Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

perfil de contratante

LICITACIÓN

Contratación del suministro e implantación de un sistema de seguridad de la información y gestión de eventos de seguridad

Referencia CN 20-02-15 A

Entidad contratante	Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM)
Dirección	c/ Jorge Juan, 106 - 28009 Madrid
Tipo de contrato	SUMINISTRO
Tipo de procedimiento	Negociado con Publicidad
Características y requerimientos	Según pliegos adjuntos
Aclaraciones sobre pliegos de condiciones	Cualquier consulta técnica relacionada con la presente licitación debe ser dirigida a la siguiente dirección de correo electrónico: sistemas.ceres@fnmt.es
Presupuesto máximo de licitación	150.000 € (IVA no incluído)
Presentación de ofertas	Las empresas participantes podrán presentar cuanta documentación consideren oportuna para presentar la empresa, describir sus soluciones y explicar la forma en que cumplimentarán los requisitos de este pliego de condiciones. Dichas ofertas se deberán presentar con la referencia CN-20-02-15-A en el **Registro de la FNMT-RCM**, en documentos separados la parte técnica de la económica (en sobres independientes) e incluyendo copia digital de los mismos en CD o memoria USB, hasta la fecha y hora indicadas en el presente anuncio, debiendo entregar documento original firmado por un responsable de la empresa con firma autorizada. Las ofertas se dirigirán a la atención de: Área de Gestión. Dirección de Sistemas de

Departamento de Compras
Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
Jorge Juan, 106 28071 – Madrid
Tel.: 91 566 66 66
Fax: 91 566 67 50
Web: www.fnmt.es/proveedores

perfil de contratante

	Información. Teléfono: 91 566 67 04, e-mail: gestión.informatica@fnmt.es Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda C/ Jorge Juan 106.
Plazo de presentación de ofertas	Hasta las 12 horas del 24 de marzo de 2015
Lugar para presentación de ofertas	Fábrica Nacional de Moneda y Timbre–Real Casa de Moneda. Registro General, calle Jorge Juan, nº 106, 28009 Madrid. Horario de Registro General de 9:00 a 14:00 horas. *Salvo el día indicado para la finalización de ofertas que solo se admitirán las recibidas antes de las 12h.*

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Pliego de prescripciones técnicas para el suministro e implantación de un sistema de seguridad de la información y gestión de eventos de seguridad (SIEM)

Versión 1

FECHA: 02/03/2015

CONTROL DE LA DOCUMENTACIÓN:

	Elaborado	Revisado	Aprobado
Nombre			
Cargo			
Firma			
Fecha			

CONTROL DE CAMBIOS					
Edición		Autor	Resumen modificaciones	Revisado	Aprobado
Versión	Fecha				
1.0					

ÍNDICE

1. Introducción y objeto

La función prioritaria del departamento CERES (CERtificación ESpañola) de la FNMT-RCM es la de proveer servicios seguros de certificación electrónica para que los ciudadanos puedan comunicarse electrónicamente y de forma segura con la Administración Pública Española. En esta línea y con objeto de cumplir con los requisitos de la normativa de aplicación a los Prestadores de Servicios de Certificación, ETSI 101 456 y Webtrust, se requiere la implantación de un sistema que permita detectar, registrar y reaccionar ante los intentos de acceso no autorizados o irregulares a sus sistemas.

En este marco de trabajo se elabora el presente pliego cuyo objeto es la adquisición de bienes (equipamiento, licencias, etc.) y la contratación de servicios para la implantación de un sistema de gestión de la seguridad de la Información y gestión de eventos de seguridad, conocido como SIEM (Security Information and Event Management) por sus siglas en inglés, que permita la monitorización en tiempo real de todos (o la mayor parte) de los dispositivos importantes de la plataforma CERES, especialmente aquellos que forman parte de la infraestructura de clave pública propiamente dicha.

En el departamento CERES se ha realizado previamente una evaluación de los productos SIEM existentes en el mercado y basándonos en las funcionalidades y objetivos de seguridad que queremos cubrir, el presente pliego queda condicionado a la implementación de un sistema SIEM de IBM QRadar y QFlow. Las principales razones de esta elección son:

- Es un producto maduro en el mercado,
- Posicionado como primer líder en el informe Gartner de 2014,
- La configuración, administración y explotación es más sencilla que otros productos evaluados,
- Ofrece la funcionalidad de Netflow para la detección de tráfico anómalo y análisis de vulnerabilidades.

El objeto del presente pliego es la contratación de bienes y servicios para implementar en la infraestructura del departamento CERES de la FNMT-RCM un sistema SIEM basado en IBM QRadar y QFlow.

El licitador deberá plantear su oferta como un proyecto llave en mano que incluya la provisión de materiales, licencias, instalaciones, configuraciones, optimización, documentación y formación.

2. Marco legal y normativo

El artículo 81 de la Ley 66/1997 establece a la fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM) como entidad pública prestadora de servicios de certificación. El Real Decreto 1317/2001, que desarrolla el artículo 81 de la Ley 66/1997, establece el reglamento por el que se rige el departamento CERES para prestación de servicios técnicos y administrativos necesarios que garanticen la seguridad, validez y eficacia de las comunicaciones de las Administraciones Públicas y los organismos públicos, a través de medios electrónicos, informáticos y telemáticos.

El departamento CERES de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, para garantizar la máxima calidad y seguridad de sus servicios de certificación electrónica, sigue las normas y estándares siguientes:

- Norma europea ETSI 101 456 “Policy requirements for certification authorities issuing qualified certificates”
- Sello WebTrust que permite que los certificados raíz de la FNMT se incluyan de forma transparente en los navegadores.

3. Alcance del suministro

Los requisitos generales de este proyecto "llave en mano" de suministro e implantación de un sistema de seguridad de la información y gestión de seguridad son:

- Suministro de la infraestructura hardware y software de un sistema SIEM, y elementos de recogida y análisis de tráfico de red, con mantenimiento y soporte a un año del fabricante,
- Servicios técnicos especializado para la instalación, configuración de fuentes de eventos, casos de uso y optimización del sistema adquirido,
- Documentación detallada de la solución implantada y transferencia de conocimientos,
- Servicios de mantenimiento preventivo y correctivo en modalidad 9x5, prestados por la empresa adjudicataria del presente pliego basado en los servicios especializados en la tecnología del fabricante para el mantenimiento anual, con asistencia in-situ en caso necesario,
- Bolsa de 100 horas de consultoría in-situ para desarrollar funciones de optimización, configuraciones específicas e implantación de nuevos casos de uso que surjan.

Para la plataforma descrita en el apartado 4, "Entorno e hipótesis de trabajo", se ha calculado que la plataforma necesitará soportar hasta 1000 EPS (Eventos por segundo) y gestionar un tráfico agregado de menos de 1Gbps. En este sentido, **se debe garantizar que los eventos producidos si se superar el límite indicado, no se descartan y que al menos son almacenados.**

Se desea que las correlaciones en tiempo real se realicen sobre los eventos incluyendo un periodo de un mes y el almacenamiento de dichos eventos en formato histórico al menos por un periodo de un año.

Se desea también la posibilidad de disponer un mecanismo de archivado a largo plazo de todos los eventos de seguridad, por lo que el sistema debe poder acceder y se debe configurar el acceso a un servicio de backup/archivado a través de una tarjeta FibreChanel a 4Gbps o superior.

A modo de tabla, el equipamiento y servicios que se quieren contratar son:

Part Number	Descripción	Cantidad
D14RALL	IBM Security QRadar Core Appliance XX28 G2 Appliance Install Appliance + Subscription and Support 12 Months Tarjeta Host Bus Adapter (4Gbps mínimo) para acceso a servicios de backup/archivado en SAN FibreChanel	1
D0V5HLL	IBM Security QRadar SIEM All-in-One 31XX Install License + SW Subscription and Support 12 Months	1
D0WTULL	IBM Security QRadar SIEM Event Capacity Increase from 1K to 2.5K EPS Install License + SW Subscription and Support 12 Months	1
D14RMLL	IBM Security QRadar QFlow Collector 1202 G2 Appliance Install Appliance + Subscription and Support 12 Months	1
--	Mantenimiento preventivo y correctivo en la modalidad de 9x5 con asistencia in-situ por un periodo de 1 año.	1
--	Bolsa de 100h para configuraciones extendidas y consultoría en general.	1

Las fases en las que se estructuran los servicios demandados con objeto de la implantación de un sistema SIEM en la infraestructura de CERES se enumeran a continuación.

Los servicios a ser ofertados por el licitante se describen extensamente en el apartado 6. (Descripción de los servicios, fases, hitos y entregables).

- **Fase 1** - Inicio del proyecto, análisis y diseño de la solución.
- **Fase 2** – Suministro, Instalación del sistema, despliegue y configuración básica de QRadar y QFlow. Implantación de correlaciones incluidas por defecto.
- **Fase 3** – Integración de fuentes: Elementos de red y elementos de seguridad perimetral de toda la infraestructura incluido en Centro de Respaldo, integración con el sistema de monitorización de la infraestructura e implantación de caso de uso: control de accesos no autorizados a los sistemas de hardware y software.
- **Fase 4** – Integración de fuentes: Elementos HW y SW de todos las redes (RED-1,RED-2, RED-3,RED-4) y sus equivalentes en el centro de respaldo, implantación de caso de uso: control de acceso no autorizado a elementos de hardware y software.
- **Fase 5** – Optimización del sistema. Nuevos y Pruebas de Aceptación
- **Fase 6** – Documentación y transferencia de conocimientos

4. Entorno e hipótesis de trabajo

El SIEM recibirá información de las redes internas del CPD principal y el CPD de respaldo. Estas incluirán los servidores (basado principalmente en la plataforma Solaris Sparc habiendo algunos servidores en la plataforma de Windows), y los elementos de red y de seguridad perimetral de la plataforma CERES así como las aplicaciones de la plataforma CERES que se consideren de interés. En particular recibirá información de las siguientes fuentes:

- servidores (Solaris sparcs y Windows)
- tráfico de FW, IPS, Balanceadores, estándares del mercado
- elementos de red (routers y switches) estándares del mercado
- aplicaciones web, BD, directorio, aplicaciones criptográficas, etc.
- dispositivos criptográficos

Los números concretos se proporcionarán a los licitantes en el momento de confección de ofertas para el correcto dimensionamiento de los servicios profesionales.

Se desea integrar el SIEM al flujo de trabajo de la plataforma CERES y al sistema de monitorización de la infraestructura así como realizar el archivado externo de los eventos de interés a largo plazo en un entorno de Backup SAN FibreChanel a una velocidad mínima de 4Gbps. Las fuentes a configurar y la infraestructura de la plataforma se detallará en las reuniones iniciales con la empresa adjudicataria.

5. Descripción general del sistema a implantar

La principal función del sistema, caso de uso; será el control de acceso a los sistemas de información, informando en tiempo real de todos los intentos de acceso no autorizados a los sistemas hardware y software de la plataforma CERES.

