PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO DE AUDITORÍA INTERNA DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ISO 27001 – ISO 27701), CONTINUIDAD DE NEGOCIO (ISO 22301) Y ESQUEMA NACIONAL DE SEGURIDAD (ENS) EN LA FNMT-RCM

PROCEDIMIENTO ABIERTO SIMPLIFICADO

PAS 420393 2025

Documento firmado electrónicamente por:
Jose Luis Manzanera Fernandez
Fecha: 05/03/2025
CSV:L9XkZY5hmXvmAUdgtRPNMw==

ÍNDICE

1. Objeto 3
2. Antecedentes 3
2.1. Contexto 3
2.2. Justificación 4
2.3. Situación de los sistemas de gestión 7
3. Descripción detallada del objeto de la contratación 11
4. Periodo de ejecución de la contratación 14
5. Condiciones de ejecución 14
5.1. Condiciones generales 14
5.2. Desarrollo de la auditoría 15
5.3. Requisitos del equipo auditor 18
6. Precio 21
7. Garantía de los trabajos 21
8. Aclaraciones sobre el pliego de prescripciones técnicas. 21
8.1. Condiciones de la oferta técnica 21

1. OBJETO

El objeto del presente pliego es establecer los requisitos técnicos para la contratación del servicio de realización de las auditorías internas anuales de varios de los sistemas de gestión en los que la FNMT-RCM se encuentra certificada y cuya gestión depende del Departamento de Seguridad.

La contratación incluye la realización de los siguientes servicios:

- Auditoría interna del Sistema de Gestión de Seguridad de la Información (ISO 27001).
- Auditoría interna del Sistema de Gestión de Privacidad de la Información (ISO 27701).
- Auditoría interna del Sistema de Gestión de la Continuidad del Negocio (ISO 22301).
- Auditoría interna de sistemas de información con certificación ENS categoría alta: CERES y NUBE-FNMT.
- Auditoría interna de sistemas de información con certificación ENS categoría media: Servicio de emisión del Bono Cultural Joven (prevista).
- Auditoría interna ENS de otros sistemas de información.

2. ANTECEDENTES

2.1. CONTEXTO

La FNMT-RCM dispone de varios sistemas de gestión conforme diferentes normativas, así como numerosos controles y procedimientos que satisfacen una abigarrada amalgama de normas que aplican a su actividad. En el siguiente enlace se pueden consultar las certificaciones de las que dispone la entidad:

https://www.fnmt.es/transparencia/planificacion-rsc-resultados-y-calidad/certificaciones-de-sistemas-de-gestion-homologados

Es la intención de esta entidad unificar los procesos de auditoría interna en algunos de estos sistemas y normativas de aplicación, en particular de las gestionadas por el Departamento de

Seguridad, motivo por el cual se contratarán los servicios de auditoría interna de forma unificada.

Para conocer las actividades que se realizan en la FNMT-RCM puede consultar la página web de la entidad, https://www.fnmt.es/institucion/informacion-institucional, donde puede encontrar más información sobre el número de empleados, resultado de los ejercicios, organigrama, presupuestos, políticas y certificaciones.

2.2. JUSTIFICACIÓN

2.2.1. AUDITORÍAS INTERNAS ISO

La cláusula 9.2 ("Auditoría interna") de las normas ISO 27001 y 22301 especifican que la empresa debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si los Sistemas de Gestión implantados son conformes con los requisitos propios de la organización para sus sistemas de gestión y con los requisitos de la Norma. También para comprobar si los sistemas de gestión se implementan y mantienen eficazmente.

2.2.2. AUDITORÍAS INTERNAS ENS

Pese a que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) no prescribe explícitamente la realización obligatoria de auditorías internas, el artículo 27 de dicho cuerpo legal exige la aplicación de los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información; exigencia que, trayendo causa del objeto del ENS, expresado en su artículo 1, se concreta igualmente en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, cuando se hace referencia al grado de confianza en las revisiones de la Dirección y en las auditorías internas del auditado.

