ATM Àrea de Barcelona
Autoritat del Transport Metropolità

Pliegos de prescripciones técnicas de licitación del contrato de servicios para la contratación por procedimiento abierto de:

“Gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IEC 24.014, e implementación de nuevas funcionalidades”

(EXP. C-42/2022)

Abril 2023

Índice

Página

1. PRESCRIPCIONES GENERALES 4
2. DESCRIPCIÓN DELS TRABAJOS 4
2.1. Antecedentes 4
2.2. Contexto 5
2.3. El Proyecto T-mobilitat 6
2.4. Justificación 8
2.5. Objeto del contracto o necesidades a cubrir 8
3. ACTIVIDADES Y FUNCIONES DE LA EMPRESA CONTRATISTA 11
3.1. Gestión de los SERVICIOS DE SEGURIDAD del SSu 11
3.1.1. Gestión integral en explotación de SERVICIOS DE SEGURIDAD criptográficos 11
3.1.2. Servicios de seguridad por dispositivo – Módulos SAMs CBT 12
3.1.3. Servicios de seguridad por dispositivo – Centre HSM 15
3.1.4. Servicios de seguridad por dispositivo – SUS 17
3.1.5. Nuevos SERVICIOS DE SEGURIDAD para implementar 19
3.1.5.1. Identificación y securización de los entornos de trabajo 19
3.1.5.2. Activación de SUS personalizados 20
3.1.5.3. Registro de Soporte anónimo 21
3.1.5.4. Gestión de versiones del ATIu 22
3.1.5.5. Securización de datos personales en la personalización de SUS 22
3.2. Gestión en explotación de COMPONENTES físicos del SSu 23
3.2.1. Gestión en explotación de los MÓDULOS DE ACCESO SEGURO, SAMs 23
3.2.2. Gestión en explotación de los CENTROS HSMs 26
3.2.3. Gestión en explotación de los DISPOSITIVO MÓVILES NFC 29
3.2.4. Servicios de Mantenimiento integral del SSu 31
3.3. Infraestructura de Gestión de CLAVES Y HERRAMIENTAS asociadas al SSu 35
3.4. Gestión y liderazgo del PROGRAMA de C&A del SSu 37
3.4.1. Programa de C&A a Serveis de Seguretat 38
3.4.2. Programa de C&A a los componentes SAMs CBT 40
3.4.3. Programa de C&A a los componentes CHSM 41
3.4.4. Programa de C&A de seguridad a los dispositivos móviles NFC 43
3.4.5. Programa de C&A Infraestructura de gestión de claves 43
3.5. Gestión y liderazgo de ESPECIFICACIONES TÉCNICAS del SSu 44
3.5.1. Sistema de Seguridad único – visión general 44

3.5.2. Servicios de Seguridad de las transacciones sin contacto T-mobilitat 45
3.5.3. Componentes de seguridad local - SAM CBT 46
3.5.4. Componentes de seguridad centralizada – Centros HSM 47
3.5.5. Componentes de seguridad por dispositivos móviles NFC 49
3.5.6. Infraestructura de gestión de claves criptográficas 50
3.5.7. Herramientas de gestión del Sistema de Seguridad único 50
3.6. TRATAMIENTO DE RIESGOS del SSu y nuevos desarrollos 51
3.7. Gestión y LIDERAZGO INTEGRAL del SSu, rol ISO/IEC 24.014 dentro del MTC 52
3.8. Módulo de GESTIÓN DE FRAUDE 53
3.9. Exportación de DATOS DEL SIC 54
4. FINALIDADES Y OBJETIVOS A ASUMIR 55
4.1. Principios básicos para cumplir 55
5. SEGUIMIENTO Y CONTROL DE LAS CONDICIONES DEL CONTRATO 56
5.1. Descripción de la forma de prestación del servicio 56
5.1.1. Planificación del Proyecto 56
5.1.1.1. Fase de Planeamiento 56
5.1.1.2. Fase de Análisis y Ingeniería 56
5.1.1.3. Fase de desarrollo 57
5.1.1.4. Fase de despliegue 57
5.1.1.5. Fase de explotación 57
5.2. Medios Técnicos y Materiales 57
5.2.1. Infraestructura necesaria para llevar a término el proyecto 57
5.3. Recursos humanos 58
5.4. Metodología para aplicar 60
5.5. Organización de la ejecución del proyecto 62
5.5.1. Control y seguimiento y seguimiento del proyecto 62
5.5.2. Plazos de ejecución 63
5.5.2.1. Calendario 63
5.5.2.2. Hitos estratégicos 65
5.6. Condiciones generales de ejecución 65
5.6.1. Confidencialidad y publicidad del servicio 65
5.6.2. Propiedad intelectual 66
5.6.3. Tratamiento de datos de carácter personal 66
5.6.4. Criterios de accesibilidad universal 66
5.6.5. Criterios de sostenibilidad y protección al medio ambiente 66
5.7. Propuesta técnica 67

1. PRESCRIPCIONES GENERALES

Este pliego de prescripciones técnicas establece las condiciones de carácter técnico que deben regir el proceso de contratación para *"Gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IEC 24.014, e implementación de nuevas funcionalidades"* para la protección de todas y cada una de las Transacciones sin contacto T-mobilitat.

En el presente documento se describen los trabajos a realizar y su desarrollo, se relacionan las materias que deben ser objeto de desarrollo, se definen las condiciones y criterios que deben servir de base y se concretan los trabajos que deberá realizar el adjudicatario para que, una vez garantizada su calidad, puedan ser aceptados por la Autoritat del Transport Metropolità de Barcelona

Con la mera presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

2. DESCRIPCIÓN DELS TRABAJOS

2.1. Antecedentes

La Autoridad del Transporte Metropolitano del área de Barcelona (en adelante ATM) es un consorcio interadministrativo de carácter voluntario, creado en 1997, al que pueden adherirse todas las administraciones titulares de servicios públicos de transporte colectivo, que pertenezcan al ámbito formado por las comarcas de la Alt Penedès, la Anoia, el Bages, el Baix Llobregat, el Barcelonès, el Berguedà, el Garraf, el Maresme, el Moianès, Osona, el Vallès Occidental y el Vallès Oriental.

Actualmente, las administraciones consorciadas son la Generalidad de Cataluña (51%) y administraciones locales (49%), compuestas por el Ayuntamiento de Barcelona, el Área Metropolitana de Barcelona (AMB) y la Agrupación de Municipios titulares de servicios de Transporte urbano de la región metropolitana de Barcelona (AMTU). Además, la Administración General del Estado está presente en los órganos de gobierno de la ATM en calidad de observador.

De acuerdo con los estatutos del consorcio, la ATM de Barcelona tiene como finalidad articular la cooperación entre las administraciones públicas titulares de los servicios y de las infraestructuras del transporte público colectivo del área de Barcelona que forman parte del consorcio, así como la colaboración con aquellas que, como la Administración General del Estado, están comprometidas financieramente o son titulares de servicios propios.

Las principales funciones de la ATM de Barcelona consisten en la planificación de las infraestructuras y servicios de transporte público colectivo, la coordinación y el seguimiento de las relaciones con los operadores de transporte colectivo, la elaboración de propuestas y la concertación acuerdos de financiación con las administraciones, la ordenación de tarifas y la tramitación de planes de movilidad.

En el ejercicio de sus funciones, la ATM inició en 2001 la implantación del sistema tarifario

integrado, resultando ser una herramienta eficiente para la mejora de las prestaciones del sistema de transporte público. El sistema tarifario integrado permite la utilización de diferentes modos de transporte (metro o, autobuses urbanos, metropolitanos e interurbanos, tranvía, Ferrocarriles de la Generalidad de Cataluña y Renfe Cercanías) necesarios para realizar un desplazamiento con un único título de transporte, despenalizando económicamente los transbordos. Actualmente el sistema tarifario abarca 356 municipios y una población de 5,7 millones de habitantes.

Parte del contenido de estas prescripciones técnicas deriva del proyecto *"Servicios de ingeniería para el diseño, desarrollo, puesta en servicio y mantenimiento de la Plataforma de gestión integral del Sistema de Seguridad Criptográfico"* C-33/2020.

2.2. Contexto

Una de las principales actividades de gestión identificadas en el **Modelo organizativo de referencia basado en roles ISO/IEC 24014** asociado a la Autoridad de Confianza es la *Gestión del Sistema de Seguridad Criptográfica* que garantice su control, evolución así como su mantenimiento integral en todos sus niveles del llamado **Sistema de Seguridad único**.

Todas las tecnologías están expuestas a **problemas de seguridad**, aunque sólo sea por el aumento exponencial de capacidad de proceso que año tras año proporciona la industria de la tecnológica que en nuestro caso, es particularmente peligroso, porque la base del Sistema Tarifario Integrado T-mobilitat es la estandarización y el uso de procedimientos normalizados, es decir, **conocidos y públicos**.

Con relación a la seguridad, en el caso del Sistema Tarifario sin contacto integrado y compartido con múltiples actores asociados al proyecto T-mobilitat, es particularmente peligroso porque la base de un *Sistema interoperable Global* es **la estandarización y el uso de procedimientos definido** es, es decir, conocidos y publicados.

Así, implantar un Sistema de Billete Electrónico sin contacto abierto e interoperable basado en Normas Internacionales conocidas tiene grandes ventajas, pero sólo si va acompañado de un verdadero Sistema de Intercambio de Información Integral compartido, transparente e interoperable, pero que sobre todo y ante todo, disponga de un **adecuado SISTEMA DE SEGURIDAD CRIPTOGRÁFICA**.

Es, precisamente, el Sistema de Seguridad criptográfica, la pieza angular que debe generar la confianza de todos los actores en el Sistema. Es el **complemento oculto** en las diferentes operativas (casos de uso) de cualquier Aplicación del Sistema, también de *la Aplicación de Transporte Interoperable única* (**ATIu**), implementando mecanismos, servicios y funciones de seguridad.

El Sistema de Seguridad criptográfica es un instrumento que ayuda a visualizar y entender el grado de confianza que se ofrece respecto a los diferentes intercambios de datos o transacciones, garantizando **la autenticidad, confidencialidad, integridad, no repudio**, etc., pero también, desde el conocimiento de las amenazas y vulnerabilidades del sistema.

En este contexto el Sistema de Seguridad criptográfico tiene una **FUNCIONALIDAD TRANSVERSAL** que afecta a todas y cada una de las áreas del Sistema de Billete Electrónico sin contacto.

La ATM, como **Gestor del Sistema de Seguridad criptográfica**, es la responsable de definir, desarrollar, publicar, mantener y evolucionar el **Sistema de Seguridad Único** Integrado.

Es en esta última área de competencia donde se ubica el **alcance de los trabajos técnicos** con relación a la "*gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IEC 24.014, e implementación de nuevas funcionalidades*", como elemento de protección oculto de todas las transacciones sin contacto del Sistema Tarifario Integrado.

La misión del Sistema de Seguridad único (SSu) es **garantizar la seguridad de las Transacciones** sin contacto del Sistema Tarifario Integrado T-mobilitat a través de establecer y evolucionar los **Servicios de Seguridad que lo sustenta**, así como de los elementos seguros en los que se almacenan estos Servicios de seguridad.

El Sistema de Seguridad único utiliza tanto **criptografía simétrica** (en servicios donde se necesita tiempo de respuestas casi real) como **criptografía asimétrica** (para la seguridad en el intercambio de información).

El principal objetivo del Sistema de Seguridad único T-mobilitat es **articular un marco de trabajo común, confidencial, compartido** con los operadores y liderado por la ATM para conseguir la permanente protección del Sistema Tarifario Integrado basado en tecnología sin contacto de proximidad.

Es en este contexto, y bajo la responsabilidad que tiene la ATM como **Gestor del Sistema de Seguridad único T-mobilitat**, en el que se enmarca la presente licitación.

2.3. El Proyecto T-mobilitat

El Proyecto T-mobilitat es un proyecto de la ATM de Barcelona que surgió de la necesidad de establecer un nuevo sistema de Ticketing electrónico sin contacto dada la manifiesta obsolescencia tecnológica de banda magnética.

Con fecha 1 de octubre de 2014 se resolvió adjudicar el procedimiento de licitación del Proyecto T-mobilitat para la implantación de un nuevo sistema tecnológico, tarifario y de gestión basado en tecnología sin contacto de proximidad ISO/IEC 14.443, así como en el modelo de roles ISO/IEC 24014 para garantizar la interoperabilidad técnica y funcional de los elementos de uso común.

El Proyecto T-mobilitat tiene como objetivo principal establecer un nuevo **MODELO TECNOLÓGICO** que puesto a disposición del **MODELO TARIFARIO** permita una mejor y más eficiente **GESTIÓN** del Sistema Tarifario Integrado que garanticen los objetivos globales para una mejor y más eficaz utilización del Transporte Púbico. Se trata de dar respuestas a una creciente necesidad de Movilidad, en la que el Transporte público desempeña un papel tractor básico.

Imagen 1: Alcance del Proyecto T-mobilitat

Bajo el desarrollo del **Modelo Tecnológico T-mobilitat** se establece un **marco de trabajo común, unificado, compartido y colaborativo** que integra todos los servicios de transporte y de movilidad basado en el *Modelo de roles ISO/IEC 24.014* que proporciona la base para al desarrollo de un **Sistema de gestión tarifaria interoperable, multi-operador, multi-proveedor y multi-servicios**.

El **MODELO TECNOLÓGICO T-mobilitat** describe las características estratégicas funcionales, organizativas y tecnológicas dividido en dos grandes áreas**; el MARCO TECNOLOGICO COMÚN**, que contiene las especificaciones y requerimientos comunes a todos los operadores, y **el MARCO TECNOLÓGICO ESPECÍFICO**, que contiene las especificaciones y requerimientos propios de cada uno de los operadores o grupo de operadores y de los que son responsables los propios operadores.

La misión del **Marco Tecnológico Común** es garantizar los principios estratégicos que la T-mobilitat ha aplicado a los elementos de uso transversal:

- la **Interoperabilidad tecnológica**, entendida con la capacidad del "HW" y del "SW" que corre a los diferentes equipos de diferentes proveedores para intercambiar y utilizar la información,
- la **Estandarización** como base para facilitar la implementación de la interoperabilidad tecnológica, y especificando lo que no esté cubierto por las normas actuales, garantizando la no existencia de "*Cajas negras*".
- la **Neutralidad tecnológica** que asegure la adaptabilidad de los elementos de uso transversal al progreso de la tecnología, alentando la innovación, el know-how y la propiedad intelectual,
- la **Independencia tecnológica** respecto a cualquier proveedor tecnológico en el Sistema T-mobilitat, y
- la **Escalabilidad** con una organización modular portable como garantía de ampliación geográfica y de evolución en el tiempo.
- El **Sistema de Seguridad único** es la pieza angular del Sistema Tarifario Integrado para garantizar una adecuada protección de todas y cada una de las transacciones sin contacto realizadas.

Podemos decir que es el complemento oculto en las diferentes operativas (validación, recarga, inspección...) de la *aplicación de Transporte Interoperable única* (ATIu) que implementa mecanismos, servicios y funciones de seguridad basado en la utilización de criptografía fuerte.

Es dentro del Proyecto T-mobilitat donde se circunscribe el contenido y alcance de la presente prestación con relación a los Servicios Tecnológicos necesarios para garantizar una *Gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IEC 24.014 e implementación de nuevas funcionalidades*", para la protección de todas y cada una de las Transacciones sin contacto T-mobilitat.

Se describen en los párrafos siguientes, los trabajos a realizar y su desarrollo, se relacionan las materias que deben ser objeto de la prestación, se definen las condiciones y criterios que deben servir de base para realizar la propuesta técnica y se concretan los trabajos que deberá realizar el adjudicatario para que, una vez garantizada su calidad de los trabajos realizados, puedan ser aceptados por la Autoritat del Transport Metropolità de Barcelona.

2.4. Justificación

El proyecto T-mobilitat es un proyecto de la ATM de Barcelona que surgió de la necesidad de establecer un nuevo Sistema de Ticketing electrónico sin contacto dada la manifiesta obsolescencia tecnológica de la banda magnética. En este sentido, y dado este novedoso sistema de Ticketing o sistema tecnológico, se promovió la implantación de un nuevo sistema tarifario y de gestión.

El Gobierno de la Generalidad de Cataluña, mediante acuerdo de 8 de octubre de 2013, dio luz verde al proyecto T-mobilitat como mecanismo fundamental de la gestión de la movilidad en un único soporte inteligente, estableciendo un sistema de información pensando en el ciudadano, con la creación de dos nuevos centros de trabajo: el Centro de Atención al Cliente y el Centro de Gestión de la información del Transporte, que de forma global, deberían informar en tiempo real del funcionamiento de la oferta de transporte público integrado en todo el territorio catalán.

La complejidad técnica, jurídica y financiera intrínseca derivada de la implementación del nuevo sistema tecnológico, tarifario y de gestión (proyecto T-mobilitat) justificó inicialmente la necesidad de disponer de un mecanismo flexible, especialmente en lo que se refiere a la asignación de riesgos, considerando por tanto como modalidad contractual óptima para licitar el proyecto T-mobilitat el contrato de colaboración entre el sector público y el sector privado.

La licitación del contrato de colaboración entre el sector público y el sector privado del "Proyecto T-mobilitat para la implantación de un nuevo sistema tecnológico, tarifario y de gestión" (expediente de contratación C-24/2012), es inició en fecha 16 de octubre de 2013, cuando se publicó el anuncio de la licitación en el Diario Oficial de la Unión Europea (DOUE) y en el Boletín Oficial del Estado (BOE), y en fecha 17 de octubre de 2013, en el Diario Oficial de la Generalidad de Cataluña.

En fecha 1 de octubre de 2014, se resolvió adjudicar el procedimiento de licitación del proyecto T-mobilitat para la implantación de un nuevo sistema tecnológico, tarifario y de gestión.

En fecha 24 de octubre de 2014 se formalizó el contrato del proyecto T-mobilitat entre la ATM y la SOCIEDAD CATALANA PARA LA MOVILIDAD, SA.

En relación con el objeto de esta contratación, el Documento descriptivo del proyecto T-mobilitat de fecha 14 de octubre de 2013, preveía expresamente en su cláusula 7.2 (alcance del objeto de los pliegos), un sistema de gestión que pudiera dar cobertura a nuevos sistemas de post-pago.

Con relación a la cláusula 19.2.l del contrato CPP de 14 de octubre de 2014 obliga a la ATM de Barcelona a gestionar y proporcionar al *Sistema de Billete sin contacto T-mobilitat*, los Servicios Tecnológicos necesarios derivados de uso del Sistema de Seguridad único en a través de la utilización de elementos seguros (SAM para la seguridad local y HSM para la seguridad centralizada) a fin de garantizar la seguridad de todas y cada una de las transacciones sin contacto T-mobilitat.

2.5. Objeto del contracto o necesidades a cubrir

El objetivo principal de este contrato es el desarrollo y puesta en servicio de nuevos Servicios de Seguridad criptográfica a implementar en la T-mobilitat, así como disponer de servicios de ingeniería y asistencia técnica para la *"Gestión Integral del Sistema de*

Seguridad único T-mobilitat en Explotación, rol ISO/IEC 24.'14, e implementación de nuevas funcionalidades" , que va desde el diseño de los nuevos procesos, hasta la puesta en servicio, el mantenimiento y la evolución de la *Plataforma de Seguridad criptográfica* .

La gestión integral del SSu no se entiende si no es de una manera holística, donde el **sistema de seguridad, sus componentes y las herramientas asociadas se analizan como un todo**, de forma global e integrada, ya que sólo desde el punto de vista operativo su funcionamiento sólo puede comprenderse de esta forma y no como la simple suma de las partes.

Este pliego de prescripciones técnicas tiene por objeto determinar el contenido y alcance de los trabajos que deberá desarrollar la empresa adjudicataria de la presente licitación.

Se describen los trabajos a realizar y su desarrollo, la interrelación de los trabajos a llevar a cabo, así como las condiciones y los criterios por los que, una vez garantizada la calidad de los trabajos realizados, puedan ser aceptados por la ATM de Barcelona.

El alcance del proceso de contratación de los servicios de ingeniería y asistencia técnica necesarios para disponer de una *"Gestión Integral del Sistema de Seguridad único T-mobilitat en Explotación e implementación de nuevas funcionalidades"* que contempla lo siguiente.

El alcance de los trabajos a desarrollar dentro de esta licitación **se circunscribe únicamente al ámbito del Sistema de Seguridad único,** que incluye la infraestructura de gestión de claves criptográficas, elementos seguros de uso local (SAM), elementos de uso centralizado (Centros HSM), capa de abstracción de la seguridad, gestión de la seguridad en dispositivos móviles NFC, entre otros.

