

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA  
CONTRATACIÓN POR PROCEDIMIENTO ABIERTO DEL  
“EVOLUCIÓN DEL SISTEMA SECEBIT Y SUBSISTEMAS  
ASOCIADOS” DEL CONSORCIO REGIONAL DE  
TRANSPORTES PÚBLICOS REGULARES DE MADRID**





## ÍNDICE

1	ANTECEDENTES Y JUSTIFICACIÓN .....	3
2	OBJETO DEL DOCUMENTO .....	3
3	ALCANCE DEL CONTRATO.....	4
4	TRABAJOS A REALIZAR .....	4
4.1	Proceso de particularización compatible con PL600 y PSI-E2:PL1500....	4
4.2	Nuevas funcionalidades para los servidores criptográficos del CRTM. ....	7
4.3	Proceso de incorporación de nuevos conjuntos de claves maestras en caliente.....	8
4.4	Desarrollo del subsistema VLAT. ....	8
4.5	Mantenimiento evolutivo del software LAT-SECU. ....	9
4.6	Integración del LAT-SECU con VLAT.....	10
4.7	Evolución del cliente ligero de carga del entorno ACTIVEX a aplicación de escritorio.....	10
4.8	Soporte integración medios de pago y pasarelas con aplicativos BIT....	11
4.9	Pruebas SECEBIT / VLAT / LAT-SECU .....	11
5	DESARROLLO, INSTALACIÓN Y PRUEBAS .....	12
6	ASEGURAMIENTO DE LA CALIDAD .....	13
7	CONDICIONES GENERALES.....	14
7.1	Introducción .....	14
7.2	Dirección del Proyecto.....	14
7.3	Seguimiento y control en la ejecución de trabajos.....	16
7.4	Carácter llave en mano.....	16
7.5	Entrega de los trabajos realizados .....	16
7.6	Entorno de trabajo .....	17
8	PLAN DE TRABAJO.....	17
9	DOCUMENTACIÓN.....	18
10	PLAZO DE EJECUCIÓN DE LOS TRABAJOS .....	19



## **1 ANTECEDENTES Y JUSTIFICACIÓN**

El CRTM (Consortio Regional de Transportes Públicos Regulares de Madrid) comenzó el desarrollo de un sistema de SEguridad CEntralizada para el sistema BIT (SECEBIT) a finales del 2006 y termino su implementación en junio del 2009. Aunque posteriormente a estas fechas se han realizado trabajos de mantenimiento y evolución. Dicho sistema que permite varios cientos de procesos concurrentes, se compone de al menos dos servidores criptográficos configurados en alta disponibilidad (balanceados), cada uno de los cuales incorpora al menos un módulo de hardware seguro (HSM) (tarjeta PCI), este dispositivo HSM es el núcleo del sistema SECEBIT, capaz de embeber claves y comandos de forma segura (software de bajo nivel). El núcleo incorpora un sistema antirrobo basado en la "tamperización", esto es un proceso autodestructivo por si se intenta abrir o quitar un dispositivo HSM. Pero para que el servidor criptográfico pueda ofrecer el servicio del núcleo se precisa una capa software que establezca la comunicación entre el exterior y el núcleo. El CRTM dispone de este software (de alto nivel), denominado HSM24. Así como de las herramientas necesarias para particularizar los núcleos.

El CRTM requiere evolucionar lo descrito anteriormente con nuevas funcionalidades, que son el objeto de este contrato y que fundamentalmente implica: mejoras de SECEBIT y evolución LAT-SECU, nuevo subsistema VLAT, e integración de VLAT con LAT-SECU, cliente de escritorio, soporte de pasarelas de pago y pruebas de todos los sistemas.

## **2 OBJETO DEL DOCUMENTO**

El objeto de este documento es establecer el alcance y las condiciones de carácter técnico que han de regir la contratación por Procedimiento Abierto de



los trabajos necesarios para el mantenimiento, desarrollo e implantación de las aplicaciones software objeto de este contrato.

También es objeto de este documento definir los procedimientos de ejecución, seguimiento, control y validación de los trabajos contemplados en el alcance del proyecto, la responsabilidad, garantía y propiedad de los trabajos aquí definidos, así como toda la documentación técnica a presentar en cada caso.

