

PLIEGO DE PRESCRIPCIONES TÉCNICAS

ANÁLISIS, ESTUDIO Y DEFINICIÓN PARA EL DESPLIEGUE Y OPERACIÓN DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD FERROVIARIO EN METRO DE MADRID



CONTROL DOCUMENTAL:

Autor del proyecto:	Fernando Galindo García	
Director del Proyecto:	Fernando Morales Aguirre	
Director Técnico:	Dionisio Izquierdo Bravo	
Edición	Fecha	Nº Actividad
1.4.4	15-03-2021	IO_20-060V

Equipo de trabajo:	Marcelo Sanz Gonzalo Fernando Morales Aguirre Fernando Galindo García Antonio Simón Martínez García Andrea Mónica Chalimón Conde	
Edición	Fecha	Nº Actividad
1.0	21-04-2020	IO_20-060V
1.4	01-03-2021	IO_20-060V
1.4.1	05-03-2021	IO_20-060V
1.4.4	15-03-2021	IO_20-060V

1.	INTRODUCCIÓN	4
1.1	ANTECEDENTES.....	4
1.2	CENTRO DE OPERACIONES DE CIBERSEGURIDAD FERROVIARIO (COCF).....	5
2.	OBJETO	9
3.	ALCANCE	9
4.	DISPOSICIONES LEGALES Y NORMAS APLICADAS	12
4.1	CONDICIONES GENERALES EXIGIDAS PARA EL CUMPLIMIENTO EN MATERIA DE MEDIO AMBIENTE	13
4.2	CONDICIONES EXIGIDAS EN MATERIA DE GESTIÓN DE RESIDUOS	14
4.3	CONDICIONES EXIGIDAS PARA EL CUMPLIMIENTO EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES DE LOS TRABAJOS A DESARROLLAR	14
4.4	MARCO LEGAL Y NORMATIVO DE ESTE PLIEGO	14
4.5	PROGRAMAS DE CÁLCULO.....	15
4.6	PLAN DE GESTIÓN DE LA CALIDAD	15
4.7	BIBLIOGRAFÍA	16
4.8	OTRAS REFERENCIAS	16
5.	DEFINICIONES Y ABREVIATURAS	16
6.	REQUISITOS DE DISEÑO	17
7.	ANÁLISIS DE SOLUCIONES	18
8.	DESCRIPCION DE LOS TRABAJOS	18
8.1	PLANIFICACIÓN INICIAL DEL PROYECTO:	18
8.2	ANÁLISIS DEL CONTEXTO:.....	18
8.3	DEFINICIÓN DEL ALCANCE:	19
8.3.1	CAPACIDADES:	19
8.3.2	PROCESOS Y FUNCIONES:	20
8.3.3	ACTIVOS A MONITORIZAR:	22
8.3.4	INFRAESTRUCTURA:.....	22
8.3.5	TECNOLOGÍA:	22

8.3.6 EQUIPO Y MODELO ORGANIZACIONAL:	23
8.4 DEFINICIÓN DE ROLES Y RESPONSABILIDADES	24
8.5 DISEÑO FUNCIONAL Y TÉCNICO:	24
8.6 DEFINICIÓN DETALLADA DE ACTIVIDADES Y PLANIFICACIÓN:	25
8.7 FORMACIÓN	26
9. EQUIPO DE TRABAJO PARA EL PRESENTE ESTUDIO	26
10. DIRECCIÓN Y SUPERVISIÓN DE LOS TRABAJOS.....	28
11. PRESCRIPCIONES TÉCNICAS GENERALES	29
11.1 RECEPCIÓN	29
11.2 CERTIFICACIÓN FINAL DE OBRA	29
11.3 PLAN DE CALIDAD	30
11.4 DOCUMENTACIÓN FINAL.....	31
11.4.1 PROPIEDAD DE LA DOCUMENTACIÓN	31
11.4.2 SOPORTE INFORMÁTICO DE LA DOCUMENTACIÓN	31
12. GARANTÍA.....	32
13. OBLIGATORIEDAD SUBSIDIARIA DEL ADJUDICATARIO ANTE LOS PERJUICIOS OCASIONADOS A TERCEROS.....	32
14. PLANIFICACIÓN	32
15. PRESUPUESTO	34
16. REVISIÓN DE PRECIOS.....	38

1. INTRODUCCIÓN

1.1 ANTECEDENTES

La información, los datos y las operaciones son considerados activos de gran importancia para Metro de Madrid S.A., en adelante METRO, de los cuales depende el buen funcionamiento de la organización.

En este sentido, mantener su disponibilidad, integridad y confidencialidad es esencial para alcanzar los objetivos de negocio y para cumplir con los requisitos legales, reglamentarios o contractuales que sean de aplicación.

A su vez, como consecuencia de la transformación digital, han surgido nuevos escenarios de riesgos de ciberseguridad que hacen que METRO esté expuesto a un mayor número de amenazas que podrían afectar a la seguridad de la información, los datos y las operaciones, pudiendo comprometer la viabilidad del negocio. Adicionalmente, la regulación en materia de ciberseguridad por parte de los gobiernos y administraciones públicas es cada vez mayor, demandando en muchos casos medidas de seguridad de obligado cumplimiento para METRO.

En consecuencia, METRO ha definido la estrategia corporativa de Ciberseguridad la cual se basa, entre otros, en los principios de anticipación, prevención, resiliencia y prestación garantizada del servicio esencial del transporte público.

De la estrategia corporativa de ciberseguridad deriva, entre otras, la necesidad de disponer de una solución coordinada y transversal a todos los sistemas de información de METRO que permita planificar, definir, desarrollar, gestionar y medir las oportunas prácticas y comportamientos a fin de disponer de capacidad para detectar, resistir, responder y recuperarse ante posibles incidentes de ciberseguridad que pongan en peligro la continuidad de los procesos de negocio o, de las tecnologías o personas implicadas en los mismos.

Para ello, se propone definir e implantar un Centro de Operaciones de Ciberseguridad (CiberSOC) adaptado a las necesidades de METRO, con sus diferentes funciones y niveles de servicio, a fin de garantizar que los posibles incidentes de ciberseguridad se identifiquen, analicen, defiendan, investiguen y notifiquen correctamente.

Se le denominará **Centro de Operaciones de Ciberseguridad Ferroviario** (COCF a partir de ahora).

1.2 CENTRO DE OPERACIONES DE CIBERSEGURIDAD FERROVIARIO (COCF)

La misión principal del COCF será monitorizar y mejorar de forma continua la capacidad de ciberseguridad de METRO mediante la prevención, detección, análisis y respuesta a incidentes de ciberseguridad.

La visión será integrada para toda la organización de forma que se establezcan sinergias coordinadas a todos los departamentos de METRO en un único CiberSOC ferroviario desde donde se supervisarán, evaluarán y defenderán todos los sistemas de información de la organización. Este centro cubrirá tanto el mundo IT (Information Technologies o de Sistemas de Información) como el mundo OT (Operational Technologies o Sistemas de Producción).

La definición e implantación del COCF deberá combinar personas, procesos, tecnología e inteligencia, sin olvidar la adecuación a la normativa vigente.



Figura 1: Elementos esenciales del COCF

En cuanto a los elementos, el COCF estará formado por:

- **Procesos:**
 - Procesos de negocio.
 - Procesos tecnológicos.
 - Procesos operativos propios.
 - Procesos analíticos.
- **Personas** repartidas en sus diferentes niveles:
 - Equipo de especialistas en tecnología.
 - Analistas.
 - Ingenieros de seguridad.
 - Profesionales de inteligencia.
 - Gestores para la supervisión de las actividades.
- **Tecnología:**

ÁREA DE INGENIERÍA

- Herramientas de monitorización y análisis de red.
- Sistema de Gestión de Eventos e Información de *Seguridad* (SIEM) que recoge los registros de sistemas, de dispositivos de red, de cortafuegos y sistemas de protección.
- Herramientas de análisis forense de equipos mediante la toma de evidencias y su análisis.
- Herramientas de análisis de vulnerabilidades.
- Sistemas de *Backup* fiables.
- **Inteligencia:**
 - Conocimiento tácito y explícito para interpretar, analizar, integrar y evaluar información relevante sobre un determinado hecho que representa una amenaza o una oportunidad para una organización, Este conocimiento proporciona una mejor toma de decisiones al reducir el nivel de incertidumbre.