El alcance de la presente Licitación tiene por objeto **desarrollar y puesta en servicio** de los nuevos servicios de seguridad identificados, así como el **mantenimiento integral**, **gestión de incidencias** y **problemas y pequeñas evoluciones** con el sistema en explotación a lo largo de todo el contrato.

Está dentro del alcance de la presente licitación se encuentran todos los servicios de ingeniería y asistencia técnica necesarios para llevar a cabo una *"Gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IE 24014, e implementación de nuevas funcionalidades".*

Así, el alcance de la presente licitación es:

1. **Gestión de los Servicios de Seguridad del SSu**

   Servicios de ingeniería para la gestión integral y mantenimiento en explotación de todos y cada uno de los **Servicios de Seguridad criptográficos** para la protección a las transacciones sin contacto implementados y distribuidos desde los Sistemas Informáticos Centrales (SICs) a los diferentes elementos seguros (SAMs y CHSM) contenidos en los terminales sin contacto de operador y en los SICs T-mobilitat en el área integrada de Barcelona. Lo que conocen como Sistema de Seguridad único T-mobilitat – rol ISO/IEC 24.014.

2. **Gestión en explotación de los componentes físicos del SSu**

   Gestión y mantenimiento integral en explotación de todos y cada uno de los **componentes del Sistema de Seguridad único** (SSu) implementados y distribuidos a lo largo de toda la infraestructura tecnológica T-mobilitat desplegada en el área integrada de Barcelona.

Así como los servicios de ingeniería para la gestión integral del sistema de **identificación y resolución de incidencias y problemas en explotación** con relación al Sistema de Seguridad único que puede afectar a los Servicios de seguridad, a los componentes del SSu y/o las herramientas tecnológicas asociadas a la T-mobilitat en el área integrada de Barcelona.

Gestión de desarrollos, implementación, integración y puesta en servicios de las pequeñas **evoluciones derivadas de la resolución de incidencias y problemas** que seguro aparecerán en la explotación de la T-mobilitat en el área integrada de Barcelona.

3. **Infraestructura de Gestión de claves y herramientas asociadas al SSu**

   Gestión y mantenimiento integral de la infraestructura de gestión de claves criptográficas y de las **herramientas tecnológicas** (plataformas tecnológicas implementadas) asociadas al Sistema de Seguridad único T-mobilitat necesarias para operar a nivel de protección de las transacciones sin contacto en el área integrada de Barcelona.

4. **Gestión del Programa de C&A del SSu**

   Gestión y mantenimiento integral del **Sistema de Conformidad y Aceptación** del Sistema de Seguridad único para garantizar en todo momento el cumplimiento de los requerimientos técnicos exigidos a los Servicios de Seguridad criptográfica, a los componentes seguros del SSu, así como a las herramientas necesarias asociadas, a la T- movilidad en explotación en el área integrada de Barcelona.

5. **Gestión de las Especificaciones técnicas del SSu**

   Gestión y mantenimiento integral de los **requerimientos técnicos** de obligado cumplimiento y de las **especificaciones técnicas** asociadas del Sistema de Seguridad único que incluye los Servicios de Seguridad criptográficos implementados, los componentes seguros y herramientas asociadas en su caso, así como **manuales de uso** en aquellos casos que se considere necesario.

6. **Tratamiento de riesgos de los SSu**

   Gestión del tratamiento de riesgos del Sistema de Seguridad único que incluye la asistencia técnica a la identificación, **análisis y viabilidad de nuevos servicios de seguridad** necesarios a implementar, nuevas evoluciones del Sistema de Seguridad único en explotación, así como de las herramientas asociadas a la plataforma de seguridad, con el objetivo de mantener el riesgo de seguridad residual en límites aceptables.

   Gestión, desarrollo, integración, pruebas de cumplimiento y aceptación y puesta en servicio de los **nuevos servicios de seguridad** identificados como necesarios a implementar en el sistema de seguridad único en T-mobilitat en el área integrada de Barcelona, siempre bajo los principios y directrices del Marco Tecnológico Común.

7. **Gestión integral, y liderazgo, del SSu como rol ISO/IEC 24.014 dentro del ATC**

   Gestión y liderazgo de las **reuniones técnicas** con el equipo técnico responsable del Marco Tecnológico Común y otros actores de temas relacionados con el Sistema de Seguridad criptográfico T-mobilitat.

Está fuera del alcance del objeto de este contrato cualquier nuevo equipamiento necesario a futuro, no incluido en la lista de mantenimiento de la plataforma de seguridad del sistema de seguridad único T-mobilitat, derivados de nuevos desarrollos.

3. ACTIVIDADES Y FUNCIONES DE LA EMPRESA CONTRATISTA

La oferta que presente la empresa licitadora debe abarcar la totalidad de las actividades y funciones especificadas en este pliego y en el pliego de cláusulas administrativas particulares, puesto que son todas obligatorias para la admisión de las propuestas.

Se describen en este apartado las principales actividades y funciones que la empresa contratista debe asumir.

3.1. Gestión de los SERVICIOS DE SEGURIDAD del SSu

3.1.1. Gestión integral en explotación de SERVICIOS DE SEGURIDAD criptográficos

Los equipos y elementos seguros que componen Sistema de Seguridad único implementan e integran un conjunto de **SERVICIOS DE SEGURIDAD que se consumen** en el Sistema Tarifario Integrado T-mobilitat.

Dentro del alcance de este contrato, el adjudicatario deberá gestionar de **forma integral todos los Servicios de Seguridad** ya implementados, así como los nuevos una vez implementados, que el SSu pone a disposición del resto de actores que operan en T-mobilitat.

Será responsabilidad del adjudicatario garantizar en todo momento la disponibilidad de todos y cada uno de los Servicios de Seguridad que el SSu pone a disposición del Sistema Tarifario Integrado del área integrada de Barcelona, de acuerdo a los niveles de calidad acordados.

El adjudicatario deberá proponer el Plan de gestión integral de los Servicios de Seguridad T-mobilitat en explotación, que aprobado por el Modelo Técnico Común (ATM), garantice la disponibilidad de todos y cada uno de los Servicios de Seguridad del SSu en la T-movilidad en explotación en el área integrada de Barcelona.

Así, los **Servicios de Seguridad** se cargan en elementos seguros físicos que están distribuidos por todo el Sistema T-mobilitat, como son:

- Los **Módulos de Acceso Seguro** – SAM

  Es un elemento seguro en formato SIM con un chip microprocesador con características criptográficas sobre la que pueden implementarse Servicios de Seguridad, así como almacenar las claves criptográficas.

- Los **Centros sáb Módulos de Hardware Seguro** – CHSM

  El Servidor Seguro es un servidor criptográfico que ofrece servicios de seguridad de todo tipo que incorpora un elemento seguro hardware con fuertes medidas de seguridad llamado SHM.

- Los **Soportes de Usuario Sin Contacto** – SUS

  Los SUS son elementos seguros que están más expuestos a ataques, ya que están en posesión del usuario y por tanto fuera del control del sistema.

El Sistema de Seguridad único SSu es un ecosistema vivo que no es un producto sino que es un **proceso de mejora continua** en relación con la idoneidad, eficacia y adecuación permanente a las necesidades ya un entorno en continuo cambio.

Así, en relación con los Servicios de Seguridad del SSu y desde un punto de vista general, deben realizarse las siguientes tareas:

A. El adjudicatario, en fase de análisis e ingeniería, deberá proponer el **Plan de gestión integral de los Servicios de Seguridad T-mobilitat en explotación**, que aprobado por el Modelo Técnico Común (ATM), garantice la disponibilidad de todos y cada uno de los Servicios de Seguridad del SSu en la T-mobilitat en explotación en el área integrada de Barcelona.

B. El adjudicatario, en fase de análisis e ingeniería deberá identificar y especificar un **Plan de mejora continua** basado en el análisis interno (y acciones asociadas) y externo (entorno cambiante), la planificación sistemática en mejora continua y el compromiso de mantener unos niveles de riesgos asumibles que aseguren en todo momento la idoneidad, eficacia y adecuación del Sistema de Seguridad único, sus componentes, la infraestructura tecnológica y las herramientas asociadas.

3.1.2. Servicios de seguridad por dispositivo – Módulos SAMs CBT

Los módulos de uso local SAM (Secure Access Module) son elementos seguros de nivel 1 que dan servicios de seguridad locales a los TIUs que están preparados para trabajar “off-line” y son muy robustos frente a quiebras de hardware, por lo que la disponibilidad es muy alta y no es necesario redundarlos.

El Sistema Tarifario Integrado sin contacto T-mobilitat utiliza módulos SAM para ofrecer en tiempo real los siguientes servicios de seguridad:

- **Almacenes seguros de información,** que permite almacenar información y disponen de mecanismos de seguridad para el acceso seguro a su contenido.
- **Almacenes seguros de claves,** que permite almacenar claves del sistema de forma controlada, cifrada y auditada.
- **Control de acceso seguro**, son los mecanismos que incorporan los equipos para controlar el acceso a los recursos que protegen: uso de PIN para la ayuda a la gestión, Autenticación para permitir el acceso a actores autorizados, Canal seguro para l intercambio seguro de información.
- **Gestión de juegos de claves de tarjeta**, según su uso para realizar desarrollos en el entorno de ingeniería, para la integración en el entorno de preproducción y reales en el entorno de producción en explotación.
- **Mecanismos de diversificación de claves**, de cálculo unidireccional para mitigar a los ricos de almacenar claves maestras en elementos distribuidos por el sistema.
- **Obtener claves diversificadas**, con mecanismos de acceso suficientes para permitir obtenerlas sólo a los actores autorizados.
- **Mecanismo de autenticación**, que permite a un sistema corroborar que un actor dice que es quién es.

- **Mecanismos de autenticación mutua**, permite a dos actores autenticar (confirmar la identidad) entre ambos mediante un medio de comunicación no seguro.

- **Obtener clave de sesión,** que se genera durante el proceso de autenticación, generada de forma aleatoria en cada autenticación, que permite que el acceso al *Soporte de Usuario Sin contacto* (SUS) T-mobilitat mediante órdenes protegidas mediante criptografía fuerte.

- **Contadores de SAM**, que se incrementan de forma automática en algunas acciones generadas al operar el sistema tarifario integrado.

- **Cuotas de SAM,** que limita la cantidad de operativas de recarga, venta, etc. que se pueden realizar con un SAM sin conectarse a un Centro HSM.

- **Canal seguro,** que permite crear un canal de comunicación entre dos actores, de forma segura, a través de un medio inseguro.

- **Mecanismos de firma,** que permite que unos actores puedan generar la firma de cierta información conocida y que otros puedan comprobar la firma de esta información para comprobar su autenticidad.

- **Autenticación de SUS,** los SAMs realizan una autenticación mutua antes de permitir al TIU correspondiente tener acceso al contenido del SUS presentado en su área activa de radiofrecuencia.

También disponen de un par de claves asimétricas que le permiten realizar autenticaciones PKI con otros dispositivos, como Centros HSMs.

- **Confidencialidad,** los módulos SAM tienen la capacidad de cifrar y descifrar los datos que envían cuando debe garantizarse la confidencialidad de los datos transmitidos porque contienen información sensible que sólo debe ser accesible para el destinatario de los datos tanto con criptografía simétrica como con criptografía asimétrica.

- **Integridad,** de los datos se garantiza mediante su firma de forma que:

    - Cuando SAM **recibe un paquete de datos firmados**, verifica la firma, rechazando los datos con firmas no válidas.

    - Cuando el SAM **envía paquetes de datos**, la firma de forma que se pueda verificar su integridad.

T-mobilitat firma todas y cada una de las transacciones sin contacto llevadas a cabo.

La firma con claves asimétricas llama también **certificado** y los SAMs preparados para generar certificados PKI.

Disponibilidad, los SAMs son dispositivos que se utilizan en los terminales TIU que tienen garantizada la alta disponibilidad debido a que el canal de comunicación con el SAM está integrado en el mismo TIU y que el riesgo de quiebra del hardware del SAM es muy bajo.

Sin embargo, si el SAM dispone de claves limitadas por cuota, cuando ésta se agota, el SAM deja de dar el servicio con esta clave. Para garantizar la disponibilidad de las claves limitadas por cuota, el TIU debe ir periódicamente actualizando la cuota del SAM mediante el Centro HSM de operador.

- **No repudio,** los SAMs aseguran el no repudio mediante la firma de datos con claves que son únicas en cada SAM que pueden ser simétricas o asimétricas.
- **Anticlonado de los SAMs,** mediante los mecanismos exigidos a todo chip autorizado a la T-mobilitat para protegerse ante la clonación de los datos que almacenan, exigiendo demostrar altos niveles de protección certificados por entidades acreditadas con Common Criteria.

También la diversificación de claves de cada SAM nos protege frente al clonado de los mensajes transmitidos, ya que el clonado de un mensaje de un SAM cifrado o firmado con una clave diversificada no sirve para suplantar el mensaje de otro SAM diferente.

- **Auditabilidad,** implementado mecanismos de identificación única y registro de todos los SAMs utilizado en la T-mobilitat, que se utiliza entre otras cosas, para auditar todas y cada una de las transacciones efectuadas con cada SUS. Estas transacciones se almacenan los sistemas centrales y permite realizar auditorías en el momento que se quiera.
- **Cálculo del número de factura,** para garantizar la unicidad del número de factura a lo largo del tiempo, incluso con cambios de ubicación del terminal ccTIU.
- **Abstracción de la seguridad del tipo de SUS, (SCAL),** que es un servicio de seguridad que implementa los SAMs CBT que permite que el uso de la seguridad del SSu sea independiente del SUS (tarjeta), se realicen menos autenticaciones rebajando los tiempos de transacción, aumenta la seguridad ya que permite controlar el acceso a campo con granularidad de campo y se puede configurar desde los Sistemas Informático Centrales en tiempo casi real.

Así, en relación con los **Servicios de Seguridad**, estos últimos ya implementados y los nuevos a anteriores, que da los **componentes de seguridad local SAM CBT**, deben realizarse las siguientes tareas:

A. Gestionar todos y cada uno de los Servicios de Seguridad que proporcionan los SAMs y asegurar la permanente disponibilidad en explotación con acuerdo a los SLA establecidos.

En fase de análisis e ingeniería el adjudicatario deberá identificar a todos y cada uno de los servicios de seguridad local, así como describir los casos de uso de las actividades relacionadas con el uso de servicios de seguridad locales.

Se requiere especial atención al servicio de seguridad de la capa de abstracción de la Seguridad, ya que es un servicio estratégico que requiere garantizar su disponibilidad de manera permanente. También, en relación con las herramientas de pruebas y plataformas de gestión.

B. Definir, desarrollar y acordar los SLA (Acuerdo de Nivel de Servicio) de cada uno de los Servicios de Seguridad local dados por los SAMs CBT, necesarios para la protección de las transacciones sin contacto.

En fase de análisis e ingeniería, se trata de acordar el nivel de servicio que esperamos de cada uno de los servicios de seguridad local que establece el nivel de calidad.

C. **Definir, desarrollar e implementar los KPIs (Indicadores Clave de Rendimiento) de los Servicios de Seguridad local** dados por los SAMs CBT, necesarios para la protección de las transacciones sin contacto.

   En fase de análisis e ingeniería, se trata de identificar KPI que nos ayuden a promover la mejora continua y la eficacia de los servicios de seguridad local en SAMs CBT.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica con relación a los Servicios de Seguridad Locales, los SLAs y los KPIs, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.3. Servicios de seguridad por dispositivo – Centre HSM

Además de los servicios de seguridad locales que ofrecen los SAMs, existen servicios de seguridad centralizados que utilizan equipos y actores de forma remota dentro de un entorno controlado como es el SIC que son los Centros HSM y que completan todo el ecosistema del Sistema de Seguridad único.

Los Centros HSM son servidores seguros que disponen de dos partes bien diferenciadas:

- **HSM** *(Hardware Security Module)*, una parte segura, formada por un conjunto de elementos seguros tamperizados, donde la lógica que ejecuta y los recursos que protege disponen de mecanismos físicos de protección contra intrusiones.
- **Servidor convencional,** formada por un hardware no seguro, donde la lógica que se ejecuta no es segura que está formada por elementos de red, ordenadores y sistemas de almacenamiento convencionales. El HSM se encuentra instalado en su interior, comunicándose mediante un bus local a él y la lógica del servidor convencional hace uso del HSM

Cada uno de los Sistemas Informáticos Centrales **incorpora un Centro HSM** para ofrecer, además de los servicios de seguridad locales que ofrecen los SAM, los siguientes servicios de seguridad centralizados disponibles para instanciar a los servidores seguros, según su tipo:

- **Autoridad certificadora** (AC), para controlar los elementos seguros (SAMs y HSMs) autorizados en el Sistema de Seguridad se realiza mediante una Autoridad Certificadora. Cada elemento seguro autorizado en el sistema debe tener un certificado válido emitido por el AC.

- **Keystore**, donde se almacenan las claves del servidor seguro HSM para protegerlas ante cualquier ataque, ya que sólo se tiene acceso a las claves dentro del propio elemento seguro.

- **Generación de claves,** donde la generación de cualquier clave del Sistema de Seguridad único tiene lugar en el elemento seguro (HSM) de los servidores seguros y no pueden salir en claro del elemento seguro bajo ningún concepto.

- **Distribución de claves,** que permite exportar de forma controlada claves del sistema de un elemento seguro a otro, es decir, de un keystore a otro.

- **Gestión de lista de acciones del SAM**, que son el mecanismo que permite actualizar su contenido desde los Sistemas Informáticos Centrales.

- **Gestión del firmware de los elementos seguros**, que debe ser actualizable "en caliente" de forma atómica y segura, es decir, una vez distribuidos y funcionando en el sistema.

- **Control de acceso por cuota a los SAM**, como mecanismo de protección contra robos para evitar que se pueda hacer un uso indebido de éstos fuera del sistema,

- **Asegurar los accesos a los SUS**, con la implementación de la *Capa de abstracción de la Seguridad de SUS* (SCAL) que es un mecanismo que permite a los terminales manejar la estructura de campos de ATIu (lectura, escritura, incremento, creación, eliminación, etc.), así como la seguridad de los SUS independientemente del tipo concreto de tarjeta, de los órdenes APDU y de su seguridad.

- **Intercambio de información entre SIC y SAM**, de forma segura mediante los Centros HSM que firman y/o encriptan la información hacia los SAM, y desencriptan y/o comprueban la información proveniente del SAM.

- **Almacenes seguros de información,** que permite almacenar información y disponen de mecanismos de seguridad para el acceso seguro a su contenido.

- **Almacenes seguros de claves,** que permite almacenar claves del sistema de forma controlada, cifrada y auditada.

- **Gestión de juegos de claves de tarjeta**, según su uso para realizar desarrollos en el entorno de ingeniería, para la integración en el entorno de preproducción y reales en el entorno de producción en explotación.

- **Mecanismos de diversificación de claves**, de cálculo unidireccional para mitigar a los ricos de almacenar claves maestras en elementos distribuidos por el sistema.

- **Obtener claves maestras,** con mecanismos de acceso fuertes para permitir obtenerlas sólo a los actores autorizados.

- **Obtener claves diversificadas**, con mecanismos de acceso suficientes para permitir obtenerlas sólo a los actores autorizados.

- **Mecanismo de autenticación**, que permite a un sistema corroborar que un actor dice que es quién es.

- **Mecanismos de autenticación mutua**, permite a dos actores autenticar (confirmar la identidad) entre ambos mediante un medio de comunicación no seguro.

- **Obtener clave de sesión,** que se genera durante el proceso de autenticación, generada de forma aleatoria en cada autenticación, que permite que el acceso al Soporte de Usuario Sin contacto (SUS) T-mobilitat mediante órdenes protegidas

mediante criptografía fuerte.

- **Mecanismos de firma,** que permite que unos actores puedan generar la firma de cierta información conocida y que otros puedan comprobar la firma de esta información para comprobar su autenticidad.

Así, en relación con los **Servicios de Seguridad**, estos últimos ya implementados y los nuevos a anteriores, que da los componentes de seguridad centralizadas Centros HSM, deben realizarse las siguientes tareas:

A. Gestionar todos y cada uno de los Servicios de Seguridad que proporcionan los Centros HSMs y asegurar la permanente disponibilidad en explotación con acuerdo a los SLA establecidos.

En fase de análisis e ingeniería el adjudicatario deberá identificar a todos y cada uno de los servicios de seguridad centralizados, así como describir los casos de uso de las actividades relacionadas con el uso de servicios de seguridad locales.

B. Definir, desarrollar y acordar los SLA (Acuerdo de Nivel de Servicio) de cada uno de los Servicios de Seguridad centralizados donados por los Centros HSM, necesarios para la protección de las transacciones sin contacto.

En fase de análisis e ingeniería, se trata de acordar el nivel de servicio que esperamos de cada uno de los servicios de seguridad centralizados que establece el nivel de calidad.

