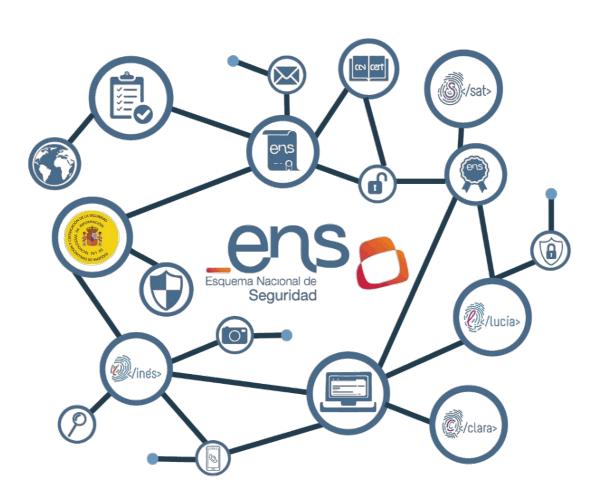




Guía de Seguridad CCN-STIC CCN-CERT IC-01/19

ENS: Criterios Generales de Auditoría y Certificación









ENS: Criterios Generales de Auditoría y Certificación

Edita:



© Centro Criptológico Nacional, 2020

Fecha de Edición: agosto de 2020

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.





ÍNDICE

1	SOF	BRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL	4
2	OBJ	ETO	4
3	CRI	TERIOS GENERALES	5
3	3.1	En relación con el alcance de auditoría	5
3	3.2	En relación con la competencia técnica de la Entidad de Certificación	5
3	3.3	En relación con los recursos de la Entidad de Certificación	6
3	3.4	En relación con la imparcialidad e independencia	7
3	3.5	En relación con la obligatoriedad del uso de las Guías CCN-STIC	7
3	3.6	En relación con el tiempo de auditoría	8
3	3.7	En relación con el desarrollo de la auditoría, la calificación de las desviacione halladas, el Informe de Auditoría y el Plan de Acciones Correctivas	
3	3.8	Resumen de los hallazgos de auditoría	. 12
3	3.9	Auditorías de certificación realizadas en modo remoto	. 12
3	3.10	En relación con la utilización de servicios compartidos	. 14
3	3.11	En relación con las certificaciones y distintivos de conformidad	. 15
3	3.12	En relación con la puesta a disposición del Informe de Auditoría	. 16
3	3.13	En relación con el período de validez de las Certificaciones de Conformidad de ENS en situaciones excepcionales.	
3	3.14	Obligaciones de las entidades de certificación	. 18
3	3.15	Aprobación Provisional de Conformidad	. 18
ΔΙ	VIEY(A MODELO DE DOCUMENTO-RESUMEN DE HALLAZGOS	20





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 servir de referencia y establecer los criterios generales para la Auditoría y Certificación de los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, especialmente los dirigidos a las Entidades de Certificación del ENS (acreditadas por la Entidad Nacional de Acreditación [ENAC] o reconocidas por el Centro Criptológico Nacional), 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 en las organizaciones del sector privado que realizan provisión de las soluciones o la prestación 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 dichos sistemas) deberán aparecer explícitamente mencionados en el Certificado de Conformidad con el ENS que, en su caso, se expida, y que se ajustará a lo dispuesto en la Resolución, de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

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 forma regular de auditorías relacionadas con la seguridad de la información, tomándose en consideración el importe de los



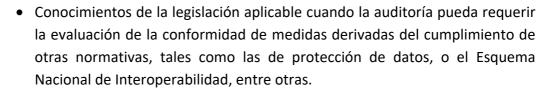


contratos, el número de certificados emitidos y las jornadas de auditor dedicadas a esta actividad.

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 deben disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación del ENS, conforme lo dispone la Resolución, de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, en todas las fases del proceso auditor: estudio documental previo, auditoría en modo remoto/in situ y redacción del Informe de Auditoría. En concreto, se exigirá disponer, al menos, de:
 - Un (1) Jefe de equipo de auditorías (Auditor Jefe).
 - Un número suficiente de auditores para la realización de las auditorías aceptadas contractualmente.
- 15. El equipo auditor deberá estar dirigido y tutelado por un Jefe de Equipo de auditoría (Auditor Jefe), que gestionará las actividades de auditoría, supervisando todo el proceso de auditoría y garantizando la exactitud de los hallazgos que se señalen en el Informe de Auditoría, así como preservar las evidencias obtenidas.
- 16. El Auditor Jefe deberá estar en condiciones de demostrar, al menos:
 - Formación en auditorías de sistemas de información, a través de certificaciones reconocidas a nivel nacional e 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, 4 (cuatro) años, en la realización regular de auditorías de tecnologías de la información.
 - Conocimientos de seguridad y gestión de riesgos de seguridad, demostrable por medio de certificaciones o experiencia de, al menos, 4 (cuatro) años en estas competencias.
 - Conocimiento de los requisitos del RD 3/2010, demostrable por medio de cursos o seminarios sobre estas competencias, de calidad y alcance suficientes, que comprendan un mínimo de 20 horas de formación.