Por otro lado, un sistema de información de categoría MEDIA y ALTA requiere disponer de un SGSI para la gestión de su seguridad, como se determina en la medida de seguridad [op.pl.2], arquitectura de seguridad, dando cabida a cualquier sistema de gestión basado en la mejora continua.

Por todo ello, la realización de auditorías internas constituye una actividad fundamental para sistemas de categorías MEDIA y ALTA, y recomendable para los sistemas de categoría

BÁSICA, puesto que constituyen la mejor forma de demostrar que el sistema es capaz de ir mejorando, todo ello con independencia de la realización de las preceptivas Auditorías de Certificación.

En consecuencia, es conveniente o necesario -atendiendo a la categoría de seguridad del sistema auditado- realizar auditorías internas anuales de seguimiento, al menos de las medidas de seguridad del Anexo II del ENS implantadas, actividad auditora que podrá desplegarse a lo largo del tiempo que media entre dos Auditorías de Certificación consecutivas.

La ausencia de una auditoría interna o sus elementos documentales esenciales, tales como su Plan de Auditoría, el correspondiente Informe de Auditoría, la no idoneidad del equipo auditor (por falta de formación, competencia o capacidad, o claro conflicto de interés, fundamentalmente), o no elaborar y abordar un Plan de Acciones Correctivas (PAC) respecto a las desviaciones a las que hubiere lugar, a juicio todo ello de la entidad certificadora, será tipificada, en el caso de sistemas de información de categorías MEDIA o ALTA, como una Observación en el Informe de Auditoría que genere la entidad certificadora, desviación que, de persistir, derivará en una No Conformidad Mayor en la siguiente Auditoría de Certificación y que provocará que el dictamen global de la auditoría sea, en consecuencia, DESFAVORABLE.[1]

[1] *Guía de Seguridad CCN-STIC CCN-CERT IC-01/19. ENS. Criterios Generales de Auditoría y Certificación*

2.2.3. JUSTIFICACIÓN DE LA CONTRATACIÓN Y SU MODIFICACIÓN PREVISTA

Para dar respuesta a los requerimientos previamente indicados, la FNMT-RCM ha acordado contratar los servicios de auditoría interna de los sistemas señalados, con los alcances indicados en los correspondientes certificados. Tal y como se señala más adelante, **dichos alcances podrán ser incrementados en el caso de que exista la intención de incluir más servicios en dicho certificado. En cualquier caso, los procedimientos de gestión y herramientas serían las mismas que las empleadas para los servicios actualmente incluidos en la certificación**.

Así mismo, se pretende con esta contratación dar respuesta a posibles requerimientos de auditorías internas no previstas en el listado anterior. Por lo tanto, se prevé la posibilidad de modificación del contrato conforme al artículo 204 de la Ley 9/2017, de 8 de noviembre, de 2017, de Contratos del Sector Público LCSP hasta un máximo del 20% del precio del contrato, en el caso de las siguientes circunstancias:

- Necesidad de realizar auditorías internas de normas o regulaciones no contempladas en el listado anterior y que resulten de obligado cumplimiento o de interés empresarial para la FNMT-RCM.

- Incremento en el número de auditorías internas ENS, por la necesidad de certificar nuevos sistemas de información conforme al RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

2.3. SITUACIÓN DE LOS SISTEMAS DE GESTIÓN

La situación actual de los Sistemas de Gestión y sistemas de información objeto de la licitación es la siguiente:

2.3.1. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) CONFORME A LA NORMA ISO 27001

- Fecha de expiración del actual certificado: 25/01/2026

- Alcance del certificado:

  Sistemas de información y privacidad que dan soporte a los siguientes procesos:

  A. Diseño y producción de moneda circulada, conmemorativa y acuñación de otros productos de valor liberatorio, billetes de banco, sellos de correos, productos impresos con elementos de seguridad, pasaportes y libretas de seguridad. El diseño, producción, montaje, ensamblado y acabado de tarjetas con y sin microcircuitos. El diseño, desarrollo y prestación de servicios de certificación para firma electrónica, servicios de terceros de confianza y autoridad de sellado de tiempo. El diseño y desarrollo de sistemas operativos para tarjetas inteligentes criptográficas y componentes software asociados. El servicio de emisión de identificadores únicos para la trazabilidad de los productos de tabaco.

  B. El diseño y producción de papel de seguridad. La transformación de papel para sellos.

  C. Servicio de Custodia de Evidencias, Documentos y Expedientes

  D. Servicios de tecnologías de registro contable distribuido (DLT) y blockchain (Nodo EBSI).

- Centros de trabajo:

  - Centro de trabajo de c/ Jorge Juan 106, 28009 Madrid. Alcances A), C), D).
  - Centro de trabajo de c/ Alcalá 526, Madrid. Alcance A).
  - Centro de trabajo de av/ Costa Rica 1, Burgos. Alcance B).

2.3.2. SISTEMA DE GESTIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN CONFORME A LA NORMA ISO 27701.

- Fecha de expiración del actual certificado: 25/01/2026

- Alcance del certificado:

Sistemas de información y privacidad que dan soporte a los siguientes procesos:

A. Diseño y producción de moneda circulada, conmemorativa y acuñación de otros productos de valor liberatorio, billetes de banco, sellos de correos, productos impresos con elementos de seguridad, pasaportes y libretas de seguridad. El diseño, producción, montaje, ensamblado y acabado de tarjetas con y sin microcircuitos. El diseño, desarrollo y prestación de servicios de certificación para firma electrónica, servicios de terceros de confianza y autoridad de sellado de tiempo. El diseño y desarrollo de sistemas operativos para tarjetas inteligentes criptográficas y componentes software asociados. El servicio de emisión de identificadores únicos para la trazabilidad de los productos de tabaco.

B. El diseño y producción de papel de seguridad. La transformación de papel para sellos.

C. Servicio de Custodia de Evidencias, Documentos y Expedientes

D. Servicios de tecnologías de registro contable distribuido (DLT) y blockchain (Nodo EBSI).

- Centros de trabajo:

- Centro de trabajo de c/ Jorge Juan 106, Madrid. Alcances A), C), D).
- Centro de trabajo de c/ Alcalá 526, Madrid. Alcance A).
- Centro de trabajo de av/ Costa Rica 1, Burgos. Alcance B).

2.3.3. SISTEMA DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO CONFORME A LA NORMA ISO 22301

Fecha de expiración del certificado: 25/01/2026

Alcance del certificado:

Sistemas de información y privacidad que dan soporte a los siguientes procesos:

A. Diseño y producción de moneda circulada, conmemorativa y acuñación de otros productos de valor liberatorio, billetes de banco, sellos de correos, productos impresos con elementos de seguridad, pasaportes y libretas de seguridad. El diseño, producción, montaje, ensamblado y acabado de tarjetas con y sin microcircuitos. El diseño, desarrollo y prestación de servicios de certificación para firma electrónica, servicios de terceros de confianza y autoridad de sellado de tiempo. El diseño y desarrollo de sistemas operativos para tarjetas inteligentes criptográficas y componentes software asociados. El servicio de emisión de identificadores únicos para la trazabilidad de los productos de tabaco.

B. El diseño y producción de papel de seguridad. La transformación de papel para sellos.

Centros de trabajo:

- Centro de trabajo de c/ Jorge Juan 106, Madrid. Alcance A).
- Centro de trabajo de c/ Alcalá 526, Madrid. Alcance A).
- Centro de trabajo de av/ Costa Rica 1, Burgos. Alcance B).

2.3.4. CERTIFICACIÓN ENS CATEGORÍA ALTA NUBE FNMT

Fecha de expiración del certificado: 04/02/2027

Alcance del certificado:

Sistema de información necesario para ofrecer, a través de su infraestructura tecnológica, la prestación de servicios en modo nube definidos por software de forma distribuida entre los CPDs de Burgos y Madrid de la FNMT- RCM, sobre una arquitectura de virtualización basada en hiperconvergencia, prestando servicios de almacenamiento, computación, virtualización, escalabilidad, gestión centralizada, electrónica de red, comunicaciones y seguridad gestionada, según la declaración de aplicabilidad vigente.

Centros de trabajo:

- CPD Costa Rica 1, 09001 Burgos.
- CPD Jorge Juan 106, 28009 Madrid.

2.3.5. CERTIFICACIÓN ENS CATEGORÍA ALTA CERES

Fecha de expiración del certificado: 22/02/2027

Alcance del certificado:

Los sistemas de información que dan soporte al proceso de:

Diseño, desarrollo y prestación de servicios de certificación para firma electrónica, servicios de terceros de confianza y autoridad de sellado de tiempo.

Centros de trabajo:

- Centro de trabajo de c/ Jorge Juan 106, Madrid.
- Centro respaldo Ceres. Av Manoteras, Madrid.
- Centro de trabajo de c/ Alcalá 526, Madrid.

3. DESCRIPCIÓN DETALLADA DEL OBJETO DE LA CONTRATACIÓN

La contratación comprende la realización de los servicios de auditoría interna anual de los siguientes sistemas, comprobando el cumplimiento de la norma correspondiente y el grado de implantación del sistema de gestión.

- Auditoría interna del Sistema de Gestión de la Seguridad de la Información (SGSI) certificado conforme a la norma **ISO 27001**.
- Auditoría interna del Sistema de Gestión de la Privacidad de la Información (SGPI) certificado conforme a la norma **ISO 27701**.
- Auditoría interna del Sistema de Gestión de la Continuidad de Negocio (SGCN) certificado conforme a la norma **ISO 22301**.
- Auditoría interna del Sistema de información Nube FNMT, con certificación ENS categoría alta.
- Auditoría interna del Sistema de información CERES, con certificación ENS categoría alta.

En el año 2025 está prevista la certificación del siguiente sistema de información, por lo que también se incorporará en el ciclo de auditorías internas:

- Sistema de información para la emisión del BONO CULTURAL JOVEN (pendiente de certificación en ENS categoría media). El alcance del mismo será:
    - Sistema de información necesario para ofrecer, a través de la plataforma AWS, la prestación de servicios de emisión de bono cultural para jóvenes y entidades colaboradoras, de acuerdo a los requerimientos de la SGAD.

Los objetivos que se abordarán para la correcta prestación del servicio son:

- Cumplir con los requisitos de las normas de referencia.
- Verificar que los sistemas de gestión implantados cumplen con los requisitos de referencia, incluidos los requisitos legales aplicables.
- Poner de manifiesto las anomalías y deficiencias detectadas.

El alcance está determinado por el certificado emitido por la entidad competente, aunque podría quedar ampliado en el caso de que exista la intención de incluir más servicios en dicho

certificado. En cualquier caso, los procedimientos de gestión y herramientas serían las mismas que las empleadas para los servicios actualmente incluidos en la certificación.

Se realizará una auditoría interna anual de los sistemas de gestión ISO en los meses de mayo-junio. El calendario para su ejecución se establecerá de común acuerdo entre los diferentes Departamentos de la FNMT-RCM involucrados y la empresa adjudicataria.

Las auditorías de los sistemas de gestión ISO (SGSI, SGPI, SGCN) se planificarán en el mismo periodo para su realización conjunta, procurando que los ámbitos de revisión comunes entre todas las normas a auditar se realicen de forma unificada. Por ejemplo, para la auditoría de controles relacionados con la formación y capacitación de las personas, la empresa adjudicataria deberá planificar el ejercicio de auditoría de tal forma que el personal del Departamento de Formación sea entrevistado / auditado una sola vez. De ese trabajo se deberán extraer las conclusiones y evidencias necesarias para la ejecución del servicio de auditoría a prestar de todas las normas identificadas en el alcance.

Las auditorías internas respecto al RD 311/2022 del ENS deberán ser específicas y el calendario de ejecución se establecerá de común acuerdo entre los diferentes Departamentos de la FNMT-RCM involucrados.

Sin perjuicio de esta particularidad, se procurará que se ejecuten en el mismo periodo que las auditorías internas de los sistemas de gestión ISO, considerando las posibles sinergias para desarrollar un proceso de auditoría lo más eficiente posible.

Se hace constar expresamente que la mayoría de las actividades de los procesos que ejecuta la FNMT-RCM se desarrollan principalmente en su sede central, sita en la calle Jorge Juan 106 de Madrid. No obstante, se subraya que también existe cierta actividad relacionada con el almacenaje de material y logística en otro centro de la ciudad de Madrid, un centro alternativo de procesamiento de datos y respaldo también en la ciudad de Madrid y, además, dispone de una Fábrica de Papel en la ciudad de Burgos. Todo ello se anuncia a efectos de las posibles visitas o desplazamientos que pudieran ser necesarios para llevar a buen término las auditorías.

Como aclaraciones al presente pliego, se recomienda consultar la información corporativa publicada: https://www.fnmt.es/institucion/informacion-institucional

AUDITORÍAS ADICIONALES ENS

Se señala que, durante el periodo de la contratación, **se podrán solicitar adicionalmente hasta un máximo de 6 auditorías internas en el periodo de ejecución de la contratación para la certificación de diferentes sistemas de información de la FNMT-RCM conforme al Esquema Nacional de Seguridad**, cuyo alcance y propósito se describiría con detalle en la solicitud de la auditoría. No obstante, a efectos de estimación de esfuerzos se considerará que los sistemas tendrían la categoría ALTA.

Se subraya que la auditoría de los sistemas para la certificación conforme al ENS puede quedar sin efecto en caso de no necesitarse. Por este motivo, si bien el licitador incluirá una propuesta de servicios en su oferta, en caso de convertirse en adjudicatario, solo facturará los servicios si la FNMT-RCM realiza una solicitud de auditoría de estas características en el periodo de vigencia del correspondiente contrato.

Estas auditorías ENS podrán solicitarse y ejecutarse en cualquier momento durante el periodo de ejecución de la contratación.

4. PERIODO DE EJECUCIÓN DE LA CONTRATACIÓN

El contrato tiene una duración prevista de UN (1) AÑO a partir de la fecha de formalización del contrato. Este plazo podrá ser prorrogado hasta en DOS (2) ocasiones por UN (1) AÑO más. El adjudicatario deberá estar en disposición de prestar el servicio desde la formalización del contrato.

5. CONDICIONES DE EJECUCIÓN

5.1. CONDICIONES GENERALES

La empresa que resulte adjudicataria deberá cumplir las siguientes condiciones:

- Demostrar fehacientemente el cumplimiento de los criterios de solvencia técnica y económica indicados en el Pliego de Condiciones Particulares de la licitación.
- El licitador debe basar su propuesta en su capacidad de auditoría interna de los sistemas de gestión indicados.
- 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 coordinador de auditorías que coordine eficientemente las actividades de los auditores y las necesidades que estos pudieran tener para la realización de su trabajo. Este responsable deberá interactuar con los responsables de los sistemas en FNMT-RCM para coordinar de forma efectiva la realización de la auditoría (planificación de entrevistas, recopilación de información, etc).
- Todo el equipo auditor deberá hablar con fluidez el idioma español. Las entrevistas se realizarán en español y la documentación a revisar por el contratista estará mayoritariamente en español. La FNMT-RCM no realizará trabajo o esfuerzo alguno para traducir su documentación a otro idioma o facilitar entrevistas en un idioma diferente al español.
- De forma previa al inicio de cualquier trabajo, 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.

- 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.
- 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. En cualquier caso, para las actividades de auditoría a realizar en las instalaciones de la FNMT-RCM siempre se realizará tal acompañamiento, asegurando así el cumplimiento en materia de calidad, seguridad y prevención.
- Las comunicaciones entre la FNMT-RCM y la empresa adjudicataria al objeto de la remisión de informes y suministro de información sensible se realizará cifrada con herramientas tipo PGP/S-MIME o mediante herramientas que la FNMT-RCM pondrá a disposición del contratista.
- Terminados los trabajos, la empresa deberá eliminar toda información sensible de la FNMT-RCM utilizada u obtenida durante prestación del servicio. La FNMT-RCM podrá utilizar o entregar los informes de auditoría a entidades que se lo requieran, según sus necesidades profesionales.
- No publicidad de relación con la FNMT-RCM sin previo consentimiento.
- Todo el trabajo desarrollado por el equipo de trabajo designado se considera propiedad exclusiva de la FNMT-RCM.

5.2. DESARROLLO DE LA AUDITORÍA

5.2.1. ACTUACIONES PREVIAS

La empresa deberá nombrar un responsable de auditoría que coordine las actividades a llevar a cabo por el equipo auditor y que será el interlocutor con los responsables de los sistemas

de gestión de la FNMT-RCM auditados. Sin perjuicio de que la figura del coordinador pueda coincidir con la figura del Auditor Jefe, será el interlocutor y coordinador de todas las actividades contempladas en el servicio a prestar.

El responsable remitirá el plan de auditoría a las personas de contacto designadas por la FNMT-RCM **al menos con dos semanas de antelación** para que se informe a las personas implicadas en la auditoría y ésta pueda desarrollarse de una forma ágil y eficaz.

Junto con el plan de auditoría, la empresa adjudicataria confirmará el equipo auditor y remitirá el currículo de cada uno de los integrantes, en el caso de aquellos auditores no contemplados en la oferta técnica original. La FNMT-RCM comprobará que todos ellos cumplen con los requisitos establecidos en el apartado 5.3 y se reserva el derecho de solicitar el cambio de aquellos auditores propuestos que no los cumplan.

Las auditorías internas respecto al RD 311/2022 del ENS deberán ser específicas y el calendario de ejecución se establecerá de común acuerdo entre los diferentes Departamentos de la FNMT-RCM involucrados.

Sin perjuicio de esta particularidad, se procurará que se ejecuten en el mismo periodo que las auditorías internas de los sistemas de gestión ISO, considerando las posibles sinergias para desarrollar un proceso de auditoría lo más eficiente posible.

Con este objetivo, de manera previa al envío del plan de auditoría, se mantendrán reuniones previas entre la FNMT y la empresa adjudicataria para la puesta en común de las necesidades de la FNMT y las posibilidades de revisión común entre las diferentes normas y sistemas de información.

5.2.2. DESARROLLO DE AUDITORÍA

Se realizará una reunión previa con el objeto de presentar el equipo auditor a los representantes de la FNMT-RCM, informar del objeto y alcance de la auditoría y aprobar el plan de auditoría.

El número de días laborables para llevar a cabo las auditorías será el necesario para revisar todos los controles de las normas incluidas, teniendo en cuenta que se deberán visitar las instalaciones de todos los centros de trabajo incluidos en el alcance.

El horario de las jornadas presenciales de auditoría estará comprendido entre las 9:00 horas y las 15:00 horas, de lunes a viernes (días laborables).

El equipo auditor buscará la constatación del cumplimiento de los requisitos especificados en la documentación de referencia, a través de las evidencias objetivas derivadas del análisis de los registros y visita a las instalaciones.

Se realizará una reunión final con los responsables de la FNMT-RCM para aclarar las posibles no conformidades detectadas.

5.2.3. EMISIÓN DE LOS INFORMES DE AUDITORÍA INTERNA

Se emitirá un informe conjunto de auditoría para las normas ISO 27001, ISO 27701 e ISO 22301, señalando las anomalías detectadas, categorizándolas como no conformidades, observaciones y opciones de mejora, que será enviado a la FNMT-RCM después de la auditoría.

Se emitirá un informe individual por cada uno de los sistemas de información auditados conforme a ENS.

Los informes se entregarán en formato digital, a las direcciones de correo electrónico que se faciliten a la empresa adjudicataria para tal fin, durante los siete días siguientes a la finalización de la auditoría.

Los informes de auditoría deberán contener información suficiente para que los hallazgos de las auditorías puedan entenderse claramente, con ejemplos ilustrativos y con el fin de que puedan establecerse las correspondientes acciones preventivas, correctoras o de mejora en forma de planes de acción que deriven en la subsanación de las deficiencias.

5.2.4. ANÁLISIS DE LAS ACCIONES PROPUESTAS POR LA FNMT-RCM PARA DAR RESPUESTA A LOS HALLAZGOS DE LAS AUDITORÍAS.

Se establecerá un plazo, de común acuerdo, para poder consultar con el equipo auditor los aspectos relacionados con los hallazgos de las auditorías recogidos en el informe de auditoría y las acciones propuestas para abordarlos por los responsables de los Sistemas de Gestión auditados. **Este plazo será, al menos, de un mes desde la recepción del informe de auditoría definitivo.**

5.3. REQUISITOS DEL EQUIPO AUDITOR

El equipo auditor debe estar compuesto por profesionales que aseguren la objetividad y la imparcialidad del proceso de auditoría y ser totalmente independientes de las actividades que sean o puedan ser objeto de la auditoría. **En ningún caso, los integrantes del equipo auditor pueden haber participado o detentado responsabilidades previas a la auditoría, al menos en los dos últimos años, en el sistema de información auditado, o bien haber sido consultores para ese sistema.**

Se requerirá un Auditor Jefe que coordine todo el proceso y un número suficiente de auditores para la correcta realización del conjunto de auditorías previstas.

El Auditor Jefe gestionará y dirigirá las actividades de auditoría, supervisando todo el proceso y garantizando la exactitud de los hallazgos que se señalen en el Informe de Auditoría, así como preservando las evidencias obtenidas.

El **Auditor Jefe** deberá probar, como mínimo:

- Formación técnica en seguridad de la información, gestión de riesgos de seguridad, continuidad y Reglamento General de Protección de Datos (GDPR), y experiencia verificable de un mínimo de 4 años trabajando con sistemas de información y seguridad de la información.
- Formación acreditada en los requisitos del RD 311/2022, por el que se regula el Esquema Nacional de Seguridad.
- Acreditación de formación en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional (Lead auditor en 27001, Lead auditor en 27701, Lead Auditor en 22301 o equivalentes), o bien a través de experiencia verificable y evidenciada de al menos 4 años, en auditorías ISO y ENS de tecnologías de la información.
- Experiencia verificable de un mínimo de **2 años como Auditor Jefe en auditorías del RD 311/2022**, por el que se regula el Esquema Nacional de Seguridad y realización de un **mínimo de 4 auditorías como Auditor Jefe**.
- Experiencia verificable de un mínimo de **2 años como Auditor Jefe en auditorías ISO (27001 o 27701 o 22301)** y un **mínimo de 4 auditorías como Auditor Jefe**.

Para el **resto de miembros del equipo auditor** se exigirán los siguientes requisitos, conforme a la norma auditada:

- **Auditoría ISO 27001:**
  - Formación técnica en seguridad de la información y gestión de riesgos de seguridad, y experiencia verificable de un mínimo de 3 años trabajando con sistemas de información y seguridad de la información.
  - Acreditación de formación en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional (Lead auditor en 27001 o equivalente), o bien a través de experiencia verificable y evidenciada de al menos 3 años en auditorías ISO 27001 de tecnologías de la información.
  - Experiencia verificable de un **mínimo de 2 años como auditor en auditorías ISO 27001 y un mínimo de 4 auditorías.**
- **Auditoría ISO 27701:**
  - Formación técnica en seguridad de la información y gestión de riesgos de seguridad y específica en el Reglamento General de Protección de Datos (GDPR); y experiencia verificable de un mínimo de 3 años trabajando con sistemas de información y seguridad de la información.
  - Acreditación de formación en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional (Lead auditor en 27701 o equivalente), o bien a través de experiencia verificable y evidenciada de al menos 2 años en auditorías ISO 27701 de tecnologías de la información.
  - Experiencia verificable de un **mínimo de 1 año como auditor en auditorías ISO 27701 y un mínimo de 2 auditorías.**
- **ISO 22301:**
  - Formación técnica en seguridad de la información y gestión de riesgos de seguridad y continuidad de negocio; y experiencia verificable de un mínimo de 3 años trabajando con sistemas de información y seguridad de la información.
  - Acreditación de formación en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional (Lead auditor en 22301 o equivalente), o bien a través de experiencia verificable y evidenciada de al menos 3 años en auditorías ISO 22301 de tecnologías de la información.

- Experiencia verificable de un **mínimo de 2 años como auditor en auditorías ISO 22301 y un mínimo de 4 auditorías.**

- **RD 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS):**
  - Formación técnica en seguridad de la información y gestión de riesgos de seguridad, y experiencia verificable de un mínimo de 3 años trabajando con sistemas de información y seguridad de la información.
  - Conocimiento acreditado de los requisitos del RD 311/2022, por el que se regula el Esquema Nacional de Seguridad.
  - Acreditación de formación en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos 3 años en auditorías ENS de sistemas de información.
  - Experiencia verificable de **un mínimo de 2 años como auditor en auditorías ENS de sistemas de información y un mínimo de 4 auditorías.**

Para comprobar que se reúnen todas las características previamente definidas, será necesario solicitar y revisar los currículos de los auditores de manera previa a la realización de las auditorías. La FNMT-RCM comprobará que todos ellos cumplen con los requisitos establecidos en este apartado y se reserva el derecho de solicitar el cambio de aquellos auditores propuestos que no los cumplan.

Los miembros deben firmar las correspondientes cláusulas de confidencialidad, incluyendo las aplicables en relación a la legislación de protección de datos de carácter personal.

De manera previa a la realización presencial de la auditoría, el equipo auditor deberá incorporar toda la información necesaria para el acceso a la FNMT en la herramienta COORDYNA. El equipo de la FNMT deberá tramitar el acceso del personal externo a las instalaciones en las fechas acordadas para la auditoría.

Sea cual sea la composición del equipo, la propiedad de los documentos de trabajo y de las evidencias, así como las responsabilidades derivadas de la emisión del informe y su contenido deben quedar siempre claramente definidas y ser inequívocas tanto en la apertura de la auditoría, como en el informe de auditoría final.

6. PRECIO

Consultar en el Pliego de Cláusulas Administrativas Particulares.

No podrá aparecer en la oferta técnica referencia alguna al precio o a la oferta económica, atendiendo a lo dispuesto en el Pliego de Cláusulas Administrativas Particulares.

En el modelo de oferta económica (Anexo I del Pliego de Cláusulas Administrativas Particulares) se establece cómo se deben desglosar los conceptos.

7. GARANTÍA DE LOS TRABAJOS

El adjudicatario deberá incluir como mínimo un año de garantía sobre los trabajos realizados y asumirá los costes asociados a la reparación en cuestión.

8. ACLARACIONES SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS.

Las consultas y detalles sobre el transcurso y procedimiento de licitación se tramitarán a través de la Plataforma de Licitación de la FNMT-RCM.

Para aclaraciones de carácter exclusivamente técnico durante el periodo de presentación de ofertas, se podrán remitir a la siguiente dirección, con una antelación mínima de tres días hábiles antes de la fecha límite de presentación de ofertas.

seguridad.informatica@fnmt.es

8.1. CONDICIONES DE LA OFERTA TÉCNICA

La oferta deberá cumplir las siguientes condiciones:

- Deberá ser incluida en el sobre que se indica en el Pliego de Cláusulas Administrativas Particulares para los criterios evaluables mediante juicios de valor.

- **No podrá aparecer en la oferta técnica referencia alguna al precio o a la oferta económica**, atendiendo a lo dispuesto en el Pliego de Cláusulas Administrativas Particulares.
- Se incluirá la siguiente documentación:
  - Currículos de los perfiles técnicos ofertados (Auditor Jefe y auditores) donde se evidencie el cumplimiento de los requisitos establecidos en el apartado 5.3 del presente pliego, así como aquellos aspectos valorables conforme a los criterios de valoración del Pliego de Cláusulas Administrativas Particulares.
  - Ejemplo de un Plan de Auditoría que plantee la revisión de manera conjunta de los procesos comunes en las distintas normas incluidas en la licitación, conforme a los aspectos valorables en los criterios de valoración del Pliego de Cláusulas Administrativas Particulares.