### **3 ALCANCE DEL CONTRATO**

Son objeto de este contrato las siguientes tareas:

- Mejoras de SECEBIT y evolución LAT-SECU (4.1, 4.2, 4.3 y 4.5)
- Implementación VLAT (4.4)
- Integración VLAT y LAT-SECU (4.6)
- Cliente de escritorio (4.7)
- Soporte de pasarelas de pago integradas con LAT-SECU (4.8)
- Pruebas de todos los sistemas (4.9)

### **4 TRABAJOS A REALIZAR**

Los trabajos objeto de contratación se describen a continuación:

#### **4.1 Proceso de particularización compatible con PL600 y PSI-E2:PL1500.**

Los HSM son los dispositivos garantes de la seguridad (con disponibilidad de 24x7x365) en los procesos más delicados del ciclo de vida de la tarjeta de



transporte pública del CRTM: prepersonalización, personalización y carga. El CRTM se encarga de particularizar todos los HSM del sistema, los del CRTM con más privilegios y permisos, y el resto de HSM del sistema que corresponden con las redes externas de carga/recarga y personalización.

Se entiende por particularización el proceso de asignar un determinado rol a un HSM, inyectar las claves y permisos correspondientes, establecer los contadores inviolables del sistema que se irán actualizando a medida que se realizan las distintas operaciones con las tarjetas de forma unitaria y parametrizar las alarmas generales.

En estos años ha evolucionado enormemente el hardware de estos dispositivos. El modelo de placa HSM que tiene el CRTM en producción PL600 ha dejado de fabricarse y es sustituida por nuevo modelo (PSI-E2:PL1500) más rápido y que incorpora mayores medidas de seguridad.

Más importante incluso que la evolución en hardware es la necesaria evolución en software. La hoja de ruta impone nuevos hitos que difícilmente pueden afrontarse si no se evoluciona la seguridad del sistema.

Esto implica que se mantengan hardware diferente con un mismo software más evolucionado. Software que sea totalmente compatible y retrocompatible con el sistema actual en producción y los nuevos escenarios que se avecinan.

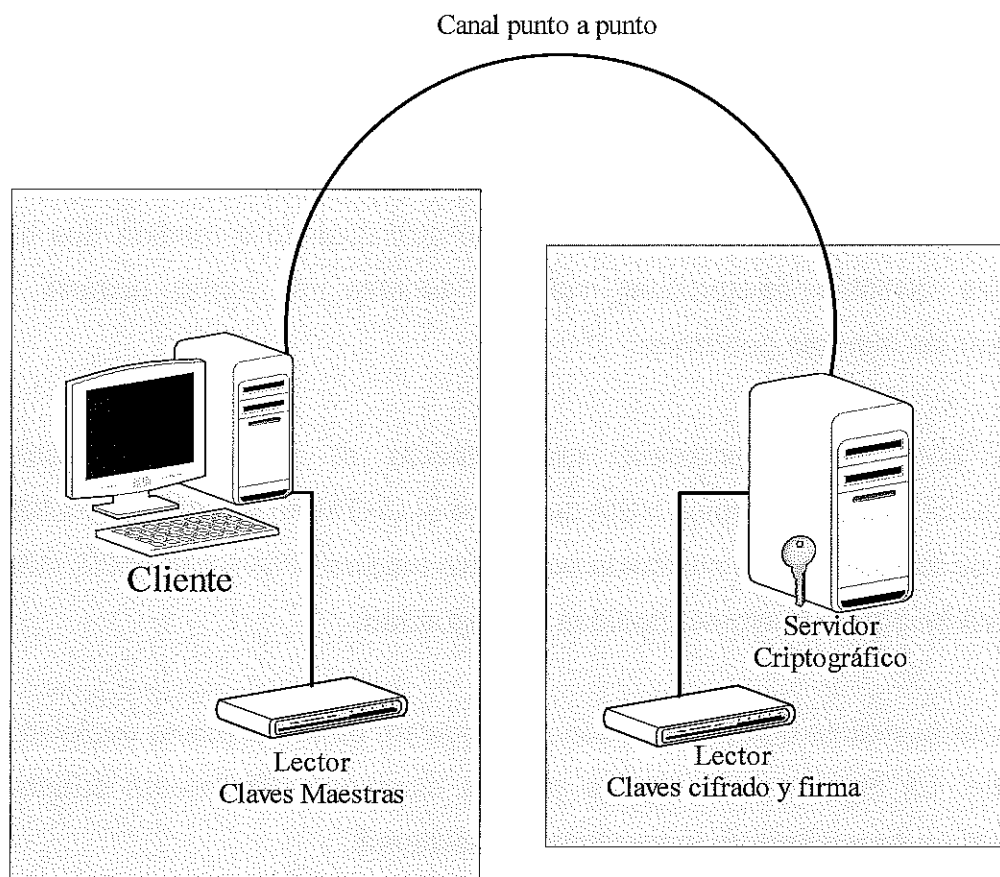
En consecuencia, el adjudicatario deberá realizar la evolución de software de particularización del CRTM tanto para placas PL600 como para placas PSI-E2:PL1500. Para lo cual deberá acreditar las siguientes certificaciones:

1. FIPS 140-2 nivel 2 y nivel 3
2. Common Criteria EAL4+
3. Compatible con ePassport BAC y EAC





Dicha evolución de software se basa en el siguiente flujo lógico:



Las placas HSMs estarán embebidas en el servidor criptográfico. Desde el cliente se realiza una conexión segura al servidor criptográfico y se lanza el proceso, que fundamentalmente consiste en inyectar en la placa lo siguiente:

1.- Comandos: Clave de Sesión, Concesión de Cupo, Diversificación, Firma, Validación, Cifrado DES, Número SubeT

2.- Claves maestras: CARDMASTERKEY, APPMASTERKEY,  
PERSONTRANSKEY, READTRANSKEY, VALIDTRANSKEY,  
CHARGETRANSKEY, INSPECTTRANSKEY, VIRTUALHSMKEY,  
LOPDHSMKEY



3.- Claves de cifrado: SAMKEY0, SAMKEY1, SAMKEY2, SAMKEY3, SAMKEY4, SAMKEY5, SAMKEY6, SAMKEY7 y SAMKEY8

4.- Contadores únicos para los TLVs del Sistema BIT

5.- Umbrales

#### **4.2 Nuevas funcionalidades para los servidores criptográficos del CRTM.**

Es necesario fortalecer y desarrollar nuevas funcionalidades en los servidores criptográficos, basados en placas HSM, para llevar a cabo los retos próximos y de futuro.

Se presentan nuevas tarjetas comerciales, nuevos entornos algunos con tecnologías de emulación de tarjetas en dispositivos móviles. Se hace necesario dar cabida a nuevos conjuntos de claves a distintos tipos de TLV al tiempo a distintos modos de autenticación. Por eso es necesario evolucionar los HSM existentes y a la hora de adquirir nuevos HSM obtenerlos con un software de seguridad nuevo, más potente. No solo es preciso mejorar la plataforma embebida también la que sustenta el sistema. Durante estos años se han realizado algunas mejoras pero llega el momento de realizar una verdadera actualización del sistema. La actualización de los HSM en paralelo con la actualización de los SAM, permitirán al CRTM mejorar la seguridad en todo el ciclo de vida de las tarjetas. Es la primera fase para ir cambiando paulatinamente los procesos de prepersonalización, personalización, carga/recarga, validación, inspección y atención al cliente. Sin la actualización previa de los dispositivos garantes de la seguridad no es posible mejorar sustancialmente la seguridad en los procesos que interactúan con la tarjeta

Los servidores criptográficos del CRTM, se componen de dos niveles de software integrados. El software a bajo nivel, que está embebido en el HSM (ya sea, una placa PL600 o la futura placa PSI-E2:PL1500) y que es inyectado en



estas placas, junto con el rol, las claves y los contadores inviolables, en el proceso de particularización. Y el software de alto nivel, que internamente establece un canal seguro con el software de bajo nivel para que este último realice los procesos de seguridad y por otro lado permite, el software de alto nivel, la concurrencia de peticiones al exterior.

