecuencia de la reunión diaria.

3.5 LA REVISIÓN DEL SPRINT (SPRINT REVIEW)

La Revisión del sprint es una reunión de gestión donde el equipo Scrum revisa qué se ha conseguido la entrega del incremento previsto y piensan qué queda por hacer

a los futuros sprints. A esta reunión puede asistir cualquier otro rol de la organización que quiera saber el estado de las actividades objeto del contrato.

Durante esta reunión se pueden identificar mejoras para próximos sprints, pero no sirve para validar las implementaciones o items entregados. La validación de los ítems entregados debe hacerse durante el siguiente sprint.

Aspectos básicos:

- Asistentes: Equipo Scrum.
- Duración máxima aproximada: 1h por cada semana de sprint.
- Entradas: Backlog del producto y meta del sprint.
- Salidas: Backlog del producto.

3.6 LA RETROSPECTIVA DEL SPRINT (SPRINT RETROSPECTIVE)

La Retrospectiva del sprint es la última reunión del sprint, donde el Equipo Scrum identifica mejoras al funcionamiento del equipo para próximos sprints.

Un formato básico de reunión es donde cada miembro del Equipo valora el sprint pasado y hace propuestas para el siguiente, respondiendo a las preguntas:

- ¿Qué ha ido bien en este sprint?
- ¿Qué ha ido mal en este sprint?
- ¿Qué acciones concretas de mejora podríamos hacer en los próximos sprints?

Es conveniente que el Scrum Master haga también propuestas de mejora, que la totalidad de las propuestas de mejoras se incluyan en el backlog y que realice un seguimiento de las mejoras propuestas durante los sprints.

Aspectos básicos:

- Asistentes: Equipo Scrum
- Entradas: Información de la ejecución del sprint
- Salidas: Backlog de ideas de mejora.

4 RECURSOS HUMANOS

El contratista tendrá que garantizar la continuidad del equipo durante todo el plazo de ejecución de los trabajos. Cualquier cambio de los integrantes del equipo deberá ser autorizado previamente por MWCapital. Los posibles cambios o modificaciones en la composición del equipo tendrán que ser comunicados por escrito a MWCapital con la debida antelación y aceptados por ésta. En este supuesto el contratista deberá proponer a una/s persona/s con la formación y experiencia mínimas requeridas en la licitación, y en su caso, teniendo en cuenta las características de las personas del equipo valorado en la licitación, de acuerdo su oferta.

4.1 FUNCIONES Y REQUISITOS POR PERFIL

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

Estos perfiles pueden ser compartidos por una misma persona, siempre que cubra todos los requerimientos expuestos, o bien repartidos entre varias personas del equipo, indicando por cada una de ellas el porcentaje de dedicación y el número de personas de cada perfil que se proponen.

MWCapital estima que los perfiles mínimos necesarios del contratista para la prestación de los servicios de esta licitación son los que se detallan a continuación.

1) Coordinador y responsable del contrato

   Función de gestión del contrato y los recursos humanos asignados, velar por la calidad del servicio, convocar a los comités y tareas de interlocución principal con MWCapital. Como coordinador del contrato asiste a los comités de dirección y se ocupa de los aspectos contractuales.

   Experiencia profesional o conocimientos mínimos requeridos:

   - Siete (7) años de experiencia en proyectos tecnológicos.
   - Cinco (5) años de experiencia en proyectos del ámbito de ciberseguridad.
   - Cuatro (4) años de experiencia como Responsable de Contrato con administración pública o sector privado.
   - Disponer de un (1) certificado Scrum de scrum.org.

2) Perfil CISO

Sus principales tareas son según se expresa en el punto 2.2. del presente pliego de prescripciones:

- Dirigir, orientar y coordinar la estrategia de seguridad.
- Definir la normativa de seguridad y procurar los medios para que se cumpla.
- Establecer e implementar políticas relacionadas con la seguridad.
- Informar y reportar a dirección.
- Garantizar la privacidad de los datos de MWCapital.
- Alinear la seguridad con la continuidad de negocio.
- Coordinar los recursos del servicio objeto del contrato.
- Capacidad para desarrollar y adaptar políticas a normativas vigentes.