C. Definir, desarrollar e implementar los KPIs (Indicadores Clave de Rendimiento) de los Servicios de Seguridad local dados por los Centros HSMS, necesarios para la protección de las transacciones sin contacto.

En fase de análisis e ingeniería, se trata de identificar KPI que nos ayuden a promover la mejora continua y la eficacia de los servicios de seguridad centralizados CHSM.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica en relación con los Servicios de Seguridad Centralizados, los SLAs y los KPIs, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.4. Servicios de seguridad por dispositivo – SUS

Los SUS son dispositivos del sistema que se utilizan para almacenar los datos de los títulos de transporte necesarios para poder viajar por la red de transportes. Estos dispositivos están en posesión del usuario, lo que les hace ser los dispositivos del sistema más propensos a ser atacados.

Los SUS T-mobilitat ofrecen y/o utilizan los siguientes servicios de seguridad:

- **Almacenes seguros de información,** que permite almacenar información y disponen de mecanismos de seguridad para el acceso seguro a su contenido.

- **Almacenes seguros de claves,** que permite almacenar claves del sistema de forma controlada, cifrada y auditada.

- **Canal seguro de comunicación,** que impide la alteración de la secuencia de datos transmitidos.

- **Mecanismo transaccional de órdenes,** que permiten la ejecución de pedidos de forma atómica.

- **Mecanismos anti-caída,** que garantizan que el acceso al sistema de archivo no quede en estados indeterminados.

- **Autenticación de SUS,** cada vez que un SUS es utilizado en el Sistema Tarifario Integrado debe demostrar su pertenencia al sistema. Si la autenticación no se realiza con éxito, el SUS es rechazado.

- **Confidencialidad,** en relación con datos sensibles almacenan en los SUS que deben ser tratados confidencialmente, tales como datos personales del usuario, en su caso.

- **Integridad,** mediante la firma de los datos como mecanismo que asegura que un actor externo al sistema no puede modificar los datos intercambiados con los SUS ya que, de hacerlo, la firma sería inválida. La clave con la que se firman los datos es una clave de sesión que se obtiene durante el proceso de autenticación.

- **No repudio,** mediante la implementación de una combinación de mecanismos que aseguren el no repudio, como la diversificación de claves, la firma de datos transmitidos y la utilización de canales seguros para transmitir los datos asegura que sólo los actores en los extremos del canal seguro pueden enviar mensajes válidos, evitando que un actor ajeno al canal seguro pueda introducir mensajes clonados en la comunicación.

- **Anticlonado,** mediante los mecanismos exigidos a todo chip autorizado a la T-mobilitat para protegerse ante la clonación de los datos que almacenan, exigiendo demostrar altos niveles de protección certificados por entidades acreditadas con Common Criteria.

- **Auditabilidad,** implementado mecanismos de identificación única y registro de todos SUS utilizado en la T-mobilitat, que se utiliza entre otras cosas, para auditar todas y cada una de las transacciones efectuadas con cada SUS. Estas transacciones se almacenan los sistemas centrales y permite realizar auditorías en el momento que se quiera.

- **Securización de datos personales en la personalización planificada de SUS,** implementando mecanismos criptográficos de protección de datos personales en SUS que incorporan datos personales impresos cuando los datos pasan a lo largo de los distintos procesos dentro del ecosistema T-mobilitat, SICs (ATM y Operadores), módulo de Producción y Personalización Planificada (P3S) y el propio personalizador.

Así, con relación con los **Servicios de Seguridad** estos últimos ya implementados y los nuevos a anteriores, que da los SUS desde el punto de vista de componentes de seguridad distribuido, deben realizarse las siguientes tareas:

A. Gestionar todos y cada uno de los Servicios de Seguridad que

proporcionan los SUS físicos y virtuales y asegurar la permanente disponibilidad en explotación con acuerdo a los SLA establecidos.

En fase de análisis e ingeniería el adjudicatario deberá identificar a todos y cada uno de los servicios de seguridad distribuidos en SUS, así como describir los casos de uso de las actividades relacionadas con el uso de servicios de seguridad locales.

B. **Definir, desarrollar y acordar los SLA (Acuerdo de Nivel de Servicio) de cada uno de los Servicios de Seguridad** dados por los Soportes de Usuarios Sin contacto, necesarios para la protección de las transacciones sin contacto.

   En fase de análisis e ingeniería, se trata de acordar el nivel de servicio que esperamos de cada uno de los servicios de seguridad que ofrecen los SUS y que deberá permitirnos saber el nivel de calidad conseguida.

C. **Definir, desarrollar e implementar los KPIs (Indicadores Clave de Rendimiento) de los Servicios de Seguridad local** dados por los SUS, necesarios para la protección de las transacciones sin contacto.

   En fase de análisis e ingeniería, se trata de identificar KPIs que nos ayuden a promover la mejora continua y la eficacia de los servicios de seguridad implementados en los SUS/Chips autorizado en T-mobilitat.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica con relación a los Servicios de Seguridad en SUS, los SLAs y los KPIs, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.5. Nuevos SERVICIOS DE SEGURIDAD para implementar

Se identifica a continuación una serie de nuevos servicios de seguridad a diseñar, desarrollar e implementar destinados a securizar ciertos procesos y funcionalidades, así como utilizar el sistema de seguridad único como ayuda a la gestión operativa de la T-mobilitat.

3.1.5.1. Identificación y securización de los entornos de trabajo

T-mobilitat dispone de tres entornos de trabajo:

1. **Ingeniería:** es el entorno de trabajo para el desarrollo
2. **Preproducción**: es el entorno donde se realizan todo tipo de pruebas sin poner en riesgo el sistema en operación.
3. **Producción**: es el entorno de operación real en explotación T-mobilitat.

Cada uno de estos entornos requiere implementar el grado de seguridad necesario, suficiente y adecuado al trabajo a desarrollar.

Por ejemplo, siendo el formato de las diferentes claves criptográficas el mismo, el entorno de ingeniería necesita claves criptográficas conocidas, el entorno de preproducción requiere generar claves criptográficas exactamente igual que las de producción pero deben ser conocidas por el gestor de seguridad, el entorno de

producción requiere claves criptográficas no conocidas por ningún actor de sistema y protegidas por varios custodios.

Así, en este contexto, deben realizarse las siguientes tareas:

A. El adjudicatario, en fase de análisis e ingeniería, tendrá **que identificar y especificar los requerimientos de seguridad** por el trabajo seguro de cada uno de estos tres entornos en relación con los diferentes elementos de uso común que intervienen SAM/TIU, SUS, SIC-Operador/CHSM-Operador, SIC-ATM/CHSM-ATM, Claves criptográficas, identificación, etc.

B. El adjudicatario, en fase de análisis e ingeniería, tendrá que **diseñar, desarrollar e implementar** los requerimientos, mecanismos y condiciones de configuración a cargar a los SAM según tipo ya sea de ingeniería, de preproducción y de producción, incluido los requisitos de personalización lógica y física.

C. El adjudicatario, a lo largo del contrato, deberá **personalizar y distribuir los SAMs** que bajo la autorización de la ATM soliciten los diferentes actores del sistema según su necesidad (ingeniería, pruebas o explotación), así como **gestionar y controlar** la su distribución y uso en el Sistema.

D. El adjudicatario, en fase de análisis e ingeniería, deberá **diseñar, desarrollar** (incluye el hardware, en su caso**) e implementar** los requerimientos, mecanismos y condiciones de configuración a cargar en los CHSM según el tipo de entorno a dar servicio, ya sea de ingeniería, de preproducción y de producción.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica del Servicio de Seguridad Local a dar por los SAMs CBT con relación a los requerimientos de seguridad en cada uno de los entornos de trabajos T-mobilitat, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.5.2. Activación de SUS personalizados

T-mobilitat requiere implementar una nueva funcionalidad para que permita el envío de los SUS personalizados por canales de distribución no seguros que no serán utilizables en T-mobilitat hasta que el cliente propietario no lo active por un canal seguro.

Así, en este contexto, deben realizarse las siguientes tareas:

A. El adjudicatario, en fase de análisis e ingeniería, deberá **analizar y proponer un mecanismo basado en la generación de un PIN de activación mediante un algoritmo criptográfico** para garantizar el uso seguro de los SUS personalizados en todo su ciclo de vida, que deberá ser aprobado por la ATM, así como la batería de pruebas necesarias que garantizan su adecuado funcionamiento.

Se tendrá que identificar y describir todo **el ciclo de vida y casos de uso de la activación del SUS personalizado** que va desde la solicitud del SUS, proceso de personalización, generación del PIN y consumo del PIN para activar el SUS por parte del usuario, incluido las mejoras y/o alternativas según el canal, por ejemplo, con el móvil NFC.

B. El adjudicatario, deberá **desarrollar e implementar el mecanismo de uso de PINes de activación de SUS** utilizando un algoritmo criptográfico que garantiza su seguridad como un nuevo Servicio de seguridad local dentro de los SAMs y dentro del CHSMs.

C. El adjudicatario, deberá **garantizar el buen funcionamiento del nuevo servicio de seguridad por el uso de PINes de activación de SUS** implementado antes de ponerlo en producción mediante la validación funcional y cumplimiento de la batería de pruebas desarrolladas en cada uno de los tres entornos (ingeniería, preproducción y producción).

El licitador hará una descripción con detalle que identifique su mejor propuesta técnica del Servicio de Seguridad Local a dar por los SAMs CBT con relación a la activación de SUS, y que están adscritas a la ejecución de este Proyecto que servirá de valoración por en la adjudicación.

3.1.5.3. Registro de Soporte anónimo

T-mobilitat también considera implementar la funcionalidad de registrar un SU anónimo para recuperar y traspasar a otro SUS los derechos de viaje contenido en un SUS que el usuario ha perdido o le han robado, y que no están dado de alta en T-mobilitat.

Así, en este contexto, deben realizarse las siguientes tareas:

A. El adjudicatario, en fase de análisis e ingeniería, deberá **analizar y proponer un mecanismo basado en PIN** para garantizar el registro de SUS anónimos a los usuarios que no quieran darse de alta como cliente T-mobilitat, y la recuperación y traspaso de los derechos de viajes (títulos de transporte), a todo su ciclo de vida, que deberá ser aprobado por la ATM, así como la batería de pruebas necesarias que garantizan su adecuado funcionamiento.

Deberá identificarse y describirse todo **el ciclo de vida y casos de uso del registro y traspaso de derechos de viajes de SUS perdidos o robados,** que va desde su generación al CHSM, tiempo de validez configurable y consumo del PIN para recuperar y traspasar los derechos de viajes, incluidas las mejoras y/o alternativas según el canal, por ejemplo, con el móvil NFC.

B. El adjudicatario deberá **desarrollar e implementar el mecanismo** de uso de PINes de activación de SUS utilizando un algoritmo criptográfico que garantiza su seguridad como un nuevo Servicio de seguridad local dentro de los SAMs y dentro de los CHSMs.

El adjudicatario, deberá **desarrollar e implementar el mecanismo**, con el algoritmo de generación de los PINes de registro como un nuevo Servicio de seguridad local dentro de los SAMs para la recuperación y traspaso de derechos de viaje a un nuevo SUS.

C. El adjudicatario, deberá **garantizar el buen funcionamiento del nuevo servicio de seguridad por el uso de PINes de registro de SUS** implementado antes de ponerlo en producción mediante la validación funcional y cumplimiento de la batería de pruebas desarrolladas en cada uno de los tres entornos (ingeniería, preproducción y producción).

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica del Servicio de Seguridad Local a dar por los SAMs CBT con relación al registro

de apoyo anónimo, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.5.4. Gestión de versiones del ATIu

El Sistema Tarifario Integrado en vivo que requiere evoluciones continuas que en mayor o menor medida afectan a todos los elementos de uso común.

Un elemento de difícil evolución es la Aplicación de Transporte Interoperable única (ATIu) debido a que almacenan los derechos de viaje adquiridos por el cliente que instanciados en los SUS que están en posesión del usuario.

Aunque la versión de versiones de ATIU en un proceso transversal en el que intervienen diferentes elementos el SAM deberá implementar un Servicio de Seguridad para gestionar en explotación el uso de versiones de ATIu.

Así, en este contexto, deben realizarse las siguientes tareas:

- **A.** El adjudicatario, deberá **desarrollar e implementar el mecanismo de seguridad a implementar para gestionar el uso de versión de ATIu en explotación** que garantiza su seguridad como un nuevo Servicio de seguridad local dentro de los SAMs CBT.
- **B.** El adjudicatario deberá **garantizar el buen funcionamiento del nuevo servicio de seguridad implementado para la gestión del uso de versiones de ATIu en explotación** antes de ponerlo en producción mediante la validación funcional y cumplimiento de la batería de pruebas desarrolladas en cada uno de los tres entornos (ingeniería, preproducción y producción), así como el desarrollo e implementación de las herramientas necesarias.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica de la gestión de versiones de ATIu, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación.

3.1.5.5. Securización de datos personales en la personalización de SUS

Hay casos en el proceso de personalización masiva de SUS que incorporan datos personales, como pueden ser los correspondientes a la T-Empleat o a la T-Rosa, se deben comunicar estos datos sensibles desde la fuente (entidad solicitante) y los diferentes sistemas hasta llegar al proveedor de la personalización, pasando, al menos, por otros sistemas como el SIC de ATM y el P3S (módulo de Producción y Personalización Planificada de SUS).

En este contexto, se tendrán que implementar mecanismos para garantizar la protección y el control de esta información sensible.

Así, en este contexto, deben realizarse las siguientes tareas:

- **A.** El adjudicatario deberá **diseñar, desarrollar e implementar los mecanismos de seguridad criptográficos** necesarios para la protección de datos personales cuando se realizan pedidos de personalización masiva de SUS y herramientas asociadas.
- **B.** El adjudicatario deberá **garantizar el buen funcionamiento del nuevo servicio de seguridad implementado para la securización de datos personales**

mediante la validación funcional y cumplimiento de la batería de pruebas desarrolladas en cada uno de los tres entornos (ingeniería, preproducción y producción), así como el desarrollo e implementación de las herramientas necesarias.

El licitador realizará una descripción con detalle que identifique su mejor propuesta técnica para la securización en los procesos de personalización masiva de SUS que incorporan datos personales, y que están adscritas a la ejecución de este Proyecto que servirá de valoración para la adjudicación

3.2. Gestión en explotación de COMPONENTES físicos del SSu

Los servicios de seguridad del SSu se cargan en distintos componentes físicos con el objetivo de ponerlos a disposición del sistema según las necesidades.

Básicamente, se identifica dos tipos de componentes a gestionar:

- Los Módulos de Acceso Seguro (SAMs CBT) para dar estos servicios cuando es necesario realizar transacciones rápidas que llamamos seguridad local,
- Los Centros de Hardware de Acceso Seguro (CHSMs) en otras situaciones que llaman seguridad centralizada.

3.2.1. Gestión en explotación de los MÓDULOS DE ACCESO SEGURO, SAMs

El Módulo de Acceso Seguro o SAM es un elemento seguro en formato SIM con un chip microprocesador con características criptográficas sobre el que se implementan servicios de seguridad, así como almacena las claves criptográficas.

Está dotado de fuertes medidas de seguridad anti-tamperización que le protege de ataques de diversos tipos (de canal lateral, de ingeniería inversa, de inyección de fallos...) que hacen que sea extremadamente difícil, si no imposible la extracción de las llaves de su interior.

Los SAMs no tienen batería, por lo que para funcionar toman la alimentación del terminal sin contacto donde están instalados.

La misión de los Módulos SAM es la de proporcionar Servicios de seguridad (autenticación, confidencialidad, integridad, no repudio…, capa de abstracción de la seguridad de los protocolos y mecanismos de seguridad utilizados en los soportes SUS autorizados en el sistema, etc.) en tiempo real allí donde el Sistema Tarifario Integrado requiera protección.

Un SAM se utiliza de diferente forma dependiendo del estado en su ciclo de vida.

Los estados se definen desde dos puntos de vista del Sistema, según la fase en la que se encuentra:

- Fabricación, Pre-operacional, Operacional, Pos-operacional y Destrucción.
- Diferentes tipos de SAM (Ingeniería, Pruebas, Producción...).

Y en función del propio ciclo de vida funcional del SAM:

- Sin Sistema Operativo, Sin kernel, Securizado, Personalizado, Activo, Suspendido, Desactivado, Comprometido y Destruido.

La transición entre estados requiere registrar el evento para auditar el estado en el que se encuentra el SAM en todo momento.

El Gestor de Seguridad de SAM tiene la misión de gestionar todos y cada uno de los estados del ciclo de vida del SAM.

Entre otras funcionalidades de bajo nivel, el Gestor de SAM se encarga de gestionar:

- Firmwares que necesita el SAM para funcionar como el firmware de base, reprogramaciones, criptografía fuerte y aplicaciones (servicios).
- Sistema de arranque,
- Versionado,
- Órdenes de personalización,
- Otro

Así, en relación con la gestión de los **Componentes SAMs CBT en explotación**, que dan los Servicios de seguridad local una vez están instalados en los Terminales sin contacto T-mobilitat, deben realizarse las siguientes tareas:

A. Gestionar, controlar y mantener actualizados todos y cada uno de los estados del ciclo de vida de los SAMs CBT fabricados y distribuidos por cada uno de los entornos de trabajo, ingeniería, pruebas y producción a lo largo de todo el contrato.

En fase de análisis e ingeniería el adjudicatario deberá **identificar de forma explícita el estado** de todos y cada uno de los servicios de seguridad distribuidos en cada uno de los entornos, así como **revisar y actualizar todos los casos de uso** de las actividades relacionadas con el uso de servicios de seguridad locales.

B. Revisar, actualizar, optimizar, en su caso, y mantener los procesos de alta y personalización física y lógica de SAMs CBT ya en explotación, correspondiente a la **fase preoperacional** del SAM.

En fase de análisis e ingeniería, se analizará, modificará y simplificará, si es posible, los procesos de:

- Personalización física garantizando la identificación única y registro que da el SIR,
- “Carga de firmware”, mediante la plantilla de personalización,
- Alta de SAM en el Sistema de Seguridad único,
- "Carga de Claves", mediante la plantilla de exportación de Keysets,
- Personalización lógica en función del rol en el sistema (Validación, recarga, consulta, etc.).

En fase de análisis e ingeniería el adjudicatario deberá identificar de forma explícita el plan de trabajo para la actualización de los procesos de personalización segura de SAMs CBT, así como la actualización de sistema de mantenimiento de SAM CBT en explotación.

C. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener la

Plataforma de personalización de SAMs CBT a lo largo del contrato y correspondiente a la **fase preoperacional**.

En fase de análisis e ingeniería, se trata de analizar explícitamente el desarrollo de la plataforma de personalización de SAM CBT para su actualización y evolución técnica, optimización y simplificación de los procesos, en su caso, etc.

D. **Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de personalización segura de SAMs CBT** a lo largo del contrato, correspondiente a la **fase preoperacional**.

   En fase de análisis e ingeniería, se trata de analizar explícitamente el programa de conformidad y Aceptación de la personalización segura de SAM CBT para su actualización, evolución y adaptación a los procesos de personalización segura de SAM CBT actualizado.

E. **Ejecutar el Programa de C&A de los SAMs solicitados** a lo largo del contrato, correspondiente a la **fase preoperacional** para garantizar su funcionalidad en la explotación.

   El licitador deberá detallar ampliamente su propuesta técnica en relación con las tareas de mejora y optimización de los procesos y funcionalidades de la personalización segura de SAM CBT, correspondiente a la **fase preoperacional** del SAM CBT, así como de la plataforma y herramientas asociadas, que servirá de valoración para la adjudicación.

F. **Revisar, actualizar, optimizar, en su caso, y mantener** los procesos correspondientes a la **fase operacional** del SAM CBT.

   En fase de análisis e ingeniería, se analizará, modificará y simplificará, en su caso, los procesos de distribución, instalación y monitorización de los SAMs CBT en explotación.

   Especial atención se tendrá con la propuesta técnica para el control y seguimiento de SAMs CBT en explotación mediante el diseño, desarrollo e implementación de herramientas de ayuda a la monitorización en tiempo real del parque de SAMs CBT en explotación.

G. **Revisar, actualizar, optimizar, en su caso, mantener y ejecutar,** tantas veces como sea necesario, los procesos **reprogramación segura en caliente** de los SAMs CBT en explotación correspondiente a la **fase operacional**.

   En fase de análisis e ingeniería, se analizará y mejorará, en su caso, los procesos de reprogramación en caliente segura de los SAMs CBT en explotación.

   Especial atención se tendrá con la propuesta técnica para el control y seguimiento de los procesos de actualización de SAM en caliente que incluye actualización rápida, segura y atómica, así como un potente programa de pruebas.

