Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PLIEGO DE PRESCRIPCIONES TÉCNICAS

CONTRATACIÓN DE SERVICIOS DE CONSULTORÍA PARA LA IMPLANTACIÓN DE PROGRAMA DE MEJORA DE LA SEGURIDAD EN EL DESARROLLO DE SOFTWARE

PROCEDIMIENTO ABIERTO SIMPLIFICADO

PAS-10/1635/2022

ÍNDICE

1.- OBJETO.

El presente documento describe las condiciones técnicas de aplicación en la contratación de servicios de consultoría para la implantación de un programa de mejora de la seguridad en el Desarrollo de Software. El alcance de esta iniciativa comprende al Área de Desarrollo del Departamento CERES de la FNMT-RCM.

2.- DESCRIPCIÓN.

2.1.- ANTECEDENTES.

En el contexto actual, la seguridad de los sistemas de información es un aspecto clave para asegurar la prestación de servicios seguros, resilientes y confiables, así como para garantizar algunos derechos fundamentales de las personas como puede ser la privacidad y protección de los datos personales.

Atendiendo al contexto de cumplimiento normativo aplicable, es preciso que la FNMT-RCM satisfaga los requisitos de desarrollo seguro derivados del Esquema Nacional de Seguridad (ENS), del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la ISO/IEC 27001, así como de otra normativa de aplicación (Reglamento UE 910/2014 eIDAS y otros).

Con el fin de satisfacer los requisitos mencionados, la FNMT-RCM establecerá un conjunto de prácticas de seguridad en el proceso de creación de software, integrando la seguridad en las diversas etapas del ciclo de vida de desarrollo, desde las fases más tempranas en la concepción del sistema de información, hasta la fase de operación. El fin último de dichas prácticas de seguridad es el de actuar y resolver de forma preventiva potenciales problemas de seguridad antes de que éstos se materialicen en vulnerabilidades del software, amenazas o incidentes.

En este escenario, se presenta la necesidad de contratar servicios profesionales que permitan definir un programa de mejora de la seguridad del software, que garantice la seguridad de los productos y servicios finales.

2.2.- DESCRIPCIÓN DETALLADA DEL OBJETO DE LA CONTRATACIÓN

Por todo lo expuesto anteriormente, FNMT-RCM presenta la presente licitación para la contratación de los servicios de consultoría necesarios para la implantación de un programa de mejora de la seguridad en el desarrollo de software.

El programa de desarrollo seguro se fundamentará en el modelo de aseguramiento del software “Software Assurance Maturity Model” (SAMM) de la organización OWASP (Open Web Application Security Project).

SAMM es un modelo de madurez enfocado en la seguridad del proceso de desarrollo y construcción del software, cuya finalidad es ayudar a las organizaciones a establecer e implementar una estrategia para la mejora de la seguridad en los procesos del ciclo de vida del software. Este modelo considera la seguridad en el proceso de desarrollo de forma holística, teniendo en cuenta las diferentes funciones o subprocesos que intervienen en el ciclo de vida del desarrollo del software y estableciendo, para cada una de ellas, un conjunto de prácticas y actividades orientadas a la producción de software seguro.

Para cumplir el objetivo previsto, la empresa adjudicataria deberá contar con personal cualificado que permita abordar las actividades asociadas con la calidad, rendimiento y seguridad que la FNMT-RCM precisa. Dicho personal tiene que tener conocimientos y experiencia, entre otros, sobre el ciclo de desarrollo de software seguro, las diversas tecnologías involucradas en la cadena de valor del proceso de desarrollo de software, las mejores prácticas de seguridad en el desarrollo de software y tener amplios conocimientos del modelo SAMM.

Además de la experiencia y conocimientos mencionados en todas las tecnologías mencionadas, el personal de la empresa adjudicataria deberá tener experiencia en el diseño e implantación de sistemas de gestión del ciclo de vida del desarrollo de software seguro (S-SDLC), así como en sistemas de gestión del ciclo de vida con enfoque SecDevOps.

3.- ALCANCE

El objetivo final de la contratación es el establecimiento de un programa iterativo de mejora de la seguridad del software que se desarrolla en el Área de Desarrollo CERES de la FNMT-RCM.

Los servicios a prestar consisten en la ejecución de trabajos de consultoría de seguridad para:

1. Evaluar el estado actual de la seguridad en el desarrollo de software.
2. Asesorar a la FNMT-RCM en la definición de la estrategia y objetivos de seguridad a alcanzar.
3. Asesorar a la FNMT-RCM y elaborar la hoja de ruta del programa de mejora de la seguridad.
4. Colaborar con la FNMT-RCM en la definición, priorización y planificación de las actividades a realizar para cumplir con la hoja de ruta establecida.
5. Prestar asistencia o ejecutar (dependiendo de la actividad) ciertas tareas definidas en el plan de acción que se establezca.
6. Evaluar periódicamente el grado de adopción y eficacia de las medidas implementadas, así como determinar la evolución del programa de mejora y del estado de la seguridad en el desarrollo de software con respecto a la situación de partida.

