centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 122

Procedimiento de Reconocimiento de Entidades de Certificación del ENS del sector público y requisitos del Órgano de Auditoría Técnica

Marzo 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-21-063-5

Fecha de Edición: marzo de 2021

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

1. El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.
2. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.
3. Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.
4. De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

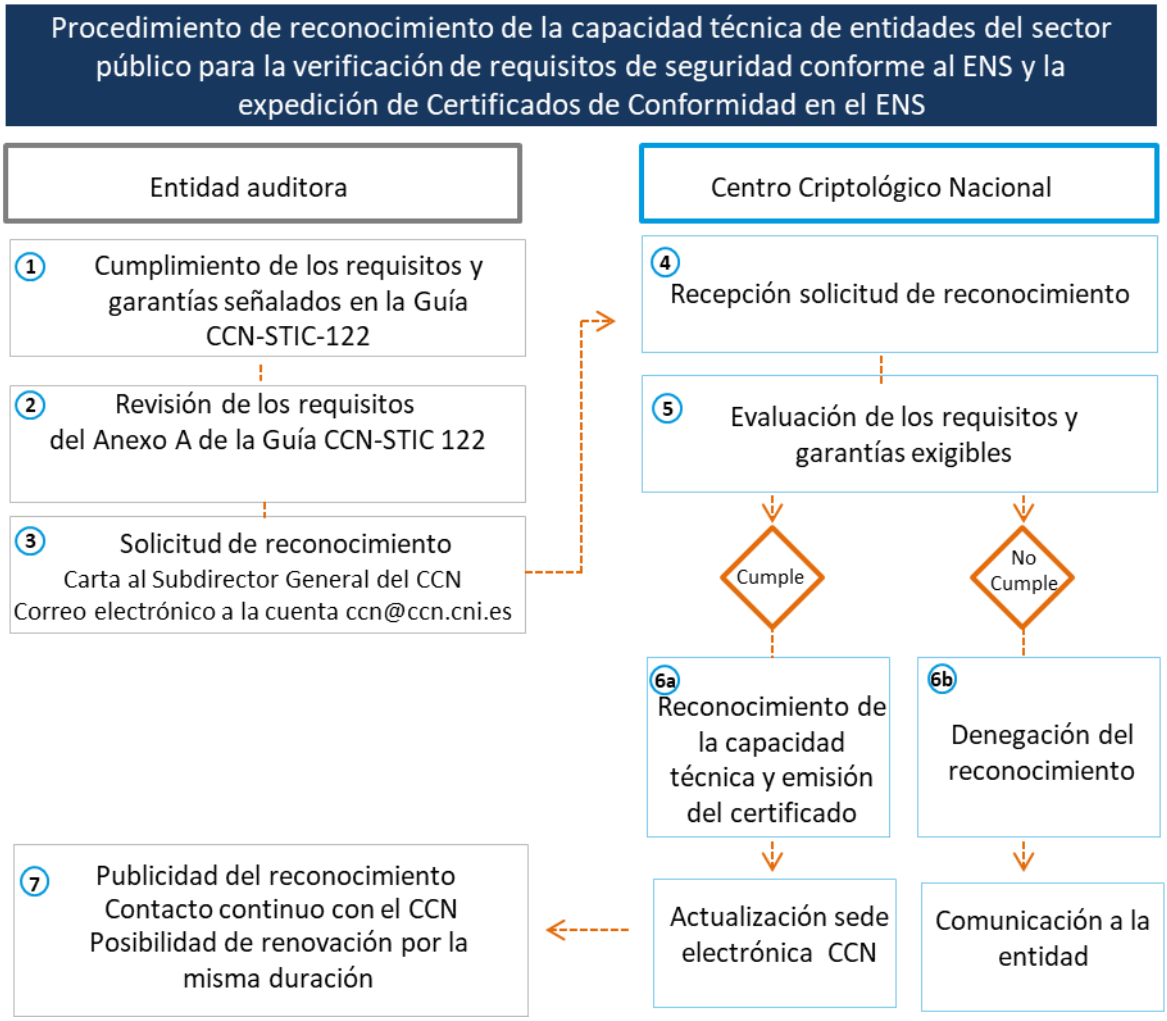
2. OBJETO

5. El presente documento tiene por objeto definir el procedimiento utilizado por el Centro Criptológico Nacional (CCN) para el reconocimiento de la capacidad técnica de entidades, órganos, organismos 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 o decretos de estructura, quede garantizada la debida imparcialidad y ausencia de conflicto de intereses entre los elementos auditor y auditado.
6. En adelante, tales órganos, organismos y unidades recibirán el nombre de Órganos de Auditoría Técnica (OAT) del Sector Público.
7. Asimismo, se definen los requisitos que deben satisfacer los OAT del Sector Público para el reconocimiento de la citada capacidad técnica para la realización Auditorías de Conformidad en el Esquema Nacional de Seguridad y de expedir los