   El licitador deberá detallar ampliamente su propuesta técnica en relación con las tareas de control y seguimiento a implementar para la **fase operacional** del SAM CBT, que servirá de valoración para la adjudicación.

H. **Revisar, actualizar, optimizar, en su caso, y mantener** los procesos correspondientes a la **fase pos-operacional** del SAM CBT.

En fase de análisis e ingeniería, se analizará, modificará y mejorará, en su caso, los procesos de gestión y control de la vida útil de los SAMs CBT en explotación, es decir, sustitución por claves comprometidas, por vida útil final y análisis derivados de las distintas casuísticas surgidas.

El licitador deberá detallar ampliamente su propuesta técnica en relación con las tareas de control y seguimiento a implementar para la **fase pos-operacional** del SAM CBT, que servirá de valoración para la adjudicación.

3.2.2. Gestión en explotación de los CENTROS HSMs

Además de los Servicios de seguridad locales que ofrecen los módulos SAM, el Sistema Tarifario Integrado ha definido servicios de seguridad centralizados que utilizan equipos y actores de forma remota dentro de un entorno controlado como el SIC.

Éstos complementan el ecosistema del sistema de seguridad único y se generan por otras necesidades de protección del sistema.

Un CHSM es un sistema que por sí mismo, a nivel lógico, funciona como un solo elemento, pero físicamente tiene una arquitectura que está formado por los siguientes elementos:

- **Nodo HSM**

  Un nodo es la unidad funcional mínima de un CHSM. Un CHSM puede dar servicio con un solo nodo, pero se instalan entre 3 y 4 para conseguir alta disponibilidad y conseguir mayor potencia de computación ya que ésta es proporcional a la cantidad de nodos en servicio.

  Los nodos son autónomos y autocontenidos y, por tanto, la caída de un nodo no afecta al resto.

  Así, un nodo, a su vez está compuesto por:

  - **Módulo HSM** (Hardware Secure Module)

    Es un componente seguro, formado por un conjunto de elementos seguros, en los que la lógica se ejecuta y los recursos que protege disponen de mecanismos físicos de protección contra intrusiones.

    Los módulos HSM, físicamente son placas PCIe y antes de poder ponerse en explotación, deben darse alta en el SSu y ser inicializadas por el gestor del SSu.

    Su contenido, a nivel lógico, está organizado en particiones y éstas, al arrancar, están desactivadas, y por tanto, el acceso a su contenido está bloqueado. Para poder acceder al contenido de las particiones, deben activarse.

  - **Ordenador host**

    Está formado por un hardware no seguro, en el que la lógica que se ejecuta no es segura.

Es un servidor estándar para trabajo en CPDs con CPU Xeon, interfaces de red y sistemas de almacenamiento convencionales.

El HSM se instalará en su interior y la lógica del ordenador hace uso del HSM.

- **Infraestructura de red**

  Son aquellos elementos necesarios para que los servidores seguros se comuniquen de forma adecuada.

  Los equipos que los componen son dos firewalls/routers configurados en alta disponibilidad y el cableado y adaptadores necesarios para interconectar los firewalls/routers con los nodos.

  Aparte de los firewalls/rúters, los CHSM disponen de balanceadores de carga que se encargan de distribuir las peticiones entre los diferentes nodos del CHSM. Los balanceadores de carga de los CHSM no son elementos en un CHSM existen tantos balanceadores de carga como nodos. Los balanceadores de carga están sincronizados entre sí y configurados en alta disponibilidad, siendo necesario tan sólo un balanceador de carga activo para que el sistema funcione correctamente.

- **Activador remoto de módulos HSM**

  Son los elementos físicos y lógicos necesarios para activar remotamente los módulos HSM.

  Estos activadores son los responsables de activar las particiones de los HSM. El mecanismo de activación, aparte de los HSM objeto de la activación, requiere de un lector de tarjetas con contactos estándar PC/SC, tarjetas activadoras y un software de activación remota

Así, en relación con la gestión de los **Componentes CHSMs en explotación**, que dan los Servicios de seguridad centralizado una vagada están instalados en los Sistemas Informáticos Centrales T-mobilitat, deben realizarse las siguientes tareas:

A. **Gestionar, controlar y actualizar, en su caso, la Arquitectura física** de los Centros HSM instalados y distribuidos por cada uno de los entornos de trabajo, ingeniería, pruebas y producción a lo largo de todo el contrato.

   En fase de análisis e ingeniería el adjudicatario deberá **analizar y revisar explícitamente la arquitectura de los Centros HSM, encontrar puntos de mejoras de optimización y/o seguridad.**

B. **Revisar, actualizar, optimizar, en su caso, los procesos de gestión** que forman parte de la infraestructura de gestión segura de claves e información que asegura el contenido del Centro HSM:

   - **Activación**, que permite la activación remota de un nodo HSM,
   - **Configuración,** que permite la configuración centralizada de los CHSM desde un servidor SFTP por parte del gestor del Sistema de Seguridad único.
   - **Registro,** que permite reportar registros de seguridad que se han generado durante la explotación del sistema T-mobilitat.

- **Monitorización,** que permite auditar el estado del CHSM mediante distintos canales (SYSLOG y SNMP) y activar las alarmas correspondientes.
- **Reloj de tiempo real (RTC),** que permite la sincronización horaria con el resto del sistema.

En fase de análisis e ingeniería el adjudicatario deberá: **analizar y revisar explícitamente los procesos de gestión de los Centros HSM.**

C. Revisar, actualizar, optimizar, en su caso, los servicios operacionales que son útiles para la operación segura del CHSM mediante la publicación de APIs o HTTP, entre ellos:

- **Procesamiento de información en ccTIU**, que permite procesar la información generada por los ccTIU con el fin de verificar la veracidad de los registros transaccionales generados en los terminales gestionados por este SIC.
- **Securización de información hacia ccTIU**, que permite cifrado completo de paquetes, parcial, firmar..., ensamblados binarios de ODs, listas de acciones, configuraciones del STI, etc.
- **Firma de SIC**, que permite que el SIC pueda firmar información para certificar su autoría. Su utilidad es firmar una determinada información que se intercambia con otros SIC o con otras autoridades.
- **Incremento on-line de cuota de SAM** que permitirá incrementar la cuota que bloquea los SAMs en explotación.

En fase de análisis e ingeniería el adjudicatario deberá: **analizar y revisar explícitamente los servicios operacionales que prestan los Centros HSM.**

D. Revisar, actualizar, optimizar, en su caso, la infraestructura de comunicaciones de los CHSM centralizados en relación con las altas exigencias de disponibilidad y redundancia de los sistemas: cómo son el diseño físico, el diseño lógico, direccionamiento IP, etc.

En fase de análisis e ingeniería el adjudicatario deberá: **analizar y revisar explícitamente la infraestructura de comunicaciones de los CHSM.**

E. Revisar, actualizar, optimizar, en su caso, el sistema de monitorización de los CHSM mediante el análisis, control y seguimiento de las métricas de monitorización que se generan los diferentes elementos que forman parte del CHSM (routers, balanceadores y nodos HSM), de los sistemas de monitorización utilizados (activa (POLLs), pasiva (TRAPs) o combinación de ambas).

En fase de análisis e ingeniería el adjudicatario deberá: **analizar y revisar explícitamente el sistema de monitorización de los CHSM.**

F. Revisar, actualizar, optimizar, en su caso, el programa de pruebas específicas de infraestructura y alta disponibilidad de los CHSM en las cuatro líneas de actuación: Pruebas de servicios, pruebas de activación, pruebas de monitorización y pruebas de mantenimiento.

En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente el sistema de pruebas específicas de infraestructura y alta disponibilidad de los CHSM, así como su ejecución.

G. **Revisar, actualizar, optimizar, en su caso, los casos de uso,** de las actividades relacionadas con el uso de servicios de seguridad centralizados, es decir, las interacciones que se realizan entre actores del Sistema de seguridad único en relación con los CHSM.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los casos de uso relacionados con los Centros HSMs.

El licitador deberá detallar ampliamente su propuesta técnica en relación con las tareas para la gestión técnica de los Centros HSMs, que servirá de valoración para la adjudicación.

3.2.3. Gestión en explotación de los DISPOSITIVO MÓVILES NFC

La T-mobilitat integra la Tecnología NFC en el centro del escenario como elemento impulsor de servicios en tiempo real utilizando los dispositivos móviles inteligentes NFC en los dos modos de trabajo que se pueden utilizar:

- Como un Terminal sin contacto de uso personal en el momento y lugar que decidimos: *"Como Terminal de Interacción con el Usuario (TIU personal)*".
- Como nuevo Soporte sin contacto para acceder directamente al Transporte" *Como nuevo Soporte de Usuario Sin contacto (SUS NFC virtual)* ".

La incorporación de:

- El Protocolo de comunicaciones *"Near Field Communication"* (NFC) en los dispositivos móviles inteligentes (smartphones), y por otra parte,
- La Tecnología *"Host Card Emulation"* (HCE) en el Sistema Operativo Android.

Unido a la versatilidad de comunicación que poseen estos dispositivos móviles inteligentes, ofrece grandes oportunidades de mejorar la experiencia cliente y ayuda a realizar un viaje inteligente.

Un viaje inteligente implica que el dispositivo móvil NFC debe interactuar con toda la infraestructura de transporte y trabajar juntos para generar una experiencia sencilla, en tiempo real e interactiva por el viajero, pero sin olvidar implementar los mecanismos de seguridad que protejan los datos del viajero y su derecho a viajar de forma anónima.

Dado que la tecnología HCE ofrece una seguridad limitada, el sistema implementa servicios y mecanismos de seguridad específicos para mitigar los riesgos asociados, como:

- **Servicio de Tokenización**.

  Que incluye la generación de los tokens mediante técnicas criptográficas implementadas de forma preceptiva dentro de un servidor seguro, así como la modificación de los tokens mediante los servicios criptográficos implementados, también dentro de elementos seguros.

La gestión de tokens tiene en cuenta procesos y funcionalidades como la autorización de modificación de tokens, firma y cifrado de tokens, validez y ampliación temporal de los tokens, mecanismos para la transferencia segura de tokens, etc.

- **Sistema de gestión de claves criptográficas:**

  Que incluye la gestión de claves criptográficas específicas para la protección de datos utilizadas en entornos inseguros como los dispositivos móviles NFC y su interacción con el Sistema Tarifario Integrado sin contacto.

  El ecosistema móvil incluye procesos y funcionalidades como la:

  - Generación de estas claves en función del lugar en el que se almacenan, así como el intercambio seguro con los sistemas centrales y/o con los elementos seguros,
  - Utilización de claves criptográficas diversificadas,
  - Autenticación mutua y uso de claves de sesión,
  - Limitación del uso temporal de claves criptográficas.

- **Mecanismos de gestión segura:**

  Que incluye la gestión de los mecanismos y servicios de seguridad para la protección de funcionalidades adicionales corresponden al ecosistema móvil.

  Contiene procesos y funcionalidades como:

  - Mecanismos seguros anti-caídas para proteger la integridad de los datos.
  - Access seguro en el sistema de archivos,
  - Firma segura de transacciones sin contacto,
  - Mecanismos seguros de registro y autenticación de usuarios,
  - Mecanismos criptográficos que aseguren canales seguros para el intercambio de datos.
  - Mecanismos criptográficos para generar y modificar la validez de los tokens,
  - Mecanismos para la detección de móviles “root”, …

Así, en relación con la **gestión segura de dispositivos móviles NFC en explotación**, para utilizar estos dispositivos NFC a T-mobilitat tanto como Soporte sin contacto como terminal sin contacto, deben realizarse las siguientes tareas:

A. Revisar, actualizar, optimizar, en su caso, la estructura de ATIu tokenizada para su uso en los dispositivos móviles NFC, gestión de acceso, autorización de modificación, tarjeta virtual, validez temporal, verificaciones de tokens, mecanismos criptográficos empleados, transferencia de tokens, gestión PKI, etc.

En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente la estructura de la ATIu tokenizada para su uso en los dispositivos móviles NFC, así como los procesos, mecanismos y algoritmos necesarios para la gestión segura de tokens.

B. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de pruebas específico para garantizar la tokenización segura de la ATIU en los dispositivos móviles NFC.

En fase de análisis e ingeniería, se trata de analizar explícitamente el programa de pruebas específicos para la securización en el uso de dispositivos móviles NFC en la T-mobilitat.

El licitador deberá detallar ampliamente su propuesta técnica con relación a las tareas para la gestión segura de dispositivos móviles NFC en la T-mobilitat, que servirá de valoración para la adjudicación.

3.2.4. Servicios de Mantenimiento integral del SSu

El Sistema de Seguridad único es un elemento crítico del Sistema Tarifario Integral T-mobilitat y como tal es necesario mantenerlo para que esté disponible siempre.

Para garantizar el funcionamiento general del Sistema de Seguridad único, todos y cada uno de los componentes y procedimientos que lo forman requieren un **Mantenimiento Integral específico de Alta Disponibilidad en base a una monitorización permanente**, un control local y remoto, así como una permanente revisión en explotación que permita:

- Prever actuaciones de forma anticipada,
- Actualización en la medida en que se identifiquen mejoras o se requieran nuevas funcionalidades, así como
- Planificación del ciclo de vida tecnológico de los componentes que lo integran.

Las principales actuaciones se concretan en los siguientes apartados:

1. Identificación de equipos y aplicaciones

El servicio de mantenimiento abarca todos y cada uno de los componentes y programas (en adelante equipos de forma genérica). Concretamente se incluyen:

- o Arquitectura del Sistema de Seguridad criptográfica,
- o Infraestructura de gestión de claves criptográficas (incluidos los procesos y funcionalidades en explotación),
- o Plataforma de gestión de seguridad criptográfica local (procesos y funcionalidades de gestión del ciclo de vida en explotación de los módulos SAMs, incluidos),
- o Servicios de seguridad específicos de área local desplegados en los módulos SAMs en explotación,
- o Los propios Módulos SAMs desplegados en el sistema, así como el control de monitorización en explotación.
- o Plataforma de gestión de seguridad criptográfica centralizada (procesos y funcionalidades de gestión de todos los componentes de seguridad).
- o Servicios de seguridad específicos de área centralizada (en la nube)

desplegados en los Centros HSMs

- Los Centros HSM instalados en cada uno de los Operadores de Transporte y la ATM,
- Centro HSM de respaldo (backup),
- Centro HSM de ingeniería/preproducción,
- Plataforma de gestión de seguridad criptográfica por dispositivos móviles NFC (procesos y funcionalidades en explotación incluidos),
- Servicios de seguridad específicos en dispositivos móviles NFC,
- Gestión documental: Mantenimiento y actualizaciones en explotación.

2. Actuaciones preventivas

Corresponden a las acciones destinadas a garantizar la fiabilidad de los equipos y componentes instalados antes de que pueda producirse un incidente, problema o avería por deterioro, incluye el mantenimiento programado y mantenimiento predictivo.

Por lo que respecta a los elementos seguros físicos como los módulos SAMs y Centros HSMs implica actuaciones periódicas de las operaciones, transacciones realizadas, parámetros operativos, rendimiento y posibles indicadores de anticipación a fallos.

El licitador deberá especificar amplia y detalladamente su propuesta técnica en relación con las actuaciones preventivas necesarias en la Fase de Explotación para llevar a cabo el mantenimiento preventivo de los diferentes equipos y componentes del Sistema de Seguridad criptográfico.

3. Actuaciones correctivas

Corresponden a la corrección de errores que puedan producirse en el funcionamiento de sistema que incluyen el mantenimiento:

- **Mantenimiento correctivo de primer nivel.**

  Es aquél que puede llevar a cabo personal no especializado, e incluye reparaciones sencillas.

- **Mantenimiento correctivo de segundo nivel.**

  Es aquél efectuado por personal cualificado (en su caso, con equipo especial) en las mismas instalaciones. Incluirá la reparación de todo tipo de averías de los equipos instalados en sus dependencias.

- **Mantenimiento correctivo de tercer nivel.**

  Se refiere a la retirada del equipo o componente del equipo que tenga un mal funcionamiento y su reparación por parte del suministrador en sus propias instalaciones.

El mantenimiento correctivo es el resultado de una incidencia debido a una situación en la que alguno de los equipos o programas en mantenimiento funciona de forma incorrecta o errónea.

Las acciones correctivas de cualquier nivel incluyen la identificación de incidencias funcionales y técnicas, detectadas en el funcionamiento del sistema en explotación, y que requieran la modificación y/o actualización de algunos de sus componentes.

Cualquier actuación sobre el software motivada por un fallo o error será considerada siempre como actividad perteneciente a la asistencia técnica correctiva.

Se debe disponer de elementos o componentes de sustitución, especialmente de los Centros HSMs, para reposición temporal del equipo o componente dañado mientras se repara o adquiere el original, cuyo suministro no está incluido en el alcance.

También se incluyen los trabajos de análisis y resolución de incidencias que, sin suponer cambio o modificaciones, puedan requerir actuaciones técnicas, revisión y modificación de datos, revisión y modificación de configuraciones, etc.

En relación con la disponibilidad del servicio se implementarán SLAs según la afectación al servicio del portal web corresponden. A modo de referencia se expone a continuación.

Incidencia (categoría)	**Tiempo de respuesta**	**Tiempo resolución**
Crítica	10 minutos en 24x7	2 horas en 24x7
Alta	20 minutos en 24x7	4 horas en 24x7
Media	1 hora en 10x5	8 horas en 24x7
Baja	Según práctica habitual de mercado	Según práctica habitual de mercado

Se entiende por incidencia:

- Crítica: pérdida completa o falta de disponibilidad total del servicio
- Alta: pérdida o falta de disponibilidad parcial del servicio.
- Media: pérdida menor del servicio: errores puntuales o problemas de rendimiento
- Baja: incidencia que carece de impacto en el servicio.

Se entiende por:

- Tiempo de respuesta: el tiempo en que el adjudicatario registra la incidencia en el sistema de gestión de tickets y ésta se comunica a los destinatarios, mediante el workflow y canales establecidos del código, la definición y la tipificación de gravedad del mismo.
- Tiempo de resolución: tiempo que pasa desde el inicio de la incidencia (y no desde el tiempo de respuesta), hasta el restablecimiento completo del servicio, es decir, hasta que las alarmas y sistemas de monitorización vuelvan notificar que el servicio es correcto.

Así, en relación con la **gestión de los servicios de mantenimiento integral del SSu en explotación**, de cada uno de sus componentes y los procedimientos que implementa, deben realizarse las siguientes tareas:

A. Revisar, actualizar y optimizar, en su caso, de los **Servicios de**

Mantenimiento integral del SSu en explotación que garantiza la alta disponibilidad del SSu que requiere el Sistema Tarifario Integrado T-mobilitat.

En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los Servicios de mantenimiento integral ya en explotación con el fin de mejorar, en su caso, realizar ajustes y modificaciones a las herramientas y el software de las plataformas.

B. **Revisar, actualizar, optimizar, en su caso, e identificar** los **Equipos y aplicaciones de los SSu que son objeto de mantenimiento** identificando al menos su arquitectura, funcionalidad y nivel de criticidad en el sistema.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente a los Equipos y Aplicaciones a mantener en explotación, incluidas las plataformas tecnológicas y herramientas asociadas al mantenimiento.

C. **Revisar, actualizar, y optimizar, en su caso, los Sistemas de monitorización permanente** de los distintos equipos y herramientas asociadas a la monitorización a fin de mantener el nivel de calidad esperado.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los sistemas de monitorización ya en explotación, incluidas las plataformas tecnológicas y herramientas asociadas al mantenimiento.

D. **Revisar, actualizar, y optimizar, en su caso, los Sistemas de mantenimiento preventivo** de los distintos equipos y herramientas asociadas para garantizar su fiabilidad y prever posibles incidencias, problemas o averías por deterioro.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los sistemas de mantenimiento preventivo, incluidas las plataformas tecnológicas y herramientas asociadas al mantenimiento, a fin de mejorar la calidad del sistema en cualquiera de sus aspectos: reestructuración del código, clarificación del código, optimización del rendimiento y eficiencia, etc.

E. **Revisar, actualizar, optimizar, en su caso, y disponer de los equipos de repuesto** de cada elemento para la sustitución temporal en caso de llevar a cabo una acción correctiva de nivel 3, mientras el equipo dañado se repara o se decide adquirir un otro original.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los equipos de repuesto y asegurar que siguen siendo disponibles y funcionando correctamente.

F. **Revisar, actualizar, y optimizar, en su caso, los Sistemas de mantenimiento correctivo** resultado de la identificación de una incidencia en el SSu, debido a que algunos de sus equipos o componentes funcionan de forma incorrecta o errónea.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los niveles de acciones correctivas (de primer, segundo y tercer nivel), los niveles de incidencias, estado de una incidencia, tiempo y compromiso de respuesta y pequeñas evoluciones del SSu como respuesta a la resolución de incidencias y problemas, a fin de mejorar la calidad del sistema en cualquiera de sus aspectos: reestructuración del código, clarificación del código, optimización del rendimiento y eficiencia, etc.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación a la revisión del Sistema de Mantenimiento Integral del SSu ya en explotación, que servirá de valoración para la adjudicación.

3.3. Infraestructura de Gestión de CLAVES Y HERRAMIENTAS asociadas al SSu

Cuando se utiliza cifrado criptográfico es obligatorio alinear los procesos a las buenas prácticas recomendadas por los organismos competentes. En este contexto, con la utilización de algoritmos criptográficos conocidos y contrastados por la comunidad de criptoanálisis se transfiere el riesgo desde los datos a proteger, en nuestro caso, las transacciones sin contacto, a una **gestión segura de las CLAVES criptográficas** utilizadas.

Las **CLAVES criptográficas forman el núcleo** de toda información informática basada en el cifrado criptográfico. Al igual que en el mundo real, de nada sirve la fortaleza de un algoritmo si la clave cae en manos equivocadas.

Generalmente, a medida que aumentan los activos por los que pasan las transacciones sin contacto protegidas mediante cifrado criptográfico, **se incrementa también el número de claves a gestionar.**

La forma tradicional de gestionar claves de cifrado es un proceso manual que requiere de muchos recursos y la participación de varias personas y funciones que implica un **alto riesgo de errores humanos.**

La mejor forma de proteger las claves criptográficas es a través de la implantación de una **INFRAESTRUCTURA (Plataforma) de alta seguridad** como soporte al uso de técnicas criptográficas extremo a extremo, que van desde algoritmos criptográficos contrastados, hasta la gestión segura de las claves criptográficas utilizadas, pasando por la utilización de hardware seguro en la generación, intercambio y almacenamiento de servicios y claves criptográficas.

La Infraestructura de alta seguridad está basada en la utilización de **servidores de alta seguridad que tienen instanciados servicios en función del tipo**, como: de Autoridad Certificadora, KeyStore; Generación de claves; Gestión de listas de acción del SAM; Gestión de firmware de los elementos seguros; Control de cuotas; Autenticar accesos a los diferentes Soportes de Usuario sin Contacto (SUS); Intercambio de información SIC y SAM; Intercambio de información entre SICs...

Esta infraestructura es implementada bajo los siguientes focos o enfoques complementarios:

- Un **enfoque estratégico** basado en las buenas prácticas recomendadas en los estándares internacionales, al objeto de:
  - Detectar y prevenir la manipulación de juegos de claves criptográficas, así como,
  - Permitir certificar que una clave realmente pertenece a una entidad autorizada en el sistema.
- Un **enfoque táctico** basado en principios y la definición de requerimientos simples y claros de obligado cumplimiento para la protección frente a:
  - La manipulación, pérdida o destrucción de claves a lo largo de todo el ciclo de vida del uso de las claves,

- La divulgación no autorizada de claves criptográficas del sistema.

- Un **enfoque operacional** basado en normas y estándares de seguridad acreditados, es decir, procedimientos y métodos que den respuestas seguras a:
  - La generación de claves por los diversos servicios de seguridad criptográficos,
  - La obtención de certificados de las claves generadas,
  - La distribución de claves criptográficas a los usuarios,
  - El almacenamiento seguro de claves para su uso en el sistema,
  - La activación y/o cambio de claves criptográficas,
  - La revocación de claves criptográficas.
  - La recuperación de llaves perdidas o corruptas,
  - El archivo de claves, por histórico de información,
  - La destrucción de claves,
  - El registro y auditorías de las actividades relacionadas con la gestión de claves.

El resultado de aplicar protección contra la manipulación, pérdida o destrucción de claves y/o divulgación no autorizada comporta la utilización preceptiva de los llamados **elementos seguros** que son equipos físicamente protegidos contra ataques en la infraestructura tecnológica del sistema.

Los elementos seguros físicos son los equipos en los que se almacenan **claves criptográficas**, así como los **servicios y mecanismos de seguridad** que garantizan una adecuada protección de las transacciones sin contacto y otra información sensible en el sistema.

Los principales, pero no únicos, servicios y mecanismos de seguridad criptográficos implementados en elementos seguros van en la línea de garantizar **la autenticación, la confidencialidad, la integridad y el no repudio** de todas y cada una de las transacciones sin contacto llevadas a cabo en el Sistema.

Así, en relación con la **Plataforma de seguridad criptográfica** para la gestión principalmente de las claves criptográficas del SSu en explotación, deben realizarse las siguientes tareas:

A. Revisar, actualizar, y optimizar, en su caso, la Plataforma de seguridad criptográfica ya en explotación que implementa los principales procesos funcionales que se pueden automatizar desde el punto de vista de la arquitectura de la plataforma, y que permitir:

- Gestión de claves criptográficas,
- Gestión de SAMs CBT
- Gestión de Plantillas
- Gestión de KeySet de claves
- Gestión de equipos

En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente la arquitectura de la plataforma de seguridad criptográfica.

B. **Revisar, actualizar, y optimizar, en su caso, los procesos de gestión de claves criptográficas**: acreditación de los actores mediante infraestructura PKI y sus componentes: autoridad certificadora, las estructuras de datos jerarquizadas, petición de firma de certificado, certificado o autorización por parte de la CA, keystore, generación, identificación, diversificación y distribución de claves, gestor de funcionalidades, servidor de seguridad, ceremonia de claves, registro y auditorías.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los procesos de gestión de claves criptográficas.

   Especial atención a la herramienta visual que se conecta al servidor de seguridad y permite realizar acciones para gestionar la seguridad: consultar los elementos seguros, registros de auditoría de los HSM, realizar ceremonia de claves, Crear CA, Crear PINes en el Keystore, dar de alta, personalizar e inicializar SAM, crear particiones HSM, etc.

C. **Revisar, actualizar, y optimizar, en su caso, los procesos de gestión de SAMs CBT y centros HSM** que permite dar de alta, personalizarlos lógicamente mediante plantillas de personalización, consultar su estado, destrucción lógica del SAM, entre otros, para cada uno de los tipos de SAMs (ingeniería, pre -producción y producción).

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los procesos de gestión de SAMS CBT.

D. **Revisar, actualizar, optimizar, en su caso, los casos de uso,** de las actividades relacionadas con infraestructura de gestión de claves criptográficas T-mobilitat, es decir, las interacciones que se realizan entre actores del Sistema de seguridad único con relación al uso seguro de las claves criptográficas

   En fase de análisis e ingeniería el adjudicatario deberá: analizar y revisar explícitamente los casos de uso relacionados con la gestión de claves criptográficas T-mobilitat.

El licitador deberá especificar de manera amplia y detallada su propuesta técnica con relación a la revisión de la Plataforma de seguridad criptográfica para la gestión de las claves criptográficas T-mobilitat, así como la carga segura en los componentes de seguridad, que servirá de valoración para la adjudicación.

3.4. Gestión y liderazgo del PROGRAMA de C&A del SSu

El Programa de Conformidad y Aceptación es el mecanismo que tiene el Modelo Técnico Común para garantizar la interoperabilidad técnica de los elementos de uso común T-mobilitat mediante la ejecución de test unitarios y de integración para comprobar y validar el cumplimiento de todos y cada uno de los requerimientos técnicos MTC, siendo uno de los principales roles ISO/IEC 24014 para garantizar la interoperabilidad técnica y funcional.

Las pruebas del SSu del programa de C&A del ATC son funcionales. Así, y debido a la gran complejidad tecnológica y confidencialidad que acompaña a los complejos procesos criptográficos implementados es necesario implementar pruebas específicas,

complementarias al programa de C&A, definidas, desarrolladas, integradas y ejecutadas desde el SSu.

En este contexto y para cada una de las áreas de trabajo, el adjudicatario deberá realizar el correspondiente programa de C&A y/o revisar y actualizar, en su caso.

3.4.1. Programa de C&A a Serveis de Seguretat

Así, en relación con las pruebas de aceptación específica complementarias a aplicar a los servicios de seguridad, a los componentes seguros ya las herramientas asociadas, para garantizar en todo momento el cumplimiento de los requerimientos técnicos exigidos, deben realizarse las siguientes tareas:

A. Diseñar, desarrollar e implementar los casos de *test* unitarios, test de integración, test de sistema y test de interoperabilidad para comprobar la funcionalidad prevista del nuevo servicio de seguridad **de "Activación de SUS personalizados"**.

El adjudicatario tendrá que incorporar estos casos de *test* al Programa de Conformidad y Aceptación de Servicios de Seguridad según el entorno al que aplique (ingeniería, preproducción o producción) y según el componente seguros a cargar estos servicios (SAMs y CHSMs).

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

B. Diseñar, desarrollar e implementar los casos de *test* unitarios, test de integración, test de sistema y test de interoperabilidad para comprobar la funcionalidad prevista del nuevo servicio de seguridad **"Registro de soporte anónimo**".

El adjudicatario tendrá que incorporar estos casos de t*est* al Programa de Conformidad y Aceptación de Servicios de Seguridad según el entorno al que aplique (ingeniería, preproducción o producción) y según el componente seguros a cargar estos servicios (SAMs y CHSMs).

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

C. Diseñar, desarrollar e implementar los casos de *test* unitarios, test de integración, test de sistema y test de interoperabilidad para comprobar la funcionalidad prevista del nuevo servicio de seguridad para la **Gestión en explotación del uso de versión de ATIu**".

El adjudicatario tendrá que incorporar estos casos de *test* al Programa de Conformidad y Aceptación de Servicios de Seguridad según el entorno al que aplique (ingeniería, preproducción o producción) y según el componente seguros a cargar estos servicios (SAMs y CHSMs).

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

D. **Revisar, actualizar, optimizar y desarrollar nuevos, en su caso, los casos de *test*** unitarios, test de integración, test de sistema y test de interoperabilidad necesarios para comprobar el correcto funcionamiento de los servicios de seguridad ya implementados en los **componentes de seguridad locales (SAM CBT)** y herramientas asociadas.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica a los Servicios de Seguridad que proporcionan los SAMs CBT y las herramientas asociadas. Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

   Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

E. **Revisar, actualizar, optimizar y desarrollar nuevos, en su caso, los casos de *test*** unitarios, test de integración, test de sistema y test de interoperabilidad necesarios para comprobar el correcto funcionamiento de los servicios de seguridad ya implementados en los **componentes de seguridad centralizados (CHSM)** y herramientas asociadas.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica a los Servicios de Seguridad que proporcionan los CHSM y las herramientas asociadas. Cada uno de estos casos de test se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

   Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

F. **Revisar, actualizar, optimizar y desarrollar nuevos, en su caso, los casos de test** unitarios, test de integración, test de sistema y test de interoperabilidad necesarios para comprobar el correcto funcionamiento de los **servicios de seguridad ya implementados en los componentes de seguridad SUS** y herramientas asociadas. En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de test específicos que aplica a los Servicios de Seguridad que proporcionan los SUS (mecanismos de autenticación, mecanismos de canal seguro, mecanismos de anti -caída, etc.) ya las herramientas asociadas. Cada uno de estos casos de test se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

   Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica en relación con el Programa de Conformidad y aceptación a fin de garantizar el uso interoperable de los Servicios de Seguridad que deberá proporcionar el Sistema de Seguridad único.

3.4.2. Programa de C&A a los componentes SAMs CBT

Así, en relación con las pruebas de aceptación específica complementarias a aplicar a los componentes de seguridad local, SAMs CBT ya las herramientas asociadas, para garantizar en todo momento el cumplimiento de los requerimientos y características técnicas exigidas en todo módulo SAM ABT antes de ser aceptado por a su uso en la T-mobilitat, se realizarán las siguientes tareas:

A. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de aceptación (test unitarios, integración, sistema e interoperabilidad) de **suministro de módulos SAMs CBT** tanto del hardware como del software a lo largo del contrato.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica la aceptación de suministro de SAMs CBT tanto en el hardware como en el software y en las herramientas asociadas. Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en *"scrips*" que permitan ejecutar las pruebas tantas veces como sea necesario.

B. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de **personalización segura de SAMs CBT** a lo largo del contrato, correspondiente a la fase preoperacional.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica la personalización de SAMs CBT para cada uno de los casos de tés unitarios, integración, sistema e interoperabilidad ya las herramientas asociadas para cada uno de los entornos de trabajo (ingeniería, preproducción y producción). Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de test a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "*scrips"* que permitan ejecutar las pruebas tantas veces como sea necesario.

C. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A por la aceptación de actualización de la **capa de abstracción de la seguridad** (SCAL) que incluye la configuración del SCAL desde los SIC, a lo largo del contrato.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que

aplica la gestión de la capa de abstracción de la seguridad (SCAL) y en las herramientas asociadas para cada uno de los entornos de trabajo (ingeniería, preproducción y producción). Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

D. **Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener** el programa de C&A de **monitorización en remoto de los SAMs ABT en explotación** a lo largo del contrato.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de test específicos que aplica la monitorización en remoto de CHSM para cada uno de los casos de tés unitarios, integración, sistema e interoperabilidad y en las herramientas asociadas para cada uno de los entornos de trabajo (ingeniería, preproducción y producción). Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

   Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en *"scrips"* que permitan ejecutar las pruebas tantas veces como sea necesario.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica en relación con el Programa de Conformidad y aceptación a fin de garantizar el uso interoperable de los Componentes de Seguridad local del Sistema de Seguridad único.

3.4.3. Programa de C&A a los componentes CHSM

Así, en relación con las pruebas de aceptación específica complementarias a aplicar a los componentes de seguridad centralizado CHSM ya las herramientas asociadas, para garantizar en todo momento el cumplimiento de los requerimientos técnicos exigidos en todo CHSM antes de ser aceptado para su uso en la T-mobilitat, deben realizarse las siguientes tareas:

A. **Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener** el programa de C&A de aceptación (test unitarios, integración, sistema e interoperabilidad) de **suministro de Centros HSM** tanto del hardware como del software a lo largo del contrato.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica la aceptación de suministro de CHSM tanto en el hardware como en el software y en las herramientas asociadas. Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos

técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de test se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

B. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de aceptación (test unitarios, integración, sistema e interoperabilidad) de la instalación de Centros HSM dentro del correspondiente SIC.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica la aceptación de la instalación de Centros HSM dentro del SIC correspondiente y de las herramientas asociadas. Cada uno de estos casos de test se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

C. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de **personalización segura de CHSM** a lo largo del contrato, correspondiente a la fase preoperacional.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica la personalización de CHSM para cada uno de los casos de tés unitarios, integración, sistema e interoperabilidad ya las herramientas asociadas para cada uno de los entornos de trabajo (ingeniería, preproducción y producción). Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de test a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en *"scrips"* que permitan ejecutar las pruebas tantas veces como sea necesario.

D. Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener el programa de C&A de **monitorización en remoto del CHSM** en explotación, a lo largo del contrato.

En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de t*est* específicos que aplica la monitorización en remoto de CHSM para cada uno de los casos de tés unitarios, integración, sistema e interoperabilidad y en las herramientas asociadas para cada uno de los entornos de trabajo (ingeniería, preproducción y producción). Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en "scrips" que permitan ejecutar las pruebas tantas veces como sea necesario.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica en relación con el Programa de Conformidad y aceptación a fin de garantizar el uso interoperable de los Componentes de Seguridad centralizado del Sistema de Seguridad único.

3.4.4. Programa de C&A de seguridad a los dispositivos móviles NFC

Así, en relación con las pruebas de aceptación específica a los mecanismos de seguridad complementarios implementados en los dispositivos móviles NFC y en las herramientas asociadas, para garantizar en todo momento el cumplimiento de los requerimientos seguridad exigidos a estos dispositivos, deben realizarse las siguientes tareas:

A. **Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener** el programa de C&A para garantizar la seguridad en los **dispositivos móviles NFC**, así como de las herramientas asociadas, a lo largo del contrato.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e identificar explícitamente todos y cada uno de los casos de *test* específicos que aplica a la seguridad que aplica a los dispositivos móviles NFC ya las herramientas asociadas. Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

   Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de test a aplicar en cada ámbito.

   Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en *"scrips"* que permitan ejecutar las pruebas tantas veces como sea necesario.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación al Programa de Conformidad y aceptación a fin de garantizar el uso interoperable de los Componentes de Seguridad por los dispositivos móviles NFC.

3.4.5. Programa de C&A Infraestructura de gestión de claves

Así, en relación con las pruebas de aceptación específica complementarias a aplicar a la Infraestructura de gestión de claves ya las herramientas asociadas, para garantizar en todo momento el cumplimiento de los requerimientos seguridad exigidos en la gestión de las claves criptográfica T-mobilitat, se deben realizar las siguientes tareas:

A. **Revisar, actualizar, mejorar, desarrollar, en su caso, y mantener** el programa de C&A para garantizar los **procesos de gestión de claves criptográficas** en relación con el ciclo de vida de las claves tecnológicas (generación, almacenamiento, distribución, uso y revocación de éstas), así como de las herramientas asociadas a lo largo del contrato.

   En fase de análisis e ingeniería el adjudicatario deberá: analizar, revisar e

identificar explícitamente todos y cada uno de los casos de test específicos que aplica a la gestión de claves criptográficas ya las herramientas asociadas. Cada uno de estos casos de *test* se revisarán y actualizarán, en su caso a lo largo del contrato.

Especial atención debe tenerse en la alineación de los diferentes requerimientos técnicos y especificaciones con los casos de *test* a aplicar en cada ámbito.

Estos casos de *test* se automatizarán en la medida de lo posible, preferentemente en las plataformas de interoperabilidad basadas en *"scrips"* que permitan ejecutar las pruebas tantas veces como sea necesario.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación al Programa de Conformidad y aceptación a fin de garantizar el uso interoperable de los Componentes de Seguridad por los dispositivos móviles NFC.

3.5. Gestión y liderazgo de ESPECIFICACIONES TÉCNICAS del SSu

La gestión de requerimientos técnicos y especificaciones técnicas de obligado cumplimiento, así como los requerimientos funcionales y casos de uso es una tarea esencial del Sistema de Seguridad único que debe implementarse con mucho cuidado y atención, y destinar recursos necesarios debido a la complejidad ya la que es información estrictamente confidencial.

Se requiere una gestión y mantenimiento integral de los requerimientos técnicos y funcionales, así como de las especificaciones técnicas y casos de uso asociadas del Sistema de Seguridad único que incluye los Servicios de Seguridad criptográficos implementados, los componentes seguros y herramientas asociadas en su caso, así como manuales de uso en aquellos casos en que se considere necesario.

La gestión de la documentación del Sistema de Seguridad único requiere un tratamiento de estricta y absoluta confidencialidad dada la información contenida en el mismo.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación a la gestión y control documental del Sistema de Seguridad único T-mobilitat, rol ISO/IEC 24.014, y según lo requerido a lo largo de todo este capítulo.

Así, en relación con la actualización y mantenimiento de las especificaciones técnicas y funcionales del SSu que aplican a los Servicios de Seguridad, a los Componentes seguros ya las herramientas asociadas, y sistema de gestión de claves criptográficas para garantizar en todo momento el cumplimiento de los requerimientos técnicos exigidos, se realizarán las siguientes tareas:

3.5.1. Sistema de Seguridad único – visión general

En este contexto, y en relación con las especificaciones técnicas y funcionales a aplicar al Sistema de Seguridad único como rol ISO/IEC 24.014 desde un punto de vista general, deben llevarse a cabo:

A. **Gestión segura de la documentación del Sistema de Seguridad único, necesaria** para operar el sistema, definiendo las mejores prácticas de confidencialidad, los métodos para garantizarla, cono y quién puede acceder a

la documentación, acuerdos de confidencialidad, etc.

El adjudicatario tendrá que proponer un Plan de trabajo para la gestión documental segura de la documentación del Sistema de Seguridad único T-mobilitat que será aprobado y mantenido por la ATM de Barcelona.

B. Definición y/o descripción del Sistema de Seguridad único que desde un punto de vista global nos dé una **visión transversal** de la protección del sistema de transacciones sin contacto T-mobilitat

C. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los requerimientos y especificaciones técnicos que definen la **plataforma de gestión del Sistema de Seguridad único** para la protección de las transacciones sin contacto T-mobilitat.

El adjudicatario deberá redactar un documento con el fin básico de dar una visión general del Modelo de Seguridad criptográfico para la protección de las Transacciones sin contacto del Sistema Tarifario integrado, así como de los componentes en los que descansa del Modelo de Seguridad Computacional.

D. Definición y/o revisión, en su caso, **mantenimiento y evoluciones de la arquitectura de seguridad** donde se identifica todos los componentes (Módulos de Acceso Seguro -SAM-, Centros de Módulos de Hardware Seguros -CHSM-, Soportes SUS de diversa procedencia, etc.), con relación a la seguridad utilizados para la protección del sistema tarifario integrado, así como el intercambio de información entre ellos.

El adjudicatario deberá especificar y mantener a lo largo del contrato la arquitectura del Sistema de Seguridad único para la protección de las Transacciones sin contacto del Sistema Tarifario integrado, así como de los componentes en los que descansa del Modelo de Seguridad único ISO/ IEC 24.014.

E. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los **casos de uso del Sistema de Seguridad único** donde se identifica las principales interacciones que llevan a cabo entre los diferentes actores que lo utilizan donde se identifica la secuencia de actividades y el resultado esperado, pero no cómo se llevan a cabo estas funcionalidades.

El adjudicatario tendrá que especificar los principales casos de uso del Sistema de Seguridad único para la protección de las Transacciones sin contacto del Sistema Tarifario integrado, así como de los componentes en los que descansa del Modelo de Seguridad único ISO/IEC 24.014.

3.5.2. Servicios de Seguridad de las transacciones sin contacto T-mobilitat

Con relación a las especificaciones técnicas a aplicar a los Servicios de seguridad de las transacciones sin contacto que se cargan en elementos seguros físicos que están distribuidos por todo el Sistema T-mobilitat, deben llevarse a cabo:

A. Definición y/o revisión , en su caso, **mantenimiento y evoluciones** de las **especificaciones técnicas** que definen los **Servicios y mecanismos de**

seguridad desde un punto de vista transversal y entorno de trabajo, en primer lugar, y desde una óptica de seguridad por dispositivos que dan estos servicios como son los Módulos de Acceso Seguros (SAMs CBT), los Centros HSMs, los Soportes de Usuario Sin contacto (SUS), servicios de seguridad a dispositivos móviles NFC y de la infraestructura de claves criptográficas, en segundo lugar.

El adjudicatario deberá redactar y/o actualizar las especificaciones técnicas de los Servicios de Seguridad de las transacciones que cargadas a los elementos seguros proporcionan estos servicios allá donde se necesitan.

3.5.3. Componentes de seguridad local - SAM CBT

Con relación a las especificaciones técnicas para la gestión de los Componentes Seguros SAMs CBT que contienen los Servicios de Seguridad local y que están instalados en todos terminales sin contacto T-mobilitat, deben llevarse a cabo:

A. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los requerimientos y características técnicas que deben cumplir los **Módulos de Seguridad Local** SAMS CBT para ser utilizados en el Sistema Tarifario Integrado T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato los requerimientos técnicos de obligado cumplimiento con relación al Hardware del chip (requerimientos de seguridad, de procesamiento, de comunicaciones, de memoria, de criptografía, etc.), en su identificación única, en las características físicas, en el firmware (kernel) y en los recursos de desarrollo necesarios (emulador, entorno de desarrollo, sistema de carga de kernel, librerías de acceso a periféricos, etc.).

Estos requerimientos y características técnicas son la base para la realización del programa de Conformidad y Aceptación de los Módulos SAMs CBT.

B. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de las especificaciones técnicas que deben cumplir los **Módulos de Seguridad Local** SAMS CBT para ser utilizados en el Sistema Tarifario Integrado T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato las especificaciones técnicas de los módulos de seguridad local SAMs CBT, es decir, información estrictamente confidencial de información sobre la implementación del SAM útil para entender su funcionamiento con los firmwares que contiene, el sistema de arranque, de reprogramación y/o formateado de firmwares, versionado, funcionalidades comunes, control de acceso, comunicaciones, órdenes APDUs, etc.

C. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de definir y especificar el procedimiento de pedidos de **personalización de SAMs CBT**, que incluye toda la información necesaria para la personalización, tanto física como lógica, así particularizar por los requerimientos de seguridad en cada uno de los entornos de trabajo (ingeniería, preproducción y producción).

El adjudicatario tendrá que especificar y mantener a lo largo del contrato el procedimiento de personalizar SAMs que va desde la petición del pedido y autorización del pedido, obtención de los SAMs físicos a personalizar, ejecución

del proceso de personalización (física y lógica), registros, pruebas de aceptación y análisis de resultados, así como la entrega de los SAMs y resolución y seguimientos de incidencias, en su caso.

D. **Definición y/o revisión** en su caso, **mantenimiento y evoluciones** de las especificaciones técnicas que aplican a la implementación y uso de la **Capa de Abstracción de Seguridad de Tarjetas Sin contacto** (SCAL) T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato las especificaciones técnicas que aplican a la Capa 'Abstracción de la Seguridad (SCAL), es decir, información estrictamente confidencial de información sobre la implementación de la SCAL, así como la su configuración, actualización, pruebas de aceptación y elementos y herramientas necesarias.

E. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** del **Manual de uso de Módulos SAMs CBT por integradores** que recopila la información necesaria para que los integradores de ODs T-mobilitat puedan hacer uso de los SUS (lectura y modificación) mediante los servicios proporcionados por los SAMs CBT y los Servidores seguros.

El adjudicatario deberá especificar y mantener a lo largo del contrato del Manual de uso de Módulos SAMs CBT por integradores para hacer el desarrollo de los integradores más fácil y mantener la confidencialidad de partes sensibles, la información que se recopila en este documento será un subconjunto de la documentación completa de los SAM y Servidores Seguros y orientada a su utilización, no a recoger su especificación confidencial de detalle, tan sólo por el uso de los servicios de seguridad que contienen los SAMs CBT.

F. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de los procedimientos y plataforma de **gestión del ciclo de vida de los SAMs CBT** en T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato los procedimientos de gestión del ciclo de vida de los SAMs CBT, es decir, las fases, flujos y estado por que pasan los SAMs en su uso a la T-mobilitat (fase de fabricación, fase preoperacional, fase operacional, fase pos-operacional y fase de destrucción) que describen las etapas, acciones, responsables, etc.

G. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de los procedimientos y plataforma de **gestión de la trazabilidad de los SAMs CBT** en T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato los procedimientos y plataforma de gestión asociada por la trazabilidad y control del SAMs CBT en todas las fases pero especialmente en las fases en las que todavía no están instalados ya que su pérdida es más probable que cuando están instalados y monitoreados en remoto desde los SICs.

3.5.4. Componentes de seguridad centralizada – Centros HSM

Con relación a las especificaciones técnicas para la gestión de los Componentes Seguros CHSM que contienen los Servicios de Seguridad centralizados y que están instalados en todos los Sistemas Informáticos Centrales SICs T-mobilitat, deben llevarse a cabo:

A. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de los requerimientos y características técnicas que deben cumplir los **Módulos de Seguridad Centralizados** CHSM para ser utilizados en el Sistema Tarifario Integrado T-mobilitat.

   El adjudicatario deberá especificar y mantener a lo largo del contrato los requerimientos técnicos de obligado cumplimiento en relación con la plataforma Hardware, donde se ejecutó la plataforma Software que proporciona los servicios de seguridad centralizados, es decir, los requisitos que aplican al conjunto de los equipos que componen los Centros HSM (Servidor host basado en CPU Xeon, equipos de red y placas HSM de seguridad. Que deberá incluir la adquisición (y pruebas de aceptación con acuerdo al programa de aceptación), instalación, puesta en servicio y monitorización.

   Estos requerimientos y características técnicas son la base para la realización del programa de Conformidad y Aceptación de los Centros HSM.

B. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de las especificaciones técnicas que deben cumplir los **Centros HSM** para ser utilizados en el Sistema Tarifario Integrado T-mobilitat.

   El adjudicatario deberá especificar y mantener a lo largo del contrato las especificaciones técnicas de los Centros HSM, es decir, información estrictamente confidencial de información sobre la arquitectura, los componentes hardware y software, flujos, etc., para entender su funcionamiento con los firmwares que contiene, el sistema de arranque, de reprogramación y/o formateado de firmwares, versionado, funcionalidades comunes, control de acceso, comunicaciones, órdenes APDUs, etc.

C. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de definir y especificar los procedimientos de **instalación y gestión de los Centros HSM en explotación**, así como su configuración por el entorno de trabajo corresponden (ingeniería, preproducción y producción).

   El adjudicatario deberá especificar y mantener a lo largo del contrato los procedimientos de instalación y gestión de los Centros HSM, que incluye toda la información necesaria para su instalación y su gestión en remoto de los Centros HSM, que incluye mecanismos seguros de activación remota, la infraestructura de comunicaciones (conexión con el CPD de operador, diseño físico y lógico, direccionalmente IP, etc.), monitorización y administración en explotación.

D. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** del **Manual de uso del Centro HSM por integradores** que recopila la información necesaria para que los integradores de ODs T-mobilitat puedan hacer uso de los SUS (lectura y modificación) mediante los servicios proporcionados por los Centros HSM. El adjudicatario deberá especificar y mantener a lo largo del contrato del Manual de uso de Centro HSM por integradores para hacer el desarrollo de los integradores más fácil y mantener la confidencialidad de partes sensibles, la información que se recopila en este documento será un subconjunto de la documentación completa de los Centros HSM y orientada a su utilización, no a recoger su especificación confidencial de detalle, tan sólo por el uso de los servicios de seguridad que contienen los CHSM.

E. **Definición y/o revisión**, en su caso, **mantenimiento y evoluciones** de los

procedimientos y plataforma de gestión de la monitorización en explotación de los Centro HSM en T-mobilitat.

El adjudicatario deberá especificar y mantener a lo largo del contrato los procedimientos y plataforma de gestión asociada por la monitorización y gestión de alarmas centralizada de todos los Centros HSM en explotación y en todos los entornos de trabajo (ingeniería, preproducción y producción).

3.5.5. Componentes de seguridad por dispositivos móviles NFC

Con relación a las especificaciones técnicas para la gestión de los Componentes de seguridad adicionales por los dispositivos móviles NFC con relación a los Servicios de Seguridad local y centralizados necesarios para la protección de las transacciones realizadas con dispositivos móviles NFC, deben llevarse a cabo:

A. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los requerimientos y características técnicas que deben cumplir los **mecanismos de tokenización, transferencia y almacenamiento de tokens**.

El adjudicatario deberá especificar y mantener a lo largo del contrato los requerimientos y características técnicos de carácter estrictamente confidencial y de obligado cumplimiento en relación con la estructura del Token, accesos, modificaciones seguras, firma, validez, etc.

Los requerimientos y características técnicas tendrán que ser identificados y definidos por el uso del dispositivo móvil NFC:

- Como Soporte de Usuario Sin contacto (SUS), aplicación que llaman NTIU.
- Como Terminal de Interacción con el Usuario (TIU), aplicación que llaman WUS.

B. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de **la arquitectura de seguridad por el uso de dispositivos móviles NFC**, y su utilización de los servicios de seguridad cargados a los componentes seguros locales (SAMs CBT) y centralizados (CHSM), para ser utilizados en el Sistema Tarifario Integrado T-mobilitat.

El adjudicatario tendrá que especificar y mantener a lo largo del contrato la arquitectura de seguridad global de las Apps móviles (NTIU y WUS) y flujos con los elementos de seguridad, así como la arquitectura general del Sistema Tarifario Integrado utilizando los dispositivos móviles NFC y los flujos con los elementos seguros SAMs CBT y CHSM, que deberá incluir la identificación única de los dispositivos móviles NFC, detección de móviles root, implementación de canales seguros por el intercambio de información, períodos de validez de los tokens, entre otros.

C. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** del **Manual de uso de Soportes virtuales por integradores** que recopila la información necesaria para que los integradores de ODs T-mobilitat puedan hacer uso de los SUS (lectura y modificación) mediante los servicios proporcionados por los SAMs CBT y los Servidores seguros.

El adjudicatario tendrá que especificar y mantener a lo largo del contrato del

Manual de uso de Soportes virtuales por integradores para hacer el desarrollo de los integradores más fácil y mantener la confidencialidad de partes sensibles, la información que se recopila en este documento será un subconjunto de la documentación completa de los SAM y Servidores Seguros y orientada a su utilización, no a recoger su especificación confidencial de detalle, tan sólo por el uso de los servicios de seguridad que contienen los SAMs CBT y los CHSM.

3.5.6. Infraestructura de gestión de claves criptográficas

En relación con las especificaciones técnicas para la gestión de claves criptográficas centralizada como base del desarrollo de Servicios de Seguridad computacional robustos que garantice la seguridad de las Transacciones del Sistema Tarifario Integrado, deben llevarse a cabo:

A. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los requerimientos y características técnicas que deben cumplir el **Sistema de gestión de Claves criptográficas** para ser utilizados en el Sistema Tarifario Integrado T-mobilitat y herramientas asociadas a la gestión de las claves criptográficas.

El adjudicatario deberá especificar y mantener a lo largo del contrato los requerimientos técnicos de obligado cumplimiento en relación con la problemática de la gestión de las claves criptográficas, ciclo de vida de las claves, actores y responsabilidades, algoritmos criptográficos a utilizar, etc ., así como de las herramientas asociadas a la generación, almacenamiento y distribución de claves criptográficas.

Deberá incluirse la gestión de claves para cada uno de los entornos de trabajo (ingeniería, preproducción y producción).

B. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de los procesos de inicialización del Sistema de Seguridad único o ceremonia de claves criptográficas por la creación del par de claves pública y privada de la Autoridad Certificadora así como los pares de claves de sus “Security Officers”, y herramientas asociadas a los procesos.

El adjudicatario deberá especificar y mantener a lo largo del contrato los procesos de la ceremonia de generación segura de las claves criptográficas que deberá incluir las diferentes etapas (crear las entidades PKI del sistema, crear claves de gestión, crear los activadores UCC y securizar con los activadores a las entidades PKI).

Habrá que incluir los casos de uso estratégicos como el alta de SAMs y de uCC, personalización de SAMs CBT, etc.

3.5.7. Herramientas de gestión del Sistema de Seguridad único

En relación con las especificaciones técnicas de las herramientas necesarias para la gestión de los Sistema de Seguridad único T-mobilitat, deben llevarse a cabo:

A. Definición y/o revisión, en su caso, **mantenimiento y evoluciones** de la Plataforma de gestión de la seguridad criptográfica o **Gestor de Seguridad** que la herramienta utilizada para la creación de las claves de la Autoridad

Certificadora T-mobilitat que ejecuta una serie de scripts, éstos son los que contienen la lógica y la funcionalidad.

El adjudicatario deberá especificar y mantener a lo largo del contrato el Gestor de Seguridad con relación a las pantallas que tendrán que detallar las funcionalidad y finalidad de cada una de ellas, selección, descripción y ejecución de scripts, versiones, logs, etc.

Deberá incluirse la gestión de claves para cada uno de los entornos de trabajo (ingeniería, preproducción y producción).

3.6. TRATAMIENTO DE RIESGOS del SSu y nuevos desarrollos

Conocer los riesgos a los que están sometidos los elementos o componentes de uso común que integran el sistema de Ticketing T-Mobilitat. Es el primer paso para poder gestionarlos y tomar las mejores decisiones en relación con la seguridad del sistema.

Entendemos como Seguridad del Sistema de Ticketing a la **capacidad para resistir a incidentes de seguridad** (acontecimientos que puedan provocar una interrupción o degradación de los servicios ofrecidos por el sistema) con un determinado nivel de confianza en relación con:

1. **Acciones ilícitas** o malintencionadas,
2. **Accidentes involuntarios,**
3. **Protección de la privacidad** de los datos y el derecho a viajar de forma anónima.

En este contexto, la gestión de la seguridad está basada en un proceso continuo **de análisis y la gestión correspondiente de los riesgos**:

- El **Análisis de riesgos del negocio** es parte esencial del proceso de seguridad sobre el que se construyen los planes de acciones para la mejora continua de la protección del sistema.
- Una vez obtenida la foto exacta de los riesgos, podemos establecer medidas de salvaguardia con el objetivo de reducirlos a un nivel que el Sistema considera aceptable. Este proceso se llama **Gestión de los riesgos**.

Aunque la caracterización del Sistema de Gestión de la Seguridad de la información (SGSI), identificación de activos, análisis y gestión de los riesgos no forman parte de esta licitación, si lo está, el **tratamiento del riesgo residual** una vez implementadas las salvaguardias de seguridad que son desarrolladas e implementadas por el SSu a fin de tener y mantener en el tiempo los riesgos dentro de un nivel aceptable.

La gestión del Tratamiento de riesgos del Sistema de Seguridad único incluye la asistencia técnica a la identificación, análisis y viabilidad de nuevos servicios de seguridad necesarios a implementar, nuevas evoluciones del Sistema de Seguridad único en explotación, así como de las herramientas asociadas a la plataforma de seguridad con el objetivo de mantener los riesgos de seguridad residual en límites aceptables.

Así, en relación con el tratamiento de riesgos residuales del SSu para mantenerlos dentro de unos niveles ricos aceptables, deben realizarse las siguientes tareas:

A. **Desarrollo y puesta en servicios de salvaguardias,** o paquetes de salvaguardias, para contrarrestar las nuevas amenazas que aparezcan a lo largo

del contrato, y que aplican sobre los activos de uso común (Interfaz de RF, SUS, TIU, Claves del SSu y Registros transaccionales).

El adjudicatario tendrá que desarrollar y/o mejorar las acciones recomendadas reales para contrarrestar amenazas de seguridad que puedan poner en peligro la seguridad de las transacciones sin contacto T-mobilitat a lo largo del contrato y que sean necesarias para mantener los riesgos a niveles asumibles.

Deberán implementarse las salvaguardias necesarias que apliquen sobre los activos de uso común para cada uno de los entornos de trabajo (ingeniería, preproducción y producción).

Dado que se desconocen las salvaguardas a implementar, debido a las nuevas amenazas que pudieran aparecer a lo largo del proyecto, así como la posible necesidad de implementar nuevos desarrollos (nuevos servicios de seguridad, nuevas funcionalidades, nuevas herramientas, etc.) establecen una bolsa de horas a consumir previa autorización de la autoridad de confianza.

3.7. Gestión y LIDERAZGO INTEGRAL del SSu, rol ISO/IEC 24.014 dentro del MTC

Dada la especialización y complejidad del Sistema de Seguridad único (SSu) basado en implementar las mejores prácticas de seguridad criptográfica se requiere que el adjudicatario gestione y lidere el funcionamiento transversal en explotación del SSu.

En este sentido, deberá conducir las reuniones técnicas ya sea con el equipo técnico del ATC y otros actores en temas de seguridad criptográfica del SSu, guiar el análisis de problemas y propuestas de solución, proponer evoluciones de mejora del SSu, etc .

En cualquier caso, corresponde a la ATM como Autoridad de Confianza aprobar cualquier cambio en el SSu.

La gestión y liderazgo integral del funcionamiento transversal del entorno de seguridad compartido T-mobilitat incluye la asistencia técnica a la identificación, análisis y viabilidad de nuevos servicios de seguridad necesarios a implementar, nuevas evoluciones del Sistema de Seguridad único en explotación, así como de las herramientas asociadas a la plataforma de seguridad. El objetivo es proporcionar permanentemente los Servicios de Seguridad necesarios para garantizar la seguridad de las transacciones T-mobilitat.

Así, en relación con la gestión y liderazgo integral del funcionamiento transversal del Sistema de Seguridad único, deben realizarse las siguientes tareas:

A. **Asistencia técnica y liderazgo** en la **gestión transversal Sistema de Seguridad único** como rol ISO/IEC 24.014, desde un punto de vista transversal e integral para mantenerlo en explotación en los niveles de seguridad mínimos requeridos, así como evolucionarlo mantener estos niveles de seguridad.

   El adjudicatario tendrá que liderar a lo largo del contrato la gestión, control y evolución de los Servicios de Seguridad del SSu , de la gestión en explotación de los componentes físicos seguros que proporcionan los Servicios de seguridad tanto locales o centralizados, de la infraestructura de claves criptográficas, de la gestión del Programa de Conformidad y aceptación del SSu, de las especificaciones técnicas corresponden, de implementar nuevas salvaguardias,

en su caso, de las herramientas asociadas, etc.

La gestión transversal incluye todos los entornos de trabajo (ingeniería, preproducción y producción).

Aunque el adjudicatario tendrá que liderar esta gestión transversal e integral del SSu la aprobación de todas las acciones propuestas tendrán que ser realizadas por ATM.

3.8. Módulo de GESTIÓN DE FRAUDE

El Sistema de Seguridad único permite proteger todas y cada una de las transacciones sin contacto T-mobilitat cuyo resultado son los registros transaccionales comunes que se envían al SIC-ATM.

En este contexto, es necesario implementar un módulo para la gestión del fraude que deberá implementar funciones específicas para la detección, gestión y control de posibles fraudes a diferentes niveles (tarjetas no reconocidas por el sistema, SAM no autorizados, descompensaciones de Ventas (Recargas) y Validaciones, etc.).

