centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 122

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

Septiembre 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.09 16:23:04 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-276-9

Fecha de Edición: septiembre de 2023

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

ÍNDICE

1. OBJETO

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 la preceptiva Certificación de Conformidad con el ENS.

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

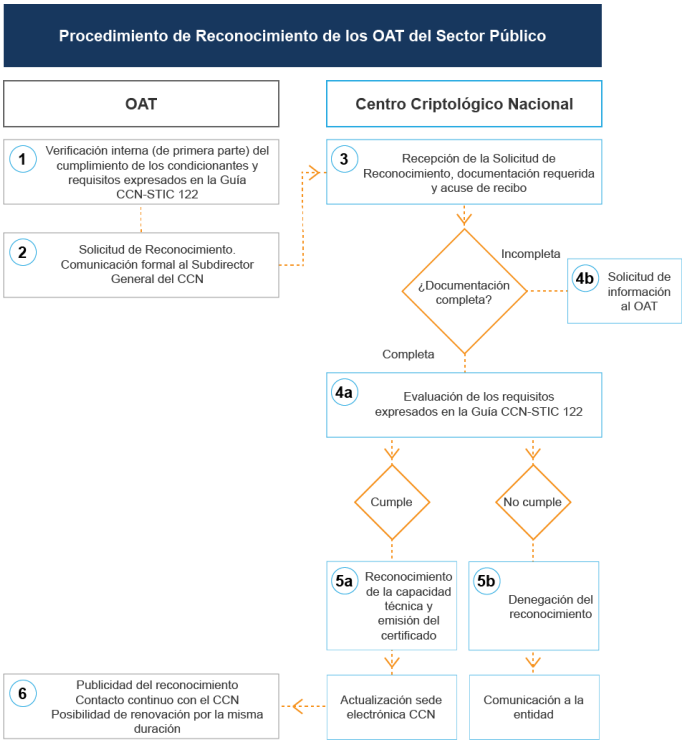
1) Capacidad técnica y organizativa para la realización de Auditorías de Seguridad, evaluando los requisitos que dispone el ENS para los sistemas de información auditados.

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

Correlativamente, el propósito de la presente Guía es asimismo participar de lo dispuesto en la Guía *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación,* según la cual, **el CCN podrá emitir una Aprobación Provisional de Conformidad (APC), a petición del Órgano de Auditoría Técnica**, que identificará las condiciones de aplicación de la APC al caso concreto, incluyendo la evaluación de las posibles medidas de mitigación de riesgo o reducción de determinadas funcionalidades, las acciones pendientes para completar el proceso y el marco temporal de validez.

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 del Sector Público, 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 auditorías interesadas en obtener el reconocimiento como OAT del Sector Público 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 ccn@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 del ENS, para lo que expedirá el correspondiente Certificado de Reconocimiento.

5. REQUISITOS GENERALES DE LOS OAT

5.1 COMPETENCIA TÉCNICA

El OAT del Sector Público 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 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.

El OAT del Sector Público 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

La OAT del Sector Público 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 del Sector Público 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 del Sector Público 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 del Sector Público 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, al menos en los dos (2) últimos años, en el sistema de información auditado, o bien haber sido consultores, para ese sistema, en el proceso de implementación de los requisitos del ENS.

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 dispondrá de 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.

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 del Sector Público 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 Órgano de Auditoría Técnica, 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.

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, asimismo, 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

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.

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* 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 reflejadas en el informe, 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 en la vigente Guía *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*.

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 del Sector Público 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 de, al menos, cuatro (4) años, en la realización regular de auditorías, evaluaciones o inspecciones de seguridad en tecnologías de la información.
- 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 con conocimientos jurídicos;
- 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.

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, respetarán lo dispuesto en la versión vigente de la Guía de Seguridad CCN-STIC *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*, que describe detalladamente, entre otros, los siguientes elementos:

<table>
<tr><th colspan="2">CRITERIOS DE AUDITORÍA</th></tr>
<tr><td>ALCANCE</td><td>Sistemas de información comprendidos en la auditoría y los servicios prestados por medio de tales sistemas.</td></tr>
<tr><td>TIEMPOS DE AUDITORÍA</td><td>Se establecerá el número de jornadas de auditoría necesarias en lo que se refiere al análisis documental previo, la elaboración del Plan de Auditoría, la materialización de la auditoría presencial (“in situ” o en remoto) al sistema auditado, la redacción del Informe de Auditoría, eventualmente la evaluación del Plan de Acciones Correctivas, la revisión del expediente y la adopción de la Decisión de certificación y posible emisión del certificado de Conformidad correspondiente.
La determinación del número total de jornadas de auditoría tendrá en cuenta la categoría del sistema de información auditado (BÁSICA, MEDIA o ALTA) aplicándose un factor de corrección, atendiendo al número de controles que fuere necesario auditar, sabiendo que, en función de los niveles adscritos del sistema auditado para cada dimensión, habrá las siguientes horquillas:
• Categoría BÁSICA: de 40 a 52 controles (hasta un 71%).
• Categoría MEDIA: de 51 a 68 controles (hasta un 93%).
• Categoría ALTA: 73 controles (100%).
La experiencia ha evidenciado que unos tiempos de auditoría razonables atenderían al siguiente criterio:
<table>
<tr><td>Fase de estudio documental previo</td><td>Mínimo, entre 0,5 y 1 jornada.</td></tr>
<tr><td>Fase de auditoría modo remoto/in situ</td><td>· Categoría BÁSICA: mínimo 1,5 jornadas.
· Categoría MEDIA: mínimo 2,5 jornadas.
· Categoría ALTA: mínimo 3,5 jornadas.</td></tr>
<tr><td>Fase de redacción de informes</td><td>Cualquier Categoría: mínimo, 1 jornada, que comprenderá la redacción del Informe de Auditoría completo y adecuadamente evidenciado (señalando cada medida auditada); en su caso, evaluación del Plan de Acciones Correctivas (PAC), revisión del expediente y decisión del Comité de Certificación (o de quién adopte la decisión).</td></tr>
</table>
</td></tr>
</table>

	Ante la determinación de tiempos de auditoría anormales, el Centro Criptológico Nacional, en el ejercicio de sus competencias, podrá examinar las circunstancias argumentadas por el OAT para tal asignación, adoptando las medidas que, en derecho, procedan.
TIEMPOS ADICIONALES	El número de jornadas obtenido en el punto anterior puede ser objeto de incremento/decremento atendiendo a otros factores, tales como Factores de Incremento • Significativo número de personas con privilegios de administración; • Infraestructura compleja, involucrando varias dependencias o ubicaciones; • Personal que habla más de un idioma (que requiere intérprete o impide que auditores individuales trabajen de forma independiente) o documentación provista en más de un idioma; • Actividades que requieran visitar ubicaciones alternativas o complementarias para confirmar las actividades de las ubicaciones habituales cuyo sistema de gestión está sujeto a certificación. Factores de decremento • Sistemas de Información que soportan Servicios con escaso riesgo; • Sistemas de Información que soportan Servicios de escasa complejidad tecnológica; • Equipos de usuarios sometidos a un mismo control organizacional, desarrollando las mismas tareas; • Conocimiento previo de la organización y del sistema auditado. (Por ejemplo, si el sistema ya ha sido certificado previamente con el ENS); • Experiencia del cliente en las certificaciones de conformidad. (Por ejemplo, sistema ya certificado o reconocido por otro esquema de certificación en materia de seguridad de la información, tal como ISO 27001, por ejemplo); • Elevada madurez del sistema de gestión de seguridad de la información. En todo caso, los factores de incremento o decremento no podrán suponer una variación mayor de un 20% respecto al cálculo inicial de jornadas de auditoría.
DESARROLLO AUDITORÍA	• Emplazamientos. • Desviaciones halladas: No Conformidades Mayores, No Conformidades Menores y Observaciones. • Verificación del Plan de Acciones Correctivas. El Centro Criptológico Nacional se reserva el derecho de acompañar a los OAT en todas aquellas auditorías que estos realicen.
RESUMEN DE HALLAZGOS DE AUDITORÍA	Los OAT deberán facilitar al CCN, a través de la solución AMPARO, el resultado del proceso de certificación incluyendo el número de hallazgos detectados durante la auditoría y su localización, ya sea en los artículos del ENS o en las medidas de su Anexo II, favoreciendo la explotación de la información proporcionada a efectos estadísticos.
AUDITORÍAS EN REMOTO	Será posible realizar inspecciones en modo remoto durante las Auditorías de Certificación del ENS usando medios telemáticos (como, por ejemplo, videoconferencia y compartición de escritorio remoto), siempre que se considere dicha actividad como viable por parte del OAT y acorde con los procedimientos de auditoría establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente a la organización auditada, y poder justificarlo adecuadamente ante el Centro Criptológico Nacional. Finalmente, será el Equipo Auditor el que determinará si es necesario complementar las evaluaciones realizadas en modo remoto con una inspección “in situ” de aquellos aspectos físicos relevantes de los que no sea posible obtener evidencias de forma remota con suficientes garantías.