- 17. El resto del equipo auditor no es necesario que posea las competencias exigidas para el Auditor Jefe, aunque debe contar con formación suficiente, tanto en seguridad como en auditoría de los sistemas de información, en función de las responsabilidades que le sean asignadas en cada proceso evaluador.
- 18. Los miembros del equipo auditor deberán estar familiarizados con las Guías de Seguridad CCN-STIC aplicables a cada caso, y disponer de conocimientos y experiencia en la administración de seguridad de sistemas operativos y aplicaciones, así como en infraestructuras de redes informáticas y mecanismos criptográficos.
- 19. En ningún caso los integrantes del equipo auditor deben haber participado o detentado responsabilidades previas a la auditoría, al menos en los dos (2) últimos años, en el sistema de información auditado, o bien haber sido consultores, para ese sistema, en el proceso de implementación de los requisitos del RD 3/2010.
- 20. 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.
- 21. 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 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, en la ITS de Conformidad con el ENS y la ISO/IEC 17065, evitando los conflictos de intereses.

3.5 En relación con la obligatoriedad del uso de las Guías CCN-STIC

23. Como señala el art. 29.1 del ENS, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad.









24. Con esta finalidad, las Guías CCN-STIC deben considerarse como "Mejores Prácticas¹", que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, principios, etc., que podrían influir en el desarrollo legislativo pudiendo asimismo ser utilizadas como referentes específicos en la actuación judicial o arbitral.

ENS: Criterios Generales de Auditoría y Certificación

- 25. Por tanto, no tratándose exactamente de normas imperativas, su cumplimiento no resulta obligatorio, aunque su inobservancia, caso de producirse algún incidente que pueda poner en riesgo la seguridad de los sistemas de información concernidos, podría derivar en responsabilidad.
- 26. En este sentido, la inadecuación total o parcial del sistema de información evaluado a lo dispuesto en la Guía CCN-STIC que resultare de aplicación en cada caso (https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es), podría ser calificada por el Equipo Auditor como una Observación, No Conformidad Menor o No Conformidad Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.

3.6 En relación con el tiempo de auditoría

- 27. 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 en modo remoto/in situ y redacción del Informe de Auditoría.
- 28. Para determinar los tiempos necesarios se observarán los siguientes factores:
 - 1. Se tendrá en cuenta el número de usuarios de la entidad (empleados, personal externo, eventual, etc.) que tienen acceso al sistema de información auditado (muy especialmente, aquellos que poseen privilegios de administrador), entendiendo que, cuanto mayor sea tal número, mayor será la superficie de exposición y más extensas deberán ser las cautelas a adoptar.
 - 2. El número de jornadas de auditor deberá considerar, igualmente, otros factores relacionados con la complejidad y diversidad tecnológica del sistema de información auditado y, por lo tanto, con el esfuerzo necesario para auditar tal sistema, entre ellos:
 - a) Complejidad del sistema de información en cuestión.

¹ En derecho anglosajón se denomina con el término *soft law* y el diccionario panhispánico del español jurídico, de la Real Academia Española, lo define como el conjunto de normas o reglamentaciones no vigentes que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, principios, etc. Influyen asimismo en el desarrollo legislativo y pueden ser utilizadas como referentes específicos en la actuación judicial o arbitral.







- b) Tipo(s) de servicio(s) sustentados por el sistema de información en cuestión.
- c) Existencia de Certificaciones de Conformidad con el ENS previas.
- d) Existencia de otro tipo de certificaciones contra otras normas o estándares internacionales aplicables a seguridad de la información, con el mismo o similar alcance (v.g. ISO 27001).
- e) Extensión y diversidad de la tecnología utilizada en el sistema de información en cuestión.
- f) Extensión de los acuerdos con terceros, en materia de seguridad de la información, dentro del alcance del sistema de información auditado.
- g) Número de emplazamientos operativos (CPD) y número de emplazamientos contingentes (recuperación de desastres).
- 3. El Anexo C de la norma ISO/IEC 27006:2015 puede utilizarse de referencia para considerar cómo distintos factores pueden tener impacto en el tiempo de auditoría.
- 29. El número de jornadas obtenido en el punto anterior puede ser objeto de incremento/decremento atendiendo a otros factores, tales como:

Factores de INCREMENTO	Factores de DECREMENTO
 Significativo número de personas con privilegios de administración; Infraestructura compleja, involucrando varias dependencias o ubicaciones; Personal que habla más de un idioma (que requiere intérprete o impide que auditores individuales trabajen de forma independiente) o documentación provista en más de un idioma; Actividades que requieran visitar ubicaciones alternativas o complementarias para confirmar las actividades de las ubicaciones habituales cuyo sistema de gestión está sujeto a certificación. 	 Sistemas de Información que soportan Servicios con escaso riesgo; Sistemas de Información que soportan Servicios de escasa complejidad tecnológica; Equipos de usuarios sometidos a un mismo control organizacional, desarrollando las mismas tareas; Conocimiento previo de la organización y del sistema auditado. (Por ejemplo, si el sistema ya ha sido certificado previamente con el ENS); Experiencia del cliente en las certificaciones de conformidad. (Por ejemplo, sistema ya certificado o reconocido por otro esquema de certificación en materia de seguridad de la información, tal como ISO 27001, por ejemplo); Elevada madurez del sistema de gestión de seguridad de la información.

- 30. En todo caso, los factores de incremento o decremento no podrán suponer una variación mayor de un 20% respecto al cálculo inicial de jornadas de auditoría.
- 31. Finalmente, el número de jornadas total de auditoría (estudio documental previo, auditoría en modo remoto/in situ y redacción del Informe de Auditoría) tendrá en cuenta la categoría del sistema de información auditado (BÁSICA, MEDIA o ALTA)





aplicándose un factor de corrección, atendiendo al número de controles que fuere necesario auditar, sabiendo que, como mínimo:

- Categoría BÁSICA: 45 controles (60%).
- Categoría MEDIA: 63 controles (84%).
- Categoría ALTA: 75 controles (100%).
- 32. La experiencia ha evidenciado que unos tiempos de auditoría razonables atenderían al siguiente criterio:

Fase de estudio documental previo	Mínimo, entre 0,5 y 1 jornada.		
Fase de auditoría modo remoto/in situ	 Categoría BÁSICA: mínimo, 1 jornada. Categoría MEDIA: mínimo, 2 jornadas. Categoría ALTA: mínimo, 3 jornadas. 		
Fase de redacción de informes	Cualquier Categoría: mínimo, 1 jornada que comprenderá la redacción del Informe de Auditoría completo y adecuadamente evidenciado (señalando cada medida auditada); en su caso, evaluación del Plan de Acciones Correctivas (PAC), revisión y decisión del Comité de Certificación.		

- 33. 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
 - 34. 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 las medidas adoptadas en cada uno de los emplazamientos ofrecen garantías de seguridad similares.
 - 35. 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.





- 36. No obstante, cuando proceda, se observará lo señalado en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales.
- 37. 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.
- 38. 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 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 significativamente a la capacidad del sistema de información para atender sus funciones esenciales.
- Cuando exista una duda razonable de que se haya implementado un control eficaz de proceso, o de que las medidas de seguridad cumplan los requisitos especificados.
- Cuando se evidencie un número significativo de no conformidades menores asociadas al mismo requisito.
- Cuando el número de no conformidades menores detectadas impidan deducir la adecuación del sistema a los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.

Se considera la existencia de una No Conformidad Menor:

- Ante un 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, sin afectar a la capacidad del sistema de protección para lograr los resultados previstos; los requisitos se satisfacen de forma manifiestamente mejorable o se aprecian incoherencias entre requisitos que deberían estar alineados.



01/19 ENS: Criterios Generales de Auditoría y Certificación

- 39. Respecto a los requisitos y las medidas de seguridad evaluadas que sean de aplicación según la categoría de seguridad del sistema y el nivel de seguridad de cada medida, el Informe de Auditoría debe poner de manifiesto no solo las desviaciones halladas, debiendo así mismo evidenciar la conformidad de las medidas de seguridad encontradas conformes, de modo que no se tengan dudas sobre el trabajo del auditor, la calidad de la evaluación realizada y la valoración de las evidencias analizadas.
- 40. Respecto del Plan de Acciones Correctivas, es necesario verificar que todas las No Conformidades se han corregido. No obstante, 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, deberá 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 y razonable en función de las no conformidades detectadas y su tipificación, traten y resuelvan las causas de las desviaciones halladas.
- 41. El Centro Criptológico Nacional se reserva el derecho de acompañar a las Entidades de Certificación en todas aquellas auditorías que estas realicen.

