GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad CCN-STIC
CCN-CERT IC-01/19

ENS: Criterios adicionales de Auditoría y Certificación

Junio 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

Fecha de Edición: julio de 2019

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. 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, 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, y en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
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 la antedicha 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 entidad del Sector Público. En el caso de operadores críticos de este sector, la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. OBJETO

5. El objeto del presente documento es señalar unos criterios adicionales para la Auditoría y Certificación de los sistemas de información del ámbito de aplicación del ENS, especialmente dirigidos a las Entidades de Certificación del ENS, de conformidad con lo señalado 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 complementando lo señalado en las Guías CCN-STIC que resulten de aplicación, de las que forma parte el presente documento.
6. Esta guía se publica bajo la taxonomía de informe CCN-CERT IC, que comprende los informes elaborados por el Consejo de Certificación del ENS (CoCENS) en cumplimiento de lo dispuesto en la guía *CCN-STIC 809 Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento*, en la que se establece que corresponde a este Consejo "Proponer para su análisis y, en su caso, redactar y publicar normas, criterios o buenas prácticas en materia de certificación de la Conformidad con el ENS".

3. CRITERIOS GENERALES

7. Las Entidades de Certificación del ENS deben ser conscientes de que las Auditorías de Conformidad con el ENS y la expresión de tal conformidad, a través de las correspondientes Certificaciones, guardan relación directa con la garantía de seguridad de los sistemas de información de las entidades públicas y de las organizaciones del sector privado prestadoras de servicios sujetos al cumplimiento del ENS, en los servicios que ofrecen a los ciudadanos y, en consecuencia, en el aseguramiento del ejercicio de los derechos y libertades que la Constitución Española proclama.
8. Para ello, las Entidades de Certificación del ENS actuarán siempre con la mayor profesionalidad y rigor, garantizando la calidad y los resultados de las auditorías y la generación de los certificados a que haya lugar.
9. Así pues, entre otras previsiones, las Entidades de Certificación del ENS deberán atender a las cautelas y recomendaciones señaladas en los siguientes epígrafes.

3.1 EN RELACIÓN CON EL ALCANCE DE AUDITORÍA

10. Definir con precisión el alcance de la auditoría, mediante la adecuada determinación de los sistemas de información comprendidos en la misma y los servicios prestados por medio de tales sistemas.
11. Tanto unos (los sistemas de información) como los otros (los servicios sustentados en tales sistemas) deberán aparecer explícitamente mencionados en el Certificado de Conformidad con el ENS que, en su caso, se expida.

3.2 EN RELACIÓN CON LA COMPETENCIA TÉCNICA DE LA ENTIDAD DE CERTIFICACIÓN

12. La Entidad de Certificación ha de tener una experiencia demostrable de, al menos, tres (3) años, en la realización de auditorías relacionadas con la seguridad de la información, tomándose en consideración el importe de los contratos y las horas de auditor dedicados a esta actividad.

3.3 EN RELACIÓN CON LOS RECURSOS DE LA ENTIDAD DE CERTIFICACIÓN

13. La Entidad de Certificación ha de mantener actualizada y a disposición del Centro Criptológico Nacional información 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.
14. Las Entidades de Certificación disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación del ENS, conforme lo dispone la ITS de Auditoría de Seguridad, 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).
- Tres (3) auditores y, en todo caso, número suficiente de auditores para la realización de las auditorías aceptadas contractualmente.

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

3.4 EN RELACIÓN CON LOS REQUISITOS DE PERSONAL

16. El equipo auditor deberá estar dirigido y tutelado siempre por un Jefe de Equipo de auditoría (Auditor Jefe), cuyas funciones principales son la supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos y recomendaciones mencionados en el informe, así como preservar las evidencias de la auditoría.
17. Los Auditores Jefe, responsables de gestionar las actividades de auditoría, deberán contar con una experiencia demostrable de, al menos, cuatro (4) años en la realización de auditorías.
18. El resto del equipo puede no cumplir con los requisitos 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.
19. A efectos de demostrar la adecuada capacidad técnica, 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.
20. Asimismo, los miembros del equipo auditor deberán estar familiarizados con 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.
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.

3.5 EN RELACIÓN CON LA IMPARCIALIDAD E INDEPENDENCIA

22. La Entidad de Certificación debe asegurarse de que su organización y personal involucrado mantiene las preceptivas condiciones de imparcialidad e independencia respecto de la entidad auditada, de conformidad con lo exigido en la ITS de Auditoría y en la ITS de Conformidad con el ENS.

3.6 EN RELACIÓN CON EL TIEMPO DE AUDITORÍA

23. La Entidad de Certificación debe determinar adecuadamente los tiempos necesarios para realizar las Auditorías de Conformidad con el ENS, en sus diferentes fases: estudio documental previo, auditoría in situ y redacción del Informe de Auditoría.

24. Los tiempos de auditoría 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 la auditoría, número de personas o usuarios directamente vinculados con el sistema de información, etc.).

