# Guía de Seguridad de las TIC
# CCN-STIC 122

# Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS



Marzo 2026

Edita:
centro criptológico nacional
© Centro Criptológico Nacional, 2026

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.03.23 12:17:25 +01'00'

Fecha de Edición: marzo de 2026

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

# ÍNDICE

**1. OBJETO ..... 4**
**2. PROCEDIMIENTO PARA EL RECONOCIMIENTO DE LOS OAT ..... 4**
**3. SOLICITUD DE RECONOCIMIENTO ..... 5**
**4. REVISIÓN DE LAS CONDICIONES DE RECONOCIMIENTO ..... 5**
**5. REQUISITOS GENERALES DE LOS OAT ..... 6**
5.1 COMPETENCIA TÉCNICA ..... 6
5.2 CONFIDENCIALIDAD, INDEPENDENCIA E IMPARCIALIDAD ..... 7
5.3 REQUISITOS PROCEDIMENTALES Y METODOLÓGICOS ..... 8
**6. ESTRUCTURA DE PERSONAL DE LOS OAT ..... 8**
6.1 PERSONAL RELEVANTE NO AUDITOR ..... 8
6.2 PERSONAL DEL EQUIPO AUDITOR ..... 9
6.3 REQUISITOS MÍNIMOS DEL PERSONAL TÉCNICO ..... 11
6.4 INCORPORACIÓN DE EXPERTOS TÉCNICOS AL EQUIPO DE AUDITORÍA ..... 13
6.5 RESUMEN DE REQUISITOS DEL PERSONAL DEL OAT ..... 14
**7. ACUERDOS SUSCRITOS POR LOS OAT CON LOS AUDITADOS ..... 15**
**8. CRITERIOS GENERALES DE AUDITORÍA ..... 15**
**9. EL PROCESO DE RECONOCIMIENTO DE UN OAT ..... 18**
9.1 FORMACIÓN PREVIA DEL PERSONAL DEL OAT ..... 18
9.2 REMISIÓN DE DOCUMENTACIÓN EN EL PROCESO DE RECONOCIMIENTO ..... 18
9.3 JORNADA DE RECONOCIMIENTO ..... 18
9.3.1 PARTE 1 ..... 18
9.3.2 PARTE 2 ..... 19
9.4 AUDITORÍA DE ACOMPAÑAMIENTO ..... 19
9.5 INFORME DE RECONOCIMIENTO ..... 19
9.6 CONCESIÓN DEL RECONOCIMIENTO ..... 20
**10. OBLIGACIONES ADICIONALES DE LOS OAT ..... 20**
10.1 DURANTE EL PROCESO DE RECONOCIMIENTO ..... 20
10.2 A LO LARGO DE SU DESEMPEÑO COMO OAT ..... 20
10.3 SUBCONTRATACIÓN DE RECURSOS ..... 21
**11. EMISIÓN DEL CERTIFICADO DE RECONOCIMIENTO COMO OAT ..... 21**
**12. PUBLICIDAD DE LOS RECONOCIMIENTOS ..... 23**
**13. VIGENCIA DEL RECONOCIMIENTO ..... 23**
**14. RENOVACIÓN DEL RECONOCIMIENTO ..... 23**
**15. RESUMEN DE LAS FASES DEL RECONOCIMIENTO ..... 24**
15.1 MATRIZ RACI DEL PROCESO DE RECONOCIMIENTO DEL OAT ..... 26
LEYENDA RACI ..... 26
**ANEXO. REVISIÓN DE REQUISITOS PARA OAT ..... 27**

## 1. OBJETO

De conformidad con lo dispuesto en el artículo 30 y en la Disposición adicional segunda del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y atendiendo a lo recogido en la cláusula VI de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, el presente documento tiene por objeto definir el proceso utilizado por el Centro Criptológico Nacional (CCN) para el reconocimiento de la capacidad técnica y resto de requisitos de aquellas entidades, organismos, órganos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información; así conste en su normativa de creación, decretos de estructura, o estatutos; quedando asimismo garantizada la debida imparcialidad y la ausencia de conflicto de intereses entre las partes auditora y auditada, en relación con las Auditorías de Seguridad exigidas por el Esquema Nacional de Seguridad (ENS) de cara a alcanzar y exhibir la preceptiva Certificación de Conformidad con el ENS.

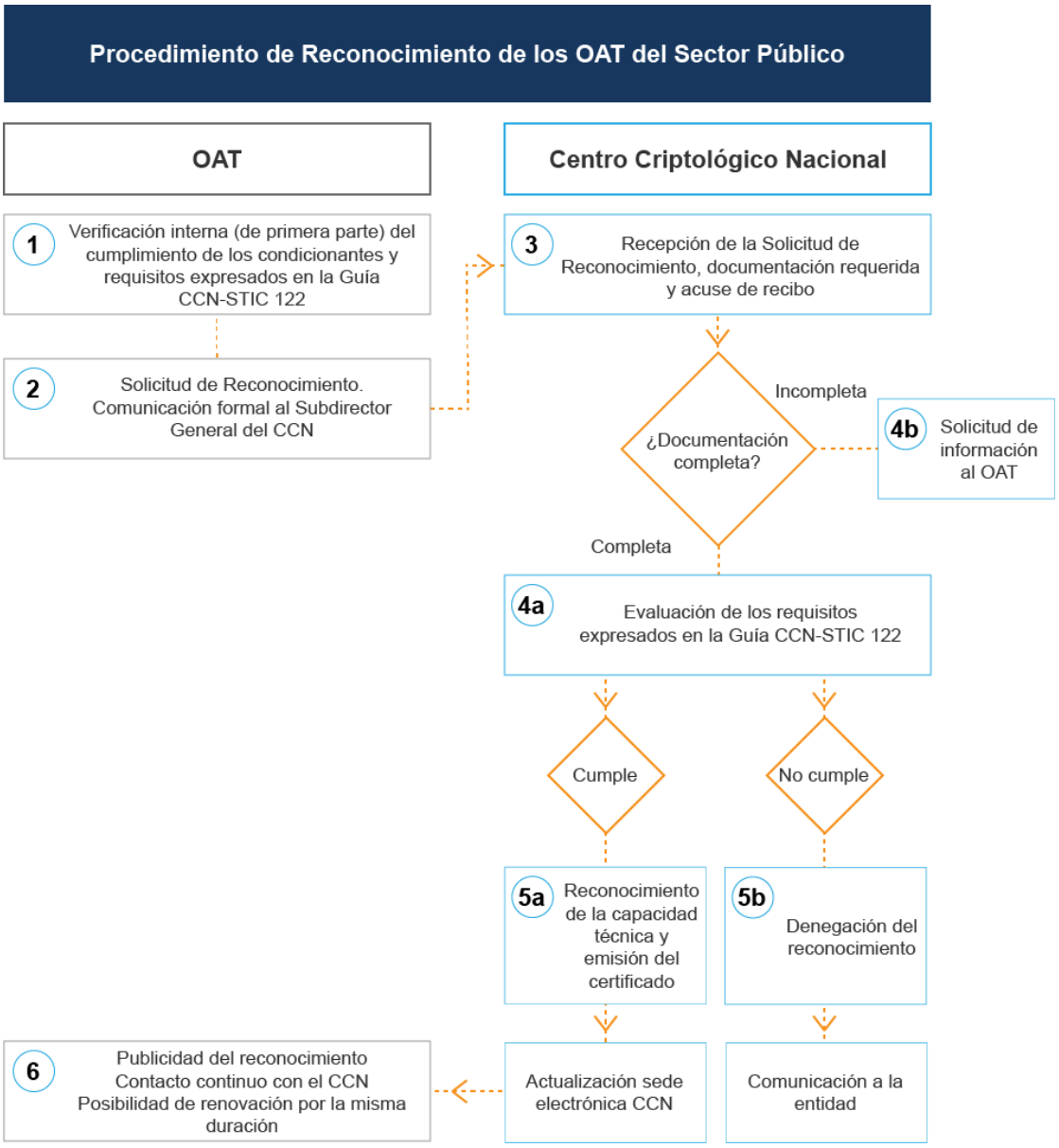
Tales órganos o unidades recibirán el nombre de Órgano de Auditoría Técnica del Sector Público (en adelante, OAT), y deberán satisfacer dos (2) requisitos fundamentales para ser reconocidos como tales:

1) Capacidad técnica y organizativa para la realización de Auditorías de Seguridad, evaluando los requisitos que dispone el ENS para los sistemas de información auditados.