3.8 Resumen de los hallazgos de auditoría

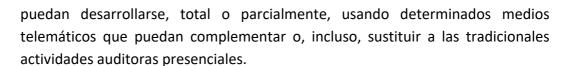
- 42. Las Entidades de Certificación del ENS deberán disponer de un procedimiento que permita obtener, para cada evaluación realizada, un documento con el número de hallazgos detectados (No Conformidades Mayores, No Conformidades Menores y Observaciones) y su ubicación, ya sea en los artículos del ENS o en las medidas de su Anexo II.
- 43. El Anexo A de la presente guía contiene un modelo del documento citado.
- 44. La información anterior deberá ser remitida al CCN, al menos con periodicidad mensual, conteniendo el resumen de las evaluaciones realizadas. En este sentido, el CCN-CERT pone a disposición de las Entidades de Certificación una funcionalidad de la solución AMPARO que permite la provisión de los datos indicados favoreciendo la automatización y eficiencia del proceso de cara a la explotación de la información proporcionada.

3.9 Auditorías de certificación realizadas en modo remoto

45. El nuevo escenario al que se ha enfrentado la sociedad mundial durante la crisis sanitaria derivada de la Covid-19 y la posibilidad de que retos similares hayan de afrontarse en el futuro, han evidenciado la necesidad de considerar nuevos procedimientos para la realización de Auditorías de Certificación que, aportando las garantías normativamente exigidas por el ENS y que no deban sufrir merma,







- 46. Como disponen el art. 34 y el Anexo III del RD 3/2010 (y desarrolla la Resolución, de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información), el objeto de una auditoría de seguridad es verificar el cumplimiento de los requerimientos del ENS, entre otros: que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información; que existen procedimientos para resolución de conflictos entre dichos responsables; que se han designado personas para dichos roles a la luz del principio de "separación de funciones"; que se ha realizado un análisis de riesgos, con revisión y aprobación anual; que se cumplen las recomendaciones de protección descritas en el Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso o que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, etc.; todo ello basado en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los requisitos del ENS.
- 47. Por todo ello, conviene incidir, en consecuencia, que es responsabilidad de la Entidad de Certificación obtener todas aquellas evidencias que le permitan emitir un dictamen de auditoría con el adecuado nivel de garantía y confiabilidad.
- 48. Para lograr lo anterior, no es estrictamente necesaria la presencia física del equipo auditor (por ejemplo, en todas aquellas cuestiones cuya evidencia pudiera evaluarse en base a pruebas documentales, fotográficas o videográficas o registros asociados a aplicaciones de auditoría, etc.), pudiendo alcanzarse los adecuados niveles de garantía usando medios electrónicos o telemáticos, debiéndose observar, eso sí, las cautelas debidas a la seguridad de las comunicaciones y la confidencialidad de la información tratada o intercambiada, la autenticidad de las evidencias observadas telemáticamente y la identidad y potestades de las personas intervinientes en las evaluaciones.
- 49. Así las cosas, y sin prejuzgar otras situaciones más amplias, parece claro que el uso de medios electrónicos y telemáticos resulta especialmente predicable en la evaluación de sistemas de información de organismos o entidades previamente conocidos y/o auditados por la Entidad de Certificación, muy especialmente cuando no se hubieren producido cambios sustanciales en los sistemas de información que induzcan a pensar que las medidas adoptadas en su momento ya no son válidas o eficaces.







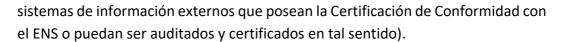
- 50. Especial atención merecen las medidas de seguridad que precisan una inspección ocular, como pueden ser las correspondientes a: protección de las instalaciones y las infraestructuras [mp.if], puesto de trabajo despejado [mp.eq.1], mecanismos de autenticación [op.acc.5] (dado que en los basados en un doble factor, podría ser necesario observar simultáneamente como se visualiza un código en un teléfono móvil, u otro dispositivo independiente, para ser inmediatamente introducido en el ordenador al que el usuario desea autenticarse), ...
- 51. En estas circunstancias será el Auditor Jefe asignado quien consensuará si puede llegar a considerar eficaz una auditoría en modo remoto de cada una de esas medidas, si se aportan, por parte del auditado, vídeos en *streaming* complementados con fotografías de detalle o cualquier otra solución que permitan las nuevas tecnologías digitales.
- 52. Un facilitador puede ser la existencia, cada vez más frecuente en los CPD, de un software de control: Building Management System (BMS) que permite la monitorización gráfica de todos los parámetros del CPD, como son la climatización, el suministro eléctrico (Trafos, cuadros, SAI, baterías, generadores...), el sistema de extinción incluyendo detectores, etc.
- 53. Por consiguiente, será posible realizar inspecciones en modo remoto durante las Auditorías de Certificación del ENS (iniciales o de renovación, sobre clientes conocidos o desconocidos), usando medios telemáticos (como, por ejemplo, videoconferencia y compartición de escritorio remoto), siempre que se considere dicha actividad como viable por parte de la Entidad de Certificación y acorde con los procedimientos de auditoria establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente a su cliente, y poder justificarlo adecuadamente ante ENAC y el Centro Criptológico Nacional.
- 54. Finalmente, será el equipo auditor el que determinará si es necesario complementar las evaluaciones en modo remoto de las Auditorías, con una **inspección "in situ"** de aquellos aspectos físicos relevantes de los que no sea posible obtener evidencias de forma remota.