En la siguiente figura se resumen los diferentes elementos que formarían parte del COCF:

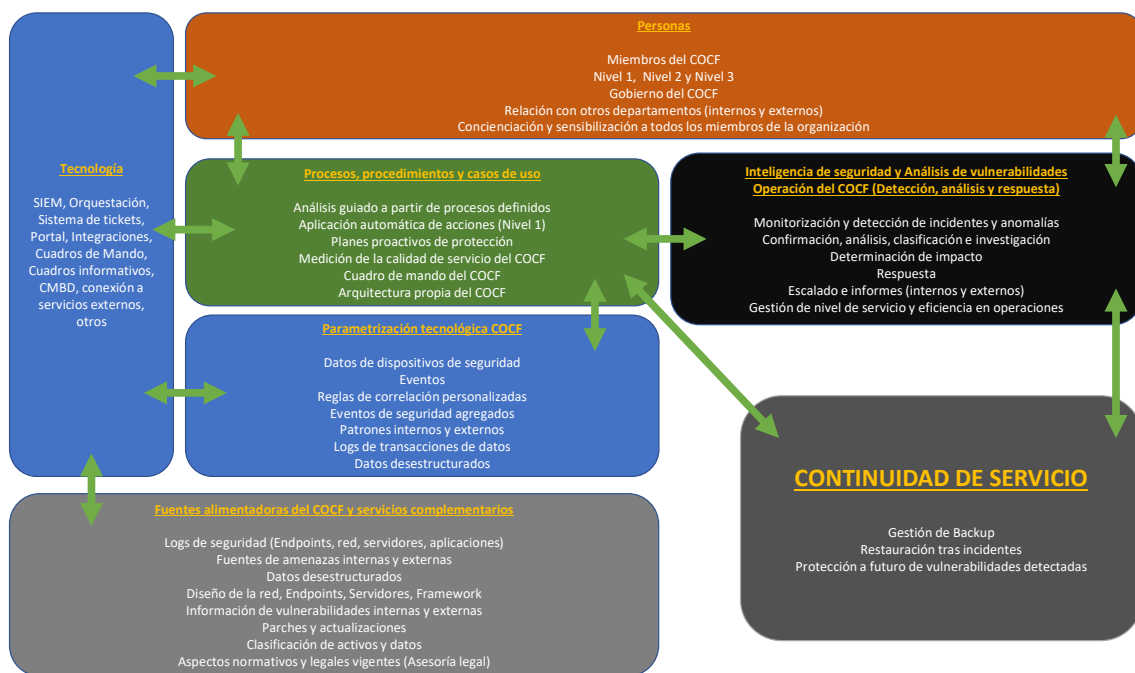


Figura 2: Elementos que determinan el COCF

En cuanto al equipo y modelo organizacional del COCF, si bien serán definidos dentro del alcance del servicio a contratar, en principio, se propone que la Operación del COCF se realice en tres (3) niveles fundamentales al que se añadiría un nivel complementario para ciertas funciones no incluidas en los niveles anteriores:

- **Nivel 1 (Monitorización y Análisis):**

Será el nivel más cercano a los equipos, elementos y/o dispositivos a monitorizar. Se trata de un primer nivel de monitorización, contención y primer análisis.

Estará formado por uno o varios analistas, que, mediante herramientas adecuadas, monitorizan de forma constante las alertas y las amenazas que puedan existir en la compañía. Hacen una clasificación basándose en la información que son capaces de recopilar e investigar para determinar si estas alertas y amenazas se pueden convertir en un incidente de seguridad o si se trata de falsos positivos.

- **Nivel 2 (Análisis Profundo y Respuesta):**

Nivel de análisis más profundo y de gestión de incidentes. Este nivel intervendrá sólo en caso de necesidad. Será el encargado de la gestión de incidentes.

Se encarga de responder al incidente tras la clasificación inicial. Este nivel 2 tiene un grado de especialización mayor. A través de una metodología y unos procedimientos definidos, se realiza un análisis del incidente, cotejando información de distintas fuentes, determinando si afecta a sistemas críticos, revisando qué conjunto de datos se han visto impactados y qué sistemas y servicios pueden estar afectados. También recomienda qué remedio se puede aplicar y proporciona soporte para realizar un análisis de este incidente. Es muy importante que tenga como fuente de información una inteligencia bien construida, creada tanto por el histórico disponible como por pertenecer a una red de Centro Operativo de Ciberseguridad global en la que se comparta información de estas amenazas. Además, deberá contar con una analítica avanzada.

En este nivel deberá existir la capacidad de identificar, a través de trazas en los sistemas, cómo tuvo lugar un compromiso, identificando el alcance, la metodología utilizada y, a partir de ahí, las contramedidas que pueden implantarse, realizando investigaciones con el fin de identificar el atacante y sus motivaciones.

Deberá estar en contacto con la parte operativa correspondiente para, conjuntamente, tomar decisiones que puedan afectar a la misma.

- **Nivel 3 (Expertos):**

Se trata del nivel con mayor cualificación y especialización, siendo todos sus componentes expertos en varias materias de seguridad, encargados de realizar las auditorías técnicas, proponer los planes de acción para la mejora y realizar algunos servicios especialmente complejos, como el análisis forense.

- **Servicios complementarios:** aquellos que se consideren necesarios para el buen funcionamiento del COCF.

En cuanto a la operativa del COCF, los objetivos en una respuesta a un incidente de seguridad deberían ser, al menos, los siguientes:

- Mantener la operación en los sistemas. Es necesaria la coordinación entre el COCF y la organización mediante documentos preestablecidos (plan de contención, procedimientos de actuación, ...).
- Asegurar el completo entendimiento del incidente.
- Lecciones aprendidas y generación de inteligencia.
- Evolución del proceso de seguridad.

Al final de la implantación, el COCF deberá cumplir con las certificaciones, buenas prácticas y validaciones necesarias que garanticen su eficiencia y cumplimiento del marco regulatorio existente. Ello llevará a mantener el COCF como un proceso continuo en el tiempo y en constante evolución.

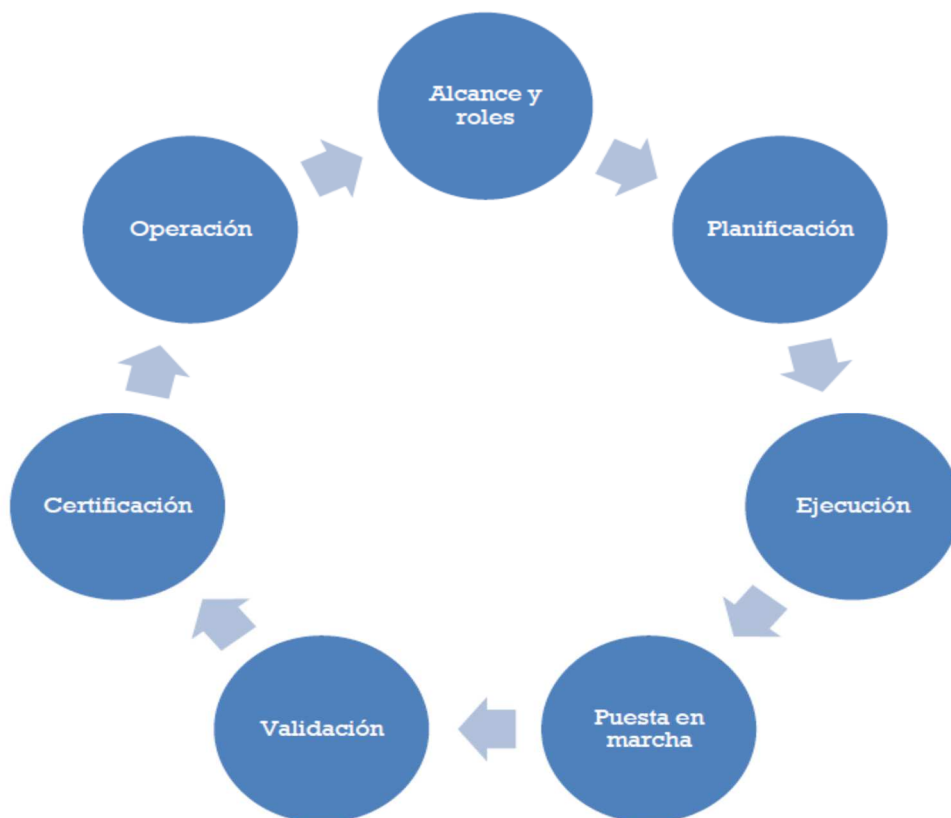


Figura 3: El COCF es un proceso continuo en el tiempo

2. OBJETO

El objeto del presente Pliego de Prescripciones Técnicas, en adelante PPT, es establecer las condiciones técnicas que regirán la presentación de ofertas en la licitación para la contratación de los servicios de análisis, estudio y definición del despliegue y operación del Centro de Operaciones de Ciberseguridad Ferroviario de METRO.

Todo ello, orientado a la potenciación de las capacidades de seguridad en materia de prevención, detección, análisis y respuesta a incidentes de seguridad.

3. ALCANCE

El proceso de construcción del COCF se llevará a cabo en siete fases:

- FASE I: Alcance y roles
 - Análisis del contexto
 - Definición del alcance
 - Definición de roles y responsabilidades
 - Diseño funcional y técnico
- FASE II: Planificación
 - Definición detallada de actividades y planificación
- FASE III: Ejecución
 - Despliegue de arquitectura / herramientas
 - Integración de fuentes de datos
- FASE IV: Puesta en marcha
 - Definición de Procesos de Actuación
 - Definición de Procedimientos de respuesta.
- FASE V: Validación
 - Cuadros de mando
 - Indicadores
 - Métricas
- FASE VI: Certificación
 - Certificaciones
- FASE VII: Operación
 - Operación del COFC

En este sentido, el alcance del servicio a contratar se circunscribe a todas las tareas necesarias para llevar a cabo la FASE I (Alcance y Roles) y la FASE II (Planificación) así como también la impartición de sesiones formativas y transferencia de conocimientos al personal de METRO.

En el proyecto se deberán acometer al menos las siguientes acciones:

1. Planificación inicial del proyecto:

Dentro de la planificación se deberán identificar claramente hitos de entrega, validación y aceptación por parte de METRO. En cuanto a los plazos de validación de cada uno de los productos entregados, estos plazos deberán ser acordes con el volumen de información entregada.

2. Análisis del contexto:

Se deberá recopilar la información necesaria para determinar el contexto, tanto interno como externo, en el cual se desarrollan las actividades principales de la organización. Entre otros, se tendrá en cuenta: el entorno económico y financiero; entorno social; entorno competitivo; entorno tecnológico; entorno legal y normativo.

3. Definición del alcance:

En base a la información recopilada en la fase anterior, se deberá determinar cuáles serán los objetivos del COCF y el alcance del mismo. En concreto, se definirá entre otros:

- Capacidades
- Procesos y funciones.
- Activos a monitorizar
- Infraestructura
- Tecnología
- Perfiles
- Equipo y Modelo Organizacional

Esta acción dará como resultado dos entregables:

- Documento de análisis de alternativas:
Documento preliminar en el que se describan las diferentes alternativas de implementación y operación del COCF (herramientas, tipología de software hardware, tipo de servicio, organización, etc.), describiendo para cada una de ellas las ventajas y desventajas, y recomendando la más adecuada.
- Documento de análisis definitivo:
Documento en el que se describa la alternativa seleccionada, así como también toda la información de detalle que sea necesaria para llevar a cabo el diseño del COCF. Entre otros, incluirá una estimación económico financiera, los parámetros de prestación de servicios más adecuados, así como el coste de los

misimos. El objetivo principal es que los servicios que proporcionará el COCF puedan adaptarse a un presupuesto determinado permitiendo la prestación de los servicios de forma realista.

Este documento deberá contener el nivel de detalle suficiente para que METRO pueda tomar una decisión en relación con el Modelo Organizacional a desarrollar e implementar.

4. Definición de Roles y responsabilidades

Una vez se haya establecido el alcance, será necesario definir los roles y responsabilidades dentro de la organización relacionados con las operaciones que se llevarán a cabo en el COCF y con la gestión del mismo.

5. Diseño funcional y técnico:

En base al documento de análisis definitivo y a la definición realizada en cuando a roles y responsabilidades, se deberá realizar un diseño detallado (a nivel funcional y técnico) del COCF.

6. Definición detallada de actividades y Planificación

Una vez definidos el alcance y diseño del COCF, se planificarán las distintas fases (ejecución, puesta en marcha, validación, certificación y operación) a acometer para implementar y validar el COCF. Asimismo, se deberán detallar las tareas que son necesarias para cumplir con los objetivos definidos.

Posteriormente, se deberán evaluar los posibles modelos de evolución del mismo a fin de definir, la fase inicial y la fase final a la que se designará como objetivo.

Al final de esta fase se deberá elaborar un plan de proyecto de implementación y puesta en marcha del COCF.

7. Formación

El adjudicatario deberá realizar una transferencia de conocimiento, así como también impartir sesiones formativas orientadas a que el personal de Metro, incluyendo los niveles de dirección, adquiera los conocimientos básicos necesarios para llevar a cabo las fases restantes del proceso de construcción del COCF (FASE III – Ejecución; FASE IV - Puesta en marcha; FASE V – Validación; FASE VI - Certificación y FASE VII - Operación), y la toma de decisiones relativas a dicho proceso.

El ámbito funcional, características, actividades y requisitos específicos de cada una de estas fases se describen en el apartado “8. Descripción de los trabajos”.

En la siguiente tabla se muestran los entregables incluidos en el presente PPT:

ENTREGABLE	CONTENIDO
1	Documento de análisis de alternativas.
2	Documento de análisis definitivo.
3	Diseño del COCF (a nivel funcional y técnico).
4	Plan de proyecto de implementación y puesta en marcha del COCF.
5	Material de formación (Plan de formación, manuales, etc.)

Tabla 1: Entregables del presente PPT

Es importante destacar que queda expresamente fuera del alcance de la licitación cualquier adquisición de hardware y/o licencias de software, así como otro servicio diferente al objeto del contrato.

Cualquier dato enumerativo que se ofrece a lo largo de este documento se hace de forma que facilite la confección de las ofertas, teniendo carácter informativo, de modo que cada oferente tenga una idea lo más aproximada del servicio objeto del contrato, debiendo comprobar o cotejar los datos que considere necesario.

4. DISPOSICIONES LEGALES Y NORMAS APLICADAS

En general, serán de aplicación las prescripciones que figuran en las normas, instrucciones o reglamentos oficiales que guardan relación con los trabajos del presente PPT, con sus instalaciones complementarias o con los trabajos necesarios para realizarlas y que se encuentran en vigor en el momento de redactar el presente PPT.

Se considerarán todas las modificaciones y ampliaciones de las citadas normas.

En caso de discrepancias entre las normas y salvo manifestación expresa en contra, se entenderá válida la prescripción más restrictiva.

Cuando en algunas disposiciones legales se haga referencia a otra que haya sido modificada o derogada, se entenderá que dicha modificación o derogación se extiende a aquella parte de la primera que haya quedado afectada.

De la misma forma, se deberán considerar siempre las últimas versiones o actualizaciones de todos los documentos referenciados a lo largo del presente PPT.

4.1 CONDICIONES GENERALES EXIGIDAS PARA EL CUMPLIMIENTO EN MATERIA DE MEDIO AMBIENTE

Con el fin de minimizar el impacto medioambiental, no sólo se tendrá en cuenta la explotación y mantenimiento de los equipos, sino también su diseño, fabricación, selección y manipulaciones de materiales. Se considerará la afección al medio ambiente desde el origen del Proyecto, y toda solución técnica o estética será precedida de un riguroso análisis para la integración de los siguientes aspectos:

- Siempre que sea viable, se presentará la alternativa de diseño que genere menos emisiones, ruidos, vibraciones y/o radiaciones electromagnéticas; así como el menor consumo de agua y energético posible.
- Se proyectarán las instalaciones y metodologías necesarias para la correcta gestión de los residuos que se vayan a generar.
- Se proyectarán e implantarán las medidas oportunas para evitar cualquier vertido de sustancias peligrosas.
- Se tendrá en cuenta que el horario de trabajo minimice las molestias que se pudieran ocasionar por ruido emitido al exterior.
- Se tendrá en cuenta el impacto visual negativo que pudiera tener la instalación/obra, tomando las medidas necesarias para minimizarlo.

En caso de que se vayan a instalar o diseñar equipos se valorará que:

- La fuente de energía sea renovable.
- La fuente de energía sea gas natural, hidrógeno o electricidad.
- El equipo no genere emisiones de gases contaminantes por combustión.
- El equipo no genere radiaciones electromagnéticas significativas.
- El equipo no genere ruidos ni vibraciones significativas.

- Se minimice el consumo de agua del equipo una vez inicie su actividad.

4.2 CONDICIONES EXIGIDAS EN MATERIA DE GESTIÓN DE RESIDUOS

Los residuos generados serán gestionados por el adjudicatario, de acuerdo con la legislación vigente y debe evidenciarlo entregando a METRO cualquier documentación que le sea requerida (autorizaciones, albaranes de entrega a gestor autorizado, documentos de control y seguimiento, etc.).

El adjudicatario está obligado a restituir a su estado original, sin que proceda abono por dicho concepto, todas las áreas utilizadas como acopios.

4.3 CONDICIONES EXIGIDAS PARA EL CUMPLIMIENTO EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES DE LOS TRABAJOS A DESARROLLAR

Los trabajos desarrollados dentro de este PPT deberán cumplir los requisitos legales en materia de prevención de riesgos laborales según lo establecido por METRO en su Sistema de Gestión de Prevención de Riesgos Laborales dentro de su Proceso referente a “Coordinación de Actividades Empresariales”.

4.4 MARCO LEGAL Y NORMATIVO DE ESTE PLIEGO

Las normas y disposiciones legales que, de manera específica, y complementando a las de ámbito más general que aplican en este PPT, aun no siendo un listado exhaustivo, son las siguientes:

- UNE 157001. Criterios generales para la elaboración formal de los documentos que constituyen un proyecto técnico, o equivalente.
- Familia de normas ISO 27000 como conjunto de estándares internacionales sobre la seguridad de la información. Algunas normas de la familia son:
 - UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información, o equivalente.
 - UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información, o equivalente.
- UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información, o equivalente.

- UNE 71505-2:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas, o equivalente.
- UNE 71506:2013 Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas, o equivalente.
- UNE-ISO/IEC TR 19791:2013 IN Tecnologías de la información. Técnicas de seguridad. Evaluación de la seguridad de sistemas operacionales, o equivalente.
- UNE-ISO/IEC TR 15446:2013 IN Tecnologías de la información. Técnicas de seguridad. Guía para la producción de perfiles de protección y objetivos de seguridad, o equivalente.
- Familia de normas IEC 62443 e ISA 99, que recogen un conjunto de definiciones y estándares sobre mejores prácticas y recomendaciones para incrementar la ciberseguridad en sistemas industriales, o equivalente.
- Estándares de buenas prácticas en gestión y control de calidad como ISO 19600 o ISO 9000, o equivalente.
- ISO 23301 sobre la gestión de la continuidad del negocio.
- ENS: Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero) en lo referido a la adopción de medidas de seguridad de las soluciones tecnológicas o la prestación de servicios ofertados.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

4.5 PROGRAMAS DE CÁLCULO

Para la realización del presente PPT no se han utilizado programas de cálculo.

4.6 PLAN DE GESTIÓN DE LA CALIDAD

El Área de Ingeniería dispone de un sistema de gestión de la calidad aplicado a sus actividades conforme a la norma UNE-EN ISO 9001, tal y como se recoge en el Certificado N.º ER-0928/2010, emitido por la entidad certificadora AENOR (Asociación Española de Normalización y Certificación).

4.7 BIBLIOGRAFÍA

Cabe mencionar el documento elaborado por el Centro de Ciberseguridad Industrial titulado “Guía para la construcción de un centro de operaciones y respuesta de ciberseguridad industrial” en su primera edición de febrero de 2019 (ISBN: 978-84-947727-8-8), del que se han extraído algunos conceptos y clasificaciones.

4.8 OTRAS REFERENCIAS

Sin referencias a destacar, informaciones generales de suministradores y documentos de proveedores de elementos de un centro de ciberseguridad.

5. DEFINICIONES Y ABREVIATURAS

A continuación, se desarrolla un glosario de términos que aparece a lo largo de este PPT con el objetivo de ayudar a comprender al lector terminologías utilizadas en el presente documento.

Acrónimo	Significado	Objeto
PPT	<i>Pliego de Prescripciones Técnicas</i>	Conjunto de documentos que define las características generales de un producto, obra, instalación servicio o software.
ISO	<i>International Standarization Organization (Organización Internacional de Normalización)</i>	Organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

Acrónimo	Significado	Objeto
UNE-EN ISO	<i>Una Norma Española – European Norm (Norma europea) – International Standardization Organization (Organización Internacional de Normalización)</i>	Normas AENOR que son estándares europeos e internacionales.
CPD	<i>Centro de Proceso de Datos</i>	Ubicaciones donde se concentra el hardware que permite habilitar el servicio de las distintas aplicaciones.
COCF	<i>Centro de Operaciones de Ciberseguridad Ferroviario</i>	Es el centro de ciberseguridad que se define en el presente documento. Sería el equivalente al denominado en otros textos como CiberSOC (Centro de Operaciones de Ciberseguridad).
ENS	<i>Esquema Nacional de Seguridad</i>	Directrices sobre seguridad a nivel nacional.
LPIC	<i>Ley de Protección de Infraestructuras Críticas</i>	Regulación sobre infraestructuras críticas.
RGPD	<i>Reglamento General de Protección de Datos</i>	Regulación sobre protección de datos.
SOC	<i>Security Operation Centre</i>	Centro de Operaciones de Seguridad.

Tabla 2: Abreviaturas y definiciones

6. REQUISITOS DE DISEÑO

A la hora de abordar la redacción del presente PPT, se han de tener en cuenta los siguientes requisitos de diseño, que condicionarán las soluciones a adoptar:

- Pronta resolución a los problemas existentes.
- Implantación de una solución óptima.
- Máximo aprovechamiento de los sistemas existentes y componentes asociados.
- Optimización de costes.

- Minimizar futuras incidencias.

7. ANÁLISIS DE SOLUCIONES

No aplica.

8. DESCRIPCION DE LOS TRABAJOS

En el presente apartado se especifican los bloques mínimos que deberán cubrirse en la oferta.

8.1 PLANIFICACIÓN INICIAL DEL PROYECTO:

Dentro de la planificación se deberán identificar claramente hitos de entrega, validación y aceptación por parte de METRO. En cuanto a los plazos de validación de cada uno de los productos entregados, estos plazos deberán ser acordes con el volumen de información entregada.

8.2 ANÁLISIS DEL CONTEXTO:

El objetivo de esta fase es realizar un análisis completo del contexto a fin de determinar, entre otros:

- Objetivos del negocio.
- Entorno económico y financiero (sobre todo en lo referente a limitaciones presupuestarias), social y competitivo, en el que se desarrollan las actividades principales de METRO.
- Arquitectura de los sistemas de información de METRO.
- Arquitectura de la red de comunicaciones.
- Servicios y sistemas críticos.
- Activos que permitan tener una visión amplia de la actividad de la organización.
- Activos desplegados en puntos clave de la organización.
- Activos que supongan un riesgo relevante para la organización.
- Sistemas en los que se maneja información de terceros.
- Servicios que utilizan sistemas de terceros para manejar información o para prestar servicios.
- Centros de operación existentes.

- Protocolos de comunicación utilizados, sobre todos los específicos del sector ferroviario.
- Marco normativo aplicable a METRO en el ámbito de la ciberseguridad.
- Principales riesgos existentes en el ámbito de la ciberseguridad.
- Puntos débiles o lugares donde focalizar o reforzar los niveles de seguridad.
- Medidas de seguridad implementadas, sobre todo en lo referente a: segmentación de redes, sistemas de seguridad lógica perimetral, gestión de vulnerabilidades, monitorización, gestión de incidentes de ciberseguridad, continuidad del negocio y resiliencia.

Para ello se recopilará la información necesaria a través de los medios que se consideren oportunos para una correcta evaluación (entrevistas con las áreas técnicas y personal clave en la organización en temas de ciberseguridad; revisión de documentación existente; ejecución de herramientas de análisis; etc.).

Al respecto cabe mencionar que:

- Cualquier tipo de revisión técnica que se realice sobre los sistemas de METRO deberá ser acordada previamente con METRO y no deberá ser intrusiva ni afectar al correcto funcionamiento de la organización.
- En la oferta técnica, se deberán indicar los medios y el detalle de herramientas a utilizar en esta fase.
- Las herramientas que se utilicen serán aportadas por el adjudicatario.
- El acceso a la información confidencial se realizará desde las instalaciones de METRO.

8.3 DEFINICIÓN DEL ALCANCE:

A partir de la información recopilada en la tarea anterior, se deberá establecer el alcance de los servicios del COCF, principalmente en cuanto a capacidades, infraestructura, recursos y modelo organizativo. Para ello se deberán tomar como referencia las normativas y buenas prácticas existentes en el mercado en esta materia.

Entre otros, se deberá definir:

8.3.1 Capacidades:

El SOC debería incorporar al menos las siguientes capacidades dentro de su estructura organizativa. En cualquier caso, durante la ejecución del proyecto podrían identificarse otras capacidades, procesos, funciones, etc., en cuyo caso serán expuestas para analizarlas conjuntamente con METRO y tomar una decisión respecto de su inclusión en el diseño.

- **Monitorización en tiempo real:**

- Disponer de un conjunto de paquetes de monitorización estándar de red y host que puedan ser adaptados a escenarios de monitorización comunes.
 - Monitorizar mediante el uso de firmas, análisis de comportamiento y reconocimiento de anomalías.
 - Incorporar capacidades de monitorización que recibirán atención periódica de analistas y/o herramientas analíticas.
- **Análisis de incidentes, coordinación y respuesta:**
 - Cubrir todo el ciclo de vida del ataque.
 - Contemplar la arquitectura de red de extremo a extremo.
 - Analizar amenazas y vectores de ataque relevantes para el alcance.
 - Consolidar todos los datos de seguridad relevantes en un repositorio integrando arquitectura analítica para la supervisión y análisis de los incidentes.
 - Aplicar correlación automática y en tiempo real.
 - Incorporar minería de datos y otras técnicas para examinar datos históricos en busca de pruebas de actividad maliciosa o anómala.
 - Crear reglas personalizadas para mejorar los esfuerzos de monitorización.
 - **Capacidades adicionales:**
 - Disponer de ingeniería para el diseño e implementación de herramientas en el SOC.
 - Mantener la visibilidad hasta el activo final consolidando el conocimiento y las operaciones a través de un equilibrio de recursos centralizados y distribuidos.
 - Proporcionar inteligencia con información necesaria en tiempo y forma para que desde el SOC se puedan tomar decisiones informadas que permitan anticiparse y prepararse mejor frente a las amenazas y a los ciberataques potenciales. Las fuentes utilizadas pueden ser entre otras, fuentes de libre acceso, como páginas web, redes sociales y blogs, así como en otros repositorios de Internet, la dark y la deep web.
 - Incorporar un programa de métricas que mida aspectos clave de la salud operativa de SOC y proporcione la gerencia del SOC impulsar la mejora del proceso y su desempeño.

8.3.2 Procesos y funciones:

Se deberán establecer los procesos mínimos que se llevarán a cabo dentro del COCF, así como también las funciones principales de cada uno de ellos.

En cuanto a los procesos operativos, se contemplarán al menos los siguientes procesos:

- **Respuesta a incidentes:**
 - Detección, clasificación, notificación, contención y remediación de incidentes.
- **Soporte de incidentes:**
 - El principal objetivo es proporcionar una estructura de funciones de soporte para la respuesta a incidentes y mantener a los interesados informados acerca de ciber-incidentes activos y de las actividades de remediación a largo plazo.
 - Las principales funciones dentro de este proceso son:
 - › Identificación y documentación
 - › Soporte de terceras partes
 - › Soporte al negocio
- **Inteligencia de amenazas:**
 - Recolección, análisis, generación, y distribución de información utilizable, relativa a amenazas relacionadas con los sistemas bajo monitorización.
 - Las principales funciones son:
 - › Origen y recolección: identificación de las necesidades de inteligencia dentro de la organización; selección de fuentes de datos adecuadas tanto internas como externas; etc.
 - › Procesamiento y explotación: análisis e interpretación de la información procedente de las fuentes de datos con el fin de generar información accionable.
 - › Análisis de amenazas: identificación de actores de amenaza, antes de que éstos hagan efectivo el compromiso de los sistemas, y proporcionar criterios, basados en riesgo, que asistan el proceso de toma de decisiones.
 - › Producción y diseminación: generación y distribución de productos que sean directamente utilizables por los consumidores (informes específicos, etc.).
- **Operaciones defensivas:**
 - Garantizar que las capacidades de detección y tratamiento de incidentes se mantienen al día y relevantes. Su objetivo principal es la adaptación constante de las capacidades de detección en tiempo real y el desarrollo de habilidades para el tratamiento proactivo de incidentes.
 - Las principales funciones dentro de este proceso son:
 - › Priorización de fuentes de datos
 - › Persecución de amenazas

- **Gestión de la superficie de ataque:**
 - Recolectar, generar y compartir información de amenazas que pueda ser inmediatamente utilizada para mejorar la postura de ciberseguridad de la organización. Las funciones principales de este proceso son:
 - › Preparación e identificación
 - › Análisis
 - › Remediación y mitigación
 - › Informes y seguimiento

8.3.3 Activos a monitorizar:

Se deberá definir, entre otros:

- Sistemas / Activos a monitorizar clasificados según criticidad a fin de definir las prioridades de integración.
- Volumetría de fuentes de datos para cada sistema/activo a monitorizar, desglosado por tecnología.
- Casos de uso mínimos a considerar para la generación de alertas.
- Información mínima a registrar en el COCF (logs/eventos; flujos; reputación Ips; actividad de red; actividad de BBDD; actividad de aplicaciones, etc.).
- Número de eventos por segundo (EPS).
- Períodos de retención a tener en cuenta respecto de los registros de eventos y alarmas de los servicios y fuentes de información.

8.3.4 Infraestructura:

Se deberán determinar los requisitos mínimos (legales, normativos, técnicos, de seguridad física y lógica) a cumplir por la Sala de Operaciones del COCF.

8.3.5 Tecnología:

Se deberá realizar un análisis detallado de las tecnologías disponibles en el mercado, así como también de las disponibles en METRO a fin de determinar, entre otros:

- Tipos de tecnología / software específico a utilizar en el COCF. Por ejemplo: Honeypots, cortafuegos, sondas y herramientas de monitorización, sistemas de orquestación, herramientas de detección de indicadores de compromiso, de detección de anomalías de red, de análisis de anomalías de sistemas, de análisis de logs, etc.
- Requisitos mínimos a cumplir por las herramientas de cada tipología, a fin de que cumplan con los requisitos y buenas prácticas en materia de ciberseguridad y puedan integrarse en la plataforma tecnológica de METRO.

- Listado de posibles herramientas a implementar para cada tipología definida. En base al análisis realizado se considerarán solamente aquellas que cumplan los requisitos identificados en el punto anterior.
- Listado de herramientas existentes en METRO (que ya están implementadas o en fase de implementación) y que serán utilizadas dentro del ámbito del SOC así como también herramientas que deberían ser adquiridas.

Nota: Para todas aquellas tecnologías, soluciones y/o herramientas, susceptibles de ser adoptadas por METRO para su despliegue y uso en el COCF, debe contemplarse la realización de demostraciones bien a través de los fabricantes o bien a través de empresas que las tengan implementadas. Asimismo, será importante facilitar la realización de reuniones con otros clientes que dispongan de un SOC, o con proveedores de servicios de SOC, para intercambiar experiencias.