2) Imparcialidad y ausencia de conflicto de intereses entre el OAT y la entidad titular, responsable o usuaria del sistema de información en cuestión.

## 2. PROCEDIMIENTO PARA EL RECONOCIMIENTO DE LOS OAT

La figura siguiente muestra de forma simplificada el procedimiento utilizado por el Centro Criptológico Nacional para el reconocimiento de los OAT, que incluirá la evaluación de la capacidad técnica para la realización de Auditorías de Seguridad del ENS, así como la verificación de la imparcialidad y ausencia de conflictos de interés.




## 3. SOLICITUD DE RECONOCIMIENTO

Las unidades de auditoría interesadas en obtener el reconocimiento como OAT para la realización de Auditorías de Certificación de la Conformidad con el ENS deberán solicitarlo al Centro Criptológico Nacional mediante una comunicación formal dirigida al Subdirector General del Centro Criptológico Nacional en la que manifiesten su intención, adelantándose vía correo electrónico a cocens@ccn.cni.es, y adjuntando la documentación que se señala en la presente Guía, así como aquella otra que el OAT considere conveniente, en apoyo a sus pretensiones.

## 4. REVISIÓN DE LAS CONDICIONES DE RECONOCIMIENTO

Una vez realizada la evaluación antedicha, respecto de la capacidad técnica del OAT y los requisitos de imparcialidad y ausencia de conflicto de interés, y

encontrándose conforme con tales requisitos, el Centro Criptológico Nacional reconocerá al OAT solicitante como Órgano de Auditoría Técnica, para lo que expedirá el correspondiente Certificado de Reconocimiento.

# 5. REQUISITOS GENERALES DE LOS OAT

## 5.1 COMPETENCIA TÉCNICA

El OAT debe tener una experiencia demostrable de, al menos, tres (3) años en la realización de forma regular de auditorías, evaluaciones o inspecciones relacionadas con sistemas de información y su seguridad, valorándose por parte del CCN durante el proceso de reconocimiento la magnitud de los proyectos realizados en tal sentido.

Dicha experiencia podrá evidenciarse mediante la aportación de la documentación adecuada que permita verificar que el OAT solicitante:

a) Ha realizado proyectos en los que figuren actividades de auditoría o inspecciones de cumplimiento funcional, normativo o técnico de sistemas de información.

b) Posee certificaciones de organismos con competencias en auditoría de seguridad de sistemas, en los que consten específicamente los trabajos de auditoría de cumplimiento normativo y técnico realizados.

La experiencia podrá ser sustituida por la competencia técnica y conocimientos necesarios para la realización de auditorías de seguridad o, eventualmente, inspecciones STIC, para lo que será necesario que el OAT solicitante exponga pormenorizadamente a un equipo de expertos designados por el CCN (por el medio que se considere oportuno, presencial o remoto) el sistema empleado, o que se empleará para la organización y gobierno del OAT solicitante, su encuadramiento orgánico, su estructura prevista de personal y sus capacidades, la metodología seguida o prevista para realizar auditorías de Certificación de Conformidad del ENS y un ejemplo de alguna auditoría del ENS realizada, al objeto de que el CCN pueda valorar adecuadamente su idoneidad para el propósito perseguido.

La competencia técnica del personal del OAT se evidenciará mediante certificados de la formación recibida para la adquisición de las competencias y habilidades en auditoría, evaluación o inspección de seguridad de sistemas de información, y más concretamente del RD 311/2022, de 3 de mayo, y de la legislación vigente en materia de protección de datos u otra normativa de privacidad o seguridad que pudiera resultar aplicable.

El OAT debe identificar las necesidades de formación del personal y ser capaz de dar respuesta a estos requisitos. Se deberá disponer de un plan de capacitación y diseño curricular asociado a cada una de las funciones del equipo auditor.

## 5.2 CONFIDENCIALIDAD, INDEPENDENCIA E IMPARCIALIDAD

El OAT debe asegurarse de que su organización y personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad auditada, de conformidad con lo exigido en la ITS de Auditoría, en la ITS de Conformidad con el ENS y la ISO/IEC 17065, evitando los conflictos de intereses:

- Entre las actividades de auditoría de Certificación de la Conformidad con el ENS del OAT y el resto de las áreas de la entidad en la que esté encuadrado el OAT.
- Entre las actividades de auditoría de Certificación de la Conformidad con el ENS del OAT y las de la entidad titular, responsable o usuaria del sistema de información auditado que pretende certificarse.

Se entiende que existe "conflicto de intereses" en una entidad cuando, teniendo varios intereses diferenciados o debiendo satisfacer distintas obligaciones, las medidas que ha de adoptar para satisfacer o alcanzar alguno de ellos perjudica o la aleja del otro u otros.

Será en el momento de la constitución del OAT, en el que residirán las capacidades de Auditoría de Certificación de la Conformidad con el ENS, cuando deberán adoptarse las cautelas precisas para asegurar, desde el mismo momento de su creación, la debida imparcialidad y ausencia de conflicto de interés entre el OAT y las restantes áreas de la entidad, u otras entidades, titulares, responsables o usuarias del sistema de información auditado, cautelas y circunstancias que se evidenciarán documentalmente.

El OAT ha de asegurar que, tanto su organización como el personal involucrado, mantiene las preceptivas condiciones de imparcialidad, independencia y ausencia de conflicto de interese respecto de la entidad titular, responsable o usuaria del sistema de información auditado.

En ningún caso los integrantes del equipo auditor deben haber participado o detentado responsabilidades previas a la auditoría, o bien haber sido consultores en el proceso de implementación de los requisitos del ENS, al menos en los dos (2) últimos años para el sistema de información auditado.

Todos los integrantes del Equipo Auditor, ya sea personal interno o externo, incluyendo a los auditores jefe, auditores y posibles expertos técnicos, deberán haber firmado, antes de comenzar a intervenir en auditorías de Certificación de la Conformidad con el ENS, un acuerdo de confidencialidad, que garantice su deber de secreto ante la información a la que tengan acceso, o elaboren, durante las auditorías.

Finalmente, el OAT solicitante evidenciará documentalmente su imparcialidad respecto de los sistemas de información concretos que pretende auditar y la ausencia

de conflicto de interés, de organización y de su personal, con las entidades, organismos, órganos, dependencias o unidades titulares de los sistemas de información auditados.

En consecuencia, el OAT elaborará y mantendrá actualizada una gestión de riesgos frente a la imparcialidad que trate y minimice aquellos riesgos evaluados como inaceptables por denotar evidentes conflictos de interés, ya sea de la propia Organización, o de su personal, en relación con los posibles auditados en el ámbito de sus competencias, así como con otras áreas de la entidad donde se encuadre el OAT.

### 5.3 REQUISITOS PROCEDIMENTALES Y METODOLÓGICOS

La entidad titular del sistema de información a auditar facilitará al OAT cuanta información fuera pertinente para realizar los trabajos de auditoría, teniendo en cuenta su alcance y las eventuales limitaciones derivadas del ordenamiento jurídico.

El Equipo Auditor está obligado a requerir y obtener las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirán los hallazgos en que se basarán las conclusiones recogidas en el Informe de Auditoría.

## 6. ESTRUCTURA DE PERSONAL DE LOS OAT

Los OAT deben mantener actualizada la información relacionada con su estructura interna, incluyendo su organización, equipos constituidos y listado nominal del personal habilitado para llevar a cabo Auditorías de Certificación de la Conformidad con el ENS.