Como se ha comentado anteriormente, los trabajos se desarrollarán siguiendo el marco de trabajo establecido por el modelo de madurez SAMM de OWASP.

En caso de necesitarse más información para la confección de la consiguiente oferta, se puede solicitar como aclaraciones al presente pliego.

4.- ETAPAS, NIVELES, O HITOS, EN LA EJECUCIÓN DE LA CONTRATACIÓN.

A continuación, se detallan las diversas fases de ejecución de los servicios.

4.1.- FASE #0: INICIO DE SERVICIO. DEFINICIÓN DE COMITÉS DE SEGUIMIENTO Y PLANIFICACIÓN

El objetivo fundamental de esta fase es sentar las bases que permitan llevar a cabo el servicio, garantizando el control y seguimiento del mismo, así como el cumplimiento de las expectativas generadas.

El adjudicatario nombrará al inicio del contrato a un responsable del servicio y a un responsable del proyecto con los siguientes roles:

1. Responsable del servicio: tiene la función de controlar la prestación del servicio, la calidad de la prestación y el cumplimiento de los niveles de servicio establecidos.
2. Responsable de proyecto: tiene como función la gestión técnica y operativa del proyecto de implantación del programa de seguridad.

El responsable del servicio tendrá las siguientes responsabilidades:

- Actuar como interlocutor entre la FNMT-RCM y el adjudicatario, canalizando la comunicación en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.
- Definir los indicadores y elementos de valoración que permitan evaluar la calidad en la ejecución del servicio. La metodología para evaluar la calidad del servicio será propuesta por parte del responsable del servicio y deberá ser aceptada por el responsable técnico de la FNMT-RCM. La metodología empleada podrá ser revisada y ajustada a lo largo de la ejecución del contrato.

El responsable de proyecto tendrá las siguientes responsabilidades:

- Actuar como interlocutor del adjudicatario frente a FNMT-RCM, canalizando la comunicación entre el adjudicatario y el responsable técnico que defina de la FNMT-RCM para el proyecto.
- Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación de los servicios contratados
- Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tiene encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.
- Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente el

adjudicatario con FNMT-RCM, a efectos de no alterar el buen funcionamiento de los servicios.

- Informar a FNMT-RCM acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato.

La FNMT-RCM nombrará a un responsable de proyecto que supervisará, realizará seguimiento del proyecto e intermediará entre la FNMT-RCM y el adjudicatario en la resolución de las cuestiones técnicas y de negocio que puedan surgir.

El responsable de proyecto de la FNMT-RCM orientará y facilitará la labor del adjudicatario en la identificación de los interlocutores de las diversas partes involucradas, así como en la adquisición del conocimiento necesario sobre la infraestructura, metodologías, y, en general, sobre cualquier aspecto relacionado con el ciclo de vida del software que tiene implantado actualmente la FNMT-RCM.

El responsable de proyecto de la FNMT-RCM será el responsable de la supervisión, control y aprobación de los trabajos realizados por el adjudicatario.

Adicionalmente, en esta fase se establecerá el calendario y planificación de las actividades del proyecto, así como los hitos y entregables asociados.

Se establecerán reuniones periódicas para analizar la calidad en la ejecución del servicio y realizar seguimiento del estado del proyecto. A estas reuniones, asistirá el responsable del servicio y el responsable del proyecto por parte del adjudicatario, junto con el responsable técnico y otros involucrados en el proyecto por parte de la FNMT-RCM.

Como parte del seguimiento y control de la ejecución del contrato, será responsabilidad del adjudicatario:

- El análisis de posibles problemas y riesgos asociados a las actividades y trabajos en curso de los que son responsables.
- Proponer medidas de mejora y medidas correctoras a posibles incidencias detectadas durante la prestación de los servicios.

- Coordinar los recursos asignados a la prestación de los servicios y velar por el cumplimiento de los acuerdos.

4.1.1.- Hitos y entregables

En esta fase se deberá generar:

- Documentación con acta de reunión de arranque, composiciones de comités de seguimiento, nombramiento de responsables, y protocolos de actuación para la gestión del proyecto, de actas de reuniones periódicas de seguimiento de la calidad de los servicios prestados, actas de seguimiento de proyecto, etc.
- Planificación del proyecto.

4.2.- FASE #1: EVALUACIÓN INICIAL

Tomando como referencia el modelo de madurez SAMM, se analizarán las prácticas que se llevan a cabo en el proceso de desarrollo de software y se evaluará el grado de madurez de las mismas.

Como resultado de la evaluación inicial se deberá proporcionar un informe que detalle todos los hallazgos detectados, las debilidades más relevantes y el grado de madurez global del proceso de desarrollo de software seguro.

4.2.1.- Hitos y entregables

- Informe de evaluación inicial.
- Cuadro de mando con el grado de madurez del proceso de desarrollo de software seguro.

4.3.- FASE #2: DEFINICIÓN DE OBJETIVOS DE SEGURIDAD Y ANÁLISIS DE GAP

Una vez realizada la evaluación inicial se determinarán los objetivos de madurez a alcanzar. Para ello, se analizará el contexto particular de la FNMT-RCM, sus necesidades de negocio y los aspectos de cumplimiento normativo aplicables, especialmente las derivadas del ENS, catálogo.

Se recopilará la información necesaria de contexto, se analizará, se identificarán los factores claves y se elaborará una propuesta, que deberá ser consensuada y validada por FNMT-RCM, con los objetivos a largo plazo del programa de mejora de la seguridad. Los objetivos que se establezcan servirán de referencia e instrumento de medida del progreso del programa de mejora.

Tras la definición de los objetivos, se realizará un análisis de GAP entre la situación de partida y la meta definida, identificando las actividades y prácticas de seguridad que deberán implementarse para alcanzar los objetivos establecidos.

4.3.1.- Hitos y entregables

- Propuesta con objetivos de madurez a alcanzar, justificando la necesidad o conveniencia de los mismos sobre la base de las necesidades de negocio y aspectos de cumplimiento normativo que son de aplicación a la FNMT-RCM.
- Informe con análisis de GAP. El informe detallará de forma especial las carencias o diferencias más destacadas.

4.4.- FASE #3. DISEÑO DEL *ROADMAP* DEL PROGRAMA DE SEGURIDAD.

Se elaborará la hoja de ruta que permita evolucionar a la FNMT-RCM desde la situación inicial hasta alcanzar los objetivos definidos. Se diseñará una estrategia del cambio que defina una hoja de ruta realista, con una serie de etapas o fases, a través de las cuales, la FNMT-RCM se irá aproximando sucesivamente al objetivo final.

Tomando como referencia el grado de madurez objetivo y el análisis de GAP realizado, se diseñará la estrategia para ejecutar el programa de mejora de la seguridad. En dicha estrategia se deberán definir una serie de objetivos de madurez intermedios que permitan establecer la hoja de ruta del programa, que incluirá las diversas etapas o fases (iteraciones de mejora) que se deberán ejecutar para alcanzar el grado de madurez objetivo final. Estos objetivos intermedios permitirán, además, medir los progresos del programa a lo largo de su implantación.

Para asegurar la viabilidad del programa de mejora de la seguridad, la hoja de ruta, el número de sus fases y la duración de las mismas deberá ser diseñada

de forma cuidadosa, teniendo en consideración las capacidades, prioridades, recursos y otros proyectos clave de la FNMT-RCM.

A la hora de diseñar la hoja de ruta, se deberán identificar aquellas acciones que puedan completarse de forma rápida y eficaz (*quick wins*) durante las primeras etapas del plan.

Con el fin de equilibrar la carga de trabajo en las diversas fases del plan, se deberá realizar una distribución racional de las actividades de la hoja de ruta, teniendo en cuenta el esfuerzo asociado, los posibles costes y las dependencias entre actividades.

Adicionalmente se estimará el impacto de la implantación del programa de mejora de la seguridad en términos de esfuerzo y recursos necesarios. En la medida de lo posible, se intentará expresar dicho impacto en términos presupuestarios.

4.4.1.- Hitos y entregables

- *Roadmap* del programa de mejora de la seguridad con planificación distribuida de las diferentes actividades e iniciativas que deberán ser abordadas para lograr los objetivos.
- Descripción de cada una de las actividades a realizar. Se proporcionarán las directrices, recomendaciones e instrucciones para llevar a cabo cada una de las acciones del plan.
- Cuadro de mando para realizar seguimiento y medir la evolución del grado de madurez de la seguridad en el desarrollo de software.

4.5.- FASE #4. EJECUCIÓN DEL PLAN.

FNMT-RCM llevará a cabo la ejecución de cada una de las fases del plan establecido, pasando por las diversas etapas definidas.