3.10 En relación con la utilización de servicios compartidos

55. En tanto los Servicios Compartidos ofrecidos por la Administración General del Estado (AGE) o, en su caso, por las Administraciones Territoriales competentes, que pudieran estar comprendidos en el alcance de la auditoría no dispongan de la preceptiva Certificación de Conformidad con el ENS, la Auditoría de 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







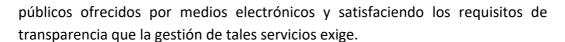
- 56. De no ser posible lo anterior, y cuando se trate de la utilización de Servicios Compartidos suministrados por la AGE o, en su caso, por las Administraciones Territoriales competentes, el alcance de la Certificación de Conformidad (y la subsiguiente Certificación de Conformidad) habrá de señalar 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.
- 57. 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.

3.11 En relación con las certificaciones y distintivos de conformidad

- 58. No podrá expedirse una Certificación de Conformidad con el ENS si existieran No Conformidades (Mayores o Menores) y no se hubiere presentado y evaluado satisfactoriamente el correspondiente Plan de Acciones Correctivas, que trate adecuadamente las desviaciones halladas.
- 59. En las Certificaciones de Conformidad expedidas, las Entidades de Certificación están obligadas a identificar y publicar con precisión el alcance de la misma (sistema o sistemas de información afectados) y, con el mayor detalle posible, los servicios comprendidos en la Certificación. Cualquier servicio que no se encuentre explícitamente reseñado en la correspondiente Certificación de Conformidad se entenderá que no está amparado por ella.
- 60. 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.
- 61. La presencia de los Distintivos de Conformidad con el ENS (ya sean Declaraciones o Certificaciones de Conformidad) en las sedes electrónicas de las entidades del Sector Público, responde, en primer instancia y de conformidad con lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público, al cumplimiento de los principios que rigen la actuación de las Administraciones Públicas, concretándose dicha obligación en lo dispuesto en el art. 41 del RD 3/2010, de 8 de enero.
- 62. Se trata, por tanto, de una cuestión de la mayor importancia, por cuanto constituye la única evidencia de que disponen los ciudadanos de verificar el preceptivo cumplimiento con el ENS de los sistemas de información concernidos, contribuyendo en consecuencia a incrementar la confiabilidad en los servicios







- 63. En consecuencia, el incumplimiento detectado en una auditoría de certificación del deber de adecuada exhibición de los Distintivos de Conformidad correspondientes será objeto de una No Conformidad Mayor, por cuanto supone el incumplimiento de uno de los preceptos obligatorios del ENS (art. 41).
- 64. Por todo ello, es necesario que, cuando resulte aplicable, entre las funciones de las Entidades de Certificación del ENS se encuentra el seguimiento de que los citados Distintivos de Conformidad con el ENS expedidos a sus clientes se exhiben adecuadamente, conforme a lo dispuesto en la ITS de Conformidad con el ENS, regulada por Resolución, de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, debiendo la Entidad de Certificación disponer de un procedimiento documentado de vigilancia en el que se indique los mecanismos para verificar, al menos semestralmente, su adecuado cumplimiento, y los procedimientos de monitorización y reporte de incidencias previstos.
- 65. Asimismo, se establece el plazo de un (1) mes para que el cliente resuelva los incumplimientos detectados en el uso de los Distintivos de Conformidad.
- 66. Si el incumplimiento se apreciara una vez concluida la auditoría de certificación y expedida la Certificación de Conformidad con el ENS, la Entidad de Certificación expedidora instará a su cliente a solventar tal situación, que, de no ser resuelta, pondrá en conocimiento del Centro Criptológico Nacional.
- 67. Cuando el incumplimiento en la adecuada exhibición del Distintivo de Conformidad fuera imputable a un proveedor de la entidad auditada, la Entidad de Certificación deberá instar a su cliente a poner remedio a esta anómala situación que, de no resolverse satisfactoriamente, obligará a la Entidad de Certificación a poner este extremo en conocimiento del Centro Criptológico Nacional, que procederá en consecuencia, conforme a derecho.

