centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 802

ENS. Anexo independiente a la guía general
(Auditorías del Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad CCN-STIC 890)

Abril 2026

Edita:

centro criptológico nacional

Fecha de Edición: abril de 2026

ÍNDICE

1. INTRODUCCIÓN

1. La única garantía de que las medidas de seguridad aplicadas a los sistemas de información sean acordes a los requerimientos de seguridad necesarios para cumplir los principios básicos y requisitos mínimos que determina el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS en adelante) en función de la categoría del sistema, o de su postura de seguridad si se acoge a determinado Perfil de Cumplimiento Específico, es mediante la realización de auditorías, como se indica en la introducción de la guía **CCN-STIC-802 ENS. Guía de auditoría** a la que se vincula este anexo independiente.

2. Al tratarse el ENS de una norma jurídica certificable significa que para obtener la Certificación de Conformidad con el ENS debe superarse una auditoría de certificación con el objetivo de sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado.

3. El Centro Criptológico Nacional (CCN en adelante), en el ámbito de sus competencias, ha aprobado perfiles de cumplimiento específicos de acuerdo con lo dispuesto en el **artículo 31.2 del ENS** que señala: "*2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información*".

4. **El presente anexo desarrolla el proceso para la ejecución de auditorías de cumplimiento respecto al ENS para sistemas que se acojan al Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (RFS en adelante) recogido en la guía CCN-STIC 890 y sus anexos.**

2. SOBRE LOS PERFILES DE CUMPLIMIENTO ESPECÍFICOS

2.1. JUSTIFICACIÓN DEL PERFIL DE CUMPLIMIENTO

5. En virtud del principio de proporcionalidad y para facilitar la conformidad con el ENS a determinado colectivo de entidades, o sectores de actividad concretos, se pueden implementar Perfiles de Cumplimiento Específico que comprenden aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación en base a una determinada postura de seguridad.

6. Las guías CCN-STIC podrán establecer Perfiles de Cumplimiento Específico para colectivos de entidades, o sectores de actividad concretos, que incluirán la relación de medidas de seguridad (requisitos base y refuerzos obligatorios) que en cada caso resulten aplicables, o los criterios para su determinación.

7. El CCN en el ejercicio de sus competencias, validará y publicará los correspondientes Perfiles de Cumplimiento Específico que se definan, como se dispone en el artículo 30.3 del ENS, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los

recursos requeridos sin menoscabo de la protección perseguida y exigible, todo ello de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda del RD 311/2022.

8. El Perfil de Cumplimiento Específico de RFS se encuentra validado por el CCN y publicado en la guía CCN-STIC 890 y sus anexos, donde se detallan los requisitos del ENS exigibles a los sistemas que se acojan a este Perfil de Cumplimiento Específico, así como su proceso de adecuación haciendo uso de la metodología µCeENS, automatizada en el Portal de Gobernanza del CCN.

2.2. PARTICULARIDADES ASOCIADAS AL PERFIL DE CUMPLIMIENTO

9. Al estar el Perfil de Cumplimiento Específico de RFS orientado a alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible, la auditoría de los sistemas de información que se acojan a este perfil deberá estar alineada con el precitado criterio de eficiencia.

10. Esta es la razón por la que los sistemas de información acogidos al Perfil de Cumplimiento Específico RFS **únicamente podrán ser auditados a efectos de obtener la Certificación de Conformidad con el ENS a través del Portal de Gobernanza dispuesto al efecto en la página web del CCN.**

11. Para ello se definirán en el Portal de Gobernanza diferentes roles a sus usuarios, de modo que unos puedan aportar evidencias de la correcta implantación del ENS por parte de la organización auditada y otros realizar la auditoría externa de Certificación de la Conformidad con el ENS, asegurando su imparcialidad e independencia.

12. El empleo del Portal de Gobernanza permite **agilizar el proceso de auditoría**, automatizando varias de las tareas necesarias como es la aportación y clasificación de evidencias por parte de la organización auditada, simplificando y sistematizando su evaluación por el auditor. Esta simplificación se traduce en una **reducción del tiempo que es necesario dedicar a la auditoría**.

13. Esta agilidad en el proceso de auditoría se reflejará en una disminución del tiempo de auditoría, pudiendo reducirse de forma extraordinaria el número mínimo de jornadas requeridas para auditar del sistema, sin menoscabo de la rigurosidad del análisis de las evidencias aportadas y, por tanto, de las medidas de seguridad evaluadas.

14. De la misma forma que una auditoría ordinaria de Certificación de la Conformidad con el ENS, será un **Órgano de Auditoría Técnica (OAT)**, con las competencias necesarias y reconocido por el CCN de acuerdo con la guía CCN-STIC 122, o una **Entidad de Certificación (EC) acreditada por ENAC**, quién realice la auditoría de certificación del Perfil de Cumplimiento Específico de RFS.

3. ADECUACIÓN AL PERFIL DE CUMPLIMIENTO

15. La **organización a ser auditada deberá haberse adecuado al ENS siguiendo la guía CCN-STIC 890 y sus anexos.**

16. La organización a ser auditada deberá dar de alta el sistema objeto de la auditoría en el Portal de Gobernanza del CCN y completar las Fases de Adecuación e Implantación a través los asistentes de INES: aportará la información del sistema, documentación, así como el resto de evidencias necesarias para demostrar la implantación de las medidas de seguridad aplicables.

17. La organización a ser auditada, en función de los activos esenciales y su valoración, firmará el Anexo III Asunción del Riesgo y Compromiso de Mejora continua, obligatorio para poder solicitar la auditoría de certificación.

18. El equipo auditor podrá visualizar la información y las evidencias introducidas por el auditado a través del Portal de Gobernanza. Entre otros, la categoría del sistema, el Plan de Adecuación, la Declaración de Aplicabilidad, los servicios sustentados por el sistema, y todas las evidencias asociadas a las medidas de seguridad del Anexo II del ENS que apliquen.

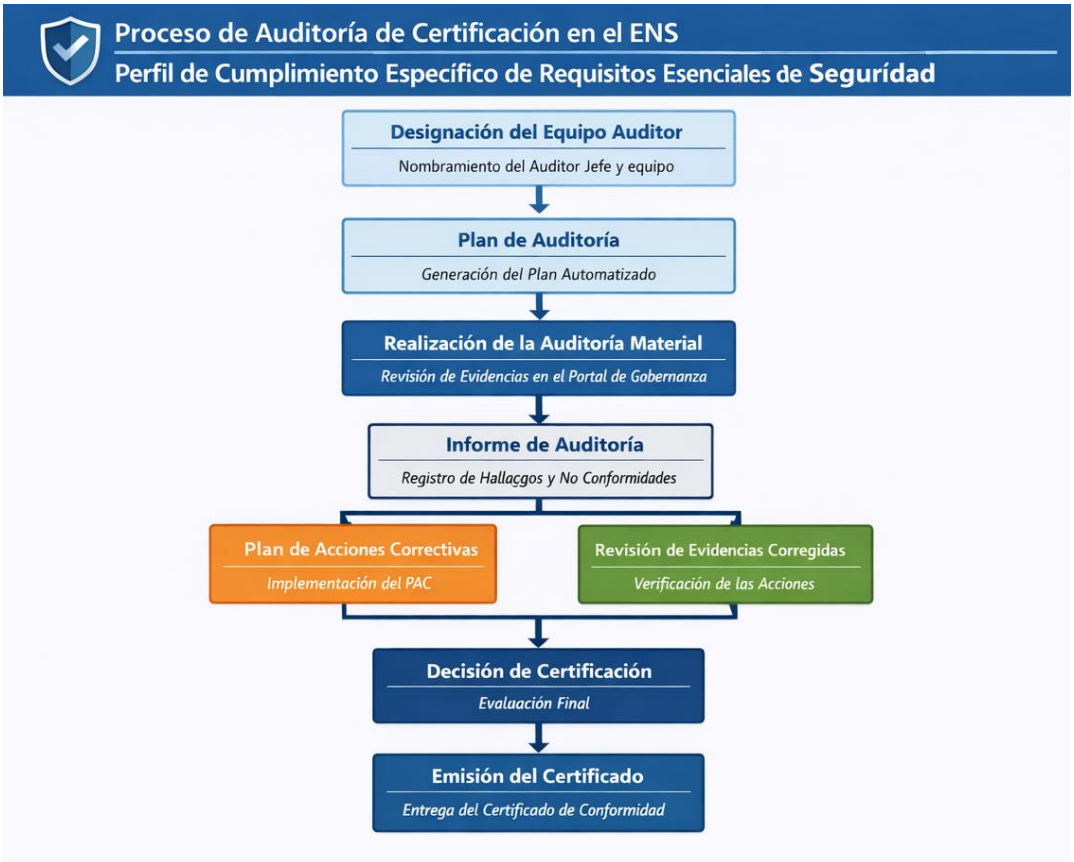
4. FASES RELEVANTES EN UNA AUDITORÍA DE CUMPLIMIENTO

19. Además de las consideraciones generalistas que constan en la guía general **CCN-STIC-802 ENS. Guía de auditoría**, se tendrán en cuenta determinadas particularidades, que se relacionan en los apartados a continuación, cuando se trate de auditar Perfiles de Cumplimiento Específico.

20. Las fases que pueden llegar a identificarse, según se desarrollan en la guía general CCN-STIC 802, son:

    - Designación del equipo auditor.
    - Estudio de la documentación del sistema.
    - Plan de Auditoría.
    - Realización de la auditoría material.
    - Reunión de cierre y dictamen de la auditoría.
    - Informe de Auditoría.
    - Plan de Acciones Correctivas.
    - Decisión de Certificación y Emisión del Certificado.