Experiencia profesional o conocimientos mínimos requeridos:

- Titulación ingeniería informática, telecomunicaciones o equivalente informática.
- Conocimiento y experiencia en nuevas tecnologías y ciberseguridad.
- Cinco (5) años de experiencia en implantación Esquema Nacional de Seguridad.
- Cinco (5) años de experiencia en gestión de seguridad de la información.
- Tres (3) años de experiencia con herramientas de seguridad SIEM y SOC.
- Tres (3) años de experiencia en cumplimiento de normativas ENS, RGPD y LOPDGDD.

3) Equipo SOC

Servicio complementario al perfil CISO, que deberá disponer de los medios y una capacitación de conocimientos y formación en seguridad informática y/o telecomunicaciones para la prestación del servicio; y, en concreto:

- Prevenir, detectar y analizar vulnerabilidades.
- Capacidad para gestionar infraestructuras de seguridad complejas.
- Respuesta a incidentes.

Experiencia profesional o conocimientos mínimos requeridos:

- Tres (3) años de experiencia con herramientas de seguridad SIEM y SOC.
- Tres (3) años de experiencia con herramientas de seguridad en equipos SOC.

4.2 SUSTITUCIONES

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

- Un período de formación, a cargo del contratista, por el nuevo miembro que se incorpore a la ejecución del contrato.
- Un período de coexistencia, de un mínimo de 15 días persona que se incorpora.

MWCapital se reserva la facultad de requerir al contratista la sustitución de cualquiera de los miembros que componen el equipo para lograr un óptimo cumplimiento del contrato. Los gastos que se deriven como consecuencia de cambios en el equipo de trabajo correrán a cargo del contratista.

En este orden de cosas, se hace constar que MWCapital queda desvinculada, a todos los efectos, de cualquier relación laboral con el personal del contratista, dado que se trata de un contrato de apoyo y asistencia que debe ser considerado como tal en su conjunto.

5 CONDICIONES DE EJECUCIÓN DEL SERVICIO

5.1 LUGAR DE PRESTACIÓN DEL CONTRATO

El equipo humano aportado por el contratista llevará a cabo las tareas para la prestación de los servicios en sus oficinas propias, sin perjuicio que pudieren ser requeridos en las oficinas de MWCapital.

En las ocasiones que lo requieran, se podrá solicitar el desplazamiento a las oficinas de MWCapital para la prestación del servicio que sea necesario, siendo obligación del contratista la aportación de las herramientas que sean necesarias para la prestación de este.

Las reuniones se realizarán en las oficinas del MWCapital o telemáticamente por videoconferencia siempre que MWCapital así lo solicite.

5.2 HORARIOS DE LA PRESTACIÓN DE LOS SERVICIOS

El horario de prestación de los servicios para el servicio regular es en el horario laboral de MWCapital: 10h x 5 (días laborales en la ciudad de Barcelona, de lunes a viernes de 9 h a 18 h).

Se requerirá para la ejecución, respuesta ante incidentes, urgencias, incidencias críticas... servicios fuera del horario estipulado sin que la prestación de los mismos suponga un coste excepcional/adicional por MWCapital respecto al precio/hora previsto en el contrato.

5.3 SISTEMA DE EVALUACIÓN DEL DESEMPEÑO DEL CONTRATISTA

Para asegurar el cumplimiento de los niveles de servicio y evaluar la calidad de la prestación, MWCapital establecerá un sistema automatizado de evaluación basado en Acuerdos de Nivel de Servicio (SLAs).

5.3.1 Evaluación Trimestral mediante SLAs

La evaluación del desempeño del contratista se realizará trimestralmente a través de métricas registradas automáticamente por la plataforma SIEM y los sistemas del SOC gestionado. Los siguientes indicadores y umbrales mínimos forman la base objetiva de esta evaluación:

Indicador SLA	Definición	Umbral mínimo	Fuente de datos
Disponibilidad SIEM/SOC	Porcentaje de tiempo operativo respecto al total previsto (24x7x365)	≥ 99,5%	Logs de disponibilidad y monitorización
Tiempo medio de respuesta (MTTR)	Tiempo medio entre la detección y la respuesta inicial a incidentes críticos*	≤ 30 minutos	Registros de incidentes (SIEM/SOC)
Informe mensual puntual	Porcentaje de informes entregados dentro del calendario acordado	100%	Registro de entregas validadas
Incidentes resueltos a tiempo	Porcentaje de incidentes críticos* resueltos dentro del plazo establecido	≥ 95%	Sistema de ticketing / gestión de incidentes
Ingesta de logs garantizada	Volumen mínimo diario de logs ingeridos en el SIEM	≥ 15 GB/día	Métricas internas del SIEM

Propuestas de mejora proactiva	Número mínimo de propuestas trimestrales de mejora del servicio	≥ 3	Actas de Comité, reuniones de seguimiento

*Un incidente crítico implica una interrupción de servicio de cualquier activo tecnológico que no permite la operación de negocio habitual con métodos alternativos.

5.3.2 Cálculo de la Puntuación Trimestral

Cada indicador será valorado sobre una escala de 0 a 100 puntos, y se aplicará una ponderación para obtener la puntuación total trimestral:

Indicador SLA	Peso en la evaluación (%)
Disponibilidad SIEM/SOC	25%
Tiempo medio de respuesta (MTTR)	25%
Informe mensual puntual	15%
Incidentes resueltos a tiempo	15%
Ingesta de logs garantizada	10%
Propuestas de mejora	10%

5.3.3 Procedimiento en caso de incumplimiento

En función de la puntuación total obtenida, MWCapital podrá:

Puntuación Trimestral	Acción Aplicable
≥ 90 puntos	Continuidad del servicio sin cambios
75 – 89 puntos	Revisión de procesos y plan de mejora obligatorio
60 – 74 puntos	Penalización del 5% mensual del importe del servicio afectado + plan correctivo
< 60 puntos	Penalización del 5% mensual + posible resolución anticipada del contrato

En caso de dos evaluaciones trimestrales consecutivas por debajo de 75 puntos, MWCapital podrá solicitar la sustitución del personal clave (CISO o equipo SOC) o resolver anticipadamente el contrato por incumplimiento.

6 CONDICIONES GENERALES

6.1 CONFIDENCIALIDAD

6.1.1 Obligación de confidencialidad

El contratista se compromete a guardar el más absoluto secreto y confidencialidad respecto a toda la información, datos, documentos y materiales, incluidos aquellos de carácter personal, a los que tenga acceso en virtud de la ejecución del presente contrato. Dicha información no podrá ser divulgada, utilizada ni transmitida a terceros, salvo autorización previa y por escrito de MWCapital.

6.1.2 Restricción de uso y Protección de Datos

El contratista se obliga expresamente a no copiar, reproducir, almacenar, modificar, utilizar o procesar la información obtenida con finalidades distintas a las estrictamente necesarias para el cumplimiento del objeto del contrato. Esto incluye, de manera especial, los datos de carácter personal, los cuales deberán ser tratados conforme a la normativa vigente en materia de protección de datos, incluyendo el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

6.1.3 Confidencialidad de Sistemas e Infraestructuras Tecnológicas

En aquellos casos en que el objeto del contrato incluya la construcción, mantenimiento o gestión de sistemas de información y/o infraestructuras tecnológicas, el deber de secreto se extiende también a los componentes tecnológicos, arquitecturas, configuraciones, metodologías, medidas de seguridad técnicas y cualquier otro elemento vinculado a dichos sistemas o infraestructuras.

6.1.4 Responsabilidad

El contratista será plenamente responsable de las violaciones al deber de confidencialidad que puedan ser cometidas por él o por cualquier miembro de su personal, subcontratistas o terceros bajo su control. Asimismo, el contratista deberá implementar y aplicar medidas específicas para garantizar el cumplimiento de los principios de mínimo privilegio y necesidad de conocer, limitando el acceso a la información exclusivamente al personal estrictamente necesario para la ejecución del contrato.

6.1.5 Devolución o destrucción de la Información

Al término de la vigencia del contrato, el contratista estará obligado a devolver a MWCapital toda la información, documentos, materiales y productos generados o utilizados durante la ejecución del contrato. Si MWCapital así lo requiere, el contratista deberá destruir dicha información, garantizando la aplicación de medidas de seguridad adecuadas y certificando por escrito dicha destrucción, de acuerdo con las mejores prácticas y estándares aplicables.