AUDITORÍAS DE SERVICIOS COMPARTIDOS	En tanto los Servicios Compartidos ofrecidos por la Administración General del Estado (AGE) o, en su caso, por las Administraciones Territoriales competentes, que pudieran estar comprendidos en el alcance de la auditoría no dispongan de la preceptiva Certificación de Conformidad con el ENS, la Auditoría de Certificación de la Conformidad con el ENS deberá concentrarse solo en los servicios que puedan satisfacerse a través de los propios sistemas de información de la organización auditada (o en sistemas de información externos que posean la Certificación de Conformidad con el ENS o puedan ser auditados y certificados en tal sentido).
PUESTA A DISPOSICIÓN DEL INFORME DE AUDITORÍA	Entendiendo que los Informes de Auditoría podrían contener información o datos sensibles, de naturaleza personal, comercial o institucional y/o encontrarse protegidos por distintas regulaciones, la facultad que la ITS de Conformidad con el ENS confiere a las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado titulares de una Declaración o Certificación de Conformidad para solicitar a tales operadores dichos Informes de Autoevaluación o Auditoría se instrumentalizará dirigiendo tal solicitud y su necesidad a la cuenta de correo electrónico cocens@ccn.cni.es del Centro Criptológico Nacional y no al Organismo de Certificación que lo ha elaborado. Será el CCN quién valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y al Organismo de Certificación responsable, ya se trate este de un OAT o de una EC.
OBLIGACIONES DE LOS OAT EN CALIDAD DE ORGANISMO DE CERTIFICACIÓN	Mantener a disposición del Centro Criptológico Nacional los Informes de Auditoría resultantes de las evaluaciones realizadas, que, de conformidad con lo dispuesto en el RD 311/2022, de 3 de mayo, podrá verificar su contenido e idoneidad. 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, atendiendo prioritariamente a las ITS que adquieren rango de norma jurídica cuando son aprobadas mediante Resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Comunicar al Centro Criptológico Nacional cualquier circunstancia que pueda impedir o limitar la calidad resultante de los trabajos del OAT, o la imparcialidad requerida.
APROBACIÓN PROVISIONAL DE CONFORMIDAD	Podrá expedirse excepcionalmente una Aprobación Provisional de Conformidad (APC) como resultado de un proceso de Certificación de la Conformidad con el ENS en el que concurran, simultáneamente, los siguientes requisitos: • Persiga la emisión del primer Certificado de Conformidad con el ENS del sistema de información auditado. • El Plan de Acciones Correctivas, por razones adecuadas y razonables, requiere un período de ejecución superior a tres (3) meses. • No podrá ser aplicado cuando se hayan detectado No Conformidades Mayores. • Solo resultará de aplicación a sistemas de información con categorías BÁSICA o MEDIA. La Aprobación Provisional de Conformidad (APC), que será emitida por el Centro Criptológico Nacional, a petición del Órgano de Auditoría Técnica o la Entidad de Certificación, identificará las condiciones de aplicación de la APC al caso concreto, incluyendo la evaluación de las posibles medidas de mitigación de riesgo o reducción de determinadas funcionalidades, las acciones pendientes para completar el proceso y el marco temporal de validez. Así expedidas, las Aprobaciones Provisionales de Conformidad desplegarán su vigencia durante un período de seis (6) meses, que podrá ser ampliado por otros seis (6) meses, cuando concurran circunstancias de seguridad que así lo aconsejen. En la aplicación de un Marco de Certificación Específico (MCE-ENS), previamente validado por el CCN para sistemas de información de categoría BÁSICA, cuando un Órgano de Auditoría Técnica o Entidad de Certificación audite la preceptiva muestra representativa de entidades adheridas a dicho MCE-ENS, un único análisis

	de la documentación normativa generada se considerará suficiente para establecer el grado de cumplimiento normativo en todas las entidades adheridas al MCE-ENS. En estos casos y, tras la emisión de la APC, el Órgano de Auditoría Técnica al que están vinculadas o del que dependen orgánicamente las entidades del Marco de Certificación, dispondrá de un período de dos (2) años para realizar auditorías a estas entidades con la finalidad de completar el proceso de certificación de las mismas y proponer, en su caso, la Certificación de Conformidad en el ENS por parte del CCN.
OBLIGATORIEDAD DEL USO DE LAS GUÍAS CCN-STIC	Como señala la Disposición adicional segunda del ENS, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad. La inadecuación total o parcial del sistema de información evaluado a lo dispuesto en la Guía CCN-STIC que resultare de aplicación en cada caso (https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es), podría ser calificada por el Equipo Auditor como una Observación, una No Conformidad Menor o una No Conformidad Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.
EN RELACIÓN CON LAS CERTIFICACIONES Y DISTINTIVOS DE CONFORMIDAD	Se aplicará lo indicado en el apartado 3.11 de la guía CCN-STIC CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación

Durante el proceso de reconocimiento y siempre que se hubieren producido cambios, el OAT del Sector Público 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.

El OAT del Sector Público 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.