Además se quiere utilizar el SIEM en los siguientes escenarios:

- Control de accesos a dispositivos, sistemas y aplicaciones
  - Configuración de todos los elementos identificados en la sección anterior[1], para que envíen logs de accesos al SIEM.
  - Configuración para que ante intentos repetidos de accesos incorrectos a cada uno de los sistemas, se genere una alerta de seguridad y avise tanto por consola, como enviando la información de la alarma a un sistema de monitorización general y por correo electrónico. El correo electrónico formará parte del flujo de Gestión de Incidencias de Seguridad ya implementado.
  - Cifrado de logs en el transporte de la fuente al recolector de eventos

- Prevención de fuga de datos (DLP)
  - Configuración de módulos o de reglas que permitan al SIEM tratar de obtener eventos que demuestren salida de información

- Monitorización y caracterización del tráfico de red para detectar amenazas desconocidas, basadas en patrones
  - Análisis de tráfico en todos los segmentos de red de la infraestructura CERES para establecer un comportamiento normal del tráfico, generando alarmas cuando se excedan unos umbrales predeterminados. Las alarmas se generarán tanto en consola como enviando mensajes al sistema de monitorización de la plataforma (mediante SNMP u otro modo establecido) como por correo electrónico. El correo electrónico servirá para generar el flujo de Gestión de Incidencias de Seguridad ya implementado.

- Almacenamiento de todos los registro de acceso a los sistemas como evidencias para Análisis Forense.
  - La retención de los logs en tiempo real para la será de 30 días para la correlación de eventos.
  - La retención de la información será de 1 año.

[1] La lista completa de todos los servidores y eventos y logs a integrar se darán al adjudicatario al inicio del proyecto.

- Almacenamiento de logs (excluyendo los de acceso) de aplicaciones
    - Se pretende utilizar el SIEM como punto único de almacenamiento de logs de aplicaciones que intervienen en el ciclo de vida de gestión de certificados electrónicos

- Archivado. Se configurará el sistema para el archivado de aquellos logs/eventos que sobrepasen el periodo de retención determinado.

- Generación automática de informes
    - Se configurará la ejecución de informes automáticos una vez al mes, para comprobar de forma tabulada y ordenada las alarmas de seguridad de forma categorizada para la toma de decisiones.
    - Se configurará informes automáticos que muestren la información de los usuarios activos de los sistemas de información.

6. Descripción de los servicios, fases, hitos y entregables

Los servicios objeto de este pliego se dividen en fases.

Cada una de las fases lleva asociada unos hitos y unos entregables cuya función es la de garantizar el cumplimiento del hito en cuestión.

El proyecto de implantación del sistema y, por tanto, el servicio ofertado por el licitador debe ajustarse a esta estructura (fase, hitos, y entregables.)

La duración aproximada del proyecto de implantación tendrá un mínimo de 7 semanas, sin incluir el periodo de transferencia de conocimientos.

Toda la documentación del proyecto junto con las implementaciones realizadas deberá entregarse como mínimo en formato digital.

6.1. Fase 1: Inicio del proyecto, análisis y diseño de la solución

6.1.1. Descripción del servicio

El objetivo de esta fase es la de establecer las pautas, objetivos, alcance y ámbito del proyecto, establecer los recursos involucrados (humanos y materiales), los mecanismos de seguimiento y control a utilizar, el calendario, las pautas a seguir, etc. Así como determinar los requisitos y casos de uso del sistema que se va a implementar a partir del análisis y diseño del sistema.

6.1.2. Hitos y entregables

Se considerará satisfecho este hito cuando se realice la reunión para la planificación del proyecto entre el departamento CERES y la empresa adjudicataria para:

- revisar el alcance y objetivos del proyecto,
- constituir los equipos de trabajo y establecer los acuerdos necesarios
- concretar la información inicial que el departamento CERES debe proporcionar al equipo de proyecto
- establecer el calendario de trabajo y mecanismos de seguimiento
- realizar un análisis y diseño de la solución, documentando
    - la arquitectura de alto nivel y detallada,
    - los sistemas y redes involucrados en la solución,
    - requisitos detallados de la arquitectura,
    - requisitos funcionales,
    - casos de uso a implantar y flujos de datos
    - personalizaciones necesarias.
    - Determinación de los datos importantes que se quieren almacenar de cada elemento de la plataforma,
    - Desarrollo del plan de pruebas de aceptación.

ENTREGABLES FASE 1

Se entregarán los documentos revisados por el departamento CERES de la FNMT-RCM sobre el plan de proyecto, el diseño y la arquitectura.

El documento del plan de proyecto incluirá:

- el alcance y los objetivos,
- el equipo involucrado,
- cronograma del proyecto,
- los mecanismos de seguimiento, etc.

El documento de diseño y arquitectura contendrá:

- diseño y arquitectura,
- requisitos del sistema,
- elementos de la infraestructura involucrados en la implantación,
- requisitos funcionales,
- casos de uso a implementar,
- personalizaciones necesarias
- datos que se van a almacenar para cada elemento de la infraestructura,
- requisitos de optimización de la recogida de logs y
- pruebas de aceptación.

Estos documentos deberán ser aceptados por el departamento CERES de la FNMT-RCM.

Tiempo estimado: 4 días.

6.2. Fase 2: Suministro, Instalación del Sistema, Despliegue y Configuración Básica de IBM QRadar y QFlow.

En esta fase se instalarán y se aplicará la configuración mínima a los equipos QRadar SIEM y QRadar QFlow para poder comenzar a recoger eventos, fuentes de logs y tráfico de nivel 7 de los distintos segmentos de red de la infraestructura.

6.2.1. Descripción del servicio

- Entrega del equipo validando los requisitos de hardware y software de la plataforma.
- Instalación y configuración inicial de los dispositivos (QRadar y QFlow) en el CPD principal de CERES,
- Configuración general de los dispositivos:
  - Configuración de los parámetros de red y test de los servicios
  - Configuración de la base de datos, el entorno y el tiempo de retención de datos
  - Instalación de últimas actualizaciones y parches
  - Creación de usuarios y roles
  - Definición de políticas
  - Configuración de SNMP
  - Configuración de actualizaciones automáticas
  - Backup de los ficheros de configuración
  - Asignar procesos de recolección de eventos
- Personalización del sistema
  - Configuración y prueba de la jerarquía de red
  - Validación y modificación de la jerarquía según necesidades del departamento CERES
  - Almacenamiento offline en un dispositivo SAN fibreChanel a 4Gbps como mínimo
  - Backup del fichero de jerarquía de red
  - Configurar el sistema para comprimir los datos en el almacenamiento offline
  - Configurar direcciones de email para envío de alarmas
- Ajustes iniciales
- Configuración de la recolección de eventos de las fuentes soportadas de manera estándar
- Configuración de flujos soportados de forma estándar
- Implantar las correlaciones por defecto que trae el sistema
- Conexión con servicio de backup/archivado
- Ejecución del plan de pruebas asociado a esta fase

6.2.2. Hitos y entregables

En esta fase se considerará cumplido el hito cuando se instalen y configuren los dispositivos con la configuración básica y personalizada, se ejecute el plan de

pruebas correspondiente a esta fase, se elaboren y aprueben los documentos asociados a esta fase.

ENTREGABLES FASE 2 –

- Licencias disponibles[2] y software descargado en las máquinas.
- Documento que detalle:
  - Descripción del sistema. Esto es, equipamiento instalado, características (versiones, capacidad, funcionalidad),
  - Versiones del software descargado en las máquinas,
  - Configuración de la base de datos y tiempos de retención de datos,
  - Configuraciones básicas realizadas, las IPs, los segmentos de red monitorizado por el QFlow,
  - Parámetros de configuración iniciales y personalizadas del sistema,
  - Esquema de las interconexiones realizadas,
  - Funciones activas en el sistema,
  - políticas y reglas de correlación implantadas (las que pueda traer por defecto) y sus acciones
  - Procedimientos para verificar y modificar los parámetros configurados,
  - las configuraciones realizadas, el procedimiento a seguir para la recuperación desde el servidor de eventos almacenados offline y poder leerlos,
  - Procedimientos para verificar el funcionamiento correcto del sistema, la localización de los logs del sistema y cualquier otra información necesaria para solucionar posibles problemas que se produzcan en el sistema
  - Procedimientos seguidos en la resolución de los problemas encontrados en esta fase.

Tiempo estimado: 3 días

[2] Se podrá empezar con licencias temporales pero al final del proyecto la licencia instalada debe ser la licencia permanente.

6.3. Fase 3: Integración de fuentes: Elementos de red y elementos de seguridad perimetral de toda la infraestructura, integración con el sistema de monitorización de la infraestructura, e implantación de caso de uso: control de accesos no autorizados a los sistemas de hardware y software

6.3.1. Descripción del servicio

Esta fase incluye:

- La configuración los elementos de red y seguridad perimetral (routers, switches, IPS, Firewalls, VPNs) de toda la plataforma (CDP principal y respaldo),
- El Cifrado el envío de los datos recolectados de eventos,
- El sellado de tiempo a los datos y flujos de las fuentes que se vayan a almacenar,
- La configuración del QFlow para el análisis del tráfico en los segmentos de red especificados,
- Configuración de NetFlow en los elementos de red de la plataforma que lo soporte (routers, switches)
- La optimización del sistema para la recogida de datos para que sólo se almacenen los datos que se consideren de interés,
- La configuración del caso de uso de accesos no autorizados a los sistemas de hardware y software,
- El filtrado de eventos para reducir falsos positivos y detectar incidencias de riesgo,
- Identificar y eliminar las fuentes de ruido
- La integración del QRadar y QFlow con el sistema de Monitorización de la infraestructura y con el sistema de gestión de incidencias de la plataforma.

6.3.2. Hitos y entregables

El hito se considerará conseguido cuando se configuren todas las fuentes implicadas en esta fase y se integre el sistema con el sistema de gestión de incidencias y de monitorización de la plataforma y se ejecute el plan de pruebas correspondiente a esta fase.

ENTREGABLE FASE 3 – Se entregará documentación que incluya:

- pasos realizados en la configuración de cada uno de los elementos implicados incluyendo configuraciones necesarias en los elementos de seguridad para permitir el tráfico de datos,
- lista de las fuentes y eventos recolectados y los que se van a almacenar,
- localización de los eventos recolectados en el servidor,
- casos de uso implementados,
- Integración con el sistema de monitorización de la infraestructura y con el sistema de gestión de incidencias,

- optimizaciones realizadas,
- cualquier problema encontrado en esta fase y los pasos realizados para resolverlos.

Tiempo estimado: 5 días

6.4. Fase 4: Integración de fuentes: Elementos HW y SW de todas las redes (RED-1, RED-2, RED-3, RED-4) y sus equivalentes en el centro de respaldo, implantación de caso de uso: control de acceso no autorizado a elementos de hardware y software.

6.4.1. Descripción del servicio

Los objetivos de esta fase son:

- Configurar los elementos del sistema que forman parte de las redes Red-1, Red-2, Red-3 y Red-4 que incluye el hardware criptográfico, software de la Autoridad de certificación, de validación, y de sellado de tiempo, así como las bases de datos implicadas, servidores de aplicación, sistemas operativos, etc… en el CPD principal y su equivalente en el CPD de respaldo,
- Cifrar de los datos en la transmisión,
- Optimizar los datos de las fuentes y de los flujos,
- Configuración de QFlow para el análisis de flujos de red
- Configurar el caso de uso de accesos no autorizados a los sistemas hardware y software
- Aplicar el sellado de tiempo de los datos que se vayan a almacenar,
- Integrar con el sistema de Monitorización de la infraestructura y con el sistema de gestión de incidencias de la plataforma
- Personalizar la pizarra de la consola principal.

6.4.2. Hitos y entregables

El hito se considerará conseguido cuando se configuren todas las fuentes de la redes indicadas y se integren el sistema con el sistema de gestión de incidencias y de monitorización de la plataforma y se ejecute el plan de pruebas correspondiente a esta fase.

ENTREGABLE FASE 4 – Documentación que incluya:

- pasos realizados en la configuración de cada uno de los elementos implicados incluyendo configuraciones necesarias en los elementos de seguridad para permitir el tráfico de datos,
- lista de los logs y eventos recolectados y almacenados,
- localización de los datos almacenados en el servidor,
- descripción los algoritmos utilizados para el cifrado de datos y el sellado de tiempo,

- Integración con el sistema de monitorización de la infraestructura y con el sistema de gestión de incidencias,
- casos de uso implementados,
- optimizaciones realizadas y reglas de correlación de las fuentes integradas
- cualquier problema encontrado en esta fase y los pasos realizados para resolverlos.

Tiempo estimado: 15 días

6.5. Fase 5: Optimización del sistema. Pruebas de Aceptación

Esta fase podrá ser realizada dos semanas después de la configuración inicial para poder tener suficiente información de eventos recogidos e identificar las posibles mejoras y optimizaciones del sistema.

Para finalizar, en esta fase se pretende verificar la correcta implementación del sistema QRadar SIEM y QRadar QFlow y para ello se ejecutará el plan de pruebas de aceptación.

6.5.1. Descripción del servicio

Los objetivos de esta fase son:

- A partir de los eventos recolectados por QRadar, se optimizará el sistema basándose en los requisitos de negocio, las políticas de seguridad de CERES, incluyendo mejora de reglas (personalización de reglas, habilitar o deshabilitar reglas, eliminar falsos positivos, etc.,) búsquedas predefinidas, gráficos e informes de interés, administrar la gestión de agregación de datos, configuración de un paquete de informes de “Compliance”, etc.
- Realización de pruebas para comprobar el correcto funcionamiento de la arquitectura desplegada.

6.5.2. Hitos y entregables

Se completará este hito cuando una vez obtenida suficiente información del comportamiento del sistema se determinen y apliquen las mejoras y optimizaciones a realizar y se completen:

- Mejoras en las reglas para eliminar falsos positivos
- Agregación de datos
- Configuración de un paquete de informes “compliance”,
- Generación de gráficos e informes de interés
- Etc.

ENTREGABLE FASE 5 – Documentación asociada con

- las configuraciones y desarrollos que se realizaron durante la optimización del sistema,
- los pasos seguidos para la resolución de cualquier problema encontrado en esta fase así como cualquier información adicional que sirva para verificar el correcto funcionamiento de esta funcionalidad.
- Documentación de las pruebas realizadas junto con el resultado de las pruebas. Esta fase se considerará finalizada cuando se resuelvan todos los problemas encontrados en esta fase y las fases anteriores.

Tiempo estimado: 8 días

6.6. Fase 6: Documentación y transferencia de conocimientos
Descripción del servicio

Creación de una guía de instalación y una de operación de la solución total que servirá de guía para la transferencia de conocimientos

Se solicitan dos sesiones de transferencia de conocimiento sobre la operación y mantenimiento del sistema implantado. Las sesiones incluirán:

- Arquitectura del sistema (HW, bases de datos que utiliza, comunicaciones con las fuentes, etc,)
- Instalación del sistema (HW, bases de datos que utiliza, integración y comunicación con otros elementos de la red, con internet, etc.)
- Instalación de los componentes QRadar SIEM y QRadar QFlow.
- Arranque y parada del servicio,
- Actualizaciones del sistema,
- Tratamiento y explotación de los datos recopilados por la herramienta (uso de la herramienta para establecer incidentes de seguridad que deban ser investigados)
- Creación de casos de uso, reglas de correlación
- Monitorización de la red y de actividades de log (filtrado de falsos positivos, búsquedas, agrupaciones y ordenaciones, almacenamiento de búsquedas, visualización de logs de auditorías, etc.)
- Optimización, análisis y resolución de problemas en el sistema,
- Configuración de fuentes específicas: parsing
- Configuración del cuadro de mando, generación y programación de informes,
- Funcionalidad de informes, tratamiento de datos e información para la detección de incidencias
- Etc.

Para todo ello se podrán utilizar como ejemplo las configuraciones y trabajos realizados en fases anteriores.

La formación se realizará en las instalaciones de la FNMT-RCM.

6.6.1. Hitos y entregables

Este hito se considerará alcanzado cuando se realicen las dos sesiones de formación y se revise la documentación aportada.

ENTREGABLE FASE 6 –

En entregable son los manuales de formación con los temas tratados en las sesiones de formación con las referencias oportunas a la documentación del fabricante, junto con manuales de operación y de instalación.

Tiempo estimado: 4 días.

6.7. Resumen de las fases

A continuación se adjunta una tabla resumen de las fases, entregables y días por cada fase.

Fase	Entregable	Jornadas
1. Inicio, análisis y diseño	Documentación del plan de proyecto y de la arquitectura y diseño	4
2. Suministro, instalación, despliegue y configuración	Hardware, licencias y documentación de configuración básica	3
3. Integración de fuentes: Elementos de red y seguridad.	Documentación de configuraciones realizadas, etc.	5
4. Integración de fuentes: Resto de elementos de la plataforma.	Documentación asociada con esta fase.	15
5. Optimización del sistema. Aceptación Sistema	Documentación de las optimizaciones realizadas Documentación de las pruebas de aceptación realizadas y sus resultados	8
6. Documentación y transferencia de conocimientos	Manuales y sesiones de formación	4
Total		39

7. Servicio de Soporte y Consultoría

7.1. Servicios de Soporte del fabricante

Se deberá incluir en la oferta, los servicios de Soporte del Fabricante para toda la infraestructura HW y SW adquirida por un periodo de 1 año. Este servicio debe contemplar al menos:

- Acceso a las nuevas actualizaciones y versiones del SW instalado.
- Soporte técnico online. Acceso a las bases de datos de conocimiento de los productos adquiridos.
- Soporte técnico telefónico para actualizaciones, nuevas implantaciones y migraciones.
- Resolución de problemas de forma telefónica para situaciones de severidad grave, las 24h del día los 7 días de la semana.
- Sustitución HW de piezas averiadas o llegado el caso cualquiera de los equipos adquiridos en formato Next Bussines Day (NBD) por un equipo de las mismas o superiores características.

NOTA

FNMT-RCM autorizará a la empresa adjudicataria de este pliego a realizar las gestiones necesarias en su nombre frente al fabricante de los productos adquiridos para la resolución de incidencias, cambio de elementos, cambio de equipos, etc… Dicha empresa debe actuar como interlocutor único entre el fabricante y FNMT-RCM.

7.2. Servicios de Mantenimiento Correctivo y Preventivo in-situ 9x5

Como complemento a los servicios proporcionados por el fabricante de los productos HW y SW adquiridos, se desea la contratación de un servicio de mantenimiento in-situ en horario de oficina 9x5, por un periodo de 1 año. Este servicio debe contemplar al menos:

- Servicios de Soporte Telefónico y Soporte In-situ en caso de no poderse solucionar el problema de forma telefónica, en horario 9x5x4 (4 horas de tiempo de respuesta).
- Interlocución única entre FNMT-RCM y el fabricante de los productos para el escalado de las incidencias y la sustitución de equipos caso de ser necesario.
- Seguimiento de las incidencias abiertas.
- Mantenimiento preventivo semestral con objetivo de detectar posibles incidencias, realización de actualizaciones de software, verificar logs del sistema así como la correcta implantación de políticas de los equipos. Realización de las copias de seguridad necesarias para una correcta restauración de los sistemas a su correcto funcionamiento o ante la necesidad de cambio por avería.

- Mantenimiento correctivo con tiempo de respuesta inmediato y tiempo de resolución de 4h o siguiente día hábil en función del horario informado de la avería.
- Así mismo se establecerán sesiones periódicas de uno a tres días cada tres meses que nos ayuden a optimizar el sistema y analizar posibles alarmas o eventos.
- Los técnicos asignados al proyecto deben disponer de amplia experiencia en instalaciones similares.
- Se debe garantizar por parte de la empresa adjudicataria, que ante avería o fallo eventual de los equipos instalados en FNMT-RCM-CERES, se realizará una sustitución por un equipo de similares o mejores prestaciones, realizando todas las configuraciones necesarias para que el sistema quede completamente operativo con la misma funcionalidad previa a la avería.

7.3. Servicios de Consultoría

Como ya se ha especificado, además de los servicios de soporte por parte del fabricante y de los servicios de soporte in-situ por parte del adjudicatario, se solicita al licitador una oferta en concepto de **bolsa de 100 horas de consultoría in-situ** para necesidades especiales que puedan surgir durante el primer año de vida del sistema como por ejemplo, sin descartar otros, los siguientes casos:

- Ayuda en la definición e implementación de nuevos casos de uso como pueden ser:
  - Creación de reglas de correlación ampliadas sobre los eventos recogidos que surjan como necesidades de FNMt-RCM-CERES
  - Detección de amenazas internas,
  - Detección de fuga de datos,
  - Detección de tráfico en puertos anómalos, servicios sospechosos, etc.,
  - Detección de ataques de SQL Injection y otros ataques web,
  - Control del estado de actualizaciones de los sistemas operativos de la plataforma,
  - Aquellos casos de usos que nos asesore el adjudicatario del pliego

Esta bolsa de horas se ejecutará bajo demanda de la FNMT-RCM pudiendo quedar sin efecto alguno en caso de que no exista necesidad de ejecución.

Las horas de la bolsa no consumidas en este año podrán añadirse a la bolsa de horas del año siguiente en el caso en el que se contrate el servicio de soporte con la empresa licitadora en el siguiente año.

La FNMT-RCM establecerá las visitas periódicas y realizará las peticiones correspondientes a esta fase con suficiente detalle y antelación para que el proveedor planifique las intervenciones necesarias.

8. Condiciones a cumplir por la empresa proveedora

La empresa adjudicataria deberá cumplir las siguientes condiciones adicionales:

- De forma previa al inicio de cualquier trabajo, la empresa licitadora deberá firmar con la FNMT-RCM el correspondiente acuerdo de confidencialidad, según modelo de la FNMT-RCM y que se puede solicitar como aclaración a la presente oferta.
- La empresa licitadora deberá aceptar y respetar las políticas de calidad y seguridad de la información de la FNMT-RCM
- La empresa licitadora deberá aceptar los términos y condiciones del contrato o pedido resultante, especialmente en lo que se refiere a los plazos de abono de facturas presentadas. No obstante, se podrán negociar tantos hitos intermedios de facturación como se estimen oportunos.
- La contratación para la realización de los servicios tendrá el carácter de "intuitu personae" por ser realizada en consideración de una persona determinada, existiendo una obligación genérica de abstenerse de toda conducta que pueda menoscabar la confianza depositada por la FNMT-RCM en el Consultor. Quedará, por tanto, prohibida la cesión a terceros del contrato y la subcontratación, total o parcial, de los trabajos objeto del mismo sin la expresa autorización por parte de la FNMT-RCM.
- La empresa adjudicataria deberá respetar el formato de los entregables indicado en este pliego. Salvo petición o consentimiento expreso no se podrán unificar.
- El calendario de trabajo se establecerá de común acuerdo entre los diferentes Departamentos de la FNMT-RCM involucrados y la empresa adjudicataria.
- 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 licitadora al objeto de la remisión de informes y suministro de información sensible se realizará cifrada con herramientas tipo PGP.
- Terminados los trabajos, la empresa adjudicataria 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

9. Condiciones de la oferta

La oferta de servicios presentada por el licitante describirá la solución propuesta para la prestación de los servicios descritos en el alcance del suministro teniendo en cuenta los siguientes requisitos:

1. La oferta debe incluir el licenciamiento a 1 año de
    a. QRadar Core
    b. QRadar SIEM
    c. QFlow

En este licenciamiento deberán estar incluidos los servicios de soporte técnico en su modalidad de 9x5 (hora laborables).

2. La FNMT-RCM deberá poder contratar los servicios de forma independiente por fases, esto es, podrá contratar servicios para una o más de una fase.

   Por este motivo, la oferta de servicios y su facturación deberá estar **totalmente desglosada** por fases, hitos y entregables.

   Se indicará claramente los costes asociados a cada uno de estos puntos de forma totalmente independiente.

   También figurará desglosado:
    a. coste de los dispositivos o equipos del sistema
    b. coste de las licencias,
    c. coste de los servicios profesionales desglosado por fases que incluirá
        a. servicio de instalación y configuración
        b. servicio de asistencia técnica que incluye la bolsa de horas
    d. Soporte y mantenimiento de los siguientes dos o tres años (primer año de garantía y sin coste adicional).[3]

Para la

Fase 6: Documentación y transferencia de conocimientos Descripción del servicio, se requiere el coste unitario por hora.

La presentación de una oferta sin la debida estructuración de costes podrá ser descartada en el proceso de selección.

3. La FNMT-RCM requiere la prestación de este tipo de servicios por parte de empresas y profesionales con conocimiento y experiencia en la materia que nos ocupa. Esta cuestión no es una opción sino un requerimiento en este pliego.

   Por este motivo, se deberá indicar expresamente:

    a. Certificado de ser “partner” o “integrador“ por el fabricante,
    b. Los proyectos similares en los que ha participado el licitador como empresa,

[3] Para tener una estimación de cuál será el coste de mantenimiento del sistema en los próximos años.

c. Independientemente de si los trabajos fueron realizados con la empresa licitante u otra distinta, los proyectos en los que ha participado el equipo de proyecto que se propone, así como el rol con el que lo hicieron.

La oferta cuyos servicios se basen en un equipo de proyecto sin conocimiento y experiencia será descartada en el proceso de selección.

4. Se deberá detallar la identidad (nombres y apellidos), **cualificaciones y certificaciones del producto de las personas que desarrollarán los trabajos (equipo de proyecto) y si se trata de personal propio o subcontratado. Estas cualificaciones y certificaciones se vincularán con las tareas y actividades que se propongan para la realización del servicio y tendrán carácter contractual**, pudiendo la empresa adjudicataria cambiar las personas que prestan el servicio pero no así la cualificación y experiencia de éstas.

   Se valorará específicamente la experiencia de las PERSONAS en proyectos similares y certificaciones PERSONALES relacionadas con las materias de este proyecto.

5. La oferta de servicio deberá presentarse bajo la forma de un proyecto. Cada función, dentro de este proyecto, deberá estar perfectamente identificada y tener asignada a una persona responsable de llevarla a efecto.
   Las ofertas deberán contener un Plan de Proyecto completo, en el que se incluirá una metodología de trabajo que permita validar su correcto funcionamiento durante la ejecución del contrato mediante los adecuados elementos de control que figurarán descritos.

6. El proyecto deberá cumplimentar lo requerido en los siguientes apartados, con la misma denominación y en el mismo orden:

   1. Descripción y metodología del proyecto
      a. Descripción de la metodología de trabajo que el licitador pretende seguir para la instalación y configuración de QRadar y QFlow y la integración con el flujo de trabajo y la herramienta de monitorización de la plataforma.
      b. Descripción de los elementos de control para el correcto desarrollo del proyecto

   2. Recursos humanos
      a. Se detallará el personal implicado incluidas certificaciones relacionadas con el servicio solicitado
      b. Se detallará el número de horas que se comprometen para la realización de los trabajos
      c. Se incluirá un detalle de las metodologías de trabajo que se utilizarán

   3. Propuesta
      Debe incluir
      a. un cronograma detallado con las actividades relativas a este servicio.

b. Hardware específico a implantar con modelo, módulos de hardware, software, capacidades y licencias
c. Implementaciones que se realizarán especificando casos de uso
d. Contenido que tendrá la documentación entregada, resaltando aquella información que pueda considerarse útil o de valor añadido para el departamento CERES de la FNMT-RCM y el porqué,

4. **Valor añadido**
   a. El licitador podrá incluir información que pueda ser relevante y diferencial al servicio demandado explicando la utilidad de ese valor añadido.
   b. Se tendrá muy en cuenta la inclusión de nuevos caos de uso y evolución del proyecto hacia escenarios más complejos.
5. **Experiencia en trabajos similares**
   a. Ejemplos de casos de éxito de los últimos dos años del licitador y su personal en proyectos similares al servicio demandado en este pliego.

9.1. Orden de prelación

En caso de que exista conflicto entre la oferta del licitante y el presente pliego de condiciones técnicas tendrá prelación lo expresado en éste último.

10. Condiciones de facturación del proyecto

La FNMT-RCM facturara en base a las fases e hitos completados:

Se facturará el hardware cuando este se reciba y se verifique su correcto funcionamiento.

La facturación del software se completará cuando se reciban e instalen las licencias definitivas.

La facturación por la instalación y configuración se realizará de la siguiente forma:

- se pagará un 35% al finalizar la fase 4,
- un 30% al completar la fase 6,
- y un 35% al completar todas las fases del proyecto.

Concepto	Facturación	Porcentaje
HW y su Mantenimiento	Cuando se verifique su funcionamiento correcto	100% del coste del HW + Mantenimiento
SW y su Mantenimiento	Cuando se reciban e instalen las licencias definitivas de los productos	100% del coste del SW + Mantenimiento
Instalación y configuración	Al completar la fase 3	25% de los Servicios Profesionales de Implantación
Instalación y configuración	Al completar la fase 4	50% de los Servicios Profesionales de Implantación
Instalación y configuración	Al completar el proyecto	25% de los Servicios Profesionales de Implantación
Mantenimiento 9x5.	Facturable mes a mes durante el periodo contratado	
Bolsa de 100h.	Facturable trimestralmente durante el periodo contratado	

11. Criterios de valoración de las ofertas

Las valoraciones de las ofertas se realizarán atendiendo a criterios económicos y técnicos sobre un total de 100 puntos.

La valoración económica atenderá al siguiente criterio:

- Se concederán 55 puntos a la oferta más económica. El resto de las ofertas se valorarán proporcionalmente.

La valoración técnica atenderá al siguiente criterio:

- Desde el punto de vista técnico, se concederán hasta 45 puntos a la oferta mejor valorada en este plano distribuyéndose de la siguiente forma:

Puntos	Descripción	Criterio
N/A	**Conformidad con el pliego**: Ajuste de la forma de la oferta a los requisitos identificados en el apartado de "Descripción de servicios hitos y entregables", "Condiciones de la oferta" y "Condiciones adicionales a cumplir por la empresa licitadora".	Excluyente[4]
45	**Calidad de la oferta presentada:** Nivel de servicio, detalle y justificación de las propuestas realizadas. Cumplimiento de objetivos perseguidos por la FNMT-RCM.	Independiente[5]

La calidad de la oferta atenderá a los siguientes criterios:

Descripción	Puntuación
1. Descripción, metodología, calidad del proyecto presentado	[0-10]
2. Ampliación de casos de uso sobre los definidos	[0-10]
3. Experiencia en trabajos similares (últimos 2 años, 2 puntos por instalación).	[0-10]
4. Mejora en acciones formativas	[0-10]

[4] La oferta se rechazará, excluyéndose del proceso de selección, si no cumple con los apartados referidos

[5] El criterio independiente viene a decir que todas las ofertas pueden llevarse el máximo de puntos en este apartado.

Descripción	Puntuación
5. Mejora en bolsa de horas de consultoría	[0-5]
Total	[0-45]

Se sugiere a la empresa licitadora que, además de realizar la descripción de los servicios a prestar como estime oportuno, indique explícitamente su propuesta de valor en torno a estos puntos para que pueda ser valorada convenientemente.

El criterio de puntuación de la oferta económica será el siguiente:

Se obtendrá la puntación correspondiente al importe de la proposición económica por los puntos asignados según la siguiente fórmula:

$$P_i = P \cdot \frac{O}{O_i}$$

Siendo:

P_i $= Puntuación\ de\ la\ oferta$ "i"

P $= Puntuación\ máxima\ (55\ Puntos)$

O $= Importe\ total\ de\ la\ oferta\ más\ económica\ presentada$

O_i $= Importe\ total\ de\ la\ oferta$ "i"

El importe económico de la oferta a evaluar no superará el máximo del presupuesto de licitación, que se ha establecido en **150.000 €.**

12. Presentación de ofertas y aclaraciones

Las empresas participantes podrán presentar cuanta documentación consideren oportuna para presentar la empresa, describir sus soluciones y explicar la forma en que cumplimentarán los requisitos de este pliego de condiciones.

Dichas ofertas se deberán presentar con la referencia CN-20-02-15-A en el Registro de la FNMT-RCM, en documentos separados la **parte técnica de la económica** (en sobres independientes) e incluyendo copia digital de los mismos en CD o memoria USB, hasta la **fecha y hora indicadas en el anuncio correspondiente del Perfil del contratante**, debiendo entregar documento original firmado por un responsable de la empresa con firma autorizada.

Las ofertas se dirigirán a la atención de:

Área de Gestión. Dirección de Sistemas de Información.

Teléfono: 91 566 67 04, e-mail: gestión.informatica@fnmt.es

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

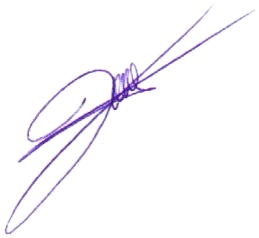
C/ Jorge Juan 106.

28009 Madrid

Cualquier consulta **técnica** relacionada con el presente pliego de condiciones puede ser dirigida a:

Área de Sistemas Ceres

e-mail: sistemas.ceres@fnmt.es



FECHA: 02/03/2015