### 6.1 PERSONAL RELEVANTE NO AUDITOR

En un OAT, además del personal que participa en las evaluaciones constituyendo el Equipo Auditor (puede haber varios equipos de auditoría en un mismo OAT), debe disponerse de otro personal que se considera muy relevante para la organización; se trata del Responsable Técnico, el Revisor de Expedientes y el Auditor Interno.

Con independencia de la estructura jerárquica o funcional de la Organización en la que se incardina, el OAT debe disponer de un Responsable Técnico que se responsabilice de la coordinación técnica del personal que participa en las evaluaciones, así como de la elaboración, adecuación o supervisión de las normas internas y procedimientos relacionados con su función evaluadora.

Una posibilidad opcional que se contempla, consiste en que la elaboración, adecuación o supervisión de las normas internas y procedimientos las asuma un nuevo rol de Responsable del Sistema de Gestión, en vez de hacerlo el propio Responsable Técnico, que se centrará en tareas de coordinación técnica del personal.

Cuando el Responsable Técnico, además de sus funciones organizativas y de coordinación del OAT, reúna la competencia técnica necesaria exigible a un Auditor Jefe o a un Revisor de Expedientes, podrá actuar adicionalmente como tal, siempre que se garantice la ausencia de conflictos de interés.

El OAT deberá disponer, adicionalmente a la figura de Responsable Técnico, de un Revisor de Expedientes, cuyas funciones son verificar los diferentes expedientes de auditoría que tramite el OAT antes de la adopción de la decisión final de certificar, o no, el sistema de información auditado. El Revisor de Expedientes puede ser un rol específico, o ser asumido entre diferentes auditores jefe, no pudiendo revisar un expediente en el que haya intervenido como auditor, en evitación de conflictos de interés.

Por último, el OAT debe tener asignada la función de auditoría interna, que será la encargada de auditar el sistema de gestión interno basado en la norma ISO/IEC 17065:2012, o en cualquier versión posterior que pueda publicarse. La persona que la asuma, podrá ser contratada en modalidad de prestación de servicios o asignarse a personal interno, procurando evitar que nadie audite su propio desempeño.

## 6.2 PERSONAL DEL EQUIPO AUDITOR

A los efectos de la presente Guía, todos los miembros de los Equipos de Auditoría que participen en las evaluaciones, ya sea personal propio del OAT, personal *freelance* contratado al efecto o personal perteneciente a terceras organizaciones con las que el OAT hubiere contratado servicios profesionales, deberán satisfacer, individualmente y con carácter personal, los requisitos de capacidad técnica y ausencia de conflicto de interés[1] que se señalan en este documento. Es responsabilidad del OAT garantizar que se exigen dichos requisitos, haciéndolo constar, cuando así proceda, en los correspondientes Pliegos de Prescripciones Técnicas y/o Administrativas, evaluando la idoneidad en la fase de valoración de ofertas y asegurando que tales requisitos se exigen y verifican en cada nueva auditoría que realice el OAT.

El OAT podrá disponer de uno o varios equipos de auditoría, estando todos ellos en su conjunto, desde el punto de vista técnico, bajo la responsabilidad y supervisión del Responsable Técnico designado.

[1] La ausencia de conflicto de interés puede definirse, en términos jurídicos, como la situación objetiva y verificable en la que una persona física o jurídica, en el ejercicio de funciones públicas o privadas, no se encuentra incursa en ninguna circunstancia, relación, vínculo, interés económico, profesional, personal o de cualquier otra naturaleza que sea idóneo para comprometer, influir o aparentar influir de manera indebida en la imparcialidad, independencia, objetividad o lealtad con la que debe adoptar decisiones o desempeñar sus funciones, de conformidad con el ordenamiento jurídico aplicable, los principios de buena administración, transparencia e integridad, y los deberes fiduciarios o de diligencia que resulten exigibles, de modo que no concurre ni conflicto real, ni potencial, ni aparente que pueda menoscabar la confianza legítima de terceros en la rectitud de su actuación.

Como ya se ha indicado, el Responsable Técnico del OAT podrá asimismo actuar en calidad de jefe de equipo de auditorías (Auditor Jefe), siempre que reúna los requisitos necesarios, algo frecuente en su constitución inicial, o en aquellos OAT que cuenten con poco personal.

El Equipo Auditor, que puede pertenecer total o parcialmente a la plantilla del OAT, deberá estar compuesto por profesionales (Auditor Jefe y, en su caso, auditores y/o expertos técnicos), debiendo poseer los conocimientos suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de las auditorías de Certificación de Conformidad con lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, en la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad y en las guías *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación, CCN-STIC-802 Guía de auditorías de cumplimiento* y *CCN-STIC-809 Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento*.

El Equipo Auditor deberá satisfacer los siguientes requisitos:

- Tanto si el Equipo de Auditoría es interno como externo, o una combinación de ambos, no deberá presentar conflictos de interés con la organización titular de los sistemas de información auditados, ni con los sistemas o servicios que sean o puedan ser objeto de la auditoría, estando formado por profesionales sobre los que pueda asegurarse su imparcialidad, objetividad, confidencialidad y ausencia de conflicto de intereses.
- El Auditor Jefe de cada equipo será el responsable de la realización de la auditoría y de la emisión del Informe de Auditoría. Además, será el encargado de confeccionar el Plan de Auditoría, de forma previa al inicio de ésta, que debe establecer con claridad la responsabilidad y asignación de funciones a cada integrante del Equipo Auditor.
- Con independencia de la adscripción de los miembros del Equipo Auditor (auditores internos o externos), el OAT mantendrá la plena responsabilidad de los actos preparatorios y del desarrollo de la auditoría de Certificación de la Conformidad con el ENS, siendo responsable último de la calidad y adecuación del Informe de Auditoría elaborado por el Auditor Jefe, revisado habitualmente por el Responsable Técnico del OAT previo a su entrega a la entidad titular del sistema de información auditado, quedando a disposición del CCN, a quién se comunicará el comienzo y el fin de la auditoría y su resultado.
- Posteriormente, antes de adoptar la decisión de certificación y una vez el auditado haya aportado en plazo el posible Plan de Acciones Correctivas (PAC)

que evidencie que se hayan resuelto las desviaciones, de haberlas, reflejadas en el Informe de auditoría, el Revisor de Expedientes lo revisará de nuevo en el marco del expediente completo.

- Al objeto de mantener la debida homogeneidad de actuación respecto del resto de auditorías de Certificación de la Conformidad con el ENS, el proceso de auditoría seguirá lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y, especialmente al actualizarse con mayor frecuencia, en las Guías *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación* y *CCN-STIC-802 Guía de auditorías de cumplimiento*, siempre en su versión vigente.

El Equipo Auditor, en el diseño de sus pruebas y revisiones, no debe limitarse a la revisión de documentos, ya que el objetivo de la auditoría es obtener evidencias eficaces para evaluar y sustentar si, en la práctica, las medidas de seguridad auditadas son adecuadas para proteger la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información tratada, almacenada o transmitida por el sistema de información auditado y los servicios prestados.

Los componentes del Equipo Auditor deberán tener una capacitación suficiente en auditoría de sistemas de información y en seguridad de la información, según se establece en los requisitos mínimos. Si se considera necesario por la complejidad del sistema, o por la presencia de tecnología innovadora, se podrán incorporar expertos técnicos en determinadas materias.

El Auditor Jefe o líder del equipo auditor deberá evidenciar que:

- Dispone de los conocimientos técnicos necesarios para abordar la Auditoría de Certificación de la Conformidad con el ENS de una forma eficiente.
- Se realizan las acciones necesarias, en la etapa preliminar, para garantizar que todos los integrantes del equipo entienden y conocen la estructura organizativa y técnica del sistema a auditar, los servicios que presta, así como el objetivo, el alcance y el criterio de la auditoría.
- Todos los auditores conocen la versión vigente del ENS (RD 311/2022) y, en la medida de las tareas asignadas, los requisitos de seguridad de otra legislación aplicable, y en particular, la relativa a tratamiento de datos personales.
- Se ha llevado a cabo el Plan de Auditoría o, en su caso, las alteraciones al mismo están debidamente fundamentadas y registradas.