8.3.6 Equipo y Modelo Organizacional:

En base al análisis realizado en las tareas anteriores y al alcance definido, se deberá definir, el equipo humano y el modelo organizacional del COCF el cual deberá ajustarse a las necesidades específicas de METRO, así como al entorno y a las capacidades y recursos disponibles. Al respecto, se propone que la operación del COCF se realice en tres (3) niveles (ver información adicional en el apartado “1.2. Centro de Operaciones de Ciberseguridad Ferroviario”).

Cabe mencionar que, además de los niveles de operación propuestos, debería tenerse en cuenta un nivel de gestión del COCF.

A fin de determinar cuál es el modelo organizacional que se adapta mejor a las características y necesidades de METRO, el adjudicatario deberá elaborar un documento de análisis preliminar en el que se describan al menos tres (3) alternativas posibles recomendando la más adecuada para su implantación e integración en el entorno de METRO. Para cada alternativa se deberá indicar, al menos:

- Niveles del COCF indicando para cada uno de ellos:
 - Horario de servicio.
 - Lugar desde donde se prestará el servicio (Dentro de las instalaciones de METRO / Fuera de las Instalaciones de METRO).
 - Procesos y funciones a desarrollar.
 - Perfiles: número de personas; tipo (recursos internos de METRO o recursos subcontratados);
 - Equipamiento y herramientas necesarias: tipología; propiedad del equipamiento (de METRO o del contratista); propiedad de las herramientas; etc.
 - Ubicación del equipamiento, de los sistemas y de los datos (en las instalaciones de METRO o en las instalaciones del contratista).
- Evaluación temporal y económico financiera del ciclo de vida de cada alternativa.

- Características, ventajas y desventajas de cada alternativa, indicando adicionalmente cuál es la alternativa recomendada.

Esta acción dará como resultado dos entregables, los cuales se describen en el apartado “3. Alcance”.

Ambos documentos deberán ser aprobados por METRO antes de pasar a la fase “Diseño Funcional y Técnico”.

8.4 DEFINICIÓN DE ROLES Y RESPONSABILIDADES

Una vez se haya establecido el alcance y se haya seleccionado el modelo a implementar, será necesario definir de forma detallada los roles y responsabilidades dentro de la organización relacionados con las operaciones que se llevarán a cabo en el COCF y con la gestión del mismo.

El resultado de esta fase deberá ser incluido en el documento de diseño funcional y técnico.

8.5 DISEÑO FUNCIONAL Y TÉCNICO:

Se deberá elaborar el diseño, tanto a nivel funcional como técnico, del COCF bajo las siguientes consideraciones:

- Para la elaboración del diseño, se deberá tener en cuenta el marco legal y normativo especificado en el apartado “5.5 Marco legal y normativo de este pliego”.
- Constará, entre otros, de memoria, anexos y planos según la norma UNE 157001 “Criterios generales para la elaboración formal de los documentos que constituyen un proyecto técnico”.
- Incluirá las especificaciones detalladas del COCF tanto a nivel funcional (diseño del Servicio) como técnico.
- El Diseño del Servicio contemplará las especificaciones a nivel funcional y alcances en cuanto a, al menos:
 - Tipo, misión y objetivos del COCF.
 - Modelo organizativo.
 - Servicios a prestar por cada uno de los niveles del COCF, incluyendo capacidades, procesos, funciones, personas, etc.
 - Activos a monitorizar.

- Tecnologías (descripción de los tipos de herramientas a utilizar, propiedad de las mismas, etc.)
 - Incluirá el detalle de procedimientos mínimos que deberían ser desarrollados para dar soporte a la operativa del COCF.
- El Diseño Técnico contemplará los requisitos (legales y normativos, técnicos, de seguridad física y de ciberseguridad) y especificaciones técnicas al menos referidas a:
- Infraestructura, sobre todo en lo referente a la sala de operaciones del COCF.
 - Tecnologías, sobre todo en lo referente a elementos de hardware y software.
 - Implantación e integración de los elementos necesarios para la construcción y operación del COCF.
 - Aspectos de Certificación del COCF a tener en cuenta según la normativa vigente para este tipo de instalaciones.
 - Además, se incluirá un apartado completo u anexo con los requisitos de seguridad que deberán ser considerados para nuevas adquisiciones y que podrá ser referenciado en futuros documentos descriptivos.

8.6 DEFINICIÓN DETALLADA DE ACTIVIDADES Y PLANIFICACIÓN:

Una vez definidos el alcance y diseño del COCF, se planificarán las distintas fases (FASE III – Ejecución; FASE IV - Puesta en marcha; FASE V – Validación; FASE VI - Certificación y FASE VII - Operación) a acometer para implementar y validar el COCF.

En este sentido, se deberá elaborar un “Plan de proyecto de implementación y puesta en marcha del COCF”, en el cual se deberá especificar entre otros:

- Modelo de evolución del COCF a fin de identificar cuál será el modelo inicial a desplegar y cuál será el modelo final (modelo objetivo).
- Planificación detallada, con tareas y duración, de las diferentes fases para la puesta en marcha y operación del COCF.
- Estudio detallado de costes que cubra desde el inicio de la puesta en marcha de las medidas y del COCF hasta los 10 años de operación. Se deberán incluir las renovaciones tecnológicas que correspondan durante ese periodo (licencias, equipamiento, formación, campañas, ...) y las recomendaciones en cuanto a reevaluación del sistema, actualización de certificaciones, etc.
- Requisitos a tener en cuenta para la validación del COCF.

8.7 FORMACIÓN

El adjudicatario deberá realizar una transferencia de conocimiento, así como también impartir sesiones formativas orientadas a que el personal de Metro, incluyendo los niveles de dirección, adquiera los conocimientos básicos necesarios para llevar a cabo las fases restantes del proceso de construcción del COCF (FASE III – Ejecución; FASE IV - Puesta en marcha; FASE V – Validación; FASE VI - Certificación y FASE VII - Operación), y la toma de decisiones relativas a dicho proceso.

El contenido de las sesiones formativas deberá ser acordado previamente de forma conjunta con METRO. En cuanto a los temas a tratar, estimándose un total de entre 15 y 20 jornadas de formación, se citan algunos a modo de ejemplo:

- Introducción a la ciberseguridad, sobre todo lo referente a tendencias actuales en cuanto amenazas y riesgos.
- Centro de Operaciones de Ciberseguridad (Qué es; objetivos; ventajas de disponer de un SOC; capacidades; etc.)
- Proceso de gestión de incidentes de ciberseguridad.
- Proceso de gestión de vulnerabilidades.

9. EQUIPO DE TRABAJO PARA EL PRESENTE ESTUDIO

Para la realización de los trabajos incluidos en el presente PPT se estima, aunque no es limitativo, que serán necesarios los siguientes perfiles:

- Jefe de Proyecto. Velará por el control de calidad de las actividades del proyecto.
- Arquitecto de ciberseguridad.
- Ingenieros, auditores, especialistas en análisis de vulnerabilidades y procesos de Ciberseguridad.
- Asesor legal.

En cualquier caso, el ofertante deberá evaluar, e incluir su valoración en la oferta, el equipo de trabajo completo que considere necesario para realizar los trabajos de forma adecuada.

Cada perfil actuará en su ámbito de conocimiento cuando sea necesario para la elaboración de los diferentes análisis y entregables considerados en el presente Pliego. Es posible que una misma persona pueda cubrir varios de los perfiles indicados anteriormente siempre que se respeten los plazos acordados con la Dirección Facultativa para la realización de los trabajos.

El oferente deberá disponer de las herramientas necesarias para la realización de análisis, pruebas de seguridad y cualquier aspecto relacionado con el contenido del presente pliego.