correspondientes Certificados de Conformidad en el ENS para los sistemas auditados.

3. PROCEDIMIENTO DE RECONOCIMIENTO

8. En la siguiente figura puede observarse una representación gráfica del procedimiento utilizado por el Centro Criptológico Nacional para el reconocimiento de las entidades anteriores como OAT del Sector Público con la capacidad técnica para la verificación del cumplimiento de requisitos de seguridad conforme al Esquema Nacional de Seguridad.



4. SOLICITUD DE RECONOCIMIENTO

9. Las entidades interesadas en obtener el reconocimiento de OAT del Sector Público para la realización de Auditorías de Conformidad con el ENS y la expedición de los correspondientes Certificados de Conformidad, 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.

5. REVISIÓN DE LAS CONDICIONES DE RECONOCIMIENTO

10. El Centro Criptológico Nacional podrá reconocer la capacidad técnica de una entidad para la realización de Auditorías de Conformidad con el ENS y la expedición de los correspondientes Certificados de Conformidad en el ENS, siempre que se cumplan los requisitos especificados en el presente documento.

6. REQUISITOS DE LAS ENTIDADES AUDITORAS

6.1 Competencias del OAT del Sector Público

11. De conformidad con lo dispuesto en 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, como norma de desarrollo del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, podrán instituirse como Entidades de Certificación en el ENS aquellas entidades públicas cuyas competencias comprendan en el momento del reconocimiento el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad[1].
12. Estas entidades deberán proporcionar al Centro Criptológico Nacional aquella normativa en la que quede debidamente reflejada la asignación de competencias para el desarrollo de auditorías de sistemas de información.

6.2 Competencia técnica

13. El OAT del Sector Público debe tener una experiencia demostrable de, al menos, dos (2) años en la realización de auditorías, evaluaciones o inspecciones relacionadas con sistemas de información y su seguridad, valorándose la magnitud de los proyectos realizados en tal sentido.
14. Dicha experiencia deberá estar refrendada por, al menos, una de las siguientes opciones:
    a) Proyectos en los que figuren trabajos de auditoría de cumplimiento funcional, normativo o técnico.

[1] Entre ellas, entidades del tipo Diputación Provincial, Cabildo, Consejo Insular o entidad competente en materia de administración electrónica o informatización de sus entidades locales dependientes, adheridas, consorciadas o conveniadas.

b) Certificados de organismos con competencias en auditoría de seguridad de sistemas, en los que consten específicamente los trabajos de auditoría de cumplimiento normativo y técnica.

15. La experiencia demostrable podrá ser sustituida por la competencia técnica y conocimientos necesarios para la realización de inspecciones STIC.

16. Dicha competencia deberá estar refrendada por certificados de los cursos necesarios para la adquisición de las habilidades en auditoría, evaluación o inspección de sistemas de información que el CCN determine.

6.3 Estructura de la entidad auditora

17. El OAT del Sector Público ha de mantener actualizada la información relacionada con su estructura interna, incluyendo la organización, equipos y listado nominal del personal habilitado para llevar a cabo inspecciones de seguridad de las TIC en el ámbito del ENS.

18. 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 uno de los puestos de trabajo.

6.4 Confidencialidad, independencia e imparcialidad

19. 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 intereses respecto de la entidad auditada.

20. **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 implantación de los requisitos del RD 3/2010.

21. Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad.

6.5 Composición del Equipo Técnico auditor

22. El equipo auditor, que puede pertenecer o no a la plantilla de la entidad, deberá estar compuesto por profesionales (Auditor Jefe y, en su caso, auditores y expertos

técnicos), debiendo poseer los conocimientos suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de las auditorías, 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, en 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", en la 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".