Esta gestión y análisis del fraude deberá permitir la definición de alarmas de detección de posible fraude (robo de equipos de recarga, robo de SAMs, uso de soportes sin contacto no autorizados, o robados, etc.).

Como respuesta a los posibles casos de fraude deberán implementarse los mecanismos de protección correspondientes como el bloqueo o anulación de Tarjetas sin contacto, bloqueo o anulación de la Aplicación de Transporte Interoperable única, bloqueo o la anulación de la identificación Usuario-Tarjeta, blog o la anulación de Perfiles de usuario y el bloqueo o la anulación de la Carga asociada a un título.

Estos mecanismos se podrán llevar a cabo por operativas dinámicas habilitadas en el sistema o mediante listas de acción.

Este módulo hará uso de estos mecanismos para defender el sistema de estos ataques.

Así, en relación con el diseño, desarrollo e implantación del módulo de gestión del fraude, deben realizarse las siguientes tareas:

A. Diseñar, desarrollar e implementar un módulo para gestionar el fraude mediante el análisis y búsqueda sistemática de incoherencias en el uso del sistema tarifario integrado T-mobilitat.

El adjudicatario deberá diseñar, desarrollar, probar y poner en servicio un módulo para la gestión posibles fraudes posibles fraudes y búsqueda de incoherencias en el uso del Sistema Tarifario integrado que proporcione información sistemática para el control y mejora del sistema T -movilidad.

Este módulo deberá correr en el Servidor host del Centro HSM, deberá permitir su permanente actualización en caliente, ser modular de forma que permita incorporar fácilmente nuevos análisis sistemáticos, la generación de informes sistemáticos y visualización de resultado en tiempo casi real.

En lista no exhaustiva, este módulo debe incluir, entre otras, las siguientes funcionalidades:

- Controlar y avisar de retrasos en el suministro de datos de determinados equipos.
- Verificación de la existencia de carga asociada a un título concreto anterior a la ejecución de Validaciones realizadas en el título, así como comprobación de la coherencia de importe adeudado y las validaciones realizadas.
- Verificación de SAM de carga registrado y activo con el que se realizó la carga asociada al título con el SAM con el que se valida para cada consumo del título. Si un SAM no está registrado y activo se incluirá en lista negra.
- Control de tiempos máximos entre el establecimiento de la comunicación y de retraso en suministro de datos de los equipos de carga con el sistema central por bloqueo del equipo en caso de que supere ese tiempo.
- Otros controles y acciones parametrizables en función de posibles fraudes que puedan aparecer.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación a la arquitectura, funcionalidades y herramientas asociadas para la gestión del fraude mediante el análisis y la búsqueda sistemática de incoherencias en el uso del sistema tarifario integrado T-mobilitat, que servirá de valoración para la adjudicación.

3.9. Exportación de DATOS DEL SIC

La gestión de fraude del Sistema Tarifario Integral requiere disponer de los datos de las transacciones realizadas en T-mobilitat en tiempo casi real.

En este contexto, es necesario implementar un módulo para la exportación de datos del SIC que nos permita disponer de los registros transaccionales sin contacto consolidados.

En este caso, deberá proponerse posibles canales de exportación de registros transaccionales vía oráculo a Kafka y/o vía CHSM a Kafka, así como con la recogida, almacenamiento y publicación de información para su consumo por otros actores, entre los cuales existe el módulo de gestión del fraude.

Así, en relación con la exportación, almacenamiento y publicación de datos de las transacciones sin contacto T-mobilitat, se realizarán las siguientes tareas:

A. Diseñar, desarrollar e implementar un módulo para gestionar la exportación de datos del SIC que nos permita disponer de los registros transaccionales sin contacto consolidados.

El adjudicatario tendrá que diseñar, desarrollar, probar y poner en servicio un módulo para la exportación de datos del SIC y puesta a disposición de estos datos a los actores autorizados, analizando posibles alternativas y desarrollando las herramientas necesarias para la publicación de registros del Sistema Tarifario Integrado vía Kafka, por ejemplo, mecanismos de recogida, almacenamiento y publicación también vía Kafka, y desarrollos por el análisis de datos para sacar conclusiones, estar mejor equipadas para tomar decisiones estratégicas y dar servicios de movilidad de acuerdo a las necesidades de los clientes del transporte público.

Este módulo deberá correr en el Servidor host del Centro HSM, deberá permitir su permanente actualización en caliente, ser modular de forma que permita incorporar fácilmente nuevos análisis sistemáticos, la generación de informes sistemáticos y visualización de resultado en tiempo casi real.

El licitador deberá especificar de forma amplia y detallada su propuesta técnica con relación a la arquitectura, funcionalidades y herramientas asociadas para la exportación de datos de uso del Sistema Tarifario Integrado T-mobilitat, que servirá de valoración para la adjudicación.

4. FINALIDADES Y OBJETIVOS A ASUMIR

Las finalidades y objetivos que deben alcanzarse mediante la realización de este contrato son los siguientes:

4.1. Principios básicos para cumplir

La presente licitación se sustenta en unos principios básicos que orientan el siguiente contenido:

- **Protección de las transacciones sin contacto T-mobilitat**

  El principal objetivo del Sistema de Seguridad único es articular un marco de trabajo común, confidencial, compartido con los distintos operadores del sistema T-mobilitat y liderado por la ATM para conseguir la permanente protección del sistema tarifario integrado basado en la tecnología sin contacto de proximidad.

- **Gestión integral de la seguridad de las transacciones sin contacto**

  El principal objetivo de la presente licitación es mantener y evolucionar el Sistema de Seguridad único T-mobilitat, a través de gestionar en explotación los Servicios de Seguridad cargados en los componentes de seguridad locales (SAM CBT), los centralizados (CHSM) y la infraestructura de claves criptográficas que lo sustenta.

- **Integración Tecnológica Intersectorial**

  La Solución tecnológica estará diseñada para confluir de forma interoperable con tecnologías de diversa procedencia (del suministro de chips seguros, de la telefonía móvil y del transporte) en un único terminal de comunicación sin contacto de proximidad.

- **Solución Tecnológica innovadora**

  La solución tecnológica para implementar será propuesta y adaptada por la ATM y los Operadores específicamente a las necesidades del Transporte Público con relación a la utilización de chips de diferentes fabricantes de silicio, con relación a la utilización de operativas dinámicas modificable en caliente ya la utilización de la capa de abstracción de la seguridad (SCAL) que requiere nuevos mecanismos de seguridad.

- **Gestión y Control completo desde T-mobilitat**

  El diseño tecnológico de la solución deberá permitir la gestión y control completo de los Servicios de Seguridad actualizables en caliente desde los Sistemas Informáticos Centrales.

- **Potente programa de Conformidad y Aceptación**

  Con el desarrollo y evolución de un potente programa de pruebas de aceptación de los componentes y procesos online con la responsabilidad operativa del Sistema de Seguridad único.

5. SEGUIMIENTO Y CONTROL DE LAS CONDICIONES DEL CONTRATO

5.1. Descripción de la forma de prestación del servicio

Se describe en este apartado los requisitos que deben cumplirse en relación con la ejecución del Proyecto para la *"Gestión integral del Sistema de Seguridad único T-mobilitat en explotación, rol ISO/IEC 24.014, e implementación de nuevas funcionalidades".*

El licitador deberá proponer, especificar y describir con detalle su propuesta de implantación de todas las actividades y funciones a realizar por el adjudicatario identificadas en el apartado 3 de estos pliegos donde se tendrán que marcar las metas, tareas relacionadas y entregables.

Cualquier otro proyecto o actividad que impacto en el desarrollo del proyecto se integrará en el plan propuesto por el Adjudicatario, de acuerdo con ATM.

5.1.1. Planificación del Proyecto

En lo que concierne al desarrollo del proyecto, se describen a continuación a modo de referencia las fases a desarrollar por parte de la empresa que resulte adjudicataria de esta licitación, así como otros aspectos esenciales para el proyecto.

5.1.1.1. Fase de Planeamiento

En lo que concierne al desarrollo del proyecto, se describen a continuación a modo de referencia las fases a desarrollar por parte de la empresa que resulte adjudicataria de esta licitación, así como otros aspectos esenciales para el proyecto.

5.1.1.2. Fase de Análisis y Ingeniería

En esta fase se analiza el contenido de los trabajos a realizar, adaptar y/o evolucionar los nuevos servicios de seguridad a implementar, módulos y componentes a los que afectan, su rendimiento, validez funcional frente a las necesidades actuales y futuras, la mantenibilidad, así como especificaciones técnicas, herramientas de trabajo asociadas, etc.

Esta fase debe tener una duración muy limitada en el tiempo.

El objetivo genérico de esta fase es el análisis de los trabajos contratados y concretarlos en los puntos necesarios, ampliando y mejorando los aspectos que sean necesarios. Es decir, el adjudicatario junto con la ATM (MTC) concretará el proyecto presentado a la oferta, ampliando y mejorando el detalle de aquellos puntos que se consideren necesarios.

A la finalización de esta fase, se dispondrá de la definición concreta, detallada y acordada de todos y cada uno de los servicios e ingeniería y asistencia técnica en relación con el servicio de gestión integral del Sistema de Seguridad único en explotación, así como el plan de trabajo en relación con los nuevos servicios de seguridad a implementar.

5.1.1.3. Fase de desarrollo

La finalidad de esta fase es el desarrollo y adaptación de los diferentes sistemas, de los módulos y componentes planificados de los nuevos servicios de seguridad a implementar identificados una vez actualizado, acordado y aprobado en la fase anterior.

Se inicia con la aceptación de la documentación de la solución a implementar y finaliza con la aceptación explicita por parte de ATM de los trabajos realizados.

Esta fase finaliza con la implantación y aceptación de los nuevos servicios de seguridad ya implementados en la T-mobilitat a nivel de preproducción.

5.1.1.4. Fase de despliegue

La finalidad de esta fase se llevará a cabo el despliegue, puesta en servicio e integración de los nuevos servicios de seguridad desarrollos y aceptados a nivel del entorno de preproducción.

Esta fase se inicia con la validación de los desarrollos realizados a nivel de preproducción y finaliza con la Aceptación Provisional de los servicios de seguridad implementados después de un período de funcionamiento sin errores.

Durante la fase de despliegue, en caso de encontrarse errores se ejecutarán los procedimientos definidos en la gestión de modificaciones en fase de despliegue, pudiendo llegar a detener el proceso de instalación y/o aceptación.

5.1.1.5. Fase de explotación

La finalidad de esta fase es asegurar el buen funcionamiento de todos los Servicios de Seguridad criptográficos dentro del Sistema de Seguridad único T-mobilitat para la protección de las transacciones sin contacto y otros servicios de seguridad implementados realizando un seguimiento y control del funcionamiento de todos y cada uno de los servicios, así como garantizar su evolución y mantenimiento a lo largo del resto del contrato.

Esta fase se inicia una vez finaliza el despliegue con relación a los nuevos servicios de seguridades desarrollados ya la firma del contrato en relación con la gestión integral del Sistema de Seguridad único en el resto de los Servicios de Seguridad ya en explotación.

5.2. Medios Técnicos y Materiales

Se describe aquí los medios técnicos que el adjudicatario deberá tener adscritos a la ejecución del contrato.

5.2.1. Infraestructura necesaria para llevar a término el proyecto

La empresa adjudicataria dispondrá de instalaciones propias adecuadas para dar cabida al equipo de proyecto, así como infraestructuras suficientes para permitir y facilitar su trabajo.

En caso de ser necesario, la ATM podrá requerir puntualmente que el equipo de proyecto de la empresa adjudicataria trabaje en las instalaciones de la propia ATM o en cualquier otra instalación que se adecue para tal efecto.

El licitador realizará una descripción que identifique la infraestructura necesaria, contenido, laboratorios, ubicación, del soporte técnico, los elementos informáticos y la base documental relacionada disponible y adscritos a la ejecución del Proyecto que

servirá de valoración para la adjudicación.

5.3. Recursos humanos

Dado que el objeto del contrato trata de un proyecto intersectorial con una solución tecnológica innovadora, única y transversal a todo el sistema con una fuerte dependencia con el modelo tarifario integrado actual T-mobilitat ya en explotación, se requiere:

a) Director/a ejecutivo/a del proyecto

- El Proyecto deberá ser dirigido y realizado por un experto con una experiencia suficiente demostrada en proyectos similares que garantiza la colaboración intersectorial necesaria, la comunicación, el trabajo en equipo, la resolución de problemas y conflictos, la gestión del tiempo y habilidades de liderazgo.

  El ***"Project Manager"*** o director/a ejecutivo/a del Proyecto es la persona encargada de alcanzar los objetivos del Proyecto cumpliendo los objetivos de tiempo, costes y funcionalidades. Deberá identificar y responder a los riesgos que surjan durante la ejecución del mismo y será el responsable de la comunicación con todos los actores que intervienen en el Proyecto.
- Para el rol de director/a ejecutivo/a del proyecto se requiere, además de los conocimientos propios de dirección de proyectos, de flexibilidad, buen juicio, fuerte liderazgo y habilidades para la negociación.
- El director/a ejecutivo/a propuesto para la dirección del proyecto de esta contratación deberá integrarse de forma activa en los grupos de trabajo que correspondan con relación a cualquier aspecto identificado con el proyecto que la dirección de T-mobilitat estime necesario.
- Con relación a su experiencia profesional, deberá haber dirigido y realizado al menos un proyecto de contenidos similares.

  La experiencia profesional y la dedicación mínima estimada que se exige al director ejecutivo del proyecto es la siguiente:

Perfil	% Dedicación mínima	Experiencia/Conocimientos
Director/a del Proyecto	5%	Titulación universitaria de ingeniero superior informático, de telecomunicaciones o industrial y con una experiencia de al menos 5 años en dirección de proyectos técnicos en proyectos tecnológicos similares.
		Deberá disponer: • conocimientos específicos en desarrollo de Sistemas de Seguridad criptográfica aplicado a Sistemas de Ticketing sin contacto de proximidad y • experiencia demostrada en el desarrollo y la implementación de proyectos de Sistema de Ticketing sin contacto de proximidad de características similares a este proyecto en relación con la Seguridad de las transacciones sin contacto utilizando elementos seguros SAMs y CHSMs.

Tabla 1: Experiencia/Conocimientos del director/a ejecutivo del proyecto.

b) Director/a técnico/a del proyecto

- A nivel técnico, el proyecto deberá ser dirigido y ejecutado por un experto en el desarrollo de Terminales basado en tecnología sin contacto de proximidad por inducción electromagnética con amplia y demostrada experiencia en el desarrollo e implementación de proyectos de Sistema de Ticketing electrónico sin contacto que utilicen elementos seguros locales (SAMs) y elementos seguros centralizados (Centros HSMs) para garantizar la seguridad de los sistemas de billete sin contacto.

  El ***"Technical Manager"*** es la persona responsable de ejecución del proyecto, por tanto es requisito necesario que sepa utilizar las herramientas adecuadas, optimizar la manera de utilizar los recursos y aportar las soluciones técnicas más idóneas.

- Para el rol de director/a técnico/a del proyecto se requiere, además de los amplios conocimientos específicos, capacidad de relación, capacidad para liderar y dirigir grupos de trabajo técnico.

- El director/a técnico/a propuesto para la ejecución del proyecto de esta contratación deberá integrarse de forma activa en los grupos de trabajo que correspondan con relación a cualquier aspecto identificado con el proyecto que la dirección de T-mobilitat estime necesario.

- Con relación a su experiencia profesional, deberá haber dirigido y realizado al menos un proyecto de contenidos similares

  La experiencia profesional y la dedicación mínima estimada que se exige al director técnico del proyecto es la siguiente:

Perfil	% Dedicación mínima	Experiencia/Conocimientos
Director/a Técnico/a del Proyecto	10%	Titulación universitaria de ingeniero superior informático, de telecomunicaciones o industrial y con una experiencia de al menos 5 años en dirección de proyectos técnicos que hayan implementado Sistemas de Seguridad criptográfica aplicada a los Sistemas de Ticketing sin contacto de proximidad utilizando elementos seguros locales SAMs y centralizados como centros HSMs.
		Deberá disponer: • conocimientos específicos en desarrollo de Terminales basado en tecnología sin contacto de proximidad y • experiencia demostrada en: o Sistemas de radiofrecuencia de proximidad (ISO/IEC 14.443 y NFC), o Soportes de Usuario Sin contacto (SUS PVC, SUS Cartón y dispositivos móviles NFC como SUS virtual), o Terminales de Interacción con el Usuario (TIUs dedicados y dispositivos inteligentes NFC como terminal), o Sistemas de Ticketing sin contacto, en Seguridad física y lógica (en Ticketing de Transporte contactless) utilizando elementos seguros (SAMs y HSMs).

Tabla 2: Experiencia/Conocimientos del director/a técnico/a del proyecto.

El Adjudicatario deberá garantizar la continuidad de los técnicos propuesto durante todo el plazo de ejecución de los trabajos.

Cualquier cambio deberá ser autorizado previamente por la ATM.

Los posibles cambios o modificaciones en la composición del equipo tendrán que ser comunicados por escrito a la ATM con la debida antelación y aceptados por ésta.

En este supuesto, el adjudicatario deberá proponer a una/s persona/s con la formación y experiencia requerida en la licitación, teniendo en cuenta las características de la persona del equipo valorada en la licitación, de acuerdo con su oferta.

Adicionalmente, en caso de sustituir al Director ejecutivo/a y/o el Director técnico/a del proyecto propuesto, se exigirá lo siguiente:

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

Aparte de estos dos perfiles, se requiere de un equipo más amplio que intervendrá en la realización de los trabajos.

c) Equipo de trabajo

Es necesario que el licitador incluya en su propuesta el equipo que se adscribirá a la ejecución del contrato indicando:

- el historial profesional detallado de cada uno de sus miembros,
- aportando los Currículum Vitae de los miembros del equipo de trabajo asignado,
- la dedicación mínima estimada para a cada perfil (excluidos los perfiles de director/a ejecutivo del proyecto i del director/a técnico/a, así como,
- su responsabilidad dentro del proyecto.

IMPORTANTE: NO se podrán incluir en los sobres A y B, ni los currículum, ni la titulación académica, ni los certificados de ejecución de los perfiles ofrecidos como Director/a ejecutivo/a o como Director/a Técnico/a del Proyecto

Tampoco se podrá presentar esta misma documentación en el sobre A con respecto al equipo de soporte.

El incumplimiento de esta condición será causa de exclusión de la licitación.

5.4. Metodología para aplicar

A fin de garantizar un adecuado proceso de gestión integral del Sistema de Seguridad único T-mobilitat en el área integrada de Barcelona y los desarrollos, aceptación y puesta en servicio de los nuevos servicios de seguridad con todas las garantías de

funcionamiento durante la fase de desarrollo en el entorno de ingeniería, en la fase de pruebas e integración en el entorno de preproducción y en la operación real en el entorno de producción, es necesario establecer una metodología de trabajo con un enfoque disciplinado y sistemático para dar los servicios solicitados, así como los desarrollos identificados en este proyecto.

Se entiende por metodología propuesta como el conjunto de procesos, técnicas, herramientas y soporte documental que ayuda a los desarrolladores a realizar y poner en servicio el nuevo software.

En este sentido de actuación se valorará:

- Con relación a los **servicios de gestión integral** del Sistema de Seguridad único T-mobilitat:
  - Existencia de pautas de trabajos sistemáticas: nivel de servicio, gestión de la capacidad, continuidad de los servicios, gestión de cambios y/o ampliaciones funcionales y técnicas, monitorización de los servicios y reporting.
  - Cobertura completa del ciclo de vida de los servicios de seguridad: pasos a realizar desde la detección de cualquier alteración del servicio, su clasificación y registro, asignar responsables hasta los planteamientos sistemáticos por su resolución.
  - Gestión del equipamiento de seguridad: procesos de actuación sistemáticos en relación con el mantenimiento preventivo y correctivo, garantizar disponibilidad, resolución eficiente de incidencias y problemas.
- En relación con el **desarrollo** de los nuevos servicios de seguridad a implementar:
  - Existencia de reglas preestablecidas: etapas, fases, tareas, entregas intermedias, técnicas y herramientas utilizadas.
  - Cobertura completa del ciclo de desarrollo: pasos a realizar desde el planteamiento hasta la aceptación del producto por parte de ATM.
  - Verificaciones intermedias: sobre los entregables de cada fase para comprobar su corrección.
- Con relación a la **integración** de los nuevos servicios de seguridad en T-mobilitat:
  - Enlace con los procesos de gestión: pautas o recomendaciones para enlazar las actividades de desarrollo técnico del Software con las actividades propias de la gestión global del proyecto.
  - Comunicación efectiva: directrices de comunicación efectiva entre los desarrolladores para facilitar el trabajo en grupo que facilite la coordinación de acuerdos consensuados.