Factores de INCREMENTO	Factores de DECREMENTO
- Significativo número de personas con privilegios de administración; - Logística complicada, involucrando más de una dependencia o ubicación; - 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 requieren visitar sitios temporales para confirmar las actividades de los sitios permanentes cuyo sistema de gestión está sujeto a certificación.	- Servicios con nulo o escaso riesgo; - Servicios de escasa complejidad; - Elevado número de personas que, bajo el mismo control organizacional, desarrollan las mismas tareas; - Conocimiento previo de la organización y del sistema auditado. (Por ejemplo, si el sistema ya ha sido certificado previamente contra el ENS); - Alta preparación del cliente para la certificación (por ejemplo, ya certificado o reconocido por otro esquema de terceros, en materia de seguridad de la información, tal como ISO 27001, por ejemplo); - Alta madurez del sistema de gestión de seguridad de la información.

25. El número de jornadas de auditor tendrá en cuenta la categoría del sistema de información auditado (Básica, Media o Alta), 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%)

26. Sin que ello deba entenderse como una imposición, la experiencia ha evidenciado que unos tiempos de auditoría razonables deberían atender al siguiente criterio:

Fase de estudio documental previo	Entre 0,5 y 1 jornada.
Fase de auditoría presencial	Categoría BÁSICA: mínimo 1 jornada, en todos los casos. Categoría MEDIA: mínimo 2 jornadas, en todos los

	casos. Categoría ALTA: mínimo 3 jornadas, en todos los casos.
Fase de redacción de informes	Mínimo: una jornada adicional, que deberá comprender la redacción de un Informe de Auditoría completo y adecuadamente evidenciado (señalando cada medida auditada), revisión detallada del Plan de Acciones Correctivas (PAC), revisión de la documentación y decisión del Comité de Certificación.

27. 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 de Certificación para tal asignación, adoptando las medidas que, en derecho, procedan.

3.7 EN RELACIÓN CON EL DESARROLLO DE LA AUDITORÍA, LA CALIFICACIÓN DE LAS DESVIACIONES HALLADAS, EL INFORME DE AUDITORÍA Y EL PLAN DE ACCIONES CORRECTIVAS

28. Cuando la auditoría 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.

29. Existiendo normativa específica sobre protección de datos (RGPD y Ley Orgánica 3/2018), la auditoría del ENS no entrará a evaluar en detalle la conformidad de los sistemas auditados sobre tales materias, más allá de la comprobación de la existencia de exigencias de carácter general y básico, tales como la designación, en su caso, de Delegado de Protección de Datos, existencia del Registro de Actividades de Tratamiento, etc.

30. Es imperativo calificar adecuadamente, de conformidad con lo señalado en la ITS de Auditoría, las desviaciones halladas en las auditorías, distinguiendo entre No Conformidades Mayores, No Conformidades Menores y Observaciones. Adicionalmente, el Informe de Auditoría podrá contener Oportunidades de mejora que, a juicio del auditor, aporten valor a la auditoría y puedan contribuir a la mejora del sistema de gestión de seguridad de los sistemas de información concernidos.

31. Sin perjuicio de lo dispuesto en la ITS de Auditoría, la calificación de las desviaciones halladas se realizará atendiendo a los siguientes criterios:

    Se considera la existencia de una No Conformidad Mayor:

    - Ante el incumplimiento total de un artículo del RD 3/2010 y/o el incumplimiento total de un conjunto de medidas/controles

pertenecientes a un dominio del ANEXO II en función de la categorización del sistema.

- Cuando existen incumplimientos de carácter legal relacionados con la seguridad de la información.
- Cuando la desviación afecta a la capacidad del sistema de información para atender sus funciones esenciales; cuando exista una duda significativa de que se haya implementado un control eficaz de proceso, o de que las medidas de seguridad cumplan los requisitos especificados, o la existencia de un número significativo de no conformidades menores asociadas al mismo requisito.

Se considera la existencia de una No Conformidad menor:

- Ante el incumplimiento parcial de algún artículo del RD 3/2010 y/o el incumplimiento parcial de alguna medida/control (o algún requisito de alguna medida/control) del ANEXO II en función de la categorización del sistema.
- Cuando no afecta a la capacidad del sistema de protección para lograr los resultados previstos; pero, o bien los requisitos se cumplen de forma manifiestamente mejorable, o se aprecian incoherencias entre requisitos que deberían estar alineados.

32. El Informe de Auditoría no deberá limitarse a evidenciar las posibles desviaciones encontradas, sino que, además, deberá evidenciar la conformidad de las medidas de seguridad encontradas conformes, de modo que no se tengan dudas sobre el trabajo del auditor y, en su consecuencia, sobre la evaluación hecha y sobre la valoración de las evidencias analizadas.
33. Respecto del Plan de Acciones Correctivas, es necesario verificar que las No Conformidades se han corregido. En caso de que la entidad auditada precise de un tiempo para la implantación de unas acciones correctivas que ataquen a la causa del problema, deberán demostrar que se han establecido acciones de remedio para el problema detectado y que el Plan de Acciones Correctivas contiene una planificación concreta de acciones precisas que, en el tiempo adecuado, traten y resuelvan las causas de las desviaciones halladas.
34. El Centro Criptológico Nacional se reservará el derecho de acompañar a las Entidades de Certificación en todas aquellas auditorías que estas realicen.