23. Este equipo podrá estar compuesto por auditores internos y/ o externos o una combinación de ambos, pero en todo caso, es necesario cumplir con los siguientes requisitos:

    - Si el equipo de auditoría es interno, no deberá presentar conflictos de interés con la organización auditada o los sistemas o servicios que sean o puedan ser objeto de la auditoría. Por lo tanto, el equipo de auditoría debiera pertenecer al grupo de Auditoría/Control Interno/Intervención, o a un grupo con responsabilidades similares constituido como tal, que asegure su independencia, objetividad y ausencia de conflicto de intereses.
    - Si participan auditores internos y externos, se debe establecer el equipo responsable de la supervisión y realización de la auditoría y de la emisión del informe, y consecuentemente, de los resultados de la auditoría. El Plan de Auditoría debe establecer con claridad la responsabilidad y asignación de funciones a cada integrante del equipo auditor.
    - Sean auditores externos, internos o un equipo mixto, la propiedad de los documentos de trabajo y de las evidencias, así como la responsabilidad por la emisión del informe y su contenido deben ser siempre inequívocas tanto en la apertura de la auditoría, como en su informe final.
    - Si la realización de la auditoría ha sido encargada a un equipo externo (organización privada o pública), los integrantes deberán firmar las preceptivas cláusulas de confidencialidad, incluyendo las cláusulas aplicables de la legislación de tratamiento de datos de carácter personal.
    - Si la auditoría es liderada por un equipo de Auditoría Interna, pero con la incorporación de expertos técnicos independientes, estos también deben firmar una cláusula de confidencialidad.

24. 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 auditado.
25. Los componentes del equipo de auditoría deberán tener una formación suficiente en auditoría de sistemas de información y en seguridad, según se establece en los requisitos mínimos. Si se considera necesario por la complejidad tecnológica o dimensiones del entorno a auditar, se podrán incorporar expertos en determinadas materias.
26. El Auditor Jefe o líder del equipo auditor deberá asegurar que:
    - Dispone de los conocimientos técnicos necesarios para abordar la auditoría 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, y el objetivo y el alcance de la auditoría.
    - Todos los auditores conocen el RD 3/2010 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 previsto y aprobado, y que las desviaciones al programa, o sus modificaciones, están debidamente fundamentadas y registradas.

6.6 Requisitos mínimos del equipo auditor

27. Los OAT del Sector Público deben disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación del ENS, conforme lo dispone 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, en todas las fases del proceso auditor: estudio documental, auditoría in situ y redacción del Informe de Auditoría. En concreto, se exigirá disponer, al menos, de:
    - Un (1) Jefe de equipo de auditorías (Auditor Jefe).
    - Un número suficiente de auditores para la realización de las auditorías aceptadas contractualmente.

28. El equipo auditor deberá estar dirigido y tutelado siempre por un Auditor Jefe también llamado Líder del equipo auditor, cuyas funciones principales son la supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionadas en el informe, así como preservar las evidencias de la auditoría.

29. El Auditor Jefe deberá estar en condiciones de demostrar, al menos:

    - 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 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 RD 3/2010, 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.

30. La ausencia de alguno de los requisitos anteriores por parte del Auditor Jefe podrá ser total o parcialmente suplida con la evidencia de cualidades, conocimientos o experiencia compensatorias, que serán valoradas por el CCN y que comporten evidencias de fiabilidad en las evaluaciones que pudieran serle asignadas.

31. El resto del equipo auditor podría no cumplir con los requisitos exigidos para el Auditor Jefe, no obstante, debe tener alguna preparación previa tanto en seguridad como en auditoría de los sistemas de información, dependiendo de, y en consonancia, con las responsabilidades asignadas. La responsabilidad por la asignación de tareas al resto del equipo, incluyendo a los expertos, corresponde a la organización (privada o pública) que aporte el equipo de auditoría.

6.7 Incorporación de expertos técnicos al equipo de auditoría

32. En el desarrollo de las actividades de auditoría, el equipo auditor tendrá que revisar temas tecnológicos diversos, como los relacionados con las transmisiones electrónicas, 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.
33. 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 con conocimientos relativos a la gestión de documentos y archivos; electrónicos.
    - y otros que se estimen pertinentes en función del sistema auditado.
34. Las necesidades de conocimiento de estos expertos dentro del equipo auditor, las establecerá el Auditor Jefe, en el momento de definir los recursos necesarios para la realización de la auditoría.
35. Estos expertos estarán sujetos a las mismas reglas de la auditoría que el resto del equipo auditor (planificación, evidencias de auditoría, supervisión por el Jefe del equipo de auditoría, y cláusulas de confidencialidad), pero no es necesario que detente las mismas cualificaciones requeridas para un auditor.
36. **En ningún caso estos expertos, deben haber participado o desempeñado 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 implantación de los requisitos del RD 3/2010.

6.8 Requisitos procedimentales y metodológicos

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

38. 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.

7. CRITERIOS GENERALES DE AUDITORÍA

39. 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 criterios:

<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>OBLIGATORIEDAD DEL USO DE LAS GUÍAS CCN-STIC</td><td>Como señala el art. 29.1 del ENS, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, para el mejor cumplimiento de lo establecido en el Esquema Nacional 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, No Conformidad Menor o No Conformidad Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.</td></tr>
<tr><td>TIEMPOS DE AUDITORÍA</td><td>Se establecerá el número de jornadas de auditoría necesarias, tanto en lo que se refiere al análisis documental previo, como a la auditoría presencial en el sistema auditado.

La determinación del número de jornadas total de auditoría (análisis documental + auditoria presencial) 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:

• Categoría BÁSICA: 45 controles (60%)
• Categoría MEDIA: 63 controles (84%)
• Categoría ALTA: 75 controles (100%)

La experiencia ha evidenciado que unos tiempos de auditoría razonables atenderán al siguiente criterio:

<table>
<tr><td>Fase de estudio documental previo</td><td>Entre 0,5 y 1 jornada.</td></tr>
<tr><td>Fase de auditoría presencial</td><td>Categoría BÁSICA: mínimo, 1 jornada.

Categoría MEDIA: mínimo, 2 jornadas.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>Categoría ALTA: mínimo, 3 jornadas.</td></tr>
<tr><td>Fase de redacción de informes</td><td>Para cualquier Categoría: 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 y decisión del Comité de Certificación.</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 la Entidad Auditora para tal asignación, adoptando las medidas que, en derecho, procedan.</td></tr>
<tr><td>DESARROLLO AUDITORÍA</td><td>

Emplazamientos
Desviaciones halladas: No Conformidades Mayores, No Conformidades Menores y Observaciones
Verificación Plan de Acciones Correctivas

El Centro Criptológico Nacional se reserva el derecho de acompañar a las Entidades de Certificación en todas aquellas auditorías que estas realicen.</td></tr>
<tr><td>RESUMEN DE HALLAZGOS DE AUDITORÍA</td><td>Las Entidades de Certificación del ENS deberán disponer de un procedimiento que permita obtener, para cada evaluación realizada, un documento con el número de hallazgos detectados y su ubicación, ya sea en los artículos del ENS o en las medidas de su Anexo II.

La información anterior deberá ser remitida al CCN, al menos con periodicidad mensual, conteniendo el resumen de las evaluaciones realizadas.

En este sentido, el CCN-CERT pone a disposición de las Entidades de Certificación una funcionalidad de la solución AMPARO que permite la provisión de los datos indicados favoreciendo la automatización y eficiencia del proceso de cara a la explotación de la información proporcionada.</td></tr>
<tr><td>AUDITORÍAS EN REMOTO</td><td>Será posible realizar remotamente las Auditorías de Certificación del ENS (iniciales o de renovación, sobre clientes conocidos o desconocidos), usando medios telemáticos (como, por ejemplo, videoconferencia y compartición de escritorio remoto), siempre que se considere dicha actividad como viable por parte de la Entidad Auditora y acorde con los procedimientos de auditoria establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente a su cliente, y poder justificarlo adecuadamente ante ENAC y el Centro Criptológico Nacional.

Será el equipo auditor el que determinará si es necesario complementar las evaluaciones en modo remoto de las Auditorías, con una inspección “in situ” de aquellos aspectos físicos relevantes de los que no sea posible obtener evidencias de forma remota.</td></tr>
</table>

AUDITORÍAS DE SERVICIOS COMPARTIDOS	En tanto los Servicios Compartidos ofrecidos por la 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 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).
CERTIFICACIONES Y DISTINTIVOS DE CONFORMIDAD EN EL ENS	No podrá expedirse una Certificación de Conformidad con el ENS si existieran No Conformidades (Mayores o Menores) y no se hubiere presentado y evaluado satisfactoriamente el correspondiente Plan de Acciones Correctivas, que trate adecuadamente las desviaciones halladas. En las Certificaciones de Conformidad expedidas, las Entidades Auditoras están obligadas a identificar y publicar con precisión el alcance de la misma (sistema o sistemas de información afectados) y, con el mayor detalle posible, los servicios comprendidos en la Certificación. Cualquier servicio que no se encuentre explícitamente reseñado en la correspondiente Certificación de Conformidad se entenderá que no está amparado por ella. La presencia de los Distintivos de Conformidad con el ENS (ya sean Declaraciones o Certificaciones de Conformidad) en las sedes electrónicas de las entidades del Sector Público, responde, en primer instancia y de conformidad con lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público, al cumplimiento de los principios que rigen la actuación de las Administraciones Públicas, concretándose dicha obligación en lo dispuesto en el art. 41 del Real ENS 3/2010, de 8 de enero (ENS). En consecuencia, el incumplimiento detectado en una auditoría de certificación del deber de adecuada exhibición de los Distintivos de Conformidad correspondientes será objeto de una No Conformidad Mayor. Se establece el plazo de un (1) mes para que el cliente resuelva los incumplimientos detectados en el uso de los Distintivos de Conformidad.

PUESTA A DISPOSICIÓN DEL INFORME DE AUDITORÍA	El Distintivo de Conformidad con el ENS, electrónicamente enlazado a la Certificación de Conformidad de la que trae causa, resulta evidencia suficiente para demostrar que el proceso de Autoevaluación o la Auditoría de Certificación a la que esté ligado ha obtenido un resultado satisfactorio, por lo que no será necesario realizar ninguna verificación adicional sobre la adecuación e idoneidad del sistema de información de que se trate. Por otro lado, entendiendo que los Informes de Autoevaluación o Auditoría podrían contener información o datos sensibles, de naturaleza personal, comercial o institucional y/o 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, que valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y a la Entidad de Certificación responsable de la emisión de la antedicha Certificación de Conformidad con el ENS.
PERIODO DE VALIDEZ DE LAS CERTIFICACIONES DE CONFORMIDAD CON EL ENS EN SITUACIONES EXCEPCIONALES	Cuando se produzca una situación excepcional, como la provocada por la Covid-19, que exija la apertura de un paréntesis temporal en la relación entre las Entidades de Certificación y sus clientes, el Centro Criptológico Nacional podrá, en el ejercicio de sus competencias, prolongar la vigencia de los Certificados de Conformidad mediante la emisión de un comunicado. La vigencia de las Acreditaciones y de los Certificados de conformidad vendrá determinada por la duración de la citada situación excepcional teniendo en cuenta que, una vez se haya dado por finalizada, se concederá un nuevo período equivalente con la misma duración que el anterior, para facilitar el restablecimiento paulatino de las relaciones entre las Entidades de Certificación y sus clientes. Por tanto, la vigencia de los certificados afectados se incrementará en un tiempo análogo al que haya durado la situación excepcional, lo que será comunicado formalmente por el CCN. Si una vez expirado el paréntesis temporal concedido, existiese una causa justificada que impidiese en algún caso particular retomar los períodos y plazos de las auditorías, las Entidades de Certificación podrán solicitar un nuevo aplazamiento al CCN, justificando las razones de la solicitud a la cuenta de correo electrónico cocens@ccn.cni.es, que se estudiarán en cada caso para conceder las debidas autorizaciones.

OBLIGACIONES DE LAS ENTIDADES 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 3/2010, podrá verificar su contenido y adecuación. 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 de los trabajos de las Entidades de Certificación o la imparcialidad requerida.
APROBACIÓN PROVISIONAL DE CONFORMIDAD	Podrá expedirse excepcionalmente una Aprobación Provisional de Conformidad (APC) como resultado de un proceso de certificación en el que concurran, simultáneamente, los siguientes requisitos: • Persiga la emisión del primer Certificado de Conformidad. • 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 de 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 una 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 emitir, en su caso, el correspondiente Certificado de Conformidad en el ENS.

40. 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 la metodología empleada por la entidad en las Auditorías de Conformidad.
41. 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.

8. GARANTÍAS DE IMPARCIALIDAD

42. La imparcialidad de las actuaciones del OAT del Sector Público debe garantizarse evitando los conflictos de interés:
    - Entre las actividades de auditoría de sistemas TIC y el resto de las áreas de la entidad en la que esté encuadrado.
    - Entre las actividades de auditoría de sistemas TIC con relación a las entidades auditadas.
43. Entenderemos 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 de otro y otros.
44. Será en el momento de la constitución de un OAT del Sector Público en el que residirán las capacidades de Auditoría de Sistemas TIC en el ámbito del ENS, donde deberán adoptarse las cautelas precisas para asegurar, desde el mismo momento de su creación, la debida imparcialidad y ausencia de conflicto de interés entre tal órgano y las restantes áreas de la entidad y las Entidades Locales auditadas.

9. OBLIGACIONES ADICIONALES DE LOS OAT del Sector Público

45. 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 de Política Territorial y Función Pública.
46. Se comunicará al Centro Criptológico Nacional cualquier circunstancia que pueda impedir o limitar la calidad de los trabajos de las Entidades Auditoras o la imparcialidad requerida.

10.CONCESIÓN DEL RECONOCIMIENTO

47. En el caso de que se cumplan los requisitos especificados, el CCN reconocerá la capacidad técnica de una entidad, órgano, organismo o unidad, vinculada o dependiente de las Administraciones Públicas, para la realización de Auditorías de Conformidad en el ENS y la expedición de los correspondientes Certificados de Conformidad.

48. Se establecerá el reconocimiento en proceso durante doce (12) meses, hasta que se lleve a cabo la primera inspección STIC, que se deberá realizar con la presencia de un equipo de expertos del CCN, que valorará la capacidad técnica de la entidad auditora.

49. El CCN comunicará a la entidad peticionaria la superación del procedimiento de reconocimiento de las capacidades de Auditoría, o su denegación, mediante carta firmada por el Subdirector General del Centro Criptológico Nacional, adelantándose por vía electrónica.

50. El CCN emitirá un certificado de reconocimiento en el que se indique que la entidad dispone de la capacidad técnica para la realización de Auditorías de Conformidad en el ENS en los términos previstos en 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 y en el presente documento y la expedición de los Certificados de Conformidad en el ENS correspondientes.

CCN
centro criptológico nacional

CERTIFICADO DE RECONOCIMIENTO

Madrid, a de de 20xx

El Centro Criptológico Nacional certifica que, en cumplimiento de lo dispuesto en la *Guía CCN-STIC 122 Reconocimiento Entidades de Certificación en el ENS para organismos del sector público*, la entidad

XXXXX
sita xxxxxxxxx

dispone de la capacidad técnica necesaria para la realización de Auditorías de Conformidad con el Esquema Nacional de Seguridad de sistemas TIC y de expedir los correspondientes Certificados de Conformidad en el ENS de los sistemas auditados.

Fecha de reconocimiento inicial: xx/xx/xxxx
Fecha de renovación del reconocimiento: xx/xx/xxxx

SECRETARIA DE ESTADO
DIRECTORA DEL CNI Y DEL CCN

Paz Esteban López

Centro Criptológico Nacional
C/Argentona, 30
28023, Madrid
www.ccn.cni.es

Pantone:
SOLID COATED
2925C

Web (HTML):
#009ade

RGB:
R: 0
G: 154
B: 222

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

51. Asimismo, el CCN mantendrá en su sede electrónica una relación actualizada de las OAT reconocidas o en vías de reconocimiento.

11. PUBLICIDAD DE LOS RECONOCIMIENTOS

52. La entidad que disponga de la capacidad de Auditoría de Sistemas en el ámbito del Esquema Nacional de Seguridad, para la realización de Auditorías de Conformidad con el ENS y la expedición de los correspondientes Certificados de Reconocimiento, podrá anunciar en su portal web o en cualquier otro medio de comunicación el reconocimiento del que es titular, pudiendo mostrar el siguiente Distintivo de Reconocimiento.

12. VIGENCIA DEL RECONOCIMIENTO

53. El reconocimiento de los OAT del Sector Público que disponen la capacidad técnica para la realización de Auditorías de Conformidad con el ENS y la expedición de Certificados de Conformidad, tendrá una validez de dos (2) años, renovable por la misma duración si se mantienen las condiciones que permitieron la emisión del primer reconocimiento.