Los núcleos de los HSM tienen que albergar diferentes juegos de claves maestras con soporte 3DES y AES. El software de alto nivel, debe ser capaz de procesar diferentes versiones de TLVs (tal y como se define en el sistema BIT). Además, tanto alto nivel como bajo nivel deberán soportar la autenticación 3DES y AES en tres pasos.

#### **4.3 Proceso de incorporación de nuevos conjuntos de claves maestras en caliente.**

Tanto el nuevo SAM, como los nuevos HSM, deben soportar incorporar nuevas familias de claves maestras, entendiendo como “familia de claves maestras” al conjunto de nueve claves definido en el epígrafe 4.1.

Lo importante del proceso es que se deben definir e implementar mecanismos, por los cuales, una vez generado una nueva familia (o conjunto de ellas) de claves maestras desde un SAM maestro o portaclaves, se deberán de manera segura (mediante certificados), en la placa embebida de todos los HSMs en producción.

#### **4.4 Desarrollo del subsistema VLAT.**

Una de las peticiones que se realiza de forma recurrente al CRTM es la posibilidad de virtualizar tarjetas en dispositivos móviles y utilizar el canal de comunicaciones NFC para realizar las validaciones. Los procesos de





prepersonalización, personalización y carga/recarga se podrían realizar bien por la interfaz OTA o bien utilizando el canal NFC. El CRTM tiene especificada al completo la lógica de la aplicación de transportes en sus distintos aplicativos y las reglas de negocio. Es necesario adaptar su plataforma para que contemple las peculiaridades especiales de las tarjetas virtualizadas. Se necesita adaptar y modificar distintos estados para que convivan al mismo tiempo las tarjetas virtuales y físicas en el sistema, y se pueda migrar de una a otra y viceversa.

Las tarjetas virtuales necesitan un control extra en el backoffice del CRTM (VLAT). Además deben garantizar los mismos estándares de seguridad o similares que se han establecido para las tarjetas físicas.

#### **4.5 Mantenimiento evolutivo del software LAT-SECU.**

El LAT-SECU es la plataforma interna del CRTM que permite lectura de saldo, cargar y/o recarga de títulos de transporte, desde cualquier dispositivo. Por ejemplo, en máquinas automáticas, internet o desde un app. Hay que aclarar que el LAT-SECU forma parte del BackOffice del CRTM y que es posible integrarse con ella mediante el desarrollo de clientes ligero, donde los procesos de acceso a la tarjeta de transportes se delegan a esta plataforma.

La arquitectura del LAT-SECU se compone de un servidor LAT (capa de aplicación de transporte) y un servidor SECU (que se ocupa de la lógica de seguridad, conectando, cuando es preciso con el sistema SECEBIT). Ambas integradas. Además, esta arquitectura gestiona las pasarelas de pago.

El CRTM tiene previsto el lanzamiento de tarjetas anónimas en 2016, por lo que se requiere adaptar el LAT-SECU para la carga y recarga de títulos 10 viajes y sencillos, así como adaptarlo a nuevos comportamientos más flexibles que los actuales.



Está previsto también adaptar la plataforma LAT-SECU para funcionar con las próximas versiones de HSM que caminan en paralelo con las versiones de software de los SAM. Así como, adaptar y conectar el LAT-SECU con la plataforma y gestión de cupones, o incluso con un TSM Hub

#### **4.6 Integración del LAT-SECU con VLAT**

La posibilidad de trabajar con tarjetas virtuales requiere evolucionar parte del LAT-SECU para integrarse con VLAT. En el escenario de las tarjetas físicas la gran parte de la seguridad ya era proporcionada por el hardware. En las tarjetas virtuales hay que completar con software la parte que no viene dada por el hardware de la tarjeta. También es necesario modificar, adaptar y añadir nuevos procedimientos de seguridad.

En consecuencia, el adjudicatario implementará un sistema completo a partir de lo definido en este epígrafe y los epígrafes 4.4. y 4.5. Permitiendo gestionar, en BackOffice del CRTM, tanto tarjetas físicas como virtuales.