La ejecución del Plan de Mejora será responsabilidad de FNMT-RCM y se llevará a cabo con recursos propios. No obstante, se estima que FNMT-RCM precisará apoyo para la realización de diversas actividades planificadas: asesoría y consultoría, ayuda en implantación de herramientas, diseño, elaboración, revisión y evaluación de estándares, procesos procedimientos, guías, manuales

o ejecución de otras tareas. Con el fin de que el servicio a contratar se adapte de forma flexible a estas necesidades de FNMT-RCM, se contratará un conjunto de esfuerzos que se emplearán bajo demanda en actuaciones (encargos) concretos (Ver subapartado "*Consultoría para la ejecución del Plan*")

Tras la finalización de cada una de las fases en las que se divide el programa de mejora de la seguridad, el adjudicatario realizará una evaluación del grado de madurez alcanzado con el fin de valorar su evolución y detectar desviaciones sobre lo previsto. En el caso de que se detecte alguna desviación, el adjudicatario propondrá las acciones correctivas que considere necesarias.

Los resultados de las evaluaciones se incorporarán al cuadro de mando establecido para el control, seguimiento y gobierno del programa.

4.5.1.- Consultoría para la ejecución del Plan

Tal y como se comentó anteriormente, con el fin de que el servicio se adapte a las necesidades y actividades del Plan de Mejora, se contratará como parte del presente pliego un conjunto de esfuerzos que se emplearán bajo demanda en actuaciones (encargos) concretos. Estas actuaciones consistirán en asesoría y consultoría, implantación de herramientas, diseño, elaboración, revisión y evaluación de procesos y procedimientos o ejecución de tareas concretas, siempre relacionadas o alineadas con la naturaleza del presente pliego. Para ello, el adjudicatario deberá disponer de los recursos apropiados, incluyendo personal con perfiles, capacidad y conocimientos especializados que puedan llevar a cabo los trabajos de diversa naturaleza mencionados.

Para la gestión de las actividades mencionadas, se define el concepto de **'Unidad de Esfuerzo Combinado' (UEC)** como la unidad de medida en la que se estimarán y contabilizarán los esfuerzos realizados para la ejecución de los diferentes encargos. La UEC queda definida de la siguiente manera:

UEC	Horas consultor senior (20%)	Horas consultor técnico (80%)	Total horas
1	2	8	10

Hay que tener en cuenta que la distribución de horas por perfil de trabajo podrá variar en función del tipo de encargo. No obstante, el esfuerzo y coste asociado a los trabajos siempre se medirá en base a la UEC ofertada. En el "*ANEXO I – Ejemplo de estimación de encargo con UECs*" del presente documento se

muestra, a modo de referencia, un ejemplo de tramitación de un encargo con UECs.

El procedimiento a seguir para gestionar las diferentes peticiones o encargos será el siguiente:

- FNMT-RCM comunicará sus necesidades de servicio al adjudicatario mediante *orden de trabajo* que describirá las necesidades de servicio de la FNMT-RCM.
- El adjudicatario realizará su propuesta de solución. Tras estudio y análisis de la solicitud, facilitará a FNMT-RCM una propuesta de solución junto con la planificación detallada de plazo y esfuerzo (en UECs) para la ejecución del encargo.
- FNMT-RCM evaluará la propuesta de solución y planificación y decidirá la aceptación o no de la misma. La FNMT-RCM podrá aceptar, matizar o rechazar la propuesta. En caso de aceptación de la propuesta, las desviaciones no atribuibles a FNMT-RCM respecto a dicha planificación serán asumidas por el adjudicatario.
- Para cada una de las peticiones de servicio o encargos, FNMT-RCM y el adjudicatario acordarán las fechas de entrega, los hitos relevantes, los entregables y los criterios de aceptación. Este acuerdo se recogerá en un documento que deberá ser firmado por ambas partes y servirá de base para efectuar la facturación correspondiente cuando se finalicen los trabajos.
- En caso de que la propuesta sea aceptada por FNMT-RCM, el adjudicatario llevará a cabo los trabajos correspondientes hasta su finalización.
- Tras la finalización y aceptación de los trabajos por parte de FNMT-RCM, se podrá realizar la correspondiente facturación del encargo.
- Adicionalmente, se llevará a cabo una encuesta de evaluación de la calidad de los trabajos realizados. Dicha evaluación será realizada por el

personal de la FNMT-RCM involucrado y será revisada con el Responsable del Servicio y Responsable de Proyecto del adjudicatario.

4.5.2.- Hitos y entregables

- Evaluación del grado de madurez parcial alcanzado tras la ejecución de cada una de las fases del plan, con propuesta de acciones correctivas en caso de desviación sobre lo previsto.
- Actualización de cuadro de mando de control, seguimiento y gobierno del programa de seguridad.

4.6.- FASE #5. EVALUACIÓN FINAL.