3.12 En relación con la puesta a disposición del Informe de Auditoría

- 68. El Distintivo de Conformidad con el ENS, electrónicamente enlazado a la Certificación de Conformidad de la que trae causa, resulta evidencia suficiente para demostrar que el proceso de Autoevaluación o la Auditoría de Certificación a la que esté ligado ha obtenido un resultado satisfactorio, por lo que no será necesario realizar ninguna verificación adicional sobre la adecuación e idoneidad del sistema de información de que se trate.
- 69. Por otro lado, entendiendo que los Informes de Autoevaluación o Auditoría podrían contener información o datos sensibles, de naturaleza personal, comercial o institucional y/o protegidos por distintas regulaciones, la facultad que la ITS de







Conformidad con el ENS confiere a las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado titulares de una Declaración o Certificación de Conformidad para solicitar a tales operadores dichos Informes de Autoevaluación o Auditoría, se instrumentalizará dirigiendo tal solicitud y su necesidad a la cuenta de correo electrónico cocens@ccn.cni.es del Centro Criptológico Nacional, que valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y a la Entidad de Certificación responsable de la emisión de la antedicha Certificación de Conformidad con el ENS.

3.13 En relación con el período de validez de las Certificaciones de Conformidad con el ENS en situaciones excepcionales.

- 70. Cuando se produzca una situación excepcional, como la provocada por la Covid-19, que exija la apertura de un paréntesis temporal en la relación entre las Entidades de Certificación y sus clientes, el Centro Criptológico Nacional podrá, en el ejercicio de sus competencias, prolongar la vigencia de los Certificados de Conformidad mediante la emisión de un comunicado.
- 71. La vigencia de las Acreditaciones y de los Certificados de conformidad vendrá determinada por la duración de la citada situación excepcional teniendo en cuenta que, una vez se haya dado por finalizada, se concederá un nuevo período equivalente con la misma duración que el anterior, para facilitar el restablecimiento paulatino de las relaciones entre las Entidades de Certificación y sus clientes. Por tanto, la vigencia de los certificados afectados se incrementará en un tiempo análogo al que haya durado la situación excepcional, lo que será comunicado formalmente por el CCN.
- 72. Una vez haya concluido el paréntesis citado, se reactivarán los períodos y plazos para obtener las Certificaciones de Conformidad correspondientes.
- 73. Si las circunstancias así lo aconsejaran, el Centro Criptológico Nacional podría ampliar el plazo anterior o, en su caso, iniciar un nuevo período de suspensión temporal de la vigencia de las antedichas Certificaciones.
- 74. Asimismo, si una vez expirado el paréntesis temporal concedido, existiese una causa justificada que impidiese en algún caso particular retomar los períodos y plazos de las auditorías, las Entidades de Certificación podrán solicitar un nuevo aplazamiento al CCN, justificando las razones de la solicitud a la cuenta de correo electrónico cocens@ccn.cni.es, que se estudiarán en cada caso para conceder las debidas autorizaciones.





3.14 Obligaciones de las entidades de certificación

- 75. Mantener a disposición del Centro Criptológico Nacional los Informes de Auditoría resultantes de las evaluaciones realizadas, que, de conformidad con lo dispuesto en el RD 3/2010, podrá verificar su contenido y adecuación.
- 76. Mantener una permanente vigilancia respecto de las últimas versiones de las Guías CCN-STIC (especialmente, las comprendidas en la serie 800) que resulten aplicables en cada situación, atendiendo prioritariamente a las ITS que adquieren rango de norma jurídica cuando son aprobadas mediante Resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial.
- 77. 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.

3.15 Aprobación Provisional de Conformidad

- 78. Podrá expedirse excepcionalmente una Aprobación Provisional de Conformidad (APC) como resultado de un proceso de certificación en el que concurran, simultáneamente, los siguientes requisitos:
 - Persiga la emisión del primer Certificado de Conformidad.
 - El Plan de Acciones Correctivas, por razones adecuadas y razonables, requiere un período de ejecución superior a tres (3) meses.
 - No podrá ser aplicado cuando se hayan detectado No Conformidades Mayores.
 - Solo resultará de aplicación a sistemas de información con categorías BÁSICA o MEDIA.
- 79. La Aprobación Provisional de Conformidad (APC), que será emitida por el Centro Criptológico Nacional, a petición de la Entidad de Certificación, identificará las condiciones de aplicación de la APC al caso concreto, incluyendo la evaluación de las posibles medidas de mitigación de riesgo o reducción de determinadas funcionalidades, las acciones pendientes para completar el proceso y el marco temporal de validez.
- 80. Así expedidas, las Aprobaciones Provisionales de Conformidad desplegarán su vigencia durante un período de seis (6) meses, que podrá ser ampliado por otros seis (6) meses, cuando concurran circunstancias de seguridad que así lo aconsejen.
- 81. Habiéndose corregido durante el período de validez de la APC las desviaciones detectadas, la Entidad de Certificación de que se trate podrá expedir el correspondiente Certificado de Conformidad en el ENS.