A continuación, se indican características de cada uno de los perfiles indicados anteriormente:

Jefe de proyecto

Responsable del proyecto, del cumplimiento de la planificación, del aseguramiento del plan de calidad y de las entregas realizadas. Para ello deberá, al menos:

- Coordinar todo el proyecto y ser el responsable, en último término, de la buena marcha de los trabajos.
- Ser el interlocutor principal con la Dirección Facultativa de METRO.
- Ejercer el mando y la responsabilidad sobre el equipo completo de trabajo.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Asegurar la ejecución de los diferentes entregables recogidos en este Pliego.
- Asegurar que todo el personal sigue los procedimientos existentes.
- Asegurar el cumplimiento del plan de calidad del proyecto.
- Gestionar permisos, problemas e incidencias, en las diferentes etapas del proyecto. Todo ello enmarcado en el presente Pliego.
- Asegurar el soporte técnico necesario para la realización de las diferentes tareas de este Pliego.
- Se requiere titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.
- Se requiere un mínimo de 5 años de experiencia

Arquitecto de ciberseguridad

Arquitectos senior especialistas funcionales y técnicos en la implantación de servicios de ciberseguridad, y por consiguiente en su diseño, despliegue de herramientas, procesos y tecnologías. Para ello deberá, al menos:

- Analizar las arquitecturas de ciberseguridad existentes en METRO.
- Conocer las alternativas técnicas existentes en su especialidad.
- Proponer las arquitecturas que considere más adecuadas para METRO.
- Proponer alternativas de plataforma centralizada de Gestión de Eventos e Información de Seguridad (SIEM), en el caso de que no existiese, teniendo en cuenta la integración de las fuentes de datos de eventos necesarias.
- Participar en la redacción de los documentos de análisis y diseño del COCF.

Se requiere titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.

Se requiere un mínimo de 5 años de experiencia

Ingenieros, auditores, analistas de seguridad de vulnerabilidades y procesos de ciberseguridad

Especialistas con experiencia en la realización de escaneos de vulnerabilidades y test de intrusión a sistemas, BBDD, sistemas operativos, entornos virtuales, redes, aplicaciones y definición de procedimientos de seguridad.

Realizarán, al menos:

- Las actividades de “Análisis de Contexto” y “Alcance” y, a partir de ahí y de forma conjunta con el personal de METRO, proponer las mejores herramientas, equipamiento, procedimientos y todos los aspectos necesarios para la generación de los diferentes documentos solicitados en el presente PPT.

Se requiere titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente, preferiblemente en Informática o Telecomunicaciones.

Se requiere un mínimo de 3 años de experiencia

Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones

Expertos en ordenamiento jurídico en materias de derecho de las tecnologías de la información y de las comunicaciones, seguridad de la información y protección de datos.

Al efecto, el oferente que presente la mejor oferta, deberá aportar el currículum vitae de las personas asignadas a la ejecución del contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).

Se requiere titulación Universitaria de Grado en Derecho, Licenciado en Derecho, o equivalente.

Se requiere un mínimo de 3 años de experiencia

10. DIRECCIÓN Y SUPERVISIÓN DE LOS TRABAJOS

En cuanto a la supervisión y dirección de los trabajos, la empresa adjudicataria designará un Responsable del Servicio quien mantendrá la necesaria y permanente coordinación con el Responsable designado por METRO, cuya función principal será la interlocución con el adjudicatario en lo que respecta a la ejecución del servicio y a la gestión y supervisión del mismo; así como, la recepción y aceptación final de los diferentes productos entregables, y la gestión de cualquier aspecto del contrato que requiera un análisis.

Así mismo, es importante que se establezca, de común acuerdo, un plan de trabajo, y de seguimiento y control del servicio con un plan de reuniones periódicas para asegurar la correcta ejecución. En este sentido, el seguimiento del servicio se estructurará en los siguientes niveles:

- Comité de Dirección

Estará integrado por las personas que METRO y la empresa adjudicataria establezcan. Será el máximo órgano de responsabilidad de supervisión del servicio vigilando por el correcto cumplimiento del contrato en los términos establecidos. Será el único competente en temas relativos a modificaciones de planificación, alcance y relativos a los componentes del equipo de trabajo.

- Comité de Seguimiento

Integrado los responsables del servicio designados tanto por la empresa adjudicataria como por METRO. Se encargarán del seguimiento técnico del servicio, así como de la coordinación de las tareas propias del servicio, y/o aquellos proyectos en que se requiera la participación del equipo de trabajo. En sí, se encargará de velar por la calidad de los trabajos realizados en el marco del servicio, así como de los diferentes entregables.

Igualmente, elevará al Comité de Dirección aquellas cuestiones y decisiones que no sean de su responsabilidad, así como las actas de las reuniones que mantengan con los temas tratados y las decisiones tomadas en cada caso.

11. PRESCRIPCIONES TÉCNICAS GENERALES

11.1 RECEPCIÓN

Una vez terminado el trabajo, METRO procederá a realizar una revisión de los documentos que incluirán las mediciones de parámetros y magnitudes de las instalaciones objeto del estudio.

Si la ejecución de los trabajos no cumpliera con todas las especificaciones, el Adjudicatario procederá, con toda urgencia, a efectuar las correcciones necesarias hasta que desaparezcan las diferencias señaladas. Una vez efectuado este trabajo, podrá procederse a la recepción de los trabajos.

11.2 CERTIFICACIÓN FINAL DE OBRA

Se procederá a la lectura del proyecto y contratos para contrastar la total ejecución de lo indicado en los citados documentos, y que en caso de no cumplirse se procederá a su resolución previo a la certificación final de obra. Como norma general, no se planteará la realización de la

certificación final de obra si no estuvieran implantadas y comprobadas todas las modificaciones surgidas.

Si el resultado es satisfactorio se realizará la certificación final de obra.

En casos absolutamente excepcionales, y para la situación en que no se superen los requisitos para la recepción, y siempre previa conformidad de la Dirección Facultativa, se podrá elevar la correspondiente acta, indicándose en la misma el plazo para la subsanación de defectos, entregas documentales, compromisos, etc., así como las consecuencias de su incumplimiento por parte de Adjudicatario.

11.3 PLAN DE CALIDAD

El Licitador aportará en la oferta un detallado Plan de Calidad donde deberá quedar reflejado, en las diversas fases del proyecto, la intervención, medios, criterios, documentos, etc. de los departamentos de calidad.

En este sentido y además de cumplimentar los datos propios de pruebas, ensayos, planillas, etc., el personal del Adjudicatario destinado en estas áreas, deberá tener la libertad adecuada para mantenerse crítico con su propia obra y la independencia suficiente como para rechazar los elementos que proceda, independientemente del estado de los trabajos, antes de ser ofrecida para la aceptación de la Dirección Facultativa y/o la Entidad Inspectora.

El Adjudicatario entregará a la Dirección Facultativa, a solicitud de éste, el manual de calidad, los procedimientos internos establecidos, con carácter general o para el contrato al que se refiere este concurso, para el adecuado seguimiento y cumplimiento de la misma, sobre todo en los aspectos de revisión de proyecto, control de modificaciones o acciones correctivas, control de rechazos, registros y revisión del sistema y aprobación de proveedores.

Asimismo, si fuera el caso, también hará entrega de todas las instrucciones de trabajo de las actividades importantes o de interés en el proceso de fabricación, montaje y aquellas otras que resulten importantes por su influencia en la explotación o mantenimiento. Para ello se establecerán programas y auditorías para constatar el cumplimiento y trazabilidad de los procesos de trabajo.

La presentación del Plan de Calidad en la oferta técnica no implica su aceptación por parte de la Dirección Facultativa, pudiendo ésta exigir modificaciones, ampliaciones e incluso la nueva redacción de dicho plan.

11.4 DOCUMENTACIÓN FINAL

La documentación final deberá ser entregada por el Adjudicatario a la Dirección Facultativa, dentro del mes siguiente a la Recepción, en las condiciones y forma que hayan establecido previamente.

Deberá disponer de la calidad suficiente para, a juicio de la Dirección Facultativa, asegurar la operación y mantenimiento de todos los elementos de las instalaciones objeto del presente PPT.

Se suministrará en soporte informático y en papel, en castellano y contendrá al menos: la memoria explicativa de lo realmente ejecutado, las modificaciones efectuadas con respecto al proyecto, planos, mediciones, presupuestos, esquemas, descripciones del funcionamiento de los equipos, especificación de los componentes, normas de uso y mantenimiento, etc.