Tras la finalización de todas las fases establecidas en la hoja de ruta del plan de mejora de la seguridad, se realizará una evaluación del grado de madurez alcanzado y elaborará un informe final con los resultados. Dicho informe incluirá las lecciones aprendidas, aspectos de mejora, así como recomendaciones y directrices para futuras iteraciones del ciclo de mejora de la seguridad en el desarrollo.

4.6.1.- Hitos y entregables

Informe final de estado de la seguridad en el desarrollo de software.

5.- CANTIDAD DE SERVICIOS OBJETO DE LA CONTRATACIÓN

En el siguiente cuadro resumen se puede ver de forma esquemática la cantidad de bienes y servicios que a priori son objeto de la contratación.

Servicio / Bien ofertado	Incluído en el contrato	Cantidades y período de ejecución
Servicios de consultoría para la implantación de un programa de mejora de la seguridad en el desarrollo de software.		
Evaluación de madurez de la seguridad en el proceso de desarrollo de software.	Sí	De conformidad con lo definido para el servicio. Ver apartado “Descripción detallada del objeto de la contratación” (aptdo. 2.2)

Definición de objetivos y diseño del plan de mejora de la seguridad	Sí	De conformidad con lo definido para el servicio. Ver apartado "Descripción detallada del objeto de la contratación" (aptdo. 2.2)
Evaluaciones incrementales de madurez	Sí	De conformidad con lo definido para el servicio. Ver apartado "Descripción detallada del objeto de la contratación" (aptdo. 2.2)
Consultoría para la ejecución del Plan	Sí	Tantas UECs como oferte el licitador.

6.- DURACIÓN Y PRECIO.

Según lo descrito en el Pliego de Condiciones Particulares

7.- CONDICIONES DE EJECUCIÓN

De forma predeterminada y salvo autorización expresa, todos los desarrollos, despliegues y pruebas se realizarán en la infraestructura de la FNMT-RCM.

Se hace constar expresamente que, salvo autorización expresa[1], el adjudicatario no debe manejar ningún tipo de información o código de la FNMT-RCM - o desarrollado para ésta - en las instalaciones de su infraestructura o medios de almacenamiento.

El adjudicatario no realizará ninguna copia de las aplicaciones, código fuente o documentación relacionada bajo ningún concepto, ni permitirá que otro pueda realizarla, salvo autorización previa, expresa y por escrito de FNMT-RCM, o en los casos en que dicha copia haya de realizarse por motivos de razonable seguridad o propósitos de *backup*, lo que deberá ser comunicado por escrito a FNMT-RCM.

El adjudicatario se asegurará de que todos sus empleados o profesionales a su cargo sean avisados de que las aplicaciones, su documentación o cualesquiera

[1] En su caso, toda la información o código deberá estar debidamente protegido conforme a las directrices de seguridad que estableciera la FNMT-RCM para tal fin.

elementos de las aplicaciones (incluidos el código fuente, el código objeto, la documentación preparatoria; la documentación técnica, los manuales de uso, los diagramas de flujo, así como cualquier otro elemento relacionado o derivado de aquéllos) constituyen información confidencial, y que cualesquiera derechos de propiedad intelectual e industrial que existan y recaigan sobre los mismos son de exclusiva propiedad de FNMT-RCM.

El incumplimiento de lo dispuesto en los párrafos anteriores por el adjudicatario y por el personal a su servicio dará lugar a la imposición de las penalizaciones establecidas o a la resolución del contrato.

El servicio tendrá que ser prestado íntegramente en castellano.

8.- MONTAJE, INSTALACIÓN.

En caso de que alguna de las tareas o encargos asociados implique la instalación, configuración, desarrollo de componentes a medida, etc., el adjudicatario realizará dichas actividades en el entorno de la FNMT-RCM donde se ejecutan las herramientas y servicios que dan soporte a ciclo de vida del desarrollo de software.

9.- DOCUMENTACIÓN.

El adjudicatario deberá entregar la documentación enumerada y definida en los distintos apartados del presente pliego.

10.-GARANTÍAS

El adjudicatario será responsable de la calidad técnica de los servicios prestados, así como de las consecuencias que se deduzcan para FNMT-RCM o para terceros de las omisiones, errores, métodos inadecuados o conclusiones incorrectas en la ejecución del contrato. El adjudicatario mantendrá indemne a FNMT-RCM de las consecuencias derivadas del incumplimiento o cumplimiento defectuoso de sus obligaciones bajo el contrato.

En el supuesto de que, a juicio de FNMT-RCM, alguno o algunos de los miembros del equipo de trabajo careciese de la necesaria cualificación técnica o no prestase los servicios con la calidad y diligencia exigidas, FNMT-RCM estará facultada para solicitar al responsable designado por el adjudicatario su sustitución por otro técnico que sí tenga los conocimientos técnicos y/o

formativos necesarios, sustitución que deberá realizarse en el plazo máximo de 15 días naturales a contar desde la comunicación que en tal sentido FNMT-RCM dirija al adjudicatario y de forma que no se resienta en modo alguno la ejecución del contrato.