Todos los datos numéricos y gráficos entregarán en formato MS-Excel, las presentaciones en MS PowerPoint, los documentos en MS Word y las planificaciones en MS-Proyectos.

En este contexto:

- El licitador tendrá que especificar la metodología seguida en el desarrollo del proyecto.

  Esta metodología deberá asegurar la implicación y participación activa con todos

los organismos, instituciones y unidades afectados por el proyecto de definición e implementación del modelo de operaciones a todos los niveles, de manera que ello facilite que se llegue a propuestas consensuadas.

- El adjudicatario deberá alinear su metodología propia de desarrollo de SW con metodología propia del Modelo Tecnológico Común T-mobilitat ya en explotación, en relación con:
  - Desarrollo del software,
  - La integración con la T-mobilitat.

5.5. Organización de la ejecución del proyecto

Con independencia de la estructura y organización interna del proyecto de gestión integral del Sistema de Seguridad única, rol ISO/IEC 24.014, en el área integrada de Barcelona, la coordinación y supervisión de los trabajos técnicos relacionados con la presente licitación recaerá en el director /a técnico/a propuesto por la empresa licitadora, previa supervisión del responsable de este proyecto nombrada por la Dirección de la T-mobilitat.

Son estos dos perfiles los únicos interlocutores para el diseño, desarrollo, ejecución, aceptación, despliegue, puesta en servicio y servicios tecnológicos en explotación del proyecto de comercialización de los canales externos T-mobilitat, evitando, de este modo, informaciones cruzadas y gestiones inconclusas por cambio de asignación de las distintas cuestiones que surjan a lo largo del desarrollo de este proyecto.

En fase de análisis e ingeniería el director/a del proyecto y el responsable del contrato detallarán por escrito las reglas de trabajo que garantice la coordinación de la ejecución del proyecto, las reuniones periódicas de seguimiento, equipos de seguimiento, informes periódicos, etc.

También se regulará el seguimiento y control de la ejecución del proyecto por parte de ATM y cómo se darán las instrucciones y directrices necesarias al adjudicatario.

5.5.1. Control y seguimiento y seguimiento del proyecto

- El adjudicatario será el responsable de realizar las tareas de dirección del proyecto para la gestión integral del Sistema de Seguridad único bajo las directrices del Marco Tecnológico Común, rol ISO/IEC 24.014, para el área integrada de Barcelona.
- El director/a de proyecto informará periódicamente del avance y contratiempo del proyecto según se especifique en el plan de proyecto.
- El adjudicatario entregará informes bimensuales en formato digital en el que describirá el grado de avance del proyecto. En estos informes se incluirán, entre otros, los siguientes aspectos:
  - Resumen de las tareas realizadas durante el período
  - Actividades previstas para la siguiente
  - Riesgos y desviaciones
  - Estado actual de la planificación.

- ATM podrá, en cualquier momento, realizar controles y solicitar informes de seguimiento de los trabajos realizados.

5.5.2. Plazos de ejecución

El plazo de ejecución del contrato de la presente licitación será dieciocho meses desde la fecha de formalización del contrato.

Se establecerá un régimen de entregas parciales según las fases y fechas previstas de estas entregas.

Las franjas de tiempo previstas en las tablas que constan en este apartado son de obligado cumplimiento por razones de financiación.

El adjudicatario está obligado durante el desarrollo del proyecto a implementar cuantas medidas sean necesarias para recuperar los posibles retrasos que existan.

El adjudicatario está obligado a informar de forma permanente de cualquier circunstancia que pueda provocar un retraso en el cumplimiento del contrato, así como proponer las medidas mitigadoras para corregir esa circunstancia.

5.5.2.1. Calendario

Las fases y fechas previstas son preceptivas y las franjas de tiempo previstas en la siguiente tabla son de obligado cumplimiento.

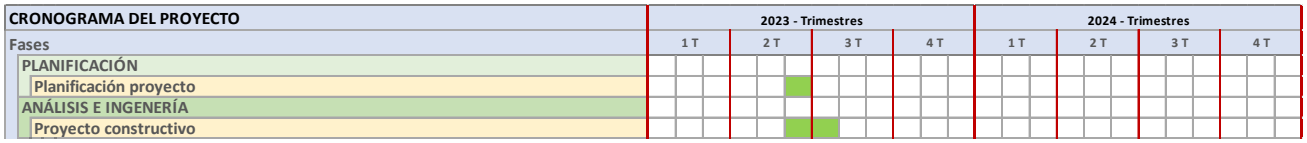
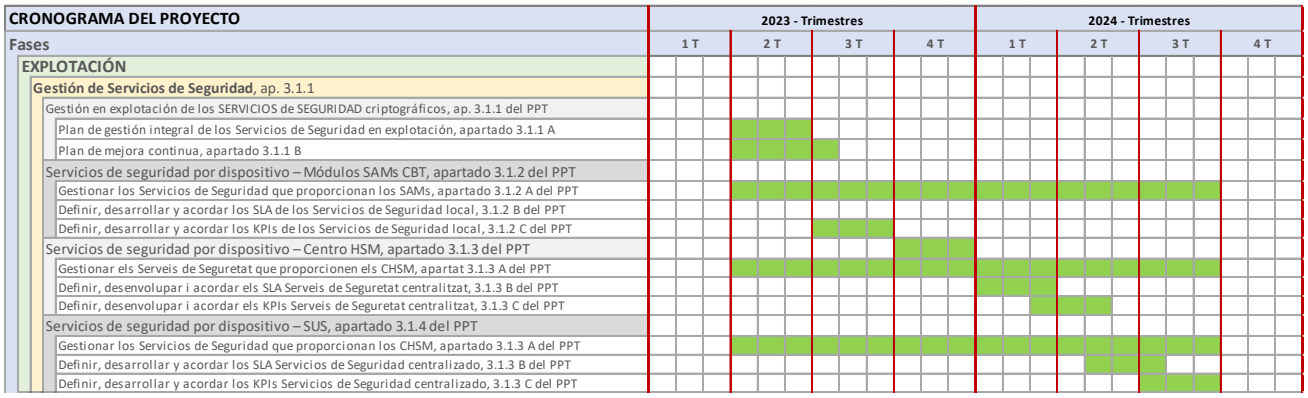


Imagen 2: Planificación y Análisis y ingeniería



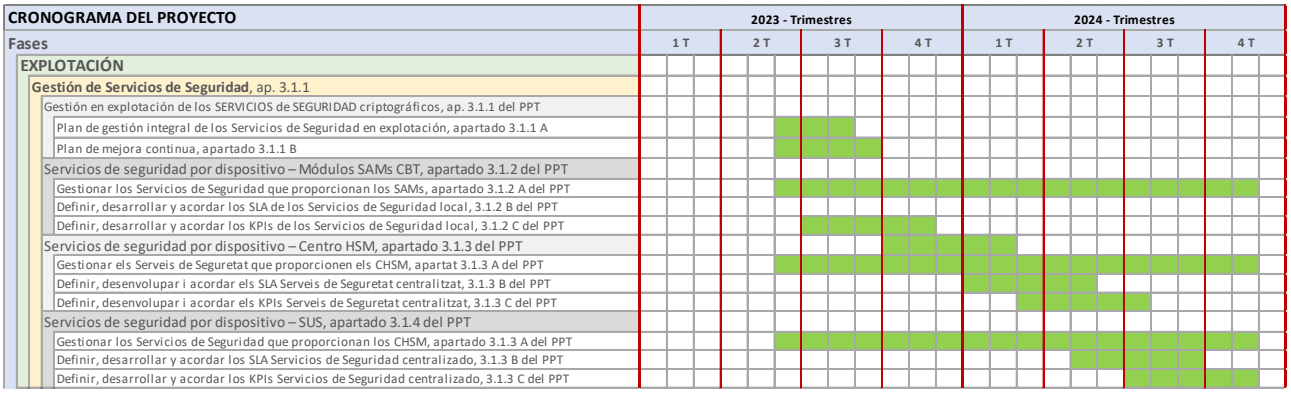


Imagen 3: Explotación – Gestión de Servicios de Seguridad

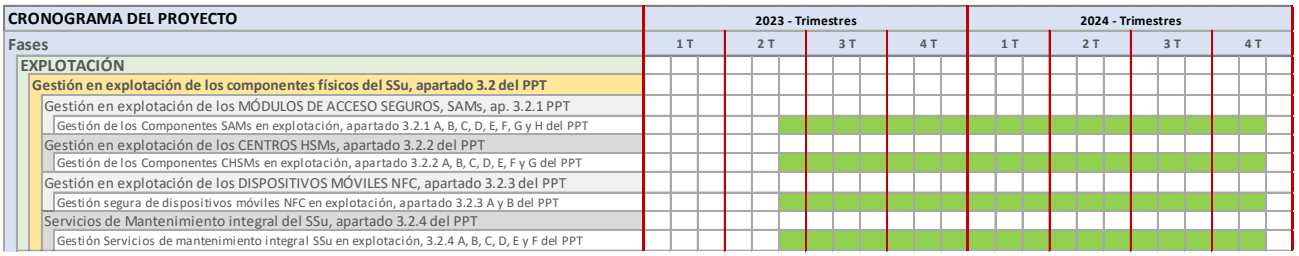


Imagen 4: Explotación – Gestión de Componentes de Seguridad

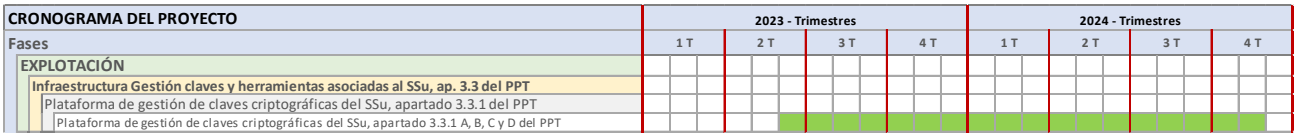


Imagen 5: Explotación – Gestión de Claves criptográficas de Seguridad

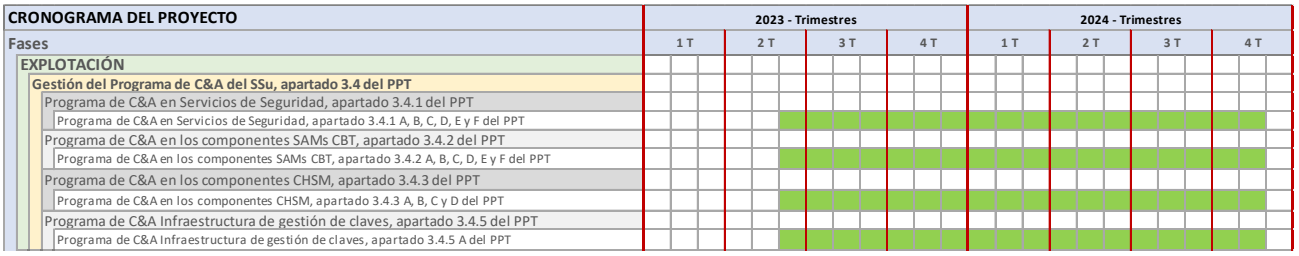


Imagen 6: Explotación – Gestión de la Conformidad y Aceptación de los componentes del SSu

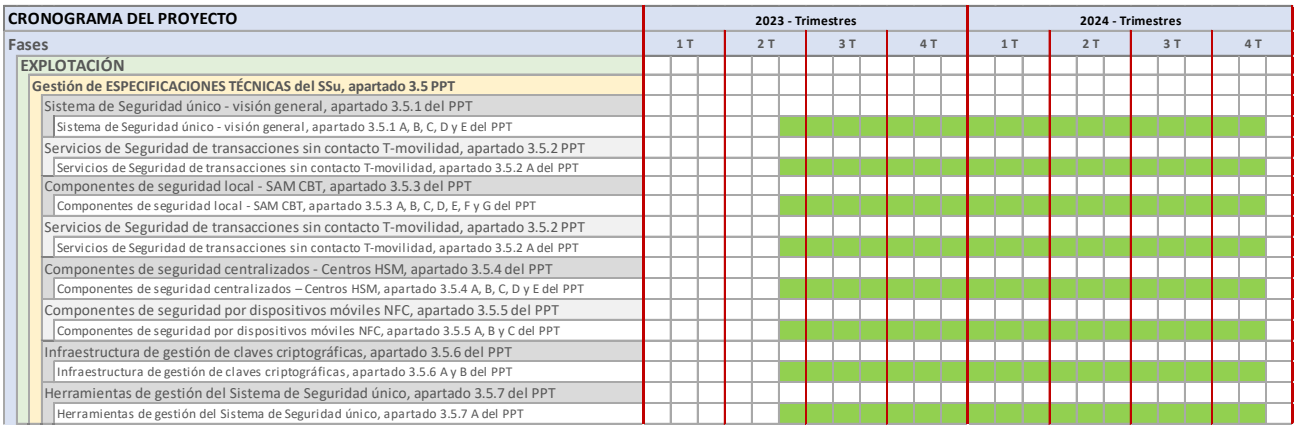


Imagen 7: Explotación – Gestión de requerimientos y especificaciones técnicas del SSu

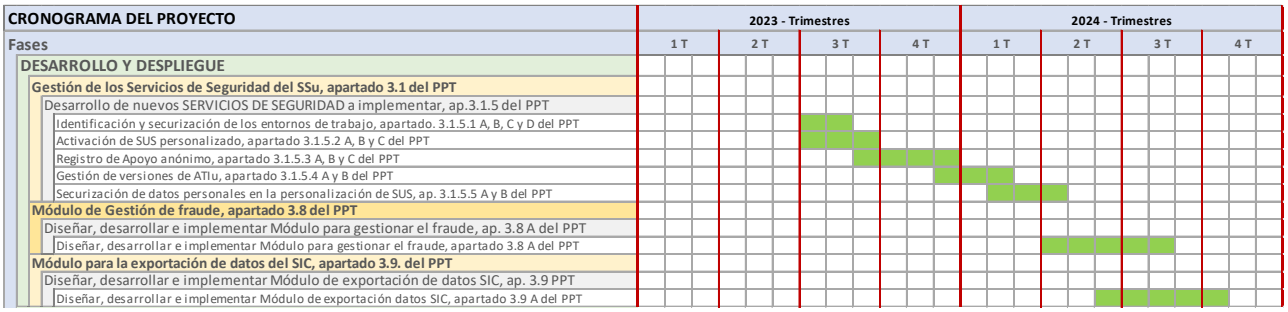


Imagen 8: Desarrollo y despliegue de nuevos Servicios de seguridad y nuevas funcionalidades

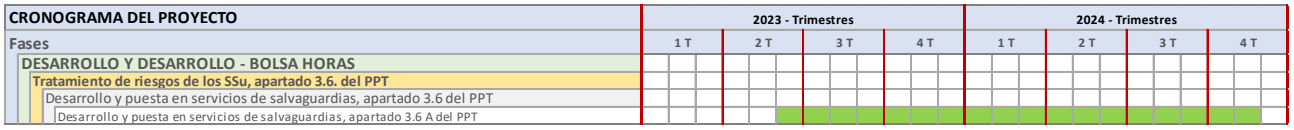


Imagen 9: Desarrollo y despliegue de Salvaguardas y nuevos desarrollos – BOLSA DE HORAS

Sin embargo, el calendario y la planificación de estos trabajos irán condicionados por el calendario del proyecto T-mobilitat.

5.5.2.2. Hitos estratégicos

Se identifican en el gráfico siguiente los hitos estratégicos del proyecto que son de obligado cumplimiento.

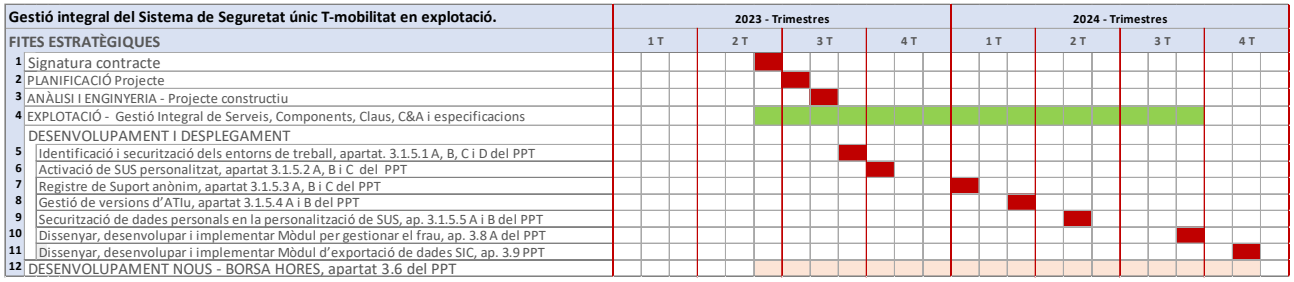


Imagen 10: Hitos estratégicos del proyecto

El hito estratégico número 3 corresponde a los servicios 24x7x365 para garantizar que se dan los servicios de seguridad de manera permanente, así es un hito de permanente cumplimiento.

El hito estratégico número 11 corresponde a la implementación de salvaguardias y otras funcionalidades necesarias, así que pueden aparecer en cualquier momento a lo largo del proyecto.

5.6. Condiciones generales de ejecución

5.6.1. Confidencialidad y publicidad del servicio

El adjudicatario está obligado a guardar secreto respecto de los datos o información que no siendo públicos o notorios estén relacionados con el objeto del contrato.

Cualquier comunicado de prensa o inserción en los medios de comunicación que el

proveedor realice en lo referente al servicio que presta a la ATM deberá ser aprobado previamente.

Se garantizará el 100% de confidencialidad en todas las actividades llevadas a cabo en el ámbito de esta contratación.

Toda la información correspondiente a los Sistemas Tecnológicos de la ATM que se trate en esta contratación debe ser tratada como estrictamente confidencial.

Todos los documentos generados en la presente contratación será propiedad de la ATM y no se podrá hacer ningún uso por parte del contratista.

5.6.2. Propiedad intelectual

Toda la documentación que se genere durante el servicio es propiedad exclusiva de la ATM.

El licitador no podrá utilizarla para otros fines sin el consentimiento expreso de la ATM.

El licitador deberá indicar en la oferta el tipo de licencia, si la hubiere, utilizada en el desarrollo de las aplicaciones que se desarrollen, siempre respetando los preceptos de propiedad intelectual, uso y explotación de desarrollos específicos para ATM.

5.6.3. Tratamiento de datos de carácter personal

El adjudicatario tratará los datos de carácter personal a los que acceda como consecuencia de la ejecución de este contrato de conformidad con lo establecido en la normativa vigente en la materia.

La empresa adjudicataria se responsabilizará del uso adecuado de la información que se pueda obtener para proteger los datos personales, a lo largo de toda la fase de realización del objeto del contrato y también una vez finalizada sobre la base de las normativas internacionales al respecto y de obligado cumplimiento, entre ellos y expresamente, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de dichos datos, así como cualquier otra normativa nacional y de la Unión Europea que sea aplicable en materia de protección de datos y en relación con los datos personales a los que tiene acceso durante la vigencia de este contrato para la puesta en servicio y servicios tecnológicos en explotación de los canales de comercialización externos T -movilidad con tecnología sin contacto.

El incumplimiento de estas obligaciones constituye la infracción tipificada en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, sin perjuicio de las responsabilidades exigidas ante la jurisdicción ordinaria.

5.6.4. Criterios de accesibilidad universal

La empresa adjudicataria se responsabilizará de cumplir con los criterios de accesibilidad universal, tal y como están definidos estos términos en el texto refundido de la Ley General de derechos de las personas con discapacidad y de inclusión social, aprobado mediante Real Decreto Legislativo 1/2013, de 29 de noviembre.

5.6.5. Criterios de sostenibilidad y protección al medio ambiente

La empresa adjudicataria se responsabilizará de cumplir los criterios de sostenibilidad y protección del medio ambiente, de acuerdo con las definiciones y principios regulados en los artículos 3 y 4, respectivamente, del *Real Decreto Legislativo 1/2016, de 16 de diciembre, por el que se aprueba el texto refundido de la Ley de prevención y control integrados de la contaminación*.

Siempre que sea posible, la empresa contratista deberá realizar una elección inteligente de materiales (uso de materiales adecuados para el medio ambiente, evitando los que no lo sean), equipos de eficiencia energética (reducir el coste energético y la huella carbono colectivo), final de la vida útil y reutilización, etc.

5.7. Propuesta técnica

El licitador deberá presentar una propuesta técnica que tendrá que una *"Memoria explicativa de la propuesta presentada"*, la cual deberá incluir una explicación descriptiva de los contenidos del proyecto objeto de la contratación, la metodología para el desarrollo y la organización del proyecto, incluyendo tanto el calendario previsto como en el equipo de trabajo necesario para la realización del proyecto (estructura del equipo).

Sílvia Roig-Serra Bricall
Directora de l'Àrea de la T-mobilitat

Firmado electrónicamente