- 82. En caso de que las desviaciones halladas no hubiesen sido adecuadamente corregidas, el CCN, a propuesta de la Entidad de Certificación de que se trate, retirará la Aprobación Provisional de Conformidad concedida.
- 83. En la aplicación de un Marco de Certificación Específico (MCE-ENS), previamente validado por el CCN para sistemas de información de categoría BÁSICA, cuando una Entidad de Certificación audite la preceptiva muestra representativa de entidades adheridas a dicho MCE-ENS, un único análisis de la documentación normativa generada se considerará suficiente para establecer el grado de cumplimiento normativo en todas las entidades adheridas al MCE-ENS.
- 84. Por otro lado, la Entidad de Certificación revisará individualmente, en cada una de las entidades de la muestra representativa, las medidas técnicas de seguridad implementadas, pudiendo, asimismo, realizar cualquier revisión documental que estime oportuna para completar o validar la revisión conjunta señalada anteriormente.
- 85. Tras un informe de auditoría no desfavorable, el Centro Criptológico Nacional podrá expedir una Aprobación Provisional de Conformidad (APC) para el resto de entidades adheridas al Marco de Certificación y que hubieren quedado fuera de la muestra representativa auditada.
- 86. En estos casos y, tras la emisión de la APC, el Órgano de Auditoría Técnica al que están vinculadas o del que dependen orgánicamente las entidades del Marco de Certificación, dispondrá de un período de dos (2) años para realizar auditorías a estas entidades con la finalidad de completar el proceso de certificación de las mismas y emitir, en su caso, el correspondiente Certificado de Conformidad en el ENS.

Centro Criptológico Nacional







ANEXO A. MODELO DE DOCUMENTO-RESUMEN DE HALLAZGOS

		Organización Categoría del sistema	ENTIDAD [BÁSICA/MEDIA/ALTA]					
		ÁREA	NC Mayor	NC menor	OBS			
	MARCO GENERAL							
A1	Art. x							
A2	Art. y							
А3	Art. z		-					
		MARCO ORGANIZATI	۷O					
1	aug 1		T	l l				
1. 2.	org.1 org.2	Política de seguridad Normativa de seguridad			-			
3.	org.3	Procedimientos de seguridad	<u> </u>		_			
4.	org.4	Proceso de autorización	<u> </u>		_			
	018.1	MARCO OPERACION	AL					
		Planificación						
5.	op.pl.1	Análisis de riesgos						
6.	op.pl.2	Arquitectura de seguridad						
7.	op.pl.3	Adquisición de nuevos componentes						
8.	op.pl.4	Dimensionamiento/Gestión de capacidades						
9.	op.pl.5	Componentes certificados						
		Control de acceso						
10.	op.acc.1	Identificación		-				
11.	op.acc.2	Requisitos de acceso						
12.	op.acc.3	Segregación de funciones y tareas						
13.	op.acc.4	Proceso de gestión de derechos de acceso						
14.	op.acc.5	Mecanismo de autenticación		-				
15.	op.acc.6	Acceso local (local logon)		-				
16.	op.acc.7	Acceso remoto (remote login)						
		Explotación						
17.	op.exp.1	Inventario de activos			-			
18.	op.exp.2	Configuración de seguridad	-	-	-			
19.	op.exp.3	Gestión de la configuración						







CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación

20.	op.exp.4	Mantenimiento			
21.	op.exp.5	Gestión de cambios			
22.	op.exp.6	Protección frente a código dañino			-
23.	op.exp.7	Gestión de incidentes			
24.	op.exp.8	Registro de la actividad de los usuarios			
25.	op.exp.9	Registro de la gestión de incidentes			-
26.	op.exp.10	Protección de los registros de actividad			
27.	op.exp.11	Protección de claves criptográficas			
		Servicios externos			
28.	op.ext.1	Contratación y acuerdos de nivel de servicio			
29.	op.ext.2	Gestión diaria			
30.	op.ext.9	Medios alternativos			
		Continuidad del servi	icio		
31.	op.cont.1	Análisis de impacto			
32.	op.cont.2	Plan de continuidad			
33.	op.cont.3	Pruebas periódicas			
		Monitorización del sist	ema		
34.	op.mon.1	Detección de intrusión			
35.	op.mon.2	Sistema de métricas		-	-
		MEDIDAS DE PROTECC	CION		
		Protección de las instalaciones e i	nfraestructuras	5	
36.	mp.if.1	Protección de las instalaciones e i Áreas separadas y con control de acceso	nfraestructuras	5	
36. 37.	mp.if.1	1.	nfraestructuras		_
		Áreas separadas y con control de acceso	nfraestructuras	-	-
37.	mp.if.2	Áreas separadas y con control de acceso Identificación de las personas	nfraestructuras	-	-
37. 38.	mp.if.2	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales	nfraestructuras	-	-
37. 38. 39.	mp.if.2 mp.if.3 mp.if.4	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica	nfraestructuras	-	-
37. 38. 39. 40.	mp.if.2 mp.if.3 mp.if.4 mp.if.5	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios	nfraestructuras	-	-
37. 38. 39. 40.	mp.if.2 mp.if.3 mp.if.4 mp.if.5 mp.if.6	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios Protección frente a inundaciones Registro de entrada y salida de	nfraestructuras	-	-
37. 38. 39. 40. 41.	mp.if.2 mp.if.3 mp.if.4 mp.if.5 mp.if.6 mp.if.7	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios Protección frente a inundaciones Registro de entrada y salida de equipamiento		-	-
37. 38. 39. 40. 41.	mp.if.2 mp.if.3 mp.if.4 mp.if.5 mp.if.6 mp.if.7	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios Protección frente a inundaciones Registro de entrada y salida de equipamiento Instalaciones alternativas		-	-
37. 38. 39. 40. 41. 42. 43.	mp.if.2 mp.if.3 mp.if.4 mp.if.5 mp.if.6 mp.if.7 mp.if.9	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios Protección frente a inundaciones Registro de entrada y salida de equipamiento Instalaciones alternativas Gestión del persona Caracterización del puesto de trabajo		-	-
37. 38. 39. 40. 41. 42.	mp.if.2 mp.if.3 mp.if.4 mp.if.5 mp.if.6 mp.if.7 mp.if.9	Áreas separadas y con control de acceso Identificación de las personas Acondicionamiento de los locales Energía eléctrica Protección frente a incendios Protección frente a inundaciones Registro de entrada y salida de equipamiento Instalaciones alternativas Gestión del persona		-	-







ENS: Criterios Generales de Auditoría y Certificación

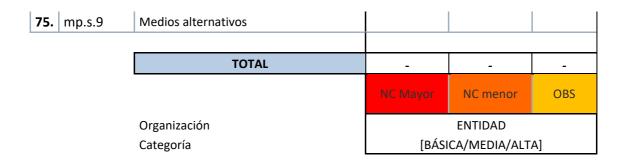
48.	mp.per.9	Personal alternativo					
		Protección de los eq	uipos				
49.	mp.eq.1	Puesto de trabajo despejado					
50.	mp.eq.2	Bloqueo de puesto de trabajo					
51.	mp.eq.3	Protección de equipos portátiles					
52.	mp.eq.9	Medios alternativos			-		
	Protección de las comunicaciones						
53.	mp.com.1	Perímetro seguro					
54.	mp.com.2	Protección de la confidencialidad					
55.	mp.com.3	Protección de la autenticidad y de la integridad					
56.	mp.com.4	Segregación de redes					
57.	mp.com.9	Medios alternativos		-			
		Protección de los soportes de	e información				
58.	mp.si.1	Etiquetado					
59.	mp.si.2	Criptografía		-			
60.	mp.si.3	Custodia					
61.	mp.si.4	Transporte		-			
62.	mp.si.5	Borrado y destrucción			-		
		Protección de las aplicacione	s informáticas				
63.	mp.sw.1	Desarrollo					
64.	mp.sw.2	Aceptación y puesta en servicio					
		Protección de la inform	nación				
65.	mp.info.1	Datos de carácter personal					
66.	mp.info.2	Calificación de la información			-		
67.	mp.info.3	Cifrado					
68.	mp.info.4	Firma electrónica					
69.	mp.info.5	Sellos de tiempo					
70.	mp.info.6	Limpieza de documentos					
71.	mp.info.9	Copias de seguridad (backup)			-		
		Protección de los ser	vicios				
72.	mp.s.1	Protección del correo electrónico			-		
73.	mp.s.2	Protección de servicios y aplicaciones web					
74.	mp.s.8	Protección frente a la denegación de servicio					







ENS: Criterios Generales de Auditoría y Certificación



❖ Las medidas compensatorias se numerarán correlativamente: MC1, MC2...