#### **4.7 Evolución del cliente ligero de carga del entorno ACTIVEX a aplicación de escritorio.**

EL CRTM cuenta con una red de clientes ligeros de carga que utilizan internet explorer10 con tecnologías ActiveX, mediante los cuales se pueden realizar operaciones de consulta de saldo y de carga/recarga con lectores de bajo coste y con pocos requerimientos de software /hardware.

Esta plataforma funciona correctamente, pero se ha detectado que no es fácil su mantenimiento y actualización. Es por ello necesario migrarlo a una plataforma que siga manteniendo la misma filosofía de mínimas exigencias pero que mejore los sistemas de actualizaciones y mantenimiento. Tras un



estudio detallado se ha llegado a la conclusión que es mejor migrar la aplicación a escritorio.

El trabajo consiste en adaptar la aplicación a escritorio y actualizar las interfaces y funcionalidad a las últimas especificaciones de lógica del BIT. Varios tipos de tarjetas comerciales, reglas de coexistencia de títulos en una tarjeta, nuevos perfiles y títulos, y en especial los títulos anónimos (multiviajes y sencillos)

#### **4.8 Soporte integración medios de pago y pasarelas con aplicativos BIT.**

Es necesaria la integración completa de las plataformas de pago y el control de las órdenes de pago con la lógica de la aplicación de transporte implantada en las OOGG (oficinas de gestión). De esta manera se tiene un control completo de las operaciones realizadas mediante pagos electrónicos desde los aplicativos del CRTM. Facilitando realizar los cuadros de caja, de operaciones y facturas.

El CRTM tiene parte del sistema integrado, pero necesita trasladarlo a todas las OOGG y que se integren con distintas pasarelas y aplicativos. Deben controlarse todas las operaciones incluyendo las anulaciones de pago y se necesita tener todas las trazas del sistema.

#### **4.9 Pruebas SECEBIT / VLAT / LAT-SECU**

El adjudicatario, con la supervisión del CRTM, realizará el conjunto de pruebas establecidas, en dos niveles:

En las fases de pruebas se cumplimentarán los protocolos definidos por el CRTM. No podrá ponerse en producción un sistema o producto sin obtener previamente la VISA de APTO del CRTM. Cualquier modificación de



software/hardware de la plataforma tiene que ser informada convenientemente al CRTM y obtener la VISA correspondiente.

NIVEL bajo: Pruebas concretas de cada comando, rendimiento de sistema, de configuración de la arquitectura, de robustez y fiabilidad y de rapidez..

NIVEL alto. Pruebas funcionales de lógica de negocio, de interfaces, de recibos y pruebas transaccionales.

## **5 DESARROLLO, INSTALACIÓN Y PRUEBAS**

Las tareas de programación e instalación se realizarán en las dependencias del CRTM, ya que, es necesario acceder al núcleo del sistema (servidores y bases de datos de producción y desarrollo) de este organismo.

Las pruebas finales, antes de autorizar un cambio de entorno, serán realizadas por el adjudicatario en presencia de personal responsable del CRTM asignado. Se adjuntarán las librerías, scripts y demás componentes utilizados para realizar la implantación, con un documento detallado de todos los pasos y requerimientos para desarrollar esta tarea.

A continuación, se detallan los hitos cuya falta de cumplimiento originarían un retraso en la planificación de puesta en marcha del proyecto, y que no sólo puede afectar al CRTM, sino también a los operadores de transporte u otros actores externos implicados:

1. Hito I: Deberá estar totalmente concluido en 2 semanas a contar desde la fecha de formalización del contrato y las tareas a implementar son las siguientes:

- Particularización embebida de la placa PSI-E2:PL1500.



2. Hito II: Deberá estar totalmente concluido en 1 mes a contar desde la fecha de formalización del contrato y las tareas a implementar son las siguientes:

- Completar la tarea 4.1

La penalización a la empresa adjudicataria por el incumplimiento de cualquiera de estos hitos será la rescisión del contrato, ya que el incumplimiento de los mismos implicaría la imposibilidad de que el CRTM efectué las tareas que tiene encomendadas según la planificación de implantación del Proyecto BIT.

## **6 ASEGURAMIENTO DE LA CALIDAD**

El oferente presentará un Plan de Aseguramiento de la Calidad del software (a partir de ahora QA) para las diferentes aplicaciones, que se realizará en el momento en que los productos estén desarrollados y antes de que lo recepcione definitivamente el CRTM.