6.1.6 Duración del Deber de Confidencialidad

El deber de confidencialidad asumido por el contratista tendrá carácter indefinido y se mantendrá vigente incluso después de la finalización del presente contrato.

6.2 CLÁUSULA DE PROPIEDAD INTELECTUAL

6.2.1 Titularidad

La propiedad intelectual de todos los trabajos, informes, diseños, documentos, metodologías, sistemas, configuraciones, herramientas, tecnología asociada, desarrollos, y cualquier otro producto o resultado generado como consecuencia de la prestación de los servicios contratados, será de titularidad exclusiva de MWCapital.

En ningún caso, el contratista podrá utilizar, reproducir, modificar, distribuir o comunicar a terceros dichos elementos sin la previa y expresa autorización por escrito de MWCapital.

El acceso a información confidencial o protegida por derechos de propiedad intelectual perteneciente a MWCapital, proporcionada al contratista para la ejecución de los servicios, se realizará exclusivamente para el cumplimiento del objeto del contrato. Dicho acceso no implicará la cesión, total o parcial, de derechos de propiedad intelectual o industrial.

El contratista se compromete a garantizar la confidencialidad y la integridad de la información y a devolver o destruir, según se indique, cualquier material proporcionado una vez finalizada la relación contractual.

6.2.2 Cesión de derechos de explotación

El contratista cede en favor de MWCapital, con carácter exclusivo y por el máximo plazo permitido por la legislación vigente, la totalidad de los derechos de explotación sobre los trabajos objeto del contrato, incluyendo, sin limitación:

- **Derechos de reproducción:** autorización para realizar copias totales o parciales por cualquier medio.
- **Derechos de** comunicación pública**:** autorización para hacer accesibles los resultados a terceros mediante cualquier medio.
- **Derechos de distribución:** autorización para la transmisión de copias a terceros.
- **Derechos de** transformación**:** autorización para realizar modificaciones, adaptaciones o derivaciones.

Esta cesión será extensiva a cualquier desarrollo tecnológico, configuración de SOC, metodologías para la gestión de incidentes de seguridad, documentación asociada al cumplimiento del Esquema Nacional de Seguridad (ENS), y cualquier otro activo creado durante la ejecución de los servicios.

6.2.3 Exclusividad y garantías

El contratista garantiza que los trabajos realizados no infringen derechos de terceros y que es titular legítimo de todos los elementos que puedan ser incorporados o utilizados en los resultados generados. Asimismo, se compromete a indemnizar a MWCapital por cualquier reclamación derivada de una infracción de derechos de propiedad intelectual o industrial.

6.3 ALCANCE Y LEGISLACIÓN APLICABLE

El contratista, así como las empresas subcontratadas, en su caso, tendrán la consideración de encargados del tratamiento de los datos y deberán cumplir estrictamente con toda la normativa vigente aplicable al desarrollo de los servicios contratados. En particular, deberán garantizar el cumplimiento de las siguientes disposiciones normativas:

1. **Normativa General del Sector Público**

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. **Gestión Documental y Administración Electrónica**

- Ley 10/2001, de 13 de julio, de Archivos y Documentos, modificada por la Ley 20/2015, de 29 de julio.
- Ley 29/2010, de 3 de agosto, del Uso de los Medios Electrónicos en el Sector Público de Cataluña.

3. Seguridad **de la Información y Requisitos Técnicos**

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015, de 23 de octubre.
- Real Decreto 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad.

4. **Reutilización de Información del Sector Público**

- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, actualizada mediante la Ley 18/2015, de 9 de julio.

5. **Protección de Datos y** Garantía **de los Derechos Digitales**

- Ley **Orgánica** 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

El contratista será responsable de garantizar que todas las actividades llevadas a cabo durante la prestación de los servicios cumplen con las normativas anteriores, así como con cualquier otra legislación nacional, autonómica o local que resulte aplicable al ámbito del contrato, incluyendo el Reglamento General de Protección de Datos (RGPD) y otras disposiciones conexas que puedan estar en vigor durante la vigencia del contrato.