En caso de que el adjudicatario considere necesaria la sustitución de personal asignado a la prestación de los Servicios, el mismo, previa comunicación motivada con 15 días naturales de antelación, pondrá en conocimiento de FNMT-RCM la necesidad de sustituir a sus empleados y garantizará que el nuevo personal que asigne a la ejecución de los servicios estará suficientemente capacitado y formado a costa del adjudicatario para el adecuado desarrollo y ejecución de los servicios.

Será de exclusiva cuenta del adjudicatario el coste y tiempo que invierta en relación a su personal ante:

- Sustituciones de personal en el adjudicatario.
- Bajas laborales por enfermedad, maternidad u otras causas.
- Movilidad funcional, traslados, ascensos o cambio de puesto.

A tales efectos, el tiempo de formación, conocimiento del entorno de FNMT-RCM, adaptación y/o en general cualesquiera otras actuaciones por parte del nuevo personal del adjudicatario asignado a la ejecución de los servicios serán de cuenta y responsabilidad del adjudicatario de conformidad con lo previsto en el presente pliego y en el plan de aseguramiento de los servicios incluido su oferta técnica.

Si las sustituciones por causas ajenas a FNMT-RCM impiden la correcta ejecución de los servicios, producen retrasos o demoras o baja calidad de servicio, el adjudicatario será responsable frente a FNMT-RCM quien podrá, además de imponer las penalizaciones establecidas, instar unilateralmente la resolución del contrato.

El adjudicatario deberá incluir, al menos, un año de garantía sobre los programas o componentes desarrollados y, en general, los servicios prestados. En caso de que se detecte un malfuncionamiento de conformidad con los especificado y aprobado formalmente, el adjudicatario asumirá los costes asociados a la reparación del malfuncionamiento en cuestión.

11.-PENALIZACIONES

De acuerdo a lo establecido en el Pliego de Condiciones Particulares.

12.-ACLARACIONES SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS.

Las **consultas de carácter técnico** relacionadas con el presente pliego de condiciones pueden ser dirigida a:

Área Técnica del Departamento CERES

Área de Desarrollo CERES

e-mail: licitacionesdev.ceres@fnmt.es

Dirección de Servicios Digitales e Innovación

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

C/ Jorge Juan, 106

28009 Madrid

13.-OTRAS CUESTIONES

13.1.- EQUIPO DE TRABAJO

A continuación, se incluyen los perfiles que la FNMT-RCM entiende necesarios para la prestación del servicio:

Perfil	*Requisitos*
Responsable de proyecto	*Titulación:* • *Ing. Informática, Telecomunicaciones o similar.* *Capacidades:* • *Conocimientos sobre modelo de OWASP SAMM* • *Conocimientos en Secure-SDLC y SecDevOps.* • *Organización y priorización de tareas.* • *Entablar buenas relaciones con colaboradores.* • *Responsabilidad en la toma de decisiones.* • *Gestión de reuniones, resolución de conflictos y presentación de resultados.*

Perfil	Requisitos
	• *Conocimientos de cumplimiento normativo y legislación aplicable en materia de seguridad de la información y comunicaciones (ISO 27001, ENS), especialmente en lo que respecta a desarrollo de software seguro.* *Certificaciones valorables:* • *PMP o similar* • *CISSP o similar* • *CSSLP o similar* *Experiencia:* • ***8 años como mínimo de experiencia demostrable en la gestión de proyectos y servicios de seguridad de la información.***
Consultor Senior	*Titulación:* • *Ing. Informática, Telecomunicaciones o similar.* *Capacidades:* • *Conocimientos sobre modelo de OWASP SAMM* • *Experto en buenas prácticas sobre desarrollo seguro, Secure-SDLC y SecDevOps.* • *Organización y priorización de tareas.* • *Entablar buenas relaciones con colaboradores.* • *Responsabilidad en la toma de decisiones.* • *Gestión de reuniones, resolución de conflictos y presentación de resultados.* *Certificaciones valorables:* • *CSSLP o similar.* *Experiencia:* • ***4 años como mínimo de experiencia demostrable en la ejecución de proyectos y servicios de seguridad de la información (de los cuales, al menos 2 en la prestación de servicios similares al demandado en el presente pliego).***
Consultor Técnico	*Titulación:* • *Ing. Informática, Telecomunicaciones o similar.* *Capacidades:* • *Conocimiento sobre buenas prácticas de desarrollo seguro y experiencia en Secure-SDLC y SecDevOps* • *Organización y priorización de tareas.* • *Entablar buenas relaciones con colaboradores.* *Certificaciones valoradas:* • *CSSLP o similar.* *Experiencia:* • ***2 años como mínimo de experiencia demostrable en la ejecución de proyectos y servicios de seguridad de la información (de los cuales, al***

Perfil	Requisitos
	menos 1 en la prestación de servicios similares al demandado en el presente pliego).