### 6.3 REQUISITOS MÍNIMOS DEL PERSONAL TÉCNICO

Los OAT deben disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación de Conformidad del ENS, conforme lo dispone la

Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, en todas las fases del proceso auditor: estudio documental previo, auditoría in situ (presencial o en remoto), redacción del Informe de Auditoría y evaluación del Plan de Acciones correctivas, en su caso. En concreto, se exigirá disponer, al menos, de:

- Un (1) Responsable Técnico, que podrá actuar en calidad de Auditor Jefe.
- Un (1) Jefe del Equipo Auditor (Auditor Jefe), para cada uno de los equipos de auditoría que se deseen constituir o, lo que es lo mismo, como auditorías de certificación desee el OAT abordar simultáneamente.
- Un número suficiente de auditores para la correcta realización de las auditorías aceptadas contractualmente.
- Al menos, un (1) revisor de los expedientes de auditoría, de conformidad con lo señalado en la norma ISO/IEC 17065:2012, rol que podrían llegar asumir entre al menos dos auditores jefes, en el supuesto de no ser un desempeño específico, cuidando siempre de que ninguno de ellos revise los expedientes en los que haya intervenido.

Debe tenerse en cuenta que es habitual la única participación del Auditor Jefe en algunas auditorías, siendo éste, conjuntamente con el Responsable Técnico del OAT, quién previamente al inicio de cada auditoría decidirá si requiere apoyo de otros auditores, o no.

El Equipo Auditor deberá estar dirigido y tutelado siempre por un Auditor Jefe, cuyas funciones principales son la supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos observados y el dictamen final, así como preservar las evidencias de la auditoría.

El Auditor Jefe deberá estar en condiciones de demostrar:

- Formación en auditorías de sistemas de información, a través de certificaciones reconocidas a nivel nacional o internacional, o cursos, seminarios o actividades formativas regladas o impartidas por entidades reconocidas, de calidad y número de horas formativas suficientes que permitan evidenciar la suficiencia de los conocimientos adquiridos.
- Experiencia verificable en la realización regular de auditorías o inspecciones de tecnologías de la información de, al menos, 20 jornadas en los últimos 4 (cuatro) años, de las cuales, 10 tienen que haberse realizado en el último año.
- Conocimientos de seguridad de la información y gestión de riesgos de seguridad, demostrable por medio de certificaciones o experiencia de, al menos, cuatro (4) años en estas competencias.

- Conocimiento de los requisitos del ENS, demostrable por medio de cursos o seminarios sobre estas competencias, de calidad y alcance suficientes, que comprendan un mínimo de veinte (20) horas de formación.
- Conocimientos de la legislación aplicable cuando la auditoría pueda requerir la evaluación de la conformidad de medidas derivadas del cumplimiento de otras normativas, tales como las de protección de datos o el Esquema Nacional de Interoperabilidad, entre otras.

Las capacidades, formación y experiencia del personal encargado de la revisión de los expedientes de Auditoría deberán ser, al menos, las exigidas para el Auditor Jefe de cara a posibilitar una ejecución de la evaluación eficaz. Todo ello de acuerdo con el epígrafe 7.5 de la norma ISO/IEC 17065:2012.

El resto de los miembros del Equipo Auditor (auditores) podría no cumplir con los requisitos exigidos para el Auditor Jefe, no obstante, deberá tener alguna preparación previa tanto en seguridad de la información, como en auditoría de los sistemas de información, en consonancia con las responsabilidades que le sean asignadas para la auditoría de que se trate.

Los miembros del equipo auditor deberán estar familiarizados con las Guías de Seguridad CCN-STIC aplicables a cada caso, y disponer de conocimientos y experiencia en la administración de seguridad de sistemas operativos y aplicaciones, así como en infraestructuras de redes informáticas y mecanismos criptográficos.

Los auditores que se vayan incorporando al OAT, constarán como auditores provisionales en cualificación. Podrán realizar el acompañamiento de cualquier auditoría de certificación, siempre que se encuentren bajo la supervisión directa del Auditor Jefe o de cualquier otro auditor experimentado.

## 6.4 INCORPORACIÓN DE EXPERTOS TÉCNICOS AL EQUIPO DE AUDITORÍA

En el desarrollo de las actividades de auditoría, el Equipo Auditor tendrá que revisar temas tecnológicos diversos, como los relacionados con la electrónica de red, sistemas abiertos o propietarios, mecanismos de cifrado, firma electrónica, gestión de documentos electrónicos, planes de continuidad, seguridad de las comunicaciones, u otros de naturaleza análoga.

Por esta razón, una vez analizada la complejidad tecnológica, es posible que el Auditor Jefe considere necesaria la incorporación de expertos técnicos en determinadas materias. Entre estos expertos técnicos también es posible que sea necesario incluir profesionales con perfiles especializados tales como:

- Expertos en materias jurídicas;
- Expertos en Procedimiento Administrativo;

- Expertos en archivística, gestión documental y conservación a largo plazo;
- Expertos tecnológicos (Blockchain, IA, etc.);
- y otros que se estimen pertinentes en función del sistema auditado.

Las necesidades de conocimiento de estos expertos dentro del Equipo Auditor las establecerá el Auditor Jefe, en coordinación con el Responsable Técnico, en el momento de definir los recursos necesarios para la realización de la auditoría.

Los expertos estarán sujetos a las mismas reglas y deberes que el resto del Equipo Auditor (planificación, evidencias de auditoría, supervisión por el Jefe del equipo de auditoría y cláusulas de confidencialidad y ausencia de conflictos de interés).

En ningún caso los expertos técnicos deben haber participado o desempeñado responsabilidades en el sistema de información auditado, o haber sido consultores para ese sistema en el proceso de implantación de los requisitos del ENS, de forma previa a la auditoría de Certificación de la Conformidad con el ENS, o al menos en los dos (2) últimos años.

## 6.5 RESUMEN DE REQUISITOS DEL PERSONAL DEL OAT

| Perfil dentro del OAT | Función principal | Requisitos mínimos exigidos |
|---|---|---|
| **Responsable Técnico** | Coordina técnicamente al OAT y supervisa normas internas, procedimientos y calidad del proceso auditor. | - Figura obligatoria en todo OAT.<br>- Responsable de la coordinación del equipo auditor.<br>- Puede actuar como Auditor Jefe si cumple requisitos y no hay conflicto de interés. |
| **Auditor Jefe (Jefe del Equipo Auditor)** | Dirige la auditoría, elabora el Plan de Auditoría y emite el Informe final. | - Formación reconocida en auditoría de sistemas.<br>- Experiencia mínima: 20 jornadas en 4 años (10 en el último año).<br>- Conocimientos en seguridad y gestión de riesgos (≥4 años).<br>- Formación ENS mínima de 20 horas.<br>- Debe garantizar evidencias, supervisión y dictamen final.<br>- Pueden ser internos o externos, sin conflictos de interés.<br>- No debe haber participado como consultor o auditor interno del sistema auditado en los últimos 2 años. |
| **Auditores (miembros del equipo auditor)** | Ejecutan pruebas, revisiones técnicas y aportan evidencias durante la auditoría. | - Preparación previa en seguridad de la información y auditoría.<br>- Familiaridad con guías CCN-STIC aplicables.<br>- Actúan bajo dirección del Auditor Jefe.<br>- Pueden ser internos o externos, sin conflictos de interés.<br>- No deben haber participado como consultor o auditor interno del sistema auditado en los últimos 2 años. |
| **Revisor de Expedientes** | Revisa el expediente completo antes de la decisión final de certificación. | - Rol obligatorio adicional al Responsable Técnico.<br>- No puede revisar expedientes en los que haya participado como auditor. |

| | | |
|---|---|---|
| | | - Capacidades equivalentes a las exigidas para Auditor Jefe.<br>- Basado en ISO/IEC 17065. |
| **Auditor Interno** | Audita el sistema de gestión interno del OAT (ISO/IEC 17065). | - Debe existir función de auditoría interna.<br>- Puede ser personal interno o contratado externo.<br>- Debe evitarse que audite su propio desempeño.<br>- El auditor interno debe evidenciar conocimiento de la norma ISO/IEC 17065. |
| **Expertos Técnicos (opcionales)** | Apoyan en materias especializadas (IA, blockchain, criptografía, jurídico, continuidad, etc.). | - Incorporación según complejidad tecnológica.<br>- Sujetos a confidencialidad y ausencia de conflicto de interés.<br>- No deben haber participado como consultor o auditor interno del sistema auditado en los últimos 2 años. |
| **Personal colaborador no auditor** | Apoya funciones organizativas o administrativas del OAT. | - Puede incluir roles de soporte relevantes.<br>- Deben mantenerse actualizados en estructura y organización del OAT. |

## 7. ACUERDOS SUSCRITOS POR LOS OAT CON LOS AUDITADOS

Los OAT suscribirán con la entidad titular del sistema de información a auditar una serie de acuerdos vinculantes para garantizar la efectividad de la auditoría, la confidencialidad de la información accedida, así como el buen uso de la posible certificación concedida al auditado durante su período de vigencia.

