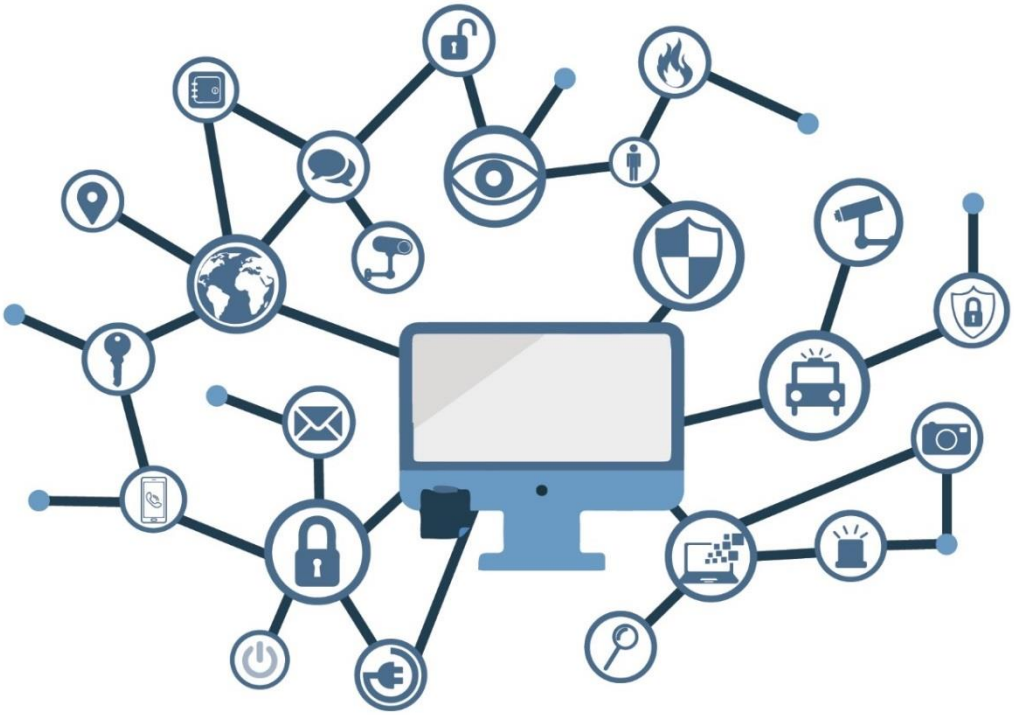
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

# PROCEDIMIENTO DE SEGURIDAD DE LAS TIC
# CCN-STIC-120

## PROCEDIMIENTO DE ACREDITACIÓN DE ENTIDADES AUDITORAS PARA VERIFICAR REQUISITOS STIC EN SISTEMAS DIFUSIÓN LIMITADA



Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.10.15 18:36:25 +02'00'



**NIPO: 083-19-003-X**

Fecha de Edición: septiembre de 2018

**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**

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE

# 1. INTRODUCCIÓN

1. La información clasificada manejada en un sistema debe protegerse contra la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, sea accidental o intencionada, y debe impedirse la pérdida de integridad y disponibilidad de los propios sistemas que manejan dicha información.

2. Al objeto de conseguir una protección de seguridad adecuada, la Política de Seguridad de las TIC (CCN-STIC-001), establecida como desarrollo de la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN), recoge la necesidad de la acreditación de los sistemas que manejan información clasificada.

3. La guía CCN-STIC-101 "Acreditación de sistemas de las TIC que manejan información clasificada" indica que los sistemas a acreditar para manejar información clasificada con el grado de DIFUSIÓN LIMITADA o equivalente deberán seguir el siguiente procedimiento específico.


**Figura 1.- Procedimiento de acreditación para DIFUSIÓN LIMITADA o equivalente**

4. La identificación de la entidad auditora de seguridad constituye el primer paso en el procedimiento de acreditación para sistemas que manejan información clasificada con el grado de DIFUSIÓN LIMITADA. A efectos de lo establecido en la guía CCN-STIC-101, es responsabilidad de la Autoridad Operativa del Sistema de las Tecnologías de la Información y la Comunicación (AOSTIC) determinar la entidad auditora, en base a los siguientes supuestos:

   a) Entidades de Certificación del Esquema Nacional de Seguridad (ENS) acreditadas por la Entidad Nacional de Acreditación (ENAC) conforme a la norma UNE-EN ISO/IEC 17065:2012 que, además, dispongan de Habilitación de Seguridad de la Empresa (HSEM) en vigor.
   b) Entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas, cuyas competencias incluyan el desarrollo de

auditorías de sistemas de información a terceros, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

c) Excepcionalmente, entre aquellas entidades acreditadas por el Centro Criptológico Nacional (CCN) que hayan demostrado la capacidad técnica suficiente para llevar a cabo inspecciones de seguridad de las TIC sobre sistemas que manejan información clasificada.

## 2. OBJETO

5. El presente documento tiene por objeto definir el procedimiento utilizado por el Centro Criptológico Nacional para la acreditación de la capacidad técnica de entidades auditoras para la verificación del cumplimiento de requisitos de seguridad de las TIC (STIC) dentro del proceso de acreditación de sistemas que manejen información clasificada hasta el grado de DIFUSIÓN LIMITADA o equivalente.

6. Así, las entidades acreditadas por el CCN darían cumplimiento a lo indicado en la guía CCN-STIC-101, pudiendo ser escogidas por la AOSTIC para la realización de una auditoría/inspección STIC.

## 3. ALCANCE

7. Este Procedimiento establece un marco de referencia para la acreditación de aquellas entidades, incluidas en el párrafo 4, epígrafe c) de este documento, que quieran llevar a cabo inspecciones de seguridad de las TIC sobre sistemas que manejan información clasificada hasta el grado de DIFUSIÓN LIMITADA o equivalente dentro del proceso de acreditación establecido, y, por tanto, es de obligado cumplimiento para la obtención de dicha acreditación.

## 4. RESPONSABILIDADES

8. La acreditación de los sistemas de la Administración 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 al Secretario de Estado Director del Centro Nacional de Inteligencia.

9. Las entidades que opten a la acreditación para llevar a cabo inspecciones STIC en sistemas que manejan información clasificada hasta el grado de DIFUSIÓN LIMITADA o equivalente deberán garantizar las condiciones de acreditación establecidas en el presente procedimiento, apartado 5.3 de Requisitos de las Entidades Auditoras.

## 5. PROCEDIMIENTO DE ACREDITACIÓN

10. En la siguiente figura puede observarse una representación gráfica del procedimiento de acreditación de entidades auditoras para llevar a cabo inspecciones STIC en sistemas clasificados hasta el grado de DIFUSIÓN LIMITADA o equivalente.

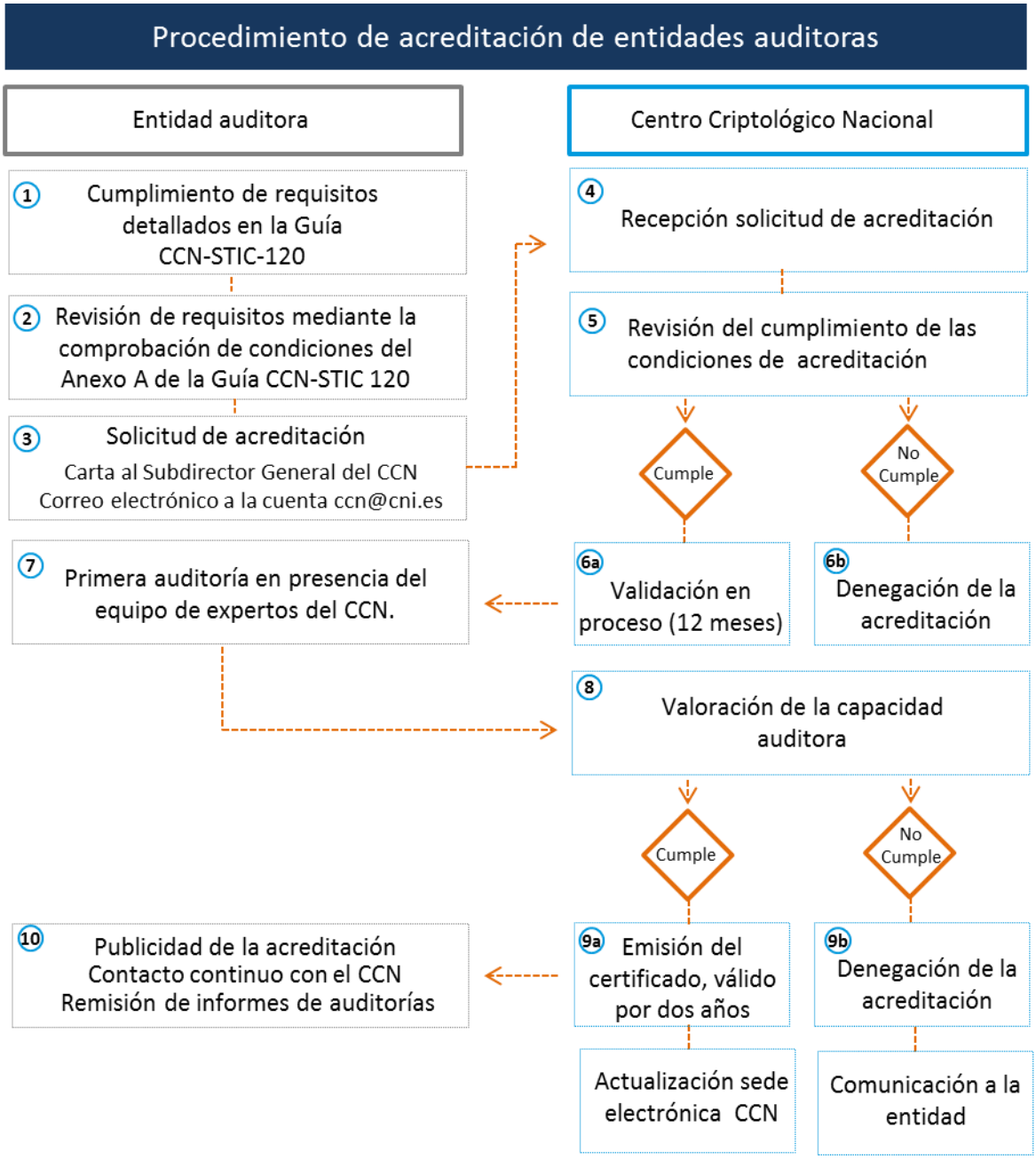



**Figura 2.- Procedimiento de acreditación de entidades auditoras**

## 5.1 SOLICITUD DE LA ACREDITACIÓN

11. Las entidades interesadas en obtener la acreditación para la realización de inspecciones STIC sobre sistemas clasificados hasta el grado de DIFUSIÓN LIMITADA o equivalente, deberán solicitarlo al CCN a través de una carta dirigida al Subdirector General del Centro Criptológico Nacional en la que manifiesten su intención.

12. La solicitud deberá ser adelantada por correo electrónico a la cuenta ccn@cni.es.

## 5.2 REVISIÓN DE LAS CONDICIONES DE ACREDITACIÓN

13. El Centro Criptológico Nacional acreditará la capacidad técnica de una entidad auditora para la realización de inspecciones STIC sobre sistemas clasificados hasta el grado de DIFUSIÓN LIMITADA o equivalente, siempre que se cumplan los requisitos especificados en este documento.

## 5.3 REQUISITOS DE LAS ENTIDADES AUDITORAS

14. En la Tabla 1, del Anexo A, de este Procedimiento se incluye una plantilla para la revisión de los requisitos que deben cumplir las entidades auditoras para obtener la acreditación.

### 5.3.1 Competencia técnica

15. La entidad auditora tiene que tener una experiencia demostrable de, al menos tres (3) años, en la realización de inspecciones STIC. Asimismo, se valorará el importe de los contratos y horas-consultor dedicados a esta actividad.

16. Dicha experiencia deberá estar refrendada por, al menos, una de las siguientes opciones:

    a) Contratos en los que figuren trabajos de auditoría de cumplimiento normativo y técnica.
    b) Certificados de organismos con competencias en acreditación de sistemas que manejan información clasificada, en los que consten específicamente los trabajos de auditoría de cumplimiento normativo y técnica.

### 5.3.2 Estructura de la entidad auditora

17. La entidad auditora ha de mantener actualizada la información relacionada con su estructura interna, que incluya organización, equipos y listado nominal del personal habilitado para llevar a cabo inspecciones de seguridad de las TIC.

18. La entidad auditora debe disponer de personal cualificado (Auditores Jefe y Auditores) para la realización de inspecciones de seguridad de las TIC. En concreto, se exigirá disponer de:

    - Al menos, un (1) Jefe de equipo de inspecciones STIC (Auditor Jefe).
    - Al menos, tres (3) auditores y, en todo caso, número suficiente de auditores para la realización de las inspecciones STIC aceptadas contractualmente.

19. La entidad auditora 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.

### 5.3.3 Confidencialidad, independencia e imparcialidad

20. La entidad auditora debe disponer de Habilitación de Seguridad de Empresa (HSEM) en vigor para el grado de clasificación CONFIDENCIAL, NATO CONFIDENTIAL, UE CONFIDENTIAL y ESA CONFIDENTIAL.
21. Todo el personal que conforma los equipos de inspección ha de disponer de Habilitaciones Personales de Seguridad (HPS) para manejar información clasificada, al menos, hasta el grado de CONFIDENCIAL o equivalente.
22. 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. Por ejemplo, ningún empleado o accionista de la entidad auditora ni sus familiares poseen ninguna relación laboral o de capital (accionista) con la entidad auditada.
23. En ningún caso, el personal auditor debe 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 consultor para el mismo.

### 5.3.4 Requisitos del personal

24. Los Jefes de Equipo de auditoría (Auditores Jefe) deberán contar con experiencia demostrable de, al menos, cinco (5) años en la realización de inspecciones STIC.
25. El personal auditor (Auditores) dispondrá de experiencia demostrable de, al menos, dos (2) años en la en la realización de inspecciones STIC.
26. Se valorará positivamente disponer de certificaciones profesionales en materia de auditoría, seguridad, gobierno y/o gestión de riesgos TIC proporcionadas por organismos académicos o entidades de reconocido prestigio.
27. Los auditores deberán estar familiarizados con el procedimiento de acreditación de sistemas clasificados, las guías de seguridad CCN-STIC y disponer de conocimientos y experiencia en la administración de seguridad de sistemas operativos y aplicaciones, así como de redes informáticas y mecanismos criptográficos.

### 5.3.5 Requisitos procedimentales y metodológicos

28. La entidad auditora debe disponer de una metodología de inspección de sistemas que manejan información clasificada, que cumpla con lo establecido en la norma CCN-STIC-303 sobre inspecciones STIC.
29. La entidad auditora estará obligada a impartir una formación, mínimo diez (10) horas, en la que se explique y detalle la metodología desarrollada por la entidad a un equipo de expertos del CCN, así como cualquier otro aspecto sobre auditorías e inspecciones de seguridad de las TIC que se considere oportuno.
30. La entidad auditora deberá proporcionar al CCN cuanta información se solicite para verificar y validar la metodología empleada por la entidad en las inspecciones STIC.

31. En este sentido, se exige que en la metodología utilizada por la entidad auditora se incluyan los requisitos que se recogen en el Anexo A de este procedimiento.

#### 5.3.5.1 Criterios generales en el proceso de inspección

32. La entidad auditora 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.

33. Se determinarán adecuadamente los tiempos necesarios para realizar las inspecciones STIC, tanto en lo que se refiere al análisis documental previo como a la inspección presencial en el sistema auditado. Para ello:

    - Los tiempos de inspección deben adaptarse atendiendo a factores o elementos que puedan incrementar o disminuir el esfuerzo requerido (complejidad del sistema de información, diversidad tecnológica, extensión, número de servicios comprendidos en el alcance de inspección, número de personas o usuarios directamente vinculados con el sistema de información, etc.)
    - Cuando la inspección se realice sobre un sistema de información que pueda encontrarse distribuido o replicado en distintos emplazamientos, podrá realizarse un muestreo suficiente que aporte evidencias razonables de que el sistema se comporta de la misma manera en todas las instalaciones.
    - Ante la asignación de tiempos de inspección anormales, el CCN, en el ejercicio de sus competencias, podrá examinar las circunstancias argumentadas por la entidad auditora para tal asignación.

34. La entidad auditora calificará la criticidad de las desviaciones halladas en las inspecciones STIC proponiendo si, a pesar de las mismas, los niveles de seguridad son adecuados para la concesión de una Autorización Provisional de Seguridad (APS) o una Acreditación de Seguridad (AS).

#### 5.3.5.2 Informes de inspección

35. La entidad auditora elaborará un informe con los resultados de la inspección STIC que será remitido al Centro Criptológico Nacional.

36. El informe contendrá, al menos, lo siguiente:

    - La fecha y duración.
    - El alcance, indicando los sistemas inspeccionados.
    - Las referencias a los documentos de seguridad que han sido analizados.
    - Las herramientas utilizadas y los resultados de las correspondientes ejecuciones.
    - Las deficiencias encontradas junto con las evidencias pertinentes.
    - La información asociada al muestreo realizado, si se ha realizado.
    - La criticidad de las deficiencias.
    - Las medidas correctoras asociadas a las deficiencias identificadas para facilitar su subsanación.
    - El resultado de la inspección STIC.

- Las conclusiones y recomendaciones.
- Cualquier otro aspecto considerado de interés por la entidad auditora.

## 5.4 CONCESIÓN DE LA ACREDITACIÓN

37. En el caso de que se cumplan los requisitos especificados, el CCN acreditará la capacidad técnica de una entidad auditora para la realización de inspecciones STIC sobre sistemas clasificados hasta el grado de DIFUSIÓN LIMITADA o equivalente.

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

39. El CCN comunicará a la entidad peticionaria la superación del procedimiento de acreditación de entidades auditoras, o en su defecto la denegación de la acreditación, mediante carta firmada por el Subdirector General del Centro Criptológico Nacional, adelantándose por vía electrónica.

40. El CCN emitirá un certificado de acreditación en el que se indique que la entidad dispone de la capacidad técnica para la realización de inspecciones STIC.

centro criptológico nacional

CERTIFICADO DE CONFORMIDAD

Madrid, a 15 de octubre de 2018

El Centro Criptológico Nacional certifica que, en cumplimiento de lo dispuesto en la Guía CCN-STIC-120 'Procedimiento de acreditación de entidades auditoras para verificar requisitos STIC en sistemas DIFUSIÓN LIMITADA', la entidad

<<xx>>

sito en C/xxx, nº xxxxx

dispone de la capacidad técnica para la verificación del cumplimiento de los requisitos STIC de sistemas que manejen información clasificada hasta el grado de DIFUSIÓN LIMITADA.

Fecha de acreditación de conformidad inicial: xx/xx/2018
Fecha de renovación de la acreditación: xx/xx/2020

Subdirector General del Centro Criptológico Nacional

<<Firma>>

Luis Jiménez

Hoja 1 de 1

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%

**Figura 3.- Certificado de Conformidad**

41. Así mismo, el CCN mantendrá en su sede electrónica una relación actualizada de las entidades acreditadas o en vías de acreditación.

## 5.5 RESPONSABILIDADES DE LA ENTIDAD AUDITORA ACREDITADA

42. Una vez obtenida la acreditación, la entidad auditora debe mantener un conocimiento y análisis permanente de las guías CCN-STIC que resulten aplicables en cada momento. En concreto, de la guía CCN-STIC-301 Requisitos STIC y resto de guías que resulten de aplicación de la anterior.

43. La entidad auditora deberá comunicar al Centro Criptológico Nacional cualquier cambio en la organización, su estructura, variaciones de los equipos de inspección STIC, altas y bajas de personal, promociones, etc. durante el período de vigencia de la acreditación.

## 5.6 PUBLICIDAD DE LAS ACREDITACIONES

44. La entidad acreditada por el CCN para la realización de inspecciones STIC de sistemas que manejen información clasificada del grado DIFUSIÓN LIMITADA o equivalente podrá anunciar en su portal web o en cualquier otro medio de comunicación la acreditación de la que es titular, pudiendo mostrar el siguiente Distintivo de Acreditación:


**Figura 4.- Distintivo de acreditación**

## 5.7 VIGENCIA DE LA ACREDITACIÓN

45. La acreditación de entidades para llevar a cabo inspecciones STIC de sistemas que manejen información clasificada hasta el grado de DIFUSIÓN LIMITADA o equivalente tendrá una validez de dos (2) años, renovable por la misma duración si se mantienen las condiciones que permitieron la emisión de la primera acreditación.

46. Con dicha periodicidad, el CCN realizará las mismas comprobaciones que dieron lugar a la acreditación inicial y procederá con la renovación de la acreditación y entrega del nuevo certificado.

47. El CCN podrá retirar el certificado de acreditación de conformidad en cualquier momento, sin necesidad de que la entidad auditora haya completado la vigencia de la acreditación.

48. El CCN se reservará el derecho de acompañar a las entidades auditoras en todas aquellas inspecciones STIC que estas realicen.

## 6. GLOSARIO

| | |
|---|---|
| AOSTIC | Autoridad Operativa del Sistema de las Tecnologías de la Información |
| APS | Autorización Provisional de Seguridad |
| AS | Acreditación de Seguridad |
| CCN | Centro Criptológico Nacional |
| ESA | European Space Agency |
| HSEM | Habilitación de Seguridad de Empresa |
| HPS | Habilitación Personal de Seguridad |
| OTAN | Organización del Tratado del Atlántico Norte |
| STIC | Seguridad de las Tecnologías de la Información y la Comunicación |
| TIC | Tecnologías de la Información y la Comunicación |
| UE | Unión Europea |

## ANEXO A. REVISIÓN DE REQUISITOS PARA ENTIDADES AUDITORAS

A continuación, se incluye una plantilla para facilitar a las entidades auditoras 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 acreditación de sistemas, refrendada por contratos o certificados de organismos competentes en la materia. | ☐ | |
| **ESTRUCTURA DE ENTIDAD AUDITORA** | | |
| Información actualizada de la estructura interna de la entidad (organización, equipos y listado de personal habilitado). | ☐ | |
| Personal cualificado para la realización de inspecciones STIC. | ☐ | |
| Uno (1) o más Jefes de equipo. | ☐ | |
| Tres (3) o más auditores. | ☐ | |
| 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 dispone de Habilitación de Seguridad de Empresa (HSEM) en vigor para el grado de clasificación CONFIDENCIAL, NATO CONFIDENTIAL, UE CONFIDENTIAL y ESA CONFIDENTIAL. | ☐ | |
| Todo el personal de los equipos de inspección dispone de HPS para manejar información clasificada hasta el grado de CONFIDENCIAL o equivalente. | ☐ | |
| El personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad auditada. | ☐ | |
| En ningún caso, el personal auditor ha participado o desempeñado responsabilidades previas a la auditoría, al menos, en los dos (2) últimos años en el sistema de información auditado o bien ha sido consultor para ese Sistema. | ☐ | |

| | | |
|---|---|---|
| **PERSONAL** | | |
| Los jefes de equipo de auditoría cuentan con experiencia demostrable de al menos cinco (5) años. | ☐ | |
| El personal auditor dispone de experiencia demostrable de al menos dos (2) años. | ☐ | |
| Dispone de certificaciones profesionales en materia de auditoría, seguridad, gobierno y/o gestión de riesgos TIC. | ☐ | |
| El personal auditor está familiarizado con los procedimientos de acreditación de sistemas clasificados, las guías de seguridad CCN-STIC y dispone de experiencia en la administración de seguridad de sistemas operativos y aplicaciones, así como redes informáticas y mecanismos criptográficos. | ☐ | |
| **PROCEDIMIENTOS Y METODOLOGÍA** | | |
| Dispone de una metodología de inspección STIC que cumple con lo establecido 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 la inspección presencial. | ☐ | |
| - 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. | ☐ | |
| - La criticidad de las desviaciones halladas en las inspecciones y la consecuente propuesta de concesión de Autorización | ☐ | |

| | | |
|---|---|---|
| Provisional de Seguridad (APS) o Acreditación de Seguridad (AS). | | |
| - La elaboración de un informe con los resultados de la inspección STIC que será remitido al CCN, conteniendo:<br>○ La fecha y duración.<br>○ El alcance.<br>○ La documentación analizada.<br>○ Las herramientas utilizadas y los resultados correspondientes.<br>○ Las deficiencias encontradas junto con las evidencias.<br>○ La información asociada al muestreo realizado.<br>○ La criticidad de las deficiencias.<br>○ Las medidas correctoras asociadas a las deficiencias identificadas.<br>○ El resultado de la inspección STIC.<br>○ Las conclusiones y recomendaciones.<br>○ Cualquier otro aspecto considerado de interés. | □ | |
| 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. | □ | |