13.2.- CONDICIONES DE LA OFERTA

La oferta deberá responder a la demanda de servicio y objeto de la contratación expresados en el presente pliego. Por este motivo deberá desarrollar la propuesta de valor del licitador, así como las características de los servicios y productos propuestos e incluidos en el alcance de la contratación y, en su caso, en torno a las fases identificadas.

Se consignan los requisitos mínimos, de forma y contenido, que ha de tener la oferta de la empresa licitante como respuesta al pliego de condiciones técnicas:

- La oferta deberá incluir el siguiente cuadro resumen con las certificaciones que el licitador considere para su mejor valoración y cumplimiento con las exigencias del presente pliego para la propia empresa, así como para los productos o servicios ofertados:

Certificación	Alcance	Fecha de caducidad	Ubicación
[Nombre de la certificación (empresa, productos, servicios)]	*[Breve descripción de los sistemas, servicios o productos incluidos en el alcance]*	*[Indicar la fecha de caducidad del sello o certificación referenciada]*	*[Indicar en dónde se puede encontrar el sello referenciado. Podría ser como anexo en la oferta o bien una URL a la entidad acreditadora/emisora]*
…	…	..	

- La oferta deberá incluir el siguiente cuadro resumen con las referencias (hasta tres años anteriores a la fecha de la oferta) que el licitador considere para su mejor valoración y cumplimiento con las exigencias del presente pliego en lo referente a experiencia empresarial:

Nombre Proyecto	Fecha inicio / Fecha fin	Empresa/ Organismo	Descripción general	Equipo de proyecto	Funciones	Precio de licitación
XXX1	201X	YYYY		Nombre y apellidos [1]	Actividades y responsabilidades	
				Nombre y apellidos [2]	Actividades y responsabilidades	
XXXn	…	…	…	…	…	
				…	…	
				…	…	

- La oferta deberá incluir el currículo de las personas, con nombres y apellidos, que desarrollarán el objeto de la contratación.
- Así mismo se deberá incluir el siguiente cuadro resumen con datos referidos al equipo de trabajo propuesto que el licitador considere para su mejor valoración y cumplimiento con las exigencias del presente pliego en lo referente al equipo de proyecto propuesto.

Datos personales, cualificación y experiencia					**Referencias (Sólo incluir proyectos realizados en los tres últimos años)**		
Nombre y apellidos	**Rol, actividades y responsabilidades**	**Cualificación (certificaciones/cursos):**	**Trabaja en:**	**Años experiencia en proyectos similares**	**Proyecto, empresa y descripción**	**Fecha inicio – Fecha fin**	**Funciones**
XXX YYY ZZZ	[Describir cómo participará en el proyecto que se propone	CISA / CISM / ITIL / Curso 1, Curso 2, etc.	[Empresa donde trabaja actualm	[¿Desde cuándo lleva participando en	[Nombre proyecto] [Empresa para la que se realiza] [Descripción general proyecto]	[Fecha inicio – Fecha fin]	[Actividades y responsabilidades en el proyecto

	en la oferta]		ente y cotiza]	proyectos relacionados con la oferta?]			referenciado]
					[Nombre proyecto] [Empresa para la que se realiza] [Descripción general proyecto]	[Fecha inicio – Fecha fin]	[Actividades y responsabilidades en el proyecto referenciado]
XXXn		…	…	…	…		…
					…		…
					…		…

- Se presentará un plan de calidad dentro de la oferta técnica que detalle los procedimientos a aplicar en relación a los siguientes temas:
    - Planificación y seguimiento.
    - Gestión de la demanda.
    - Gestión de recursos humanos.
    - Gestión de riesgos
    - Gestión de cambios
    - Gestión del aseguramiento de la calidad del servicio
- En el caso de que se oferten servicios de valor añadido sobre lo demandado en el pliego (pudiendo ser éstos de pago o simplemente añadidos sin coste al servicio demandado originalmente) éstos deberán estar bien identificados.

13.3.- CONDICIONES A CUMPLIR POR EL ADJUDICATARIO

El licitador que resulte ser la empresa adjudicataria deberá cumplir las siguientes condiciones:

- De forma previa al inicio de los trabajos, se deberá firmar con la FNMT-RCM el correspondiente acuerdo de confidencialidad en cuyo alcance

figure expresamente el alcance de los trabajos de esta contratación. El modelo de acuerdo será el propuesto por la FNMT-RCM.