3.8 EN RELACIÓN CON LA UTILIZACIÓN DE SERVICIOS COMPARTIDOS

35. 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).

36. De no ser posible lo anterior, y cuando se trate de la utilización de Servicios Compartidos suministrados por la AGE o, en su caso, por las Administraciones Territoriales competentes, el alcance de la Certificación de Conformidad (y la subsiguiente Certificación de Conformidad) habrá de señalar la parte que ha sido auditada, mencionando, expresamente, que la porción no auditada (ACCEDA o GEISER, por ejemplo) no se encuentra comprendida en tal alcance.

37. No obstante, cuanto tales servicios compartidos logren la Certificación de Conformidad, la Entidad de Certificación podrá generar un nuevo Certificado de Conformidad, eliminando la precisión anterior.

3.9 EN RELACIÓN CON LA CERTIFICACIÓN DE SISTEMAS DE INFORMACIÓN

38. El Centro Criptológico Nacional ha analizado la adecuación y certificación de sistemas de información on-premise que originariamente hubieren sido desplegados en modo Cloud, debido a que su casuística no encaja con la certificación de conformidad del ENS al uso (más enfocado a sistemas y servicios) y tampoco se ajusta al tipo de producto cualificado que se incluye en el catálogo (CPSTIC) para su utilización en el ENS, al no tratarse específicamente de un producto cuyas funciones principales están asociadas a la seguridad. Ante esta situación, parece necesario definir los requisitos para certificar el mencionado sistema de información.

39. Las Entidades de Certificación deben evaluar la adecuada adopción de las medidas del Anexo II del RD 3/2010, de 8 de enero, que sean de aplicación, dadas las características particulares del objeto de la certificación. En estos casos, habrá que determinar qué medidas (o controles dentro de ellas) son responsabilidad de una configuración correcta del sistema de información on-premise y qué medidas (o controles dentro de ellas) son parte de un correcto despliegue y uso por parte del usuario.

40. El fabricante del sistema de información debe disponer de los siguientes documentos, que serán verificados por la Entidad de Certificación:

    - Guía de instalación de la aplicación, de forma compatible y alineada con el ENS.
    - Procedimiento de “cliente-usuario” para utilizar el sistema instalado de forma compatible y alineado con el ENS.

41. La Entidad de Certificación, junto con la Certificación de conformidad con el ENS, deberá remitir al CCN los documentos mencionados en el punto anterior.

42. Los requisitos descritos deberán incluirse en los correspondientes Pliegos de Contratación.

3.10 EN RELACIÓN CON LAS CERTIFICACIONES Y DISTINTIVOS DE CONFORMIDAD

43. No podrá expedirse una Certificación de Conformidad con el ENS si existe una No Conformidad y no se ha presentado un Plan de Acciones Correctivas que trate adecuadamente tal desviación.

44. Verificar que las Certificaciones y Distintivos de Conformidad con el ENS concedidos a las entidades-cliente cumplen escrupulosamente con lo dispuesto en la ITS de Conformidad con el ENS, debiendo la Entidad de Certificación mantener una vigilancia periódica razonable (menor en todo caso al período de validez de la Certificación expedida) respecto de la utilización que, sobre tales Certificaciones y Distintivos, hacen las entidades titulares de los sistemas de información certificados, informando a la propia entidad y, en su caso, reportando al Centro Criptológico Nacional, cualquier circunstancia que suponga un uso anormal o no adecuado de dichas Certificaciones o Distintivos. Se entiende que una vigilancia semestral sería adecuada, debiendo mantener la Entidad de Certificación evidencias y registro de tal vigilancia.

45. En relación con lo anterior, las Entidades de Certificación deben identificar y publicar con precisión y el mayor nivel posible de detalle en cada Certificación de Conformidad que expidan, el alcance de la misma respecto a los sistemas de información que comprenda, haciendo constar claramente los servicios soportados.

46. Cuando el alcance de la Certificación de Conformidad con el ENS comprenda sistemas de información utilizados para la prestación de servicios comercializados bajo signos distintivos (marcas y nombres comerciales), la denominación de tales signos deberá figurar, explícitamente, en la Certificación de Conformidad.

3.11 OBLIGACIONES DE LAS ENTIDADES DE CERTIFICACIÓN

47. Mantener a disposición del Centro Criptológico Nacional los Informes de Auditoría realizados, que, de conformidad con los dispuesto en el RD 3/2010, podrá verificar su contenido y adecuación.

48. Mantener una permanente vigilancia respecto de las Instrucciones Técnicas de Seguridad del ENS que pudieran ir publicándose en el BOE.

49. 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.

50. 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.