9. EL PROCESO DE RECONOCIMIENTO DE UN OAT

9.1 FORMACIÓN PREVIA DEL PERSONAL DEL OAT

Para que una organización, o tal vez una unidad, área, sección o departamento de la misma, sea reconocida como un 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 PRESENTACIÓN DEL OAT DURANTE EL RECONOCIMIENTO

Habitualmente la presentación del OAT, con independencia de la documentación facilitada previamente al CCN, tendrá una duración mínima de dos (2) días.

En el primero de ellos, 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, etc.

En el segundo día, el OAT expondrá un caso de auditoría, que puede tratarse de una simulación, para presentar mediante un ejercicio práctico la forma en que se prevé afrontar las evaluaciones de la Conformidad con el ENS, así como los registros que deben irse cumplimentando antes, durante y después de finalizarse la auditoría material.

9.3 AUDITORÍAS DE ACOMPAÑAMIENTO

El Centro Criptológico Nacional, dentro del proceso de reconocimiento de un OAT, no atenderá únicamente a verificar su estructura, procedimientos, competencia y formación del personal asignado, sino que tendrá en cuenta la materialización de auditorías de acompañamiento desde dos (2) perspectivas:

- Acompañamiento del personal colaborador del OAT, asistiendo a un mínimo de dos (2) auditorías de Certificación de la Conformidad con el ENS realizadas por el propio CCN, o por otros OAT, en calidad de observador.
- Acompañamiento de personal asignado por el CCN al menos a las dos (2) primeras auditorías realizadas por el OAT en el desempeño real de sus competencias.

Una vez constatado el correcto desenvolvimiento práctico del OAT en la realización y registro de este tipo de auditorías, en el ámbito de sus competencias, y verificada la idoneidad de su sistema interno de gestión para la Certificación de la Conformidad con el ENS, podrá concederse el reconocimiento.

10. OBLIGACIONES ADICIONALES DE LOS OAT DEL SECTOR PÚBLICO

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, atendiendo prioritariamente a las ITS que adquieren rango de norma jurídica cuando son aprobadas mediante Resolución de la Secretaría de Estado competente.

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.

11. CONCESIÓN DEL RECONOCIMIENTO

En el caso de que se cumplan los requisitos especificados en el presente documento y en la normativa o Guías CCN-STIC aplicables, el CCN reconocerá la capacidad técnica de una entidad, organismo, órgano o unidad, vinculada o dependiente de las Administraciones Públicas, para la realización de Auditorías de Conformidad en el ENS y las cautelas exhibidas para garantizar la imparcialidad y la ausencia de conflictos de interés.

El CCN comunicará al OAT solicitante la superación del procedimiento de reconocimiento mediante el Certificado de Reconocimiento correspondiente.

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.

centro criptológico nacional

CERTIFICADO DE RECONOCIMIENTO

ÓRGANO DE AUDITORÍA TÉCNICA

El Centro Criptológico Nacional 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

NOMBRE COMPLETO DE LA ENTIDAD

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 entrada en vigor: xx de xxxxxxxxx de 20xx

Número de certificado: ENS-OAT/xxx

Madrid, xx de xxxxxxxxx de 20xx

El Subdirector General del Centro Criptológico Nacional

D. Luis Jiménez Muñoz

Centro Criptológico Nacional
Centro Nacional de Inteligencia
c/ Argentona, 30
28023 Madrid

Pantone:
SOLID COATED
2925C

Web (HTML):
#009ade

RGB:
R: 0
G: 154
B: 222

CMYK:
C: 77%
M: 24%
Y: 0%
K: 0%

Asimismo, el CCN mantendrá en su sede electrónica una relación actualizada de los OAT del Sector Público 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 del Sector Público 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 del Sector Público en todas aquellas auditorías de Certificación de la Conformidad con el ENS que realicen.

ANEXO. REVISIÓN DE REQUISITOS PARA OAT DEL SECTOR PÚBLICO

A continuación, pese a no ser una lista exhaustiva, se incluye una plantilla para facilitar a los OAT del Sector Público 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 de, al menos, cuatro (4) años en la realización regular de auditorías de sistemas de información.	☐	
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: • La fecha y duración. • El alcance. • La categoría del sistema auditado relativa al ENS. • La documentación analizada. • Las herramientas utilizadas y los resultados correspondientes. • Las desviaciones encontradas junto con las evidencias. • La información asociada al muestreo realizado.	□	

• La criticidad de las desviaciones: "No conformidades mayores, menores u observaciones". • Las posibles medidas correctoras asociadas a las desviaciones. • El resultado de la auditoría como FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE. • Las conclusiones y, • 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 dos) 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 las dos (2) primeras auditorías de Certificación de la Conformidad con el ENS que realice el OAT.	☐	

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL