

Guía de Seguridad de las TIC

CCN-STIC 120

Procedimiento de Acreditación de Entidades de Inspección para verificar requisitos STIC en sistemas que manejan Información Clasificada del grado de DIFUSIÓN LIMITADA



Diciembre 2023



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

Edita:



CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL, o=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2023.12.11 17:05:44 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023
NIPO: 083-21-063-5

Fecha de Edición: diciembre 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

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

cpage.mpr.gob.es

ÍNDICE

1. INTRODUCCIÓN	4
2. ARMONIZACIÓN ENTRE NORMAS.....	5
3. DEFINICIONES	5
4. OBJETO	6
5. PROCEDIMIENTO PARA LA ACREDITACIÓN DE LAS EI-STIC.....	7
6. SOLICITUD DE LA ACREDITACIÓN COMO EI-STIC	7
7. REVISIÓN DE LAS CONDICIONES DE LA ACREDITACIÓN	8
8. REQUISITOS GENERALES DE LAS EI-STIC.....	8
8.1 COMPETENCIA TÉCNICA.....	8
8.2 CONFIDENCIALIDAD, INDEPENDENCIA E IMPARCIALIDAD	9
8.3 REQUISITOS PROCEDIMENTALES Y METODOLÓGICOS.....	10
9. ESTRUCTURA DE PERSONAL DE LAS EI-STIC.....	11
9.1 PERSONAL RELEVANTE NO AUDITOR.....	11
9.2 PERSONAL DEL EQUIPO DE INSPECCIONES STIC.....	12
9.3 REQUISITOS MÍNIMOS DEL PERSONAL TÉCNICO.....	14
9.4 INCORPORACIÓN DE EXPERTOS TÉCNICOS AL EQUIPO DE INSPECCIONES STIC ...	15
10. ACUERDOS SUSCRITOS POR LAS EI-STIC CON LOS AUDITADOS.....	16
11. CRITERIOS GENERALES DE INSPECCIÓN STIC.....	17
12. EL PROCESO DE ACREDITACIÓN DE UNA EI-STIC	19
12.1 FORMACIÓN PREVIA DEL PERSONAL DE LA EI-STIC.....	19
12.2 DEMOSTRACIÓN DE LA EI-STIC DURANTE LA ACREDITACIÓN DE LA ENTIDAD	19
12.3 AUDITORÍAS DE ACOMPAÑAMIENTO	19
13. OBLIGACIONES ADICIONALES DE LAS EI-STIC	20
14. CONCESIÓN DE LA ACREDITACIÓN	20
15. PUBLICIDAD DE LA ACREDITACIÓN	21
16. VIGENCIA DE LA ACREDITACIÓN.....	21
ANEXO. REVISIÓN DE REQUISITOS PARA EI-STIC	22

1. INTRODUCCIÓN

La protección de la información sensible, especialmente la relacionada con la defensa y la seguridad nacional, constituye un elemento indispensable para la salvaguarda de los intereses fundamentales de España y de los españoles.

El objeto a proteger no es sólo la información asociada a las operaciones militares, policiales o de inteligencia, y que permite al Gobierno tomar las decisiones adecuadas, sino también aquellas informaciones ligadas a esas actividades diplomáticas, científicas, económicas o industriales que contribuyen de manera decisiva al desarrollo y progreso económico y social de España.

Por otra parte, el incesante incremento de las acciones de ciberespionaje, de ciberdelincuencia y el crecimiento exponencial del número de ciberataques sufridos en todos los sectores de actividad de nuestra sociedad, convierten la necesidad de proteger nuestra información estratégica en una exigencia clave para la estabilidad y seguridad nacionales.

La enorme importancia de proteger este tipo de información aparece claramente recogida en la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO, en adelante), que define las “materias clasificadas” aquellos “asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado”.

La LSO fue desarrollada por Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la LSO, y finalmente modificada por la Ley 48/1978, de 7 de octubre.

Además de en tales cuerpos legales, este tipo de información es tratada en la vigente Estrategia de Seguridad Nacional de 2019, donde se reconoce que la información clasificada es un objetivo fundamental para los servicios de inteligencia hostiles, para grupos terroristas que tienen por objetivo la amenaza a nuestra seguridad y la desestabilización de nuestro sistema democrático, y para otros países con intereses económicos o comerciales en competencia con los de nuestra industria.

En virtud de lo dispuesto en la LSO, las materias clasificadas pueden tener la clasificación de SECRETO o RESERVADO. Además de estas clasificaciones, y en aplicación de la normativa relativa a las materias de reserva interna, este tipo de información sensible puede poseer los grados de CONFIDENCIAL o DIFUSIÓN LIMITADA (DL, que usaremos a lo largo de esta guía).

La información clasificada manejada por un sistema de información debe protegerse contra las posibles amenazas, ya se trate de acciones voluntarias o involuntarias, internas o externas, que puedan derivar en una pérdida de la confidencialidad, integridad, trazabilidad o autenticidad, o de la disponibilidad del propio sistema que trata dicha información y los servicios que la utilizan.

Por consiguiente, al objeto de alcanzar la adecuada protección será necesario aplicar un conjunto equilibrado de medidas de seguridad, de distinta naturaleza que permitan la creación de un entorno seguro en el que operen los sistemas de información concernidos.

Así pues, en aplicación de lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN, en adelante), se establece una Política de Seguridad de las TIC (CCN-STIC-001), que recoge la necesidad de la Acreditación de los sistemas que manejan información clasificada.

2. ARMONIZACIÓN ENTRE NORMAS

En España, además de la LSO, el tratamiento de la información clasificada también se encuentra regulado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), constituido por los principios básicos y por los requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Ambas normas, LSO y ENS, confluyen en el artículo 2 de este último cuerpo legal, sobre ámbito de aplicación, donde se señala que, *“sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales”*.

Para alcanzar la antedicha seguridad y, en su caso, exhibir el correspondiente certificación de conformidad, la antedicha legislación y sus normas de desarrollo han creado el Esquema de Evaluación y Certificación de la Conformidad, posibilitando la existencia de Entidades de Certificación del ENS (organizaciones privadas y Órganos de Auditoría Técnica del Sector Público) que, además de precisar acreditarse o ser reconocidos para desarrollar sus actividades de evaluación y certificación de la conformidad con el ENS, también pueden ser acreditadas como entidades aptas para poder llevar a cabo la fase de inspecciones STIC, fase necesaria dentro del proceso completo de acreditación de aquellos sistemas que manejan información clasificada, realizada por la Oficina Nacional de Seguridad (ONS).

3. DEFINICIONES

Es importante no confundir la *acreditación de entidades* con la *acreditación de sistemas de información*, para lo que podrá tenerse en cuenta las siguientes definiciones y características asociadas:

- Una **Entidad de Certificación (EC)**, que pertenecerá siempre al sector privado, debe ser acreditada por la Entidad Nacional de Acreditación (ENAC) para poder realizar auditorías de Certificación de la Conformidad con el ENS.
- Un **Órgano de Auditoría Técnica (OAT) del Sector Público**, que debe ser reconocido por el CCN para poder realizar asimismo auditorías de Certificación de la Conformidad con el ENS en su ámbito de competencia.

- **Un sistema que maneja información clasificada** debe ser acreditado para tal fin en el grado correspondiente al más alto de la información que maneja.
- El **Centro Criptológico Nacional (CCN)** acredita a una entidad (que podrá ser un OAT, una EC o una Entidad de Inspección STIC (EI-STIC) para poder realizar **inspecciones de seguridad de las TIC (STIC)** del grado DL, dentro del proceso global de acreditación de un Sistema.
- El **Centro Criptológico Nacional (CCN)** emite **Declaraciones de Cumplimiento** como resultado de una **inspección STIC** y evidencia que un Sistema cumple con los requisitos de Seguridad TIC para manejar información clasificada del grado que se indique.

***Nota:** la acreditación de los sistemas del Sector Público que manejen información clasificada procedente de OTAN, UE o de otros países u organizaciones con los que se hayan establecido acuerdos internacionales, será realizada por la Autoridad Nacional de Seguridad Delegada (ANS-D), que corresponde a la persona titular de la Dirección del Centro Nacional de Inteligencia.*

4. OBJETO

El presente documento tiene por objeto definir el procedimiento utilizado por el CCN para acreditar la capacidad técnica y resto de requisitos exigibles de aquellas entidades, públicas o privadas, que demuestren competencias suficientes para poder realizar **inspecciones STIC** dentro de un proceso de acreditación de sistemas que manejan información clasificada hasta el grado de DL, evidenciando asimismo que queda garantizada su debida imparcialidad y la ausencia de conflicto de intereses entre las partes auditora y auditada.

Tales entidades serán designadas como **Entidad de Inspección STIC** (en adelante, **EI-STIC**), pudiendo tratarse de:

- Entidades de Certificación (EC) del ENS del sector privado, acreditadas por la Entidad Nacional de Acreditación (ENAC) conforme a la norma ISO/IEC 17065:2012 que, además, dispongan de Habilitación de Seguridad de Empresa (HSEM) en vigor.
- Órganos de Auditoría Técnica del ENS del Sector Público (en adelante, OAT), reconocidos por el CCN, constituidos por entidades, organismos, órganos o unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información y dispongan de una estructura de información clasificada.
- Excepcionalmente, entidades acreditadas por el CCN que hayan demostrado la capacidad técnica y la imparcialidad suficientes para llevar a cabo inspecciones STIC sobre sistemas que manejan información clasificada.

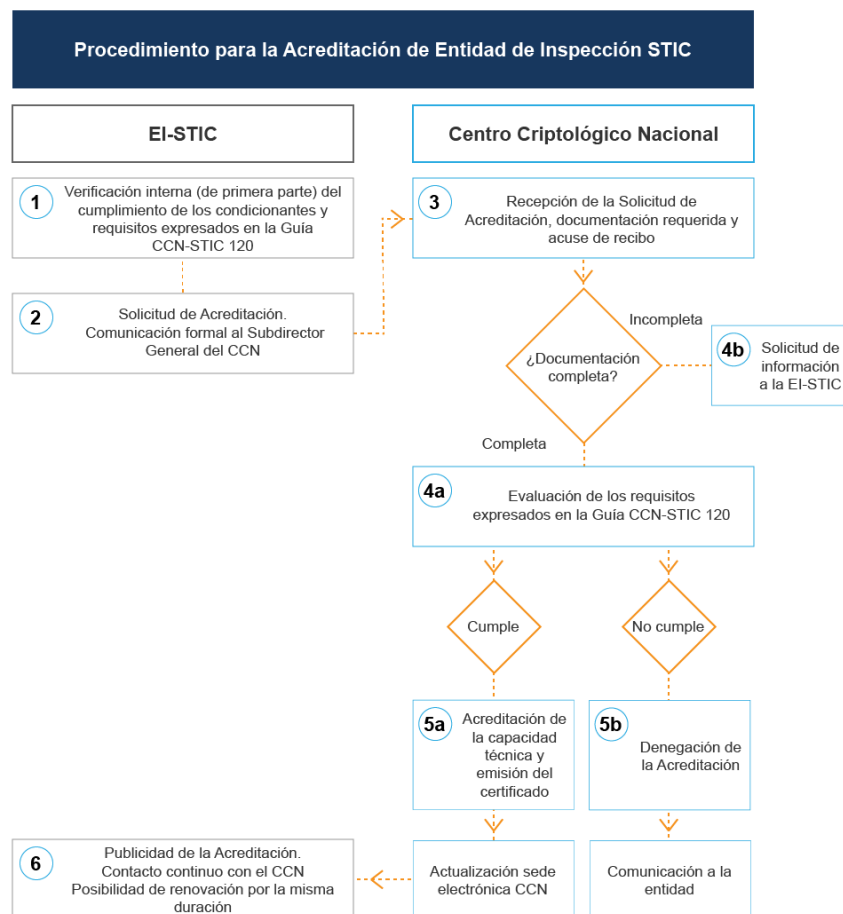
Todas las EI-STIC deberán satisfacer dos (2) requisitos fundamentales para ser acreditadas por el CCN:

- 1) Capacidad técnica y organizativa para la realización de inspecciones STIC, evaluando los requisitos que deben cumplir los sistemas que manejan información clasificada.
- 2) Imparcialidad y ausencia de conflicto de intereses entre la EI-STIC y la entidad titular, responsable o usuaria del sistema de información auditado.

Nota: en esta guía emplearemos el término “inspección” para hacer referencia al conjunto de actuaciones (verificaciones de aspectos técnicos y cumplimiento normativo) asociados a una auditoría, “evaluación” a la revisión de aspectos de cumplimiento normativo y “auditoría” al compendio de inspecciones y actuaciones que permiten obtener un dictamen.

5. PROCEDIMIENTO PARA LA ACREDITACIÓN DE LAS EI-STIC

La figura siguiente muestra de forma simplificada el procedimiento utilizado por el CCN para la acreditación de las EI-STIC, que incluirá la evaluación de la capacidad técnica para la realización de auditorías o inspecciones de seguridad, así como la verificación de la imparcialidad y ausencia de conflicto de intereses.



6. SOLICITUD DE LA ACREDITACIÓN COMO EI-STIC

Las entidades interesadas en obtener la acreditación como EI-STIC, para la realización de inspecciones de seguridad TIC a sistemas que manejan información clasificada, deberán solicitarlo al Centro Criptológico Nacional mediante una

comunicación formal dirigida al Subdirector General del Centro Criptológico Nacional, en la que manifiesten su intención, adelantándola vía correo electrónico a ccn@ccn.cni.es, y adjuntando la documentación que se señala en la presente Guía, así como aquella otra que la candidata a EI-STIC considere conveniente en apoyo a sus pretensiones.

7. REVISIÓN DE LAS CONDICIONES DE LA ACREDITACIÓN

Una vez realizada la evaluación de la capacidad técnica de la entidad solicitante y los requisitos de imparcialidad y ausencia de conflicto de intereses, y encontrándose conforme con tales requisitos, el CCN acreditará a la entidad solicitante como EI-STIC para lo que expedirá el correspondiente Certificado de Acreditación (<https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion>).

8. REQUISITOS GENERALES DE LAS EI-STIC

8.1 COMPETENCIA TÉCNICA

La entidad que desee acreditarse como EI-STIC 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 acreditación la magnitud de los proyectos realizados en tal sentido.

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

- a) Ha realizado proyectos en los que figuren actividades de auditoría de cumplimiento funcional, normativo o técnico de sistemas de información.
- b) Posee certificados de organismos con competencias en auditoría o inspecciones de seguridad de sistemas, en los que consten específicamente los trabajos de auditoría de cumplimiento normativo y técnico realizados.

En ausencia de dicha experiencia por parte de la entidad solicitante de la acreditación, especialmente en aquellas de reciente creación, el CCN podrá considerar en su lugar la experiencia de su personal relevante, como es el Responsable Técnico, el Revisor de Expedientes o los Auditores Jefe.

Asimismo, la experiencia podrá ser sustituida por la competencia técnica y conocimientos necesarios para la realización de inspecciones STIC o, eventualmente, auditorías o inspecciones técnicas de seguridad, para lo que será necesario que la entidad 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 de la entidad solicitante, su encuadramiento orgánico, su estructura prevista de personal y sus capacidades, la metodología seguida o prevista para realizar inspecciones STIC de sistemas que manejan información clasificada y un ejemplo de alguna inspección STIC realizada, al objeto de que el CCN pueda valorar adecuadamente su idoneidad para el propósito perseguido.

La competencia técnica del personal de la entidad 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.

La entidad que pretenda acreditarse como EI-STIC deberá identificar las necesidades de formación del personal y ser capaz de dar respuesta a estos requisitos, debiendo disponer de un plan de capacitación y diseño curricular asociado a cada una de las funciones del Equipo de Inspecciones STIC.

8.2 CONFIDENCIALIDAD, INDEPENDENCIA E IMPARCIALIDAD

La entidad que desee acreditarse como EI-STIC debe asegurarse de que su organización y personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad inspeccionada, de conformidad con lo exigido en la ISO/IEC 17065, evitando conflicto de intereses:

- Entre las actividades de inspección STIC y el resto de las áreas de la Organización en la que esté encuadrada la EI-STIC.
- Entre las actividades de inspección STIC de la EI-STIC y las de la entidad titular, responsable o usuaria del sistema de información inspeccionado que pretende obtener la Declaración de Cumplimiento.

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 de la EI-STIC cuando deberán adoptarse los mecanismos y las cautelas precisas para asegurarse la debida imparcialidad y ausencia de conflicto de intereses entre la EI-STIC y las restantes áreas de la organización u otras entidades titulares, responsables o usuarias del sistema de información inspeccionado, cautelas y circunstancias que se evidenciarán documentalmente y se mantendrán a lo largo del tiempo.

La EI-STIC 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 titular, responsable o usuaria del sistema de información inspeccionado.

En ningún caso los integrantes del Equipo de Inspecciones STIC deben haber participado o detentado responsabilidades previas a la inspección STIC, al menos en los dos (2) últimos años, en el sistema de información inspeccionado, o bien haber sido consultores, para ese sistema, en el proceso de implementación de sus requisitos de seguridad.

Cuando la entidad solicitante de la acreditación para constituirse como EI-STIC disponga de un departamento, área o unidad de consultoría, es preceptivo que contemplen dicha circunstancia en su análisis de riesgos frente a la imparcialidad, al

objeto de segregar las áreas de consultoría de las áreas de inspección o estableciendo mecanismos que salvaguarden la imparcialidad de la EI-STIC.

Todos los integrantes del Equipo de Inspecciones STIC, ya sea personal interno o externo, incluyendo a los auditores jefe, auditores y posibles expertos técnicos, deben suscribir un acuerdo de imparcialidad y ausencia de conflicto de intereses de forma previa a cada una de las Inspecciones STIC en las que participen, documento que se incorporará al expediente. El Responsable Técnico, el Revisor de Expedientes y quién adopte la decisión de proponer la Declaración de Cumplimiento del sistema, deberán suscribir un acuerdo genérico tras su designación en la EI-STIC.

Todos los integrantes del Equipo de Inspecciones STIC, 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 inspecciones STIC, un acuerdo de confidencialidad, que garantice su deber de secreto ante la información a la que tengan acceso, o elaboren, durante las inspecciones STIC. Esto es extensible a todo el personal de la EI-STIC que tenga acceso a la información de las inspecciones STIC.

Asimismo, dada la naturaleza de las inspecciones STIC realizadas a sistemas que manejan información clasificada, todo el personal que tenga acceso a la información de las inspecciones STIC que se realicen **deberá estar en posesión de la Habilitación Personal de Seguridad (HPS) en vigor.**

Finalmente, la EI-STIC solicitante evidenciará en el procedimiento documentado o en la metodología de realización de inspecciones STIC su imparcialidad respecto de los sistemas de información que pretende inspeccionar y la ausencia de conflicto de interés, de la organización y de su personal, con las entidades, organismos, órganos, dependencias o unidades titulares de los sistemas de información inspeccionados.

Para valorar la antedicha imparcialidad, la EI-STIC solicitante dispondrá de una gestión de riesgos frente a la imparcialidad que trate y minimice aquellos riesgos evaluados como inaceptables por denotar evidente conflicto de intereses, ya sea de la propia organización, o de su personal, en relación con los posibles auditados en el ámbito de sus competencias.

8.3 REQUISITOS PROCEDIMENTALES Y METODOLÓGICOS

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

El Equipo de Inspecciones STIC está obligado a requerir y obtener durante las inspecciones STIC 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 Inspección STIC.

9. ESTRUCTURA DE PERSONAL DE LAS EI-STIC

La EI-STIC debe mantener actualizada la información relacionada con su estructura interna, incluyendo su organización, equipos constituidos y listado nominal del personal habilitado para llevar a cabo las precitadas inspecciones STIC.

9.1 PERSONAL RELEVANTE NO AUDITOR

En una EI-STIC, además del personal que participa en las inspecciones, denominado Equipo de Inspecciones STIC (puede haber varios equipos de inspecciones STIC en una misma EI-STIC), debe disponerse de otro personal relevante para la organización, a saber: el 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 la EI-STIC, ésta debe disponer de un Responsable Técnico que se responsabilice de la coordinación técnica del personal que participa en las evaluaciones o inspecciones, 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 de la EI-STIC, 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 conflicto de intereses.

La EI-STIC deberá disponer, asimismo, de un Revisor de Expedientes, cuyas funciones son verificar los diferentes expedientes de auditoría que tramite la EI-STIC antes de la adopción de la decisión final de considerar favorable, o no, la fase de inspección STIC del sistema de información inspeccionado. 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 conflicto de intereses.

Además de lo anterior, deberá determinarse la persona física, órgano colegiado o unidad que tomará la decisión de recomendar al CCN la Declaración de Cumplimiento del sistema de información inspeccionado, pudiendo tratarse del Responsable Técnico, un comité constituido por el Responsable Técnico y el Revisor de Expedientes, etc. siempre y en todo caso, asegurando que quién participe en la toma de la decisión no haya intervenido directamente en la inspección, por ejemplo, como Auditor Jefe.

Por último, la EI-STIC debe tener asignada la función 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.

9.2 PERSONAL DEL EQUIPO DE INSPECCIONES STIC

La EI-STIC podrá disponer de uno o varios equipos de inspecciones STIC, estando todos ellos, desde el punto de vista técnico, bajo la responsabilidad y supervisión del Responsable Técnico designado.

El Responsable Técnico de la EI-STIC podrá asimismo actuar en calidad de jefe de equipo de inspecciones (Auditor Jefe), siempre que reúna los requisitos necesarios, algo frecuente en su constitución inicial, o en aquellas EI-STIC que cuenten con poco personal.

El Equipo de Inspecciones STIC, que puede pertenecer total o parcialmente a la plantilla de la EI-STIC, 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 inspecciones STIC.

El Equipo de Inspecciones STIC, junto a otro personal de la EI-STIC, deberá satisfacer los siguientes requisitos:

- Tanto si el Equipo de Inspecciones STIC es interno como externo, o una combinación de ambos, no deberá presentar conflicto de intereses con la organización titular de los sistemas de información inspeccionados, ni con los sistemas o servicios que sean o puedan ser objeto de la inspección STIC, 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 inspección STIC y de la generación del Informe de Inspección STIC. 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 de Inspecciones STIC.
- Con independencia de la adscripción de los miembros del Equipo de Inspección (auditores internos o externos), la EI-STIC mantendrá la plena responsabilidad de los actos preparatorios y del desarrollo de la fase de inspección STIC, siendo responsable último de la calidad y adecuación del Informe de Auditoría elaborado por el Auditor Jefe, revisado habitualmente por el Responsable Técnico de la EI-STIC previo a su entrega a la entidad titular del sistema de información inspeccionado, quedando a disposición del CCN, a quién se comunicará el comienzo y el fin de la inspección STIC y su resultado.
- El resultado de una auditoría podrá ser FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE.
- En el caso de un dictamen FAVORABLE CON NO CONFORMIDADES, una vez que la entidad inspeccionada hubiere remitido en tiempo y forma el preceptivo Plan de Acciones Correctivas (PAC) será evaluado por el Auditor Jefe, que verificará que se hayan resuelto las desviaciones reflejadas en el Informe de Inspección

inicial, dando como resultado un documento formal con dicho análisis y el dictamen resultado de la evaluación del PAC.

- Seguidamente, todo el expediente será revisado por el Revisor de Expedientes, que se reflejará en un documento formal que, de ser satisfactorio, se comunicará a la persona física, órgano colegiado o unidad encargada de la toma de decisión. La decisión final de la EI-STIC en esta fase únicamente podrá ser FAVORABLE o DESFAVORABLE.
- El Responsable Técnico informará de la decisión finalmente adoptada al CCN por los canales establecidos, junto a las fechas de inicio y final de la inspección STIC, de presentación del PAC, y demás información relevante, al objeto de que el CCN pueda emitir, en su caso, la **Declaración de Cumplimiento**. El expediente lo conservará la EI-STIC a disposición del CCN.

El Equipo de Inspecciones, en el diseño de sus pruebas y revisiones, no debe limitarse a la revisión de documentos, ya que el objetivo de la inspección STIC 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 inspeccionado.

Los componentes del Equipo de Inspecciones deberán tener una capacitación suficiente en inspecciones STIC, auditoría de sistemas de información y en seguridad de la información en general. Si se considerara 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 de Inspecciones STIC deberá evidenciar que:

- Dispone de los conocimientos técnicos necesarios para abordar las diferentes inspecciones STIC de 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 inspeccionar, los servicios que presta, la información que maneja (especialmente la clasificada), así como el objetivo, el alcance y el criterio de la inspección STIC.
- Todos los auditores conocen en la medida de las tareas asignadas, los requisitos de seguridad derivadas de toda la legislación aplicable al sistema de información que se inspecciona, en particular de seguridad de la información como puede ser la relativa a sistemas que manejan información clasificada, al RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que también se aplica a dichos sistemas, etc.
- Se ha llevado a cabo el Plan de Auditoría o, en su caso, las modificaciones al mismo están debidamente fundamentadas y registradas.

9.3 REQUISITOS MÍNIMOS DEL PERSONAL TÉCNICO

Las EI-STIC deben disponer de personal cualificado y suficiente para la realización de inspecciones STIC en todas las fases del proceso auditor: estudio documental previo, inspección STIC in situ (presencial o en remoto), redacción del Informe de Inspección y evaluación del Plan de Acciones Correctivas, en su caso junto a la revisión del expediente completo. 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 de Inspecciones STIC (Auditor Jefe), para cada uno de los equipos de inspecciones STIC que se deseen constituir o, lo que es lo mismo, como inspecciones STIC desee abordar simultáneamente.
- Un número suficiente de auditores para la correcta realización de las inspecciones STIC 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 desempeñar varios 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.
- Definir quién tomará la decisión de recomendar la **Declaración de Cumplimiento** del sistema auditado, que podrá ser una persona física (el Responsable Técnico, por ejemplo), un órgano colegiado o una unidad.

Debe tenerse en cuenta que podría ser el Auditor Jefe el único interviniente en determinadas evaluaciones, en función del tamaño y características del sistema a inspeccionar, siendo éste, conjuntamente con el Responsable Técnico de la EI-STIC, quién previamente al inicio de cada evaluación decidirá si requiere apoyo de otros auditores o no.

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

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 de los sistemas que manejan información clasificada del grado DL y 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 inspección STIC pueda requerir la evaluación de la conformidad de medidas derivadas del cumplimiento de otras normativas en el ámbito de la seguridad de la información, la administración electrónica o la protección de datos.

La capacitación, 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 de Inspecciones STIC (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 inspección STIC de que se trate.

Los miembros del Equipo de Inspecciones STIC deberán estar familiarizados con las Guías de Seguridad CCN-STIC (<https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es>) aplicables a cada caso (como puede ser la CCN-STIC 101 sobre Acreditación de sistemas de las TIC que manejan información clasificada) 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 a la EI-STIC constarán como auditores provisionales en cualificación. Podrán realizar el acompañamiento de cualquier inspección STIC, siempre que se encuentren bajo la supervisión directa del Auditor Jefe o de cualquier otro auditor experimentado.

Debe existir un procedimiento o normativa interna de cualificación de auditores, para elevar su calificación de auditor en formación a auditor cualificado y, en su caso, a Auditor Jefe.

9.4 INCORPORACIÓN DE EXPERTOS TÉCNICOS AL EQUIPO DE INSPECCIONES STIC

En el desarrollo de las actividades de inspección STIC, el Equipo de Inspecciones STIC 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 archivística y conservación a largo plazo;
- Expertos en tecnologías clásicas o en desarrollo (Blockchain, Inteligencia Artificial, Computación Cuántica, etc.);
- y otros que se estimen pertinentes en función del sistema inspeccionado.

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

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

En ningún caso los expertos técnicos deben haber participado o desempeñado responsabilidades en el sistema de información inspeccionado, o haber sido consultores para ese sistema en el proceso de implantación de los requisitos de seguridad, de forma previa a la inspección STIC, o al menos en los dos (2) últimos años.

10. ACUERDOS SUSCRITOS POR LAS EI-STIC CON LOS AUDITADOS

Las EI-STIC suscribirán con la entidad titular del sistema de información a inspeccionar una serie de acuerdos vinculantes para garantizar la efectividad de la inspección STIC, la confidencialidad de la información accedida, etc.

Dichos acuerdos pueden resumirse en uno solo, suscrito entre la EI-STIC y la entidad titular del sistema inspeccionado, siendo el de derechos y obligaciones de quién se certifica.

- Derechos como, por ejemplo, poder recurrir el resultado de la inspección STIC si el auditado no está de acuerdo con ella.
- Deberes como, por ejemplo, no hacer declaraciones engañosas durante la inspección STIC, y permitir que el personal del CCN, organismos o administraciones competentes, asista como observador a la realización de cualquier tipo de inspección STIC efectuada por la EI-STIC en las instalaciones del inspeccionado.
- Dicho acuerdo suele incluir un compromiso de confidencialidad y protección de datos por parte de la EI-STIC.

11. CRITERIOS GENERALES DE INSPECCIÓN STIC

Los Criterios de Inspección STIC, respetarán los siguientes elementos:

CRITERIOS DE INSPECCIÓN STIC	
ALCANCE	Sistemas de información comprendidos en la inspección STIC y la información clasificada tratada por medio de tales sistemas.
RECABAR INFORMACIÓN AL AUDITADO	La EI-STIC dispondrá de un formulario de toma de datos con aquella información necesaria para poder realizar una oferta de servicios de Inspección STIC, para dimensionar los recursos necesarios (de personal y de herramientas), así como para poder realizar el cálculo de tiempo necesario de inspección.
TIEMPOS DE INSPECCIÓN STIC	Se establecerá el número de jornadas de inspección necesarias para la inspección STIC en lo que se refiere al análisis documental previo, la elaboración del Plan de Auditoría, la materialización de la inspección STIC al sistema inspeccionado, la redacción del Informe de Inspección, eventualmente la evaluación del Plan de Acciones Correctivas, la revisión del expediente y la adopción de la Decisión final de considerar la auditoría como FAVORABLE, FAVORABLE CON NO CONFORMIDADES o DESFAVORABLE. Ante la determinación de tiempos de inspección STIC anormales, el Centro Criptológico Nacional, en el ejercicio de sus competencias, podrá examinar las circunstancias argumentadas por la EI-STIC para tal asignación, adoptando las medidas que, en derecho, procedan.
TIEMPOS ADICIONALES	El número de jornadas de inspección STIC 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 acreditación. Factores de decremento • Sistemas de Información muy reducidos o con 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 inspeccionado previamente); • 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 inspección STIC.
PRESENTACIÓN DE LA OFERTA DE SERVICIOS Y CONTRATACIÓN	Deberá aportarse una detallada oferta de servicios, exclusivamente respecto a la inspección STIC, en base a la información recabada de la organización que pretende acreditar su sistema en una fase previa. Dicha oferta será aceptada por el cliente mediante un acuerdo contractual.
CLÁUSULAS DE DERECHOS Y OBLIGACIONES	Deberán suscribirse por ambas partes (organización inspeccionada y EI-STIC) un acuerdo vinculante de derechos y obligaciones de quién pretende acreditar un Sistema.

DESIGNACIÓN EQUIPO DE INSPECCIONES STIC Y PLAN DE AUDITORÍA	Debe designarse el equipo de inspecciones STIC y comunicarse al cliente por si decidiera recusar a alguno de sus miembros por un posible conflicto de intereses que podría invalidar la inspección STIC. Asimismo se presentará un Plan de Auditoría que planifique detalladamente la misma.
DESARROLLO DE LA INSPECCIÓN	• Emplazamientos. • Desviaciones halladas: No Conformidades Mayores, No Conformidades Menores y Observaciones. • Niveles de criticidad encontrados: Sin relevancia, Bajo, Medio, Alto y Crítico. • Verificación del Plan de Acciones Correctivas. El Centro Criptológico Nacional se reserva el derecho de acompañar a las EI-STIC en todas aquellas auditorías que estos realicen.
RESUMEN DE HALLAZGOS DE LA INSPECCIÓN	Las EI-STIC deberán facilitar al CCN el resultado del proceso de inspección incluyendo el número de hallazgos detectados durante la inspección y su localización, favoreciendo la explotación de la información proporcionada a efectos estadísticos. El CCN pondrá a disposición de las EI-STIC soluciones adaptadas a tal efecto (por ejemplo, ANA-SC, CLARA, etc...) en el Portal de Gobernanza (https://gobernanza.ccn-cert.cni.es/).
INSPECCIONES EN REMOTO	La realización de inspecciones en modo remoto deberá <u>considerarse con mucha cautela</u> y siempre que se considere dicha actividad como viable por parte de la EI-STIC (debe tenerse en cuenta que son sistemas que manejan información clasificada) y acorde con los procedimientos de auditoría establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente dichos sistemas y poder justificarlo adecuadamente ante el Centro Criptológico Nacional. Finalmente, será el Equipo de Inspecciones STIC el que determinará si es necesario complementar parte de 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 para la seguridad del propio sistema o para la calidad de la inspección STIC.
PUESTA A DISPOSICIÓN DEL INFORME DE AUDITORÍA O INSPECCIÓN	Entendiendo que los Informes de Inspección podrían contener información o datos clasificados, sensibles, de naturaleza personal, y/o encontrarse protegidos por distintas regulaciones, será el CCN quién autorizará su solicitud por parte de un tercero, debiendo dirigirse ésta y su necesidad a la cuenta de correo electrónico cocens@ccn.cni.es del Centro Criptológico Nacional y no a la EI-STIC que lo ha elaborado. Será el CCN quién valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y a la EI-STIC responsable, ya se trate este de un OAT, de una EC o de cualquier otra organización auditora.

Durante el proceso de acreditación de la EI-STIC y siempre que se hubieren producido cambios, la entidad 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 inspecciones STIC, con el objetivo de verificar y validar el sistema que se empleará para gestionar el proceso de inspección STIC y la metodología empleada por la EI-STIC en las correspondientes auditorías.

La EI-STIC mantendrá permanentemente informado al CCN de las fechas y el personal encargado de llevar a cabo las inspecciones STIC para las que hubieren sido requeridos sus servicios.

12. EL PROCESO DE ACREDITACIÓN DE UNA EI-STIC

12.1 FORMACIÓN PREVIA DEL PERSONAL DE LA EI-STIC

Para que una organización, o una unidad, área, sección o departamento de la misma, sea reconocida como EI-STIC es necesario que su personal relevante asista a uno o varios cursos ‘on-line’ síncronos, algunos específicos para una EI-STIC, impartidos por personal asignado por el CCN.

12.2 DEMOSTRACIÓN DE LA EI-STIC DURANTE LA ACREDITACIÓN DE LA ENTIDAD

Habitualmente, el proceso de dar evidencia por parte de la EI-STIC, con independencia de la documentación facilitada previamente al CCN, tendrá una duración mínima de dos (2) días.

- En el primero de ellos, la EI-STIC 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, la EI-STIC expondrá un caso de inspección STIC (que podrá tratarse de una simulación, si no dispusiere de casos relevantes que pueda mostrar) para presentar mediante un ejercicio práctico la forma en que se afronta o prevé afrontar las inspecciones STIC de sistemas que manejan información clasificada del grado DL, así como los registros que deben irse cumplimentando antes, durante y después de finalizarse la inspección STIC material.

12.3 AUDITORÍAS DE ACOMPAÑAMIENTO

El Centro Criptológico Nacional, dentro del proceso de acreditación de una EI-STIC, 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 de la EI-STIC, asistiendo a un mínimo de dos (2) inspecciones STIC realizadas por el propio CCN, o por otras EI-STIC acreditadas, en calidad de observador.
- Acompañamiento de personal asignado por el CCN al menos a las dos (2) primeras inspecciones STIC realizadas por la EI-STIC en el desempeño real de sus competencias.

Una vez constatado el correcto desenvolvimiento práctico de la EI-STIC en la realización y registro de este tipo de inspecciones en el ámbito de sus competencias, y verificada la idoneidad de su sistema interno de gestión para la realización de inspecciones STIC a sistemas que manejan información clasificada podrá concederse la acreditación a la entidad.

13. OBLIGACIONES ADICIONALES DE LAS EI-STIC

Se deberá mantener una permanente vigilancia respecto de las últimas versiones de las Guías CCN-STIC que resulten aplicables en cada caso.

Se comunicará al CCN cualquier circunstancia que pueda impedir o limitar la calidad de los trabajos de las EI-STIC o la imparcialidad requerida.

14. CONCESIÓN DE LA ACREDITACIÓN

En el caso de que se cumplan los requisitos especificados en el presente documento y en la normativa o Guías CCN-STIC aplicables, incluyendo las cautelas para garantizar la imparcialidad y la ausencia de conflicto de intereses, el CCN reconocerá la capacidad técnica de una Organización, u órgano o unidad de la misma, como EI-STIC acreditada para la realización de inspecciones STIC a sistemas que manejen información clasificada del grado DL.

Pantone:
SOLID COATED
2925C

Web (HTML):
#009ade

RGB:
R: 0
G: 154
B: 222

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

El CCN comunicará a la EI-STIC solicitante la superación del procedimiento de acreditación mediante el Certificado de Acreditación correspondiente.

El CCN emitirá un Certificado de Acreditación en el que se indique que la EI-STIC dispone de la capacidad técnica para la realización de inspecciones STIC a sistemas que manejan información clasificada del grado DL, según se dispone en el presente documento.

Asimismo, el CCN mantendrá en su portal una relación actualizada de las EI-STIC acreditadas (<https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion>).

15. PUBLICIDAD DE LA ACREDITACIÓN

La EI-STIC que disponga de un Certificado de Acreditación vigente podrá dar publicidad, en su portal web o en cualquier otro medio de comunicación, de la acreditación de la que es titular, pudiendo mostrar el siguiente Distintivo de Acreditación.



16. VIGENCIA DE LA ACREDITACIÓN

La acreditación de las EI-STIC para la realización de inspecciones STIC a sistemas que manejan información clasificada del grado DL 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 Certificado de Acreditación.

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

En cualquier momento, durante su vigencia, el CCN podrá retirar a una EI-STIC el Certificado de Acreditación concedido si se confirmara la presencia de circunstancias que no permitan garantizar la satisfacción por parte de la entidad de los requisitos exigidos para su concesión.

El CCN se reservará el derecho de acompañar a las EI-STIC en todas aquellas inspecciones STIC que realicen a sistemas que manejan información clasificada del grado DL.

ANEXO. REVISIÓN DE REQUISITOS PARA EI-STIC

A continuación, pese a no ser una lista exhaustiva, se incluye una plantilla para facilitar a las EI-STIC la revisión del cumplimiento de las condiciones de acreditación, 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 DE LA EI-STIC		
Información actualizada de la estructura interna de la EI-STIC (incardinamiento orgánico, estructura organizativa, equipos y listado de personal habilitado para llevar a cabo inspecciones STIC como fase dentro de la acreditación de un sistema).	☐	
Personal cualificado para la realización de inspecciones STIC.	☐	
Un (1) Responsable Técnico de la EI-STIC	☐	
Al menos un (1) Jefe del Equipo de Inspecciones (Auditor Jefe), que inicialmente podría ser el Responsable Técnico si cumple los requisitos.	☐	
Número suficiente de auditores para la realización de las inspecciones STIC a las que se comprometa la EI-STIC.	☐	
Un (1) revisor de expedientes, función que podría ser compartida entre al menos dos (2) Auditores Jefe, sin que pueda revisarse un expediente en el que se haya intervenido.	☐	
Dispone de un Plan de Formación/Capacitación y diseño curricular asociado a cada uno de los desempeños relacionados con el proceso de inspecciones STIC (en especial el Equipo de Inspecciones STIC, el Responsable Técnico y el Revisor de Expedientes).	☐	
CONFIDENCIALIDAD, INDEPENDENCIA, IMPARCIALIDAD		
La EI-STIC 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 conflicto de intereses).	☐	
La EC que sea EI-STIC debe estar en posesión de la Habilitación de Seguridad de Empresa (HSEM) en vigor.	☐	
La EI-STIC 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 de Inspecciones STIC deben haber participado, detentado responsabilidades previas a la inspección STIC, o bien haber sido consultores en el proceso de implantación de los requisitos de seguridad del sistema, al menos en los dos (2) últimos años, en el sistema de información inspeccionado.	☐	
Todos los integrantes del Equipo de Inspecciones STIC, sean estos externos o internos, incluyendo a los posibles expertos técnicos, deberán haber firmado un acuerdo de confidencialidad antes de participar en las inspecciones STIC que lleve a cabo la EI-STIC. Esto es extensible al Responsable Técnico, Revisor de Expedientes y Auditor Interno.	☐	
Todo el personal de la EI-STIC que tiene acceso a información de las inspecciones STIC debe estar en posesión de la Habilitación Personal de Seguridad (HPS) en vigor.	☐	
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 conocimiento de los requisitos de los sistemas que manejan información clasificada del grado DL y 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.	☐	
Los demás miembros del Equipo de Inspecciones STIC (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 de Inspecciones STIC deberán estar familiarizados con las Guías	☐	

de Seguridad CCN-STIC aplicables a cada caso, como puede ser la CCN-STIC 101.		
PROCEDIMIENTOS Y METODOLOGÍA		
Dispone de una metodología para el desarrollo de las inspecciones STIC acorde con la norma ISO/IEC 17065:2012 o versiones posteriores.	☐	
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 las evaluaciones, tanto en lo que se refiere al análisis documental previo, como a las inspecciones presenciales y demás actuaciones relacionadas como son la elaboración de los preceptivos informes.	☐	
- Que los tiempos de inspección STIC se modulen atendiendo a factores o elementos que puedan incrementar o disminuir el esfuerzo requerido.	☐	
- Que tiempos considerados irrazonables a todas luces para las inspecciones STIC 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 aun estando distribuido en distintos emplazamientos.	☐	
- Resumen de los hallazgos de auditoría. La EI-STIC deberá disponer de un modelo de Informe de Inspección 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 evaluación extraordinaria.	☐	
- La elaboración de un Informe de Inspección con los resultados de la inspección STIC, que será remitido al CCN, además de a la Organización cuyo sistema de información ha sido evaluado, conteniendo: • La fecha y duración. • El alcance. • El grado máximo de información clasificada manejada.	☐	

• 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 ACREDITACIÓN		
Ha hecho llegar al CCN los documentos relevantes (normas internas y procedimientos) constituyentes del sistema de gestión de la EI-STIC.	☐	
Ha impartido, o va a impartir, una sesión de acreditación de la entidad en la que se detalle el sistema de gestión de la EI-STIC y la metodología desarrollada para el proceso de realizar inspecciones STIC a un equipo de expertos del CCN.	☐	
Proporcionar al CCN cuanta información se solicite para verificar y validar el sistema de gestión de la EI-STIC y la metodología empleada.	☐	
Ha participado, o pretende participar, el personal de la EI-STIC en auditorías de acompañamiento, mínimo dos (2), invitado por el CCN como observador en aquellas que realice directamente o que realice otra EI-STIC acreditada.	☐	
Ha invitado a participar al CCN como observador, al menos en las dos (2) primeras inspecciones STIC que realice la EI-STIC como fase dentro del proceso de acreditación de un sistema que maneja información clasificada.	☐	