El primer acuerdo, suscrito entre el OAT y la entidad titular del sistema auditado, es el de derechos y obligaciones de quién se certifica.

- Derechos como, por ejemplo, a hacer uso del Sello o Distintivo de Certificación de Conformidad para hacer constar dicha condición, o a poder recurrir la decisión de Certificación si el auditado no está de acuerdo con ella.
- Deberes como, por ejemplo, no hacer declaraciones engañosas durante la auditoría, y permitir que el personal del CCN, organismos o administración competentes, asistan como observadores a la realización de cualquier tipo de auditoría efectuada por la OAT en sus instalaciones. Dicho acuerdo suele incluir un compromiso de confidencialidad y protección de datos por parte del OAT.

El segundo acuerdo, suscrito únicamente por la entidad titular del sistema auditado, son compromisos respecto a las marcas de certificación, como puede ser el compromiso de no publicitar que se está certificado con un alcance o categoría mayor del que realmente se está, o la prohibición de difundir sellos o certificados incompletos o enmendados.

## 8. CRITERIOS GENERALES DE AUDITORÍA

Los criterios de auditoría que considerará el OAT en su proceso de realizar la Certificación de la Conformidad con el ENS se recogen en el propio Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS y, de forma detallada, en las

vigentes guías publicadas por el CCN relacionadas con la auditoría y la certificación del ENS, así como en las Instrucciones Técnicas de Seguridad.

Entre las guías más relevantes, cabe destacar las que se muestran en la tabla a continuación:

| Guías del CCN directamente relacionadas con auditoría y certificación | |
|---|---|
| **CCN-STIC 802**. ENS. Guía de auditorías de cumplimiento | Considera detalladamente todas las fases de una auditoría de certificación de la conformidad con el ENS, la metodología a emplear, la clasificación de los hallazgos, requisitos para el OAT y su personal, etc. |
| **CCN-CERT IC-01/19**. ENS. Criterios generales de auditoría y certificación | Es una guía muy dinámica que incorpora aquellos aspectos de la certificación que deben matizarse. Considera aspectos de competencia y recursos del OAT, imparcialidad, tiempos de auditoría, formato y validez certificados, perfiles de cumplimiento, etc. |
| **CCN-STIC 808**. ENS. Verificación del cumplimiento. | Explica las medidas compensatorias y las complementarias de vigilancia. Define el grado de implantación de una medida y muestra cómo debe auditarse cada una de las 73 medidas de seguridad del ENS, así como lo que se consideran requisitos nucleares. También incide en cómo auditar los artículos relevantes del ENS. |
| **CCN-STIC 819**. Medidas compensatorias. | Determina qué información debe documentar la organización auditada para cada una de las posibles medidas compensatorias que aplique al sistema y refleje en la declaración de aplicabilidad. Esta estructura y contenido es la que verificará el auditor de certificación durante la auditoría del sistema. |
| **CCN-STIC 809**. Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento | Concreta y diferencia la Declaración de Conformidad de la Certificación de Conformidad, la comunicación de certificaciones al CCN por parte del OAT, la aprobación provisional de conformidad y el Consejo de Certificación del ENS (CoCens). |

En la tabla siguiente se muestran las cuatro (4) Instrucciones Técnicas de Seguridad promulgadas. Las dos primeras son las más relacionadas con auditoría y certificación del ENS. Debe considerarse que las ITS no se actualizan tan frecuentemente como las guías del CCN:

| Instrucciones Técnicas de Seguridad (ITS) | |
|---|---|
| **ITS de Auditoría de la Seguridad**: Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. | Establece las condiciones para la realización general de auditorías del ENS. |
| **ITS de Conformidad con el ENS:** Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. | Considera tanto la Declaración como la Certificación de Conformidad con el ENS, estableciendo los procedimientos para dar publicidad a la conformidad, incluyendo el formato de los sellos oficiales, así como los requisitos exigibles a los organismos de certificación. |
| **ITS del informe INES:** Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. | Establece las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en el Sector Público. Recordar que, a partir a partir del 5 de mayo de 2024, también las organizaciones del sector privado comprendidas en el ámbito de aplicación del ENS deberán cumplimentar el formulario INES. |
| **ITS de Notificación de Incidentes**: Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. | Tiene por objeto la notificación y gestión de incidentes de seguridad en los sistemas de información de las entidades del Sector Público del ámbito de aplicación de dicho cuerpo legal, cuando tales incidentes tengan un impacto significativo en la seguridad de la información que manejan o los servicios que prestan, en relación con la categoría del sistema y con independencia de los requerimientos adicionales que cada organismo o entidad implemente para adaptarlos a sus entornos singulares. |

# 9. EL PROCESO DE RECONOCIMIENTO DE UN OAT

## 9.1 FORMACIÓN PREVIA DEL PERSONAL DEL OAT

Para que una organización o alguna de sus unidades, áreas, secciones o departamentos pueda ser reconocida como OAT, es necesario que su personal relevante asista a uno o varios cursos 'on-line' síncronos, algunos específicos para Órganos de Auditoría Técnica y otros para Organismos de Certificación en general (sean OAT o EC), impartido por personal asignado por el CCN.

## 9.2 REMISIÓN DE DOCUMENTACIÓN EN EL PROCESO DE RECONOCIMIENTO

En los procesos de reconocimiento inicial de los OAT, la organización solicitante deberá remitir al CCN la siguiente documentación básica:

- Estructura prevista para el OAT y su incardinamiento orgánico y funcional en el organismo del que dependa.
- Relación del personal involucrado en las actividades de auditoría del ENS previstas, incluyendo su adscripción (total, parcial o subcontratada), formación y experiencia previa en tales actividades.
- Análisis de los posibles riesgos que pudieran atentar a la imparcialidad y ausencia de conflicto de interés del OAT y de su personal, incluyendo las medidas para su tratamiento y mitigación, en su caso.
- Experiencia previa del OAT, o de su personal relevante, en la realización de actividades relacionadas con inspecciones/auditorías de seguridad.
- Metodología y procedimiento para la realización de auditorías de seguridad del ENS, cubriendo las fases pertinentes contempladas en la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.

El CCN analizará la idoneidad y adecuación de la documentación presentada por el OAT, sobre la que emitirá un Informe de Estudio Documental con los hallazgos que se hubieren encontrado y que exijan subsanación o acciones correctivas. Durante dicho proceso de análisis documental el CCN podrá requerir al OAT la aportación de documentación adicional.

## 9.3 JORNADA DE RECONOCIMIENTO

La jornada de reconocimiento constará de dos partes:

### 9.3.1 Parte 1

El OAT presentará la base documental del sistema de gestión de auditorías que pretende usar para el desarrollo de su actividad auditora, tomando como base la Metodología y procedimiento para la realización de auditorías de seguridad del ENS,

cubriendo las fases pertinentes contempladas en la norma *UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios*, e incluyendo la presentación de aquella documentación adicional que fue objeto de análisis previo por parte del CCN, en su caso, actualizada a su última versión.

Dicha presentación comprenderá los registros, las normas y los procedimientos internos elaborados y aprobados para su gestión, la de su personal, para la realización de evaluaciones, para conducir el proceso de certificación en general, etc.

### 9.3.2 Parte 2

El OAT presentará, en la segunda parte de la jornada, las acciones desarrolladas en la auditoria del ENS de un caso real (o una simulación en base a un caso determinado), en el que se mostrará la aplicación práctica de la metodología y procedimientos descritos en la Parte 1, incluyendo los registros o documentación que se han obtenido o cumplimentado en cada fase del proceso de certificación.

Como resultado de la evaluación de las acciones desarrolladas en la Parte 1 y la Parte 2, el CCN podrá considerar necesario completar el proceso de reconocimiento con la realización de una Auditoría de Acompañamiento.

## 9.4 AUDITORÍA DE ACOMPAÑAMIENTO

El CCN, a la vista del resultado de las acciones señaladas en el epígrafe 9.3, y dentro del proceso de reconocimiento, podrá considerar la necesidad de personarse como Observador en una Auditoría de Acompañamiento al OAT, en la que verificará de forma real el desempeño del equipo auditor designado por el OAT en la realización de dicha auditoría del ENS.

Para planificar adecuadamente el acompañamiento, se le solicitará al OAT la relación de las próximas auditorías previstas, al efecto de organizar la auditoría de acompañamiento.

## 9.5 INFORME DE RECONOCIMIENTO

Como resultado de las acciones desarrolladas en la Parte 1 y la Parte 2 de la Jornada de Presentación y, en su caso, en el Acompañamiento, el CCN emitirá un Informe de Reconocimiento con los hallazgos encontrados.

Tras la recepción del Informe de Reconocimiento, y caso de existir desviaciones que deban ser corregidas, el OAT deberá remitir al CCN, en un plazo no superior a un mes, el correspondiente Plan de Acciones Correctivas en el que se aporten evidencias del tratamiento y corrección de las desviaciones halladas.

### 9.6 CONCESIÓN DEL RECONOCIMIENTO

Una vez analizado el sistema de gestión usado por el OAT, incluidos su metodología y procedimientos, junto a su correcto desenvolvimiento práctico en la realización y registro de las auditorías de Certificación de la Conformidad con el ENS, el CCN, en el ámbito de sus competencias, emitirá la correspondiente Certificación de Reconocimiento como OAT, cuya validez se extenderá durante dos años siempre que se mantengan las condiciones requeridas para su concesión.

Transcurrido dicho periodo el OAT deberá someterse a un nuevo proceso de reconocimiento (epígrafes 9.3 y, en su caso, 9.4) que acredite que mantiene la observancia a las condiciones impuestas inicialmente.

## 10. OBLIGACIONES ADICIONALES DE LOS OAT

### 10.1 DURANTE EL PROCESO DE RECONOCIMIENTO

Durante el proceso de reconocimiento y siempre que se hubieren producido cambios, el OAT deberá proporcionar al CCN cuanta información se solicite relativa a sus recursos societarios o administrativos, incluyendo organización, estructura, metodologías, equipos de auditores y listado nominal del personal habilitado para llevar a cabo auditorías, con el objetivo de verificar y validar el sistema que se empleará para gestionar el proceso de Certificación de la Conformidad con el ENS y la metodología empleada por el OAT en las correspondientes auditorías.

### 10.2 A LO LARGO DE SU DESEMPEÑO COMO OAT

Se deberá mantener una permanente vigilancia respecto de las últimas versiones de las Guías CCN-STIC (especialmente, las comprendidas en la serie 800) que resulten aplicables en cada situación, como a las ITS que adquieren rango de norma jurídica cuando son aprobadas mediante Resolución de la Secretaría de Estado competente, siempre considerando, no obstante, su período de actualización más dilatado.

Se comunicará al Centro Criptológico Nacional cualquier circunstancia que pueda impedir o limitar la calidad de los trabajos de los OAT o la imparcialidad requerida.

El OAT mantendrá permanentemente informado al CCN de las fechas y el personal encargado de llevar a cabo las Auditorías para las que hubieren sido requeridos sus servicios.

### 10.3 SUBCONTRATACIÓN DE RECURSOS

De conformidad con lo recogido en la norma ISO 17065, el OAT debe asegurarse de que dispone en todo momento de personal suficiente para acometer las Auditorías de Seguridad del ENS que le fueren requeridas.

No obstante, en determinadas circunstancias o en periodos de tiempo definidos, podría suceder que el OAT precisara disponer de personal auditor adicional que pueda ser subcontratado de forma externa. En estos casos, y dejando claro que, aunque podrían subcontratarse las funciones de auditor, auditor jefe, responsable técnico o revisor de expedientes, la toma de decisión constituye una responsabilidad indelegable, que en ningún caso podrá ser objeto de subcontratación. Los requisitos exigibles para tales roles serán los mismos que para el personal de plantilla, poniendo un especial cuidado en garantizar la debida imparcialidad, la ausencia de conflicto de interés en los términos previstos en la presente Guía y en aquella otra normativa que pueda resultar de aplicación, tanto respecto de las personas subcontratadas como de las entidades auditadas.

Si, por exigencias derivadas de la aplicación de la legislación en materia de contratación pública o de los requisitos impuestos por los eventuales Pliegos de Prescripciones Administrativas/Técnicas que regularan las condiciones aplicables, la subcontratación tuviera que extenderse a una persona jurídica, el OAT deberá asegurarse que dicha entidad no realiza actividades de consultoría o bien que las actividades de auditoría son desarrolladas por una entidad bajo una separación jurídica, funcional y operativa efectiva (incluyendo NIF diferenciado) respecto de aquellas otras que pudieran desarrollar actividades de consultoría, comprobando en todo caso que mantienen los procedimientos adecuados para garantizar la imparcialidad de sus actividades, verificando asimismo la debida ausencia de conflictos de interés entre la entidad que se pretende subcontratar y la entidad auditada, en los términos descritos en la presente Guía.

## 11. EMISIÓN DEL CERTIFICADO DE RECONOCIMIENTO COMO OAT

En el caso de haberse concedido el reconocimiento como se señala en el epígrafe 9.6 al cumplir el OAT los requisitos especificados en el presente documento y en la normativa o Guías CCN-STIC aplicables, junto a considerar las cautelas exhibidas para garantizar la imparcialidad y la ausencia de conflictos de interés, el CCN reconocerá la capacidad técnica de la entidad, organismo, órgano o unidad, vinculada o dependiente de las Administraciones Públicas, para la realización de Auditorías de Conformidad en el ENS.

A partir de la publicación y consiguiente entrada en vigor de la presente Guía, el CCN comunicará al OAT solicitante la superación del procedimiento de reconocimiento mediante el Certificado de Reconocimiento correspondiente, que contendrá el correspondiente Distintivo de Reconocimiento del CCN, con un código individualizado

mediante el cual podrá comprobarse la autenticidad de dicho reconocimiento en la sede electrónica del CCN.

El CCN emitirá un Certificado de Reconocimiento en el que se indique que el OAT dispone de la capacidad técnica para la realización de Auditorías de Certificación de la Conformidad con el ENS, según se dispone en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y en el presente documento.



CCN
centro criptológico nacional

CERTIFICADO DE RECONOCIMIENTO
ÓRGANO DE AUDITORÍA TÉCNICA

El Centro Criptológico Nacional del Centro Nacional de Inteligencia certifica que, en cumplimiento de lo dispuesto en la Guía CCN-STIC 122 Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica (OAT) del Esquema Nacional de Seguridad (ENS), la entidad / organismo / órgano / dependencia / unidad:

ORGANIZACIÓN

dispone de la capacidad técnica necesaria para la realización de Auditorías de Seguridad del ENS, de conformidad con lo dispuesto en la Resolución, de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

| | |
|---|---|
| Fecha de concesión: | DD/MM/YYYY |
| Fecha de expiración: | DD/MM/YYYY |
| Número de certificado: | ENS-OAT-YYYY-XXX |

Emitido en Madrid, XX de mmmmm de YYYY

El Subdirector General del Centro Criptológico Nacional
D. Javier Candau Romero

RECONOCIMIENTO ÓRGANO DE AUDITORÍA TÉCNICA DEL SECTOR PÚBLICO
Nº XXX

Centro Criptológico Nacional
Centro Nacional de Inteligencia
Calle Argentona, 30
28023 Madrid

Asimismo, el CCN mantendrá en su sede electrónica una relación actualizada de los OAT reconocidos o en proceso de reconocimiento.