54. Con dicha periodicidad, el CCN realizará las mismas comprobaciones que dieron lugar al reconocimiento inicial y procederá con la renovación del reconocimiento y entrega del nuevo certificado.

55. El CCN podrá retirar el certificado de reconocimiento de conformidad en cualquier momento, sin necesidad de que el OAT del Sector Público haya completado la vigencia del reconocimiento.

56. El CCN se reservará el derecho de acompañar a los OAT del Sector Público en todas aquellas inspecciones TIC, en el ámbito del ENS, que estos realicen.

ANEXO A: REVISIÓN DE REQUISITOS PARA OAT

57. A continuación, 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 dos (2) años, en la realización de auditorías, evaluaciones o inspecciones relacionadas con sistemas de información y su seguridad.	□	
ESTRUCTURA DE ENTIDAD AUDITORA		
Información actualizada de la estructura interna de la entidad (organización, equipos y listado de personal habilitado para llevar a cabo inspecciones de seguridad de las TIC en el ámbito del ENS).	□	
Personal cualificado para la realización de inspecciones STIC en el ámbito del ENS.	□	
Un (1) Jefe del equipo de auditorías. (Auditor Jefe)	□	
Nº suficiente auditores para la realización de las auditorías.	□	
Puede responder a las necesidades identificadas de formación del personal.	□	
Dispone de un plan de capacitación y diseño curricular asociado a cada uno de los puestos de trabajo.	□	
CONFIDENCIALIDAD, INDEPENDENCIA, IMPARCIALIDAD		
La entidad auditora ha de asegurar que tanto su organización como el personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad auditada.	□	
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 implantación de los requisitos del RD 3/2010.		
Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán haber firmado antes de comenzar la auditoría, un acuerdo de confidencialidad.	□	
PERSONAL		
El Auditor Jefe deberá contar con experiencia demostrable de, al menos, cuatro (4) años.	□	
El personal auditor dispone de preparación previa tanto en seguridad como en auditoría de los sistemas de información.	□	
Dispone de certificaciones profesionales en materia de auditoría, seguridad, gobierno y/o gestión de riesgos TIC.	□	
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 de redes informáticas y mecanismos criptográficos.	□	
PROCEDIMIENTOS Y METODOLOGÍA		
Dispone de una metodología para el desarrollo de la auditoría de seguridad que cumple con lo establecido en la Guía CCN-STIC 802 sobre Auditorías en el ENS, CCN-STIC 804 sobre implantación en el ENS y CCN-STIC 808 sobre verificación del Cumplimiento de las medidas del ENS, así como en la norma CCN-STIC-303 sobre inspecciones STIC.	□	
La metodología contempla:		
- La comunicación al CCN de las fechas y el personal encargado de llevar a cabo las inspecciones STIC.	□	
- La determinación adecuada de los tiempos necesarios para realizar inspecciones STIC, tanto en lo que se refiere al análisis	□	

documental previo como a las inspecciones remotas o presenciales.		
- Que los tiempos de inspección se modulan atendiendo a factores o elementos que puedan incrementar o disminuir el esfuerzo requerido.	□	
- 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.	□	
- La valoración por parte del CCN de circunstancias o tiempos de inspección anormales.	□	
- Resumen de los hallazgos de auditoría. Las Entidades Auditoras deberán disponer de un procedimiento para obtener, un documento con el número de hallazgos detectados: No conformidades Menores, Mayores y Observaciones.	□	
- Respecto al Plan de Acciones Correctivas, 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.	□	
- La criticidad de las desviaciones halladas en las inspecciones 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 inspección STIC que será remitido al CCN, conteniendo: ・ La fecha y duración. ・ El alcance. ・ 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 medidas correctoras asociadas a las desviaciones. ・ El resultado de la inspección STIC. ・ Las conclusiones y recomendaciones.	□	

• Cualquier otro aspecto considerado de interés, pudiendo incluir oportunidades de mejora relacionadas con el Plan de Acciones Correctivas.		
Ha impartido o va a impartir una formación, mínimo 10 horas, en la que se detalle la metodología desarrollada por la entidad a un equipo de expertos del CCN.	□	
Proporcionar al CCN cuanta información se solicite para verificar y validar la metodología empleada.	□	