Barcelona, a 27 de marzo de 2025

Eduard Martín
Chief Innovation Officer
Fundació Barcelona Mobile World Capital Foundation

Anexo I

INFRAESTRUCTURA TECNOLÓGICA Y PLAN DIRECTOR

Debido al **carácter confidencial** de la información recogida en los **documentos (i) Infraestructura Tecnológica y (ii) Plan Director**, los licitadores interesados en concurrir al presente procedimiento de licitación y que quieran tener acceso a los mismos deberán enviar una solicitud mediante correo electrónico a MWCapital, siguiendo las instrucciones y requisitos que se reproducen a continuación:

INSTRUCCIONES PARA SOLICITAR EL ACCESO A LOS DOCUMENTOS

1. **Envío de solicitud de acceso mediante correo electrónico del licitador interesado a MWCapital:**

   - **Destinatario**: procurement@mobileworldcapital.com
   - **Asunto**: A/F202503/S – Solicitud documentos Anexo I PPT
   - **Solicitud**: "*Por el presente declaro estar interesado en el procedimiento de licitación de referencia por lo que solicito tener acceso a los documentos del Anexo I del Pliego de Prescripciones Técnicas: Infraestructura Tecnológica y Plan Director*".
   - **Identificación**: El licitador interesado debe identificarse en su correo electrónico indicando los siguientes datos:
     - Nombre operador económico
     - NIF/CIF
     - Representante legal
   - **Documentación adjunta**: Debe adjuntarse en documento PDF el Anexo II: "*Acuerdo de Confidencialidad y no divulgación de secretos*" que sigue a continuación debidamente rellenado y firmado por el licitador interesado.

2. **Envío de la documentación solicitada:**

   - Una vez recibida la solicitud de acceso así como el documento Anexo II: "*Acuerdo de Confidencialidad y no divulgación de secretos*" en PDF y debidamente rellenado y firmado por el representante legal o autorizado del licitador interesado, MWCapital comprobará su adecuación y pondrá a disposición del mismo mediante correo electrónico los documentos **(i) Infraestructura Tecnológica y (ii) Plan Director** en un plazo máximo de veinticuatro (24) horas desde su recepción.

NOTA: Cualquier solicitud de acceso a la documentación del Anexo I que no siga y cumpla fielmente las instrucciones más arriba referenciadas serán rechazadas, en cualquier caso.

Anexo II

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE SECRETOS
NON -DISLOSURE AGREEMENT (NDA)

REUNIDOS

De una parte, [el/la] [Sr./Sra.] [*], mayor de edad, con DNI/NIF núm. [*], y en calidad de [*], por tanto, actuando, en virtud de escritura pública y/o autorización pertinente, en nombre y representación de **XXXXXXX**., con domicilio en [*], [*], [*], CIF/NIF núm. [*] e inscrita en el Registro Mercantil de [*] al tomo [*], folio [*], hoja [*] ("**[*]**").

Y, de otra parte, el Sr. Francesc Fajula de Quintana, en su condición de Director General de **FUNDACIÓ BARCELONA MOBILE WORLD CAPITAL FOUNDATION,** con domicilio social en Plaza Pau Vila, número 1, planta 2-C, edificio Palau de Mar, 08039 de Barcelona, NIF G65760431, con facultades suficientes según resulta de la escritura de apoderamiento autorizada en fecha de 15 de julio de 2022 ante el Notario de Barcelona, D. Ignacio Javier Boisán Cañamero, con el número 1762 de su protocolo ("**MWCapital**").

Las referidas partes, en adelante, podrán ser denominadas, individualmente, la "**Parte**" y conjuntamente, las "**Partes**", reconociéndose mutuamente capacidad legal suficiente para contratar y obligarse

EXPONEN

I. Que [*] está interesada en la posibilidad de presentarse al procedimiento de licitación impulsado por MWCapital con el título "Servicio de CISO, servicio de SOC gestionado y el suministro de una plataforma de SIEM" y número de expediente A/F202503/S, en el marco del cual ha solicitado a MWCapital tener acceso a los documentos (i) Infraestructura Tecnológica y (ii) Plan Director de MWCapital ("**Información Confidencial**") con la finalidad de potencialmente presentar su oferta técnica al referido procedimiento (la "**Finalidad**").

II. Que, en consecuencia, las Partes acuerdan suscribir el presente acuerdo de confidencialidad y no divulgación a fin de regular los deberes de confidencialidad de [*] como receptor de Información Confidencial (el "**Acuerdo**"), el cual se regirá por las siguientes

CLÁUSULAS

1. Lo previsto en este Acuerdo aplicará a toda la Información Confidnecial que MWCapital pueda revelar a [*], con independencia de la forma o soporte en el que se revele, con la excepción de: (a) toda información que ya esté o pase a estar en el dominio público por causas distintas de un incumplimiento por [*] de este Acuerdo; o b) cualquier información de la que [*] ya tenga conocimiento y que no estuviera sujeta a ningún deber de secreto o confidencialidad antes de la revelación de la misma por MWCapital a [*].

2. [*] se compromete a no utilizar la Información Confidencial para cualquier fin distinto a la Finalidad, sin obtener el previo consentimiento por escrito de MWCapital.

3. [*]se compromete a mantener la Información Confidencial en estricta confidencialidad, así como a no divulgarla a ningún tercero salvo aquellos empleados, asesores y colaboradores que requieran acceder a la misma para el desempeño de sus funciones relativas a la Finalidad, y siempre bajo un deber de confidencialidad como mínimo equivalente al regulado en este Acuerdo.

4. Ni el presente Acuerdo ni la información (incluida la Información Confidencial) que MWCapital pueda compartir con [*] implican la concesión de ninguna licencia ni derecho de propiedad intelectual, industrial y/o de cualquier otra naturaleza excepto el derecho a utilizar la Información Confidencial únicamente en la medida necesaria para la Finalidad y siempre conforme a las instrucciones de MWCapital.

5. El presente Acuerdo no impedirá a [*] la revelación de Información Confidencial a la que pueda venir obligado por ley o por orden judicial, si bien en dicho caso lo pondrá en el previo conocimiento de MWCapital, y hará todo lo posible para intentar que se otorgue un tratamiento confidencial a la misma.

6. A petición de MWCapital en cualquier momento y en todo caso a la finalización del presente Acuerdo, [*] deberá devolver, o bien destruir, según le indique MWCapital, toda copia de la Información Confidencial que tenga en su poder.

7. [*] tratará la Información Confidencial únicamente para la Finalidad y siempre conforme a la normativa aplicable, incluida la relativa a protección de datos de carácter personal.

8. Los representantes legales de las Partes reconocen quedar informados y consienten expresamente que sus datos personales reflejados en el presente Acuerdo sean tratados por ambas entidades (respectivamente) con la finalidad de gestionar el presente Convenio. En cualquier momento, dichos interesados pueden ejercer sus derechos de acceso, rectificación, supresión, limitación a su tratamiento, oposición y portabilidad ante el responsable del tratamiento que corresponda; en el caso de dirigirse a [*], a la siguiente dirección [*], o en el caso de dirigirse a MWCapital, a la dirección Pl. Pau Vila 1, Sector 2C (Edificio Palau de Mar), 08039 Barcelona; o bien también mediante correo electrónico, a la dirección dpo@mobileworldcapital.com. En caso de que los interesados así lo deseen, podrán acudir a la Agencia Española de Protección de Datos para cualquier reclamación derivada del tratamiento de sus datos personales.

9. El presente Acuerdo entrará en vigor en la fecha de su firma y permanecerá vigente hasta que toda la Información Confidencial esté en dominio público.

10. El presente Acuerdo se rige por la legislación española. Las Partes acuerdan someter todo conflicto resultante de la ejecución o interpretación del Acuerdo a los juzgados y tribunales de la ciudad de Barcelona, con renuncia expresa a su propio fuero, si otro les correspondiere.

Y EN PRUEBA DE CONFORMIDAD Y ACEPTACIÓN DE TODO LO ESTABLECIDO, ambas Partes firman este Acuerdo mediante signatura electrónica otorgándole el mismo efecto legal que la firma manuscrita.

Francesc Fajula de Quintana Director General **FUNDACIÓ BARCELONA MOBILE WORLD CAPITAL FOUNDATION**	[*] [Cargo] **[ENTIDAD]**