## 12. PUBLICIDAD DE LOS RECONOCIMIENTOS

El OAT que disponga de un Certificado de Reconocimiento vigente podrá dar publicidad, en su portal web o en cualquier otro medio de comunicación, el reconocimiento del que es titular, pudiendo mostrar el siguiente Distintivo de Reconocimiento.




## 13. VIGENCIA DEL RECONOCIMIENTO

El reconocimiento de los OAT para la realización de auditorías de Certificación de la Conformidad con el ENS, tendrá una validez de dos (2) años, pudiendo ser renovado por la misma duración si se mantienen las condiciones que permitieron la emisión del primer reconocimiento.

Con dicha periodicidad, el CCN realizará las mismas comprobaciones que dieron lugar al reconocimiento inicial y, de ser satisfactoria dicha evaluación, mantendrá el Certificado de Reconocimiento con su fecha de entrada en vigor vigente.

En cualquier momento, durante su vigencia, el CCN podrá retirar a un OAT el Certificado de Reconocimiento concedido si se confirmara la presencia de circunstancias que no permitan garantizar la satisfacción por parte del OAT de los requisitos exigidos para su concesión.

El CCN se reservará el derecho de acompañar a los OAT en todas aquellas auditorías de Certificación de la Conformidad con el ENS que realicen.

## 14. RENOVACIÓN DEL RECONOCIMIENTO

Una vez transcurrida la validez del reconocimiento inicial, los OAT deberán iniciar un proceso de renovación del reconocimiento en el que se evidenciará el mantenimiento de las condiciones evaluadas en el reconocimiento inicial y descritas en este procedimiento.

Una vez realizada la solicitud de renovación por parte del OAT, el CCN indicará los medios a través del cual el OAT presentará las normas y procedimientos internos elaborados y aprobados para su gestión, la de su personal, para la realización de evaluaciones, para conducir el proceso de certificación en general, y cualquier otra documentación necesaria para evaluar el mantenimiento de la competencia del OAT.

Junto a los procedimientos y normativas, se deberá entregar un listado de la documentación entregada, indicando si el documento ha sido actualizado desde el último proceso de reconocimiento y, en su caso, una descripción breve de las modificaciones realizadas o los motivos que han llevado a modificar el documento.

Adicionalmente el OAT remitirá el listado actualizado de las auditorías realizadas y certificados emitidos desde el último reconocimiento realizado, así como próximas auditorías que estén planificadas. Sobre este listado, el CCN seleccionará una muestra de la que solicitará toda la documentación relacionada con el expediente, incluyendo los documentos necesarios para su planificación, informe de auditoría y certificado de conformidad.

Una vez remitida la documentación será evaluada por el CCN para asegurar que se mantenga el cumplimiento de los requisitos especificados en el presente documento y en la normativa o Guías CCN-STIC aplicables.

Si este proceso no fuera suficiente para evidenciar el cumplimiento de los requisitos, el CCN podrá solicitar la recopilación de evidencias o aclaraciones adicionales al personal del OAT y se reservará el derecho de acompañar a los OAT en una auditoría de Certificación de la Conformidad con el ENS para completar la evaluación del reconocimiento.

El CCN comunicará al OAT solicitante la superación del proceso de renovación y emitirá la actualización del Certificado de Reconocimiento correspondiente.

## 15. RESUMEN DE LAS FASES DEL RECONOCIMIENTO

| Fases que componen el proceso de reconocimiento de un OAT | |
|---|---|
| **Desarrollo documental y verificación interna** | El OAT desarrolla los documentos necesarios que constituirán su sistema de gestión y revisa que cumple los requisitos de capacidad técnica, organizativa, imparcialidad y competencia. |
| **Formación previa del personal** | El personal relevante debe asistir a cursos específicos impartidos por el CCN relacionados con el funcionamiento del OAT y la auditoría del ENS. |
| **Solicitud formal al CCN** | Se envía una comunicación oficial al Centro Criptológico Nacional para proceder con el proceso de reconocimiento como OAT, incluyendo determinada documentación básica, detallada en epígrafes anteriores de esta guía. |

| | |
|---|---|
| **Revisión de la solicitud y de la documental inicial.** | El CCN analiza la solicitud y emite un Informe de Estudio Documental con los hallazgos que se hubieren encontrado y que exijan subsanación o acciones correctivas. Durante dicho proceso de análisis documental el CCN podrá requerir al OAT la aportación de documentación adicional. |
| **Jornada de presentación del OAT** | El OAT realiza una presentación formal, de una jornada de duración, dividida en dos partes: en la primera muestra los documentos y registros que constituyen su sistema de gestión interno, mientras que en la segunda expone un caso práctico, que puede ser simulado, de la realización de un proceso completo de auditoría del ENS incluyendo todos los registros y documentos cumplimentados. |
| **Elaboración del informe del reconocimiento** | Una vez finalizada la sesión de reconocimiento, el CCN facilita un informe del reconocimiento con las desviaciones encontradas que, de haberlas, deberán subsanarse antes de un mes natural desde la recepción de dicho informe. |
| **Auditoria de acompañamiento al OAT** | El CCN podrá considerar la necesidad de personarse como Observador en una Auditoría de Acompañamiento al OAT, en la que verificará de forma real el desempeño del equipo auditor designado por el OAT en la realización de dicha auditoría del ENS. |
| **Concesión del reconocimiento** | Una vez subsanadas las desviaciones encontradas durante la jornada de reconocimiento y, en su caso, corroborado el adecuado desenvolvimiento del OAT durante el acompañamiento, el CCN, en el ámbito de sus competencias, emitirá la correspondiente Certificación de Reconocimiento como OAT. |
| **Vigencia y publicidad** | El reconocimiento tiene validez de 2 años y puede hacerse público en medios oficiales del OAT, a la vez que constará en el portal del ENS. |
| **Renovación del reconocimiento** | Al finalizar la vigencia, el OAT debe evidenciar el mantenimiento de condiciones, aportar al CCN la relación de las auditorías realizadas y, a partir de ella, algún expediente que se le solicite. |

### 15.1 MATRIZ RACI DEL PROCESO DE RECONOCIMIENTO DEL OAT

| Fase del proceso | OAT (Entidad solicitante) | Personal auditor del OAT | CCN |
|---|---|---|---|
| Desarrollo documental y verificación interna | **R/A** | C | C |
| Formación previa del personal | A | **R** | **C/A** |
| Solicitud formal al CCN | **R** | C | **I** |
| Revisión documental inicial | C | I | **R/A** |
| Presentación del OAT ante el CCN | **R** | **R** | **A/C** |
| Auditorías de acompañamiento | **R** | **R** | **I/A** |
| Concesión del reconocimiento | I | I | **R/A** |
| Vigencia y publicidad | **R** | I | **I** |
| Renovación del reconocimiento | **R** | **R** | **A** |

### Leyenda RACI

- **R (Responsable):** ejecuta la actividad.
- **A (Aprobador):** valida o toma la decisión final.
- **C (Consultado):** participa aportando soporte o evidencias.
- **I (Informado):** debe estar al tanto del resultado.