Este plan de QA estará a su vez compuesto por planes de pruebas unitarias de cada una de las aplicaciones desarrolladas o implantadas y de un plan de pruebas de integración de todos y cada uno de los sistemas nuevos o existentes en el alcance del proyecto.

La estructura de estos planes incluirá, al menos, los siguientes aspectos:

- Planificación temporal y de dependencias de las pruebas a realizar.
- Casos de prueba basados en los casos de uso del sistema.
- Guiones de pruebas para cada uno de los casos anteriores.
- Registro de los resultados para cada uno de los guiones de prueba.



## **7 CONDICIONES GENERALES**

### **7.1 Introducción**

La realización de los trabajos se atenderá a las especificaciones al respecto contenidas en el Pliego de Cláusulas Administrativas Particulares que le es anejo al presente Pliego de Prescripciones Técnicas.

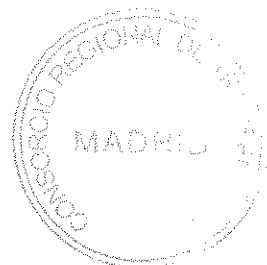
El adjudicatario realizará la totalidad de los trabajos especificados en el presente Pliego de Prescripciones Técnicas en cumplimiento del contrato que se establezca.

El adjudicatario será el único responsable de los desarrollos determinados en el contrato, limitándose el CRTM a controlar dichos desarrollos y, en general, a verificar y asegurar que estos se efectúan de acuerdo con lo que se establece en el presente pliego.

La Administración facilitará al adjudicatario cuanta información disponga relacionada con el objeto de este Contrato así como su acceso a la documentación existente que considerase de interés para el proyecto.

### **7.2 Dirección del Proyecto**

La dirección del proyecto se llevará a cabo por parte del Consorcio de Transportes de Madrid. Por otro lado el contratista determinará un Director Técnico que salvo fuerza mayor, y previa justificación y aprobación ante el CRTM, será único a lo largo de la ejecución del proyecto.



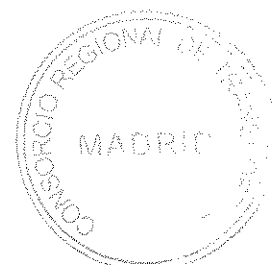
Las funciones del Director de Proyecto del CRTM serán:

- Dirigir y supervisar la realización y desarrollo de los mismos.
- Facilitar la información necesaria para la ejecución de los trabajos descritos.
- Determinar y hacer cumplir las Normas de Procedimiento.
- Decidir la aceptación de las modificaciones propuestas por el Director Técnico en el desarrollo de los trabajos.
- Realizar las certificaciones parciales de servicios prestados.

Las funciones del Director Técnico del contratista serán:

- Ser el único Interlocutor entre el grupo de trabajo del contratista y el CRTM.
- Organizar la ejecución de los trabajos y poner en práctica las órdenes de la dirección de los mismos.
- Ostentar la representación del equipo técnico contratado en sus relaciones con la Administración, en lo referente a la ejecución de los trabajos.
- Observar y hacer observar las Normas de Procedimiento.
- Proponer a la Dirección del Proyecto las modificaciones en el contenido y realización de los trabajos necesarios para el desarrollo de los mismos.
- Realizar el acta de todas y cada una de las reuniones de trabajo que se tengan.

Previamente al arranque del proyecto el contratista propondrá un Director Técnico al CRTM que deberá ser aprobado por éste.





### **7.3 Seguimiento y control en la ejecución de trabajos**

Corresponde a la Dirección del Proyecto, el control de la productividad y calidad de los trabajos ejecutados por el contratista, siendo potestad suya solicitar nuevamente la realización y/o el cambio de cualquiera de los desarrollos o servicios prestados.

Para realizar el seguimiento del proyecto, se mantendrán reuniones quincenales en las oficinas del CRTM el mismo día de la semana y hora que se acuerde al comienzo del proyecto. Según la evolución de los trabajos y si se considera necesario las reuniones pasarán de quincenales a semanales.