- La empresa adjudicataria garantizará y será responsable de la confidencialidad e integridad de la información y los servicios que pudieran verse afectados por los trabajos objeto del presente pliego.
- Prestar los servicios con la diligencia de un profesional tecnológico experto, conforme a los términos, condiciones y acuerdos de nivel de servicio previstos en este pliego, siendo responsable de la observancia de dicha diligencia en cuantos trabajos, documentos y entregables sean realizados en ejecución del mismo.
- Asignar a la ejecución de las prestaciones objeto del presente pliego personal cualificado y con conocimientos en la materia con los niveles y perfiles técnicos adecuados a la prestación de los servicios.
- La falsedad en el nivel de conocimientos técnicos del personal ofertado, deducida del contraste entre los valores especificados en la oferta y los conocimientos reales demostrados en la ejecución de los trabajos, implicará la sustitución del mismo y, en su caso, la resolución del contrato.
- Nombrar un responsable del servicio para supervisar y controlar la ejecución del servicio y la calidad de la prestación.
- Nombrar un coordinador/responsable de proyectos para la ejecución, dirección y coordinación directa de los profesionales que realicen cada una de las peticiones de servicio.
- Elaborar y proporcionar a la FNMT-RCM toda la documentación y entregables derivados de la ejecución de las actividades realizadas durante la duración del contrato.
- Identificar e informar a la FNMT-RCM de los riesgos que puedan poner en peligro la consecución de los objetivos del contrato o de los proyectos que se lleven a cabo y mitigar el efecto que pudieran ejercer sobre el funcionamiento de las aplicaciones o servicios.

- Se deberán aceptar y respetar las políticas de calidad y seguridad de la información de la FNMT-RCM.
- El calendario de trabajo se establecerá de común acuerdo entre los diferentes Departamentos de la FNMT-RCM involucrados y la empresa.
- La empresa licitadora no podrá subcontratar los servicios objeto de esta licitación para la realización de los trabajos objeto de la contratación, salvo autorización expresa por parte de la FNMT-RCM.
- De forma predeterminada y salvo autorización expresa, los trabajos objeto de la contratación se realizarán en las instalaciones de la FNMT-RCM.
- Para la realización de determinados trabajos, la FNMT-RCM se reserva el derecho de acompañar en todo momento a la persona que los realice, supervisando así su actividad y el tratamiento de la información a la que tendrá acceso.
- Las comunicaciones entre la FNMT-RCM y la empresa licitante, al objeto de la remisión de informes y suministro de información sensible, se realizará cifrada con herramientas tipo PGP/S-MIME.
- Terminados los trabajos, la empresa deberá eliminar toda información sensible de la FNMT-RCM utilizada u obtenida durante prestación del servicio.
- No publicidad de relación con la FNMT-RCM sin previo consentimiento.

ANEXO I – EJEMPLO DE ESTIMACIÓN DE ENCARGO CON UECS

Supongamos un encargo que consiste en definir un proceso que permita estandarizar la evaluación de amenazas de seguridad de las aplicaciones y creación de los requisitos de seguridad asociados:

- La FNMT-RCM comunicará la necesidad de servicio.
- El adjudicatario realizará su propuesta de solución y estimará el número de UECs que se consumirán. A modo de ejemplo, se muestra la siguiente tabla de descomposición del trabajo:

Ejemplo petición servicio: Evaluación de amenazas	C. Senior (h)	C. Técnico (h)
Recopilar información de contexto.	2	8
Diseño del proceso.	0	10
Desarrollo de artefactos para implementar la práctica.	2	20
Formación a equipo de desarrollo FNMT.	3	8
Total Horas	**7**	**46**

- Tras la ejecución de la misma, se han obtenido las siguientes horas gastadas en la ejecución de la acción:

Ejemplo petición servicio: instalación Git	C. Senior (h)	C. Técnico (h)
Total Horas Realizadas.	7	46
UEC Gastadas	3,5 UECs + 18 horas perfil consultor técnico	

En este caso, como se observa existe un exceso de horas del consultor técnico (18 horas) que equivaldrían a 1,57 UEC. Este valor de 1,57 se calcula multiplicando el "exceso" de horas por la tarifa hora/cons. técnico y dividiendo entre el precio de UEC ofertado[2]. Por tanto, para el ejemplo considerado, el gasto total ejecutado en términos de UEC será de 5,1 UEC.

[2] Se ha calculado para una tarifa hora/cons. técnico de 40€ y un precio de UEC de 460 €.

Los UECs consumidos se irán descontando del total de UECs ofertados por el adjudicatario. Para el caso del ejemplo descrito, si el adjudicatario ofertó 50 UECs, quedarán disponibles 44,9 UECs para futuros encargos.