## ANEXO. REVISIÓN DE REQUISITOS PARA OAT

A continuación, pese a no ser una lista exhaustiva, se incluye una plantilla para facilitar a los OAT la revisión del cumplimiento de las condiciones de reconocimiento, previo a su solicitud.

| REQUISITO | CUMPLIMIENTO | OBSERVACIONES |
|---|---|---|
| **COMPETENCIA TÉCNICA** | | |
| Experiencia demostrable de, al menos tres (3) años, en la realización de auditorías, evaluaciones o inspecciones relacionadas con sistemas de información y su seguridad. | ☐ | |
| **ESTRUCTURA DEL OAT** | | |
| Información actualizada de la estructura interna del OAT (incardinamiento orgánico, estructura organizativa, equipos y listado de personal habilitado para llevar a cabo auditorías de Certificación de la Conformidad con el ENS). | ☐ | |
| Personal cualificado para la realización de inspecciones STIC en el ámbito del ENS. | ☐ | |
| Un (1) Responsable Técnico del OAT | ☐ | |
| Al menos un (1) Jefe del equipo de auditorías (Auditor Jefe), que inicialmente podría ser el Responsable Técnico si cumple los requisitos. | ☐ | |
| Nº suficiente auditores para la realización de las auditorías a las que se comprometa el OAT. | ☐ | |
| Un (1) revisor de expedientes, función que podría ser compartida entre al menos dos Auditores Jefe, sin que pueda revisarse un expediente en el que se haya intervenido. | ☐ | |
| Dispone de un Plan de Formación o Capacitación y diseño curricular asociado a cada uno de los desempeños relacionados con el proceso de certificación (en especial el Equipo Auditor). | ☐ | |
| **CONFIDENCIALIDAD, INDEPENDENCIA, IMPARCIALIDAD** | | |
| El OAT ha de asegurar que tanto su organización como el personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad titular, responsable o usuaria del sistema de información auditado (ausencia de conflictos de interés). | ☐ | |
| El OAT dispone de una gestión de riesgos respecto a la imparcialidad, evidenciando que se mitigan aquellos evaluados como inaceptables. | ☐ | |
| En ningún caso los integrantes del equipo auditor deben haber participado, detentado responsabilidades previas a la auditoría, o bien haber sido consultores en el proceso de implantación de los requisitos del ENS, al menos | ☐ | |

| | | |
|---|---|---|
| en los dos (2) últimos años, en el sistema de información auditado. | | |
| Todos los integrantes del equipo auditor, sean estos externos o internos, incluyendo a los posibles expertos técnicos, deberán haber firmado un acuerdo de confidencialidad antes de participar en las auditorías de Certificación de la Conformidad con el ENS que lleve a cabo el OAT. | ☐ | |
| **PERSONAL** | | |
| El Auditor Jefe deberá contar con Formación en auditorías de sistemas de información, a través de certificaciones reconocidas, cursos, seminarios o actividades formativas impartidas por entidades reconocidas, de calidad y adecuado número de horas, que permitan evidenciar la idoneidad y suficiencia de los conocimientos adquiridos. | ☐ | |
| El Auditor Jefe deberá contar con experiencia verificable en la realización regular de auditorías o inspecciones de tecnologías de la información de, al menos, 20 jornadas en los últimos 4 (cuatro) años, de las cuales, 10 tienen que haberse realizado en el último año. | ☐ | |
| El Auditor Jefe dispone de conocimientos de seguridad y gestión de riesgos de seguridad, demostrable por medio de certificaciones o experiencia de, al menos, cuatro (4) años en estas competencias. | ☐ | |
| El Auditor Jefe dispone de conocimientos de los requisitos del RD 311/2022, demostrable por medio de cursos o seminarios sobre estas competencias, de calidad y alcance suficientes, que comprendan un mínimo de 20 horas de formación. | ☐ | |
| Los demás miembros de equipo auditor (auditores y expertos técnicos) disponen de preparación previa tanto en seguridad de la información como en auditoría de los sistemas de información. | ☐ | |
| Todos los miembros del equipo auditor deberán estar familiarizados con las Guías de Seguridad CCN-STIC aplicables a cada caso. | ☐ | |
| **PROCEDIMIENTOS Y METODOLOGÍA** | | |
| Dispone de una metodología para el desarrollo de la auditoría de Certificación de la Conformidad con el ENS que cumple con lo establecido en la Guía CCN-STIC 802 sobre Auditorías en el ENS y CCN-STIC 808 sobre verificación del Cumplimiento de las medidas del ENS. | ☐ | |
| **La metodología contempla:** | | |
| - La comunicación al CCN de las fechas y el personal encargado de llevar a cabo las auditorias de Certificación de la Conformidad con el ENS | ☐ | |

| | | |
|---|---|---|
| - La determinación adecuada de los tiempos necesarios para realizar las auditorías, tanto en lo que se refiere al análisis documental previo, como a las auditorías presenciales ("in situ" o remotas) y demás actuaciones relacionadas como son la elaboración de los preceptivos informes. | □ | |
| - Que los tiempos de auditoría se modulen atendiendo a factores o elementos que puedan incrementar o disminuir el esfuerzo requerido, según se detalla en la Guía CCN-CERT IC-01/19 sobre criterios generales de certificación del ENS. | □ | |
| - Que se tengan en cuenta los tiempos mínimos de auditoría que establece la guía CCN-CERT IC-01/19, cuyo incumplimiento puede resultar en la adopción de las medidas que en derecho procedan por parte del CCN. | □ | |
| - La realización de un muestreo suficiente que aporte evidencias razonables de que el sistema se comporta de la misma manera en sistemas distribuidos en distintos emplazamientos. | □ | |
| - Resumen de los hallazgos de auditoría. El OAT deberá disponer de un modelo de Informe de Auditoría conteniendo, entre otros aspectos, los hallazgos detectados: No conformidades Menores, Mayores y Observaciones. | □ | |
| - Respecto al Plan de Acciones Correctivas (PAC), la verificación de la corrección de las No Conformidades descritas, o en su caso, las evidencias de que se han planificado acciones precisas para la resolución de las causas de las desviaciones halladas. En su caso, la necesidad de una auditoría extraordinaria. | □ | |
| - La criticidad de las desviaciones halladas en las evaluaciones y la consecuente propuesta de Aprobación Provisional de Conformidad (APC) o de Certificación de Conformidad con el ENS. | □ | |
| - La elaboración de un Informe de Auditoría con los resultados de la auditoría de Certificación de la Conformidad con el ENS, que será remitido al CCN además de a la Organización cuyo sistema de información ha sido auditado, conteniendo:<br>• La fecha y duración.<br>• El alcance.<br>• La categoría del sistema auditado relativa al ENS.<br>• La documentación analizada.<br>• Las herramientas utilizadas y los resultados correspondientes.<br>• Las desviaciones encontradas junto con las evidencias.<br>• La información asociada al muestreo realizado. | □ | |

| | | |
|---|---|---|
| • La criticidad de las desviaciones: "No conformidades mayores, menores u observaciones".<br>• Las posibles medidas correctoras asociadas a las desviaciones.<br>• El resultado de la auditoría como FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE.<br>• Las conclusiones y,<br>• Cualquier otro aspecto considerado de interés, como es el indicar los siguientes pasos (cómo elaborar el PAC, plazos de que se dispone, etc.). | | |
| **PROCESO DE RECONOCIMIENTO** | | |
| Ha hecho llegar al CCN los documentos relevantes (normas internas y procedimientos) constituyentes del sistema de gestión del OAT. | ☐ | |
| Ha impartido, o va a impartir, una sesión de reconocimiento en la que se detalle el sistema de gestión del OAT y la metodología desarrollada para el proceso de Certificación de la Conformidad del ENS a un equipo de expertos del CCN. | ☐ | |
| Proporcionar al CCN cuanta información se solicite para verificar y validar el sistema de gestión del OAT y la metodología empleada. | ☐ | |
| Ha participado, o pretende participar, el personal del OAT en auditorías de acompañamiento (mínimo una) invitado por el CCN como observador en aquellas que realice directamente o que realice otro OAT. | ☐ | |
| Ha invitado a participar al CCN como observador, al menos en una de las primeras auditorías de Certificación de la Conformidad con el ENS que realice el OAT. | ☐ | |