### **7.4 Carácter llave en mano**

El contratista deberá entregar aplicaciones terminadas, probadas e implantadas, y consecuentemente tendrá la obligación global de realizar todas las prestaciones necesarias o complementarias de los desarrollos a realizar, incluyendo la instalación o ajuste del software base (bases de datos, servidores de aplicaciones, etc.).

El director nombrado por el CRTM será el encargado de validar la totalidad de las aplicaciones, y por tanto el proyecto no se considerará finalizado hasta su validación.

### **7.5 Entrega de los trabajos realizados**

El adjudicatario, deberá entregar todos los programas (fuentes y ejecutables), librerías, scripts de compilación, especificaciones o cualquier otro componente que constituyan elementos del proyecto, embebido en una máquina virtual, o si lo decide el CRTM, en un repositorio subversión con toda la documentación técnica necesaria.





El adjudicatario no podrá hacer otras reproducciones, ni para uso propio ni para cesiones a terceros, no pudiendo quedarse con copia alguna de los mismos, debiendo contar con una autorización expresa y por escrito de la dirección del proyecto en el caso de que desee utilizarlos para alguna otra finalidad diferente de las derivadas del objeto del Contrato.

El adjudicatario no podrá utilizar para sí ni proporcionar a terceros, dato alguno de los trabajos contratados, ni publicar, total o parcialmente, el contenido de los mismos sin autorización escrita de este organismo. En todo caso el adjudicatario será responsable de los daños y perjuicios que se deriven del incumplimiento de esta obligación.

## **7.6 Entorno de trabajo**

El trabajo se realizará en las oficinas del adjudicatario.

## **8 PLAN DE TRABAJO**

Con carácter previo a la ejecución de los trabajos objeto de la contratación regida por el presente Pliego de Prescripciones Técnicas (PPT) la empresa adjudicataria deberá presentar un plan de trabajo para cada aplicativo, que se someterá a la dirección del proyecto, el cual deberá contener, como mínimo, los siguientes elementos:

- Metodología pormenorizada según la cual se propone el adjudicatario realizar los trabajos, desarrollada hasta los niveles operativos y acompañada de las justificaciones pertinentes.
- Cronograma de actividades (diagrama de Gantt), desagregado por fases y principales grupos de tareas.





- Relación de recursos humanos integrantes del equipo técnico asignados a cada tarea, según los currículos presentados.
- Recursos técnicos que se pondrán a disposición del trabajo.
- Información de partida que el equipo técnico contratado hubiera recopilado o se propusiera recopilar con vistas a la ejecución de los trabajos.
- Definición clara de los documentos que se generarán tanto de reporte y seguimiento, como entregables finales.
- Plazos de ejecución y duración total de los trabajos.

## **9 DOCUMENTACIÓN**

Durante la ejecución de los trabajos, el contratista deberá elaborar y presentar al Director del Proyecto del CRTM la documentación necesaria correspondiente a las diferentes fases de los trabajos que permitan a este realizar el control y seguimiento de los trabajos contratados. A la finalización del contrato el adjudicatario aportará los correspondientes manuales de usuario para su validación por parte del CRTM, siendo lo suficientemente exhaustivos y completos para el posterior mantenimiento de las aplicaciones objeto del contrato. Por lo tanto será preciso elaborar al menos la siguiente documentación:

- Actas de cada una de las reuniones de proyecto mantenidas.
- Especificaciones técnicas de los módulos a desarrollar y/o adaptar.
- Diseño Técnico de los módulos a desarrollar y/o adaptar.
- Manuales de usuario.
- Manuales de Administración y mantenimiento.

El soporte de la documentación será papel impreso y DVD, y en un formato que permita su posterior edición e impresión en papel.



CONSEJERÍA DE TRANSPORTES,  
VIVIENDA E INFRAESTRUCTURAS

**Comunidad de Madrid**



## 10 PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo de ejecución será de doce meses, prorrogables por un periodo igual, a contar desde la formalización del contrato que se estima el 1 de septiembre de 2016.

Madrid, 28 de septiembre de 2016

EL DIRECTOR GERENTE,

Juan Ignacio Merino de Mesa

CONFORME,

EL ADJUDICATARIO