Así mismo, se deberán entregar los manuales y procedimientos relacionados con cualquiera de las herramientas hardware o software empleadas incluyendo, si es el caso, los documentos acreditativos de licencias y la forma de obtención y renovación de las mismas.

11.4.1 Propiedad de la documentación

La documentación final podrá ser utilizada por METRO en la forma que estime conveniente, siempre y cuando sea únicamente en su provecho y no para terceros.

11.4.2 Soporte informático de la documentación

Se entregará en soporte informatizado de acuerdo a las siguientes normas y formatos:

- Los textos se entregarán en el formato del procesador de textos Word de Microsoft. A cada documento le corresponderá un único fichero. Asimismo, se entregará un único fichero del conjunto de documentos en formato PDF. Toda la documentación se generará con las plantillas corporativas de METRO que serán entregadas al adjudicatario en fase de ejecución del proyecto.
- Los planos se suministrarán en formato DWG y DXF.
- Para ciertos esquemas, en lugar de planos, se podrá utilizar Microsoft Visio 2016 o superior.
- La documentación será entregada a METRO en un soporte SSD externo con el fin de garantizar la robustez del soporte físico de la información.

12. GARANTÍA

No procede, la finalidad del presente pliego consiste en una serie de entregables documentales que deberán ser aprobados por METRO para su aprobación. Una vez realizados dichos trabajos no aplicaría tiempo de garantía sobre los mismos.

13. OBLIGATORIEDAD SUBSIDIARIA DEL ADJUDICATARIO ANTE LOS PERJUICIOS OCASIONADOS A TERCEROS

Con independencia de las posibles penalizaciones establecidas en el Pliego de Condiciones Particulares para la Contratación, si durante el desarrollo de los servicios y por causas imputables al adjudicatario se produjera un perjuicio a terceros, el adjudicatario se hará cargo de todos los costes y penalizaciones derivados del mismo sin repercusión alguna para METRO. Esto se aplica tanto a cualquier afección que una mala ejecución de los servicios descritos en el presente PPT pudiera ocasionar a otras instalaciones sean o no propiedad de METRO, como al perjuicio causado por el retraso en la ejecución de las mismas, que pueda suponer la pérdida parcial o total de los servicios prestados por dicha instalación a terceros. Todo ello siempre y cuando las causas sean imputables al adjudicatario.

14. PLANIFICACIÓN

Teniendo en cuenta todos los trabajos descritos en el presente PPT, METRO fija un plazo para la ejecución de los mismos, incluidas las pruebas de recepción, de **SEIS (6) MESES**.

El Plan incluido en este PPT debe tomarse a título orientativo y puede sufrir modificaciones, por la realización de los ajustes que sean precisos.

En las ofertas se indicará, no obstante, un plan detallado del servicio, no siendo superior a un carácter mensual ya que sino carecería de validez.

Este plan deberá adaptarse a las distintas fases que se definan con el fin de garantizar el cumplimiento de los plazos.

Se propone la siguiente planificación:

PLANIFICACIÓN DE LOS TRABAJOS

MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
-------	-------	-------	-------	-------	-------

Análisis de contexto (**)						
Definición de alcance (*)						
Definición de roles y responsabilidades (*)						
Diseño funcional y técnico (*)						
Definición detallada de actividades y Planificación (*)						
Formación (*)						

(*) En el final del periodo se deberá disponer del entregable totalmente terminado

(**) no conlleva entregable asociado

Tabla 4: Plan de Servicio

15. PRESUPUESTO

ENTREGABLE	CONTENIDO	COSTE ESTIMADO
1	Análisis de contexto	34.720,00 €
2	Definición de alcance	30.720,00 €
3	Definición de roles y responsabilidades	14.666,67 €
4	Diseño funcional y técnico	94.186,67 €
5	Definición detallada de actividades y Planificación	29.626,67 €
6	Formación	14.960,00 €

Tabla 5: Coste estimado por entregables

Costes directos:	186.598,46 €
Costes indirectos (5%)	3.731,97 €
TOTAL, PRESUPUESTO DE EJECUCIÓN MATERIAL:	190.330,43 €
Gastos Generales (9%)	17.129,74 €
Beneficio Industrial (6%)	11.419,83 €
BASE IMPONIBLE:	218.880,00 €
I.V.A. (21%):	45.964,80 €
PRESUPUESTO BASE DE LICITACIÓN:	264.844,80 €

Tabla 6: Importe económico

La base imponible del presente proyecto asciende a la cantidad de 218.880,00 € (DOSCIENTOS DIECIOCHO MIL OCHOCIENTOS OCHENTA EUROS).

Dicha cantidad se justifica en las tablas 7, 8 y 9.

Los costes horarios son algo superiores a los de una asistencia técnica para otros entornos debido al precio de mercado que tienen los analistas y especialistas en ciberseguridad.

La periodificación en el tiempo será la indicada en la tabla número 9.

ESTIMACIÓN DE PORCENTAJE DE DEDICACIÓN POR PERFIL EN FUNCIÓN DEL TRABAJO

	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Jefe de proyecto (JP)	100%	100%	100%	100%	100%	100%
Arquitecto de ciberseguridad (AC)	50%	25%	100%	100%	100%	25%
Ingenieros, auditores, analistas de seguridad de vulnerabilidades y procesos de ciberseguridad (IA)	200%	200%	200%	300%	300%	200%
Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones (AL)	50%	25%	10%	10%	10%	15%
DEDICACIÓN TOTAL	400%	350%	410%	510%	510%	340%
TOTAL PERSONAL EQUIVALENTE POR MES	4,00	3,50	4,10	5,10	5,10	3,40

Tabla 7: Estimación de porcentaje de dedicación por perfil en función de trabajo indicado en el Plan de Obra (Tabla 4)

	€/hora (**)	€/mesXpax (***)
Jefe de proyecto (JP)	61,00 €	9.760,00 €
Arquitecto de ciberseguridad (AC)	50,00 €	8.000,00 €
Ingenieros, auditores, analistas de seguridad de vulnerabilidades y procesos de ciberseguridad (IA)	53,00 €	8.480,00 €
Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones (AL)	50,00 €	8.000,00 €

(**) Incluye la parte proporcional de herramientas, aplicaciones y todos los materiales necesarios para la realización del proyecto. Incluye costes indirectos, gastos generales y beneficio industrial

(***) Se consideran meses de 4 semanas y jornada de 8 hora diarias.

Tabla 8: Estimación económica del coste de cada perfil

ESTIMACIÓN DEL COSTE TOTAL DE JORNADAS DEL SERVICIO POR LOS DIFERENTES PERFILES

	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Jefe de proyecto (JP)	9.760,00 €	9.760,00 €	9.760,00 €	9.760,00 €	9.760,00 €	9.760,00 €
Arquitecto de ciberseguridad (AC)	4.000,00 €	2.000,00 €	8.000,00 €	8.000,00 €	8.000,00 €	2.000,00 €
Ingenieros, auditores, analistas de seguridad de vulnerabilidades y procesos de ciberseguridad (IA)	16.960,00 €	16.960,00 €	16.960,00 €	25.440,00 €	25.440,00 €	16.960,00 €
Asesor legal especialista en derecho de las tecnologías de la información y de las comunicaciones (AL)	4.000,00 €	2.000,00 €	800,00 €	800,00 €	800,00 €	1.200,00 €
COSTE TOTAL POR PERIODO	34.720,00 €	30.720,00 €	35.520,00 €	44.000,00 €	44.000,00 €	29.920,00 €
COSTE ESTIMADO TOTAL DEL PROYECTO	218.880,00 €					

Tabla 9: Estimación económica del proyecto. El importe del mes 5 se reparte en un 20% para el curso y en un 80% para la realización el PPT

Los precios no incluyen IVA.

16. REVISIÓN DE PRECIOS

NO PROCEDE. Los precios se mantendrán fijos durante toda la vigencia del contrato.

Madrid, marzo de 2021	
DIRECTOR DEL PROYECTO:	AUTOR DEL PROYECTO:
 D. Fernando Morales Aguirre	 D. Fernando Galindo García
DIRECTOR TÉCNICO	
 D. Dionisio Izquierdo Bravo	