    Analizaremos a lo largo de los apartados que siguen, aquellas que presenten peculiaridades frente a la guía general.



21. Considerando que las auditorías realizadas a sistemas de información acogidos al Perfil de Cumplimiento Específico de RFS están semiautomatizadas en el Portal de Gobernanza, **el tiempo dedicado a su realización podrá ser inferior a los tiempos mínimos de auditoría** reflejados en la guía IC 01/29 Criterios Generales de Auditoría y Certificación, entendiendo que, para garantizar la correcta revisión de la documentación y evidencia del sistema, **este tiempo de auditoría nunca deberá ser inferior a media jornada**.

4.1. DESIGNACIÓN DEL EQUIPO AUDITOR

22. La organización seleccionada para realizar la auditoría, tras recibir y aceptar a través del Portal de Gobernanza dicha solicitud, debe designar obligatoriamente por dicho medio a un Auditor Jefe y, opcionalmente, otros miembros del equipo auditor.
23. Todos los miembros del equipo auditor deben disponer de usuario en el Portal de Gobernanza con un rol asignado de acuerdo con su responsabilidad en el proceso de auditoría.
24. Los designados serán quienes únicamente podrán interactuar en la auditoría con la información y las evidencias aportadas, siendo notificados automáticamente a la organización auditada.

4.2. ESTUDIO DE LA DOCUMENTACIÓN DEL SISTEMA

25. La estructuración que aporta el Portal de Gobernanza en el acceso a la documentación, permite reducir el tiempo destinado a esta fase y por ende a la auditoría en su conjunto.

26. En este caso, se entenderá el estudio de la documentación y de las evidencias aportadas como **parte de la realización de la auditoría material y no como fase previa diferenciada.**

4.3. PLAN DE AUDITORÍA

27. El Portal de Gobernanza dispone de un **generador automatizado del Plan de Auditoría** en base a las medidas a auditar como consecuencia de acogerse a un determinado Perfil de Cumplimiento Específico, en este caso el de RFS.

28. Este Plan de Auditoría generado contiene la información necesaria para la notificación a la entidad auditada de los aspectos más relevantes sobre el proceso. Esencialmente, esta planificación contendrá las fechas y jornadas en la que se realizará el proceso de auditoría, así como el equipo auditor seleccionado junto con el listado de medidas a auditar y un margen temporal.

29. Al no haber interacción directa con la organización a ser auditada, **evitando las reuniones presenciales o videollamadas**, sino que la auditoría la realiza el equipo auditor directamente sobre la información obtenida desde el Portal de Gobernanza, la planificación queda muy simplificada.

4.4. REALIZACIÓN DE LA AUDITORÍA MATERIAL

30. La automatización del proceso en el Portal de Gobernanza, que abarca el conjunto de evidencias ya preparadas sin necesidad de que el auditado emplee tiempo en encontrarlas, simplifica mucho la fase de auditoría material.

31. Las evidencias se encuentran estructuradas según el articulado del Real Decreto 311/2022, los anexos de la guía CCN-STIC 890 y las medidas de seguridad que aplican en base a la Declaración de Aplicabilidad de Perfil de Cumplimiento Específico al que se acoge el sistema de información auditado, en este caso de RFS.

32. Con el objetivo de no prolongar los tiempos de auditoría más de lo estrictamente necesario, las aclaraciones sobre la documentación y las evidencias presentadas al auditor deberán evitarse durante el proceso de auditoría, exponiéndose estas dudas en el posterior Informe de Auditoría en caso de suponer posibles desviaciones a la conformidad del sistema. Estas aclaraciones podrán remitirse, por parte de la entidad auditada, en la forma de un Plan de Acciones Correctivas a través del Portal de Gobernanza.

4.5. REUNIÓN DE CIERRE Y DICTAMEN DE LA AUDITORÍA

33. Al estar sistematizada y asistida la auditoría de un sistema de información acogido a determinado Perfil de Cumplimiento Específico, en este caso de RFS, y no contemplarse interacción entre la organización auditada y el equipo auditor, no se recoge el concepto de reunión de cierre.

4.6. INFORME DE AUDITORÍA

34. El equipo auditor podrá incluir, en el Portal de Gobernanza, para cada medida de seguridad los hallazgos, No Conformidades, observaciones y notas que considere oportunas.
35. Toda esta información quedará reflejada en un Informe de Auditoría que, a partir del trabajo del equipo auditor, **se generará automáticamente dese el Portal de Gobernanza.**
36. Este informe será remitido a la entidad auditada para la resolución de las No Conformidades detectadas y la presentación de una Plan de Acciones Correctivas (PAC), en el caso de ser necesario.
37. **Los plazos de presentación del PAC e informe de auditoría seguirán lo establecido para las auditorías de certificación ordinarias del ENS.**

4.7. PLAN DE ACCIONES CORRECTIVAS

38. Una vez generado el Informe de Auditoría, si constan en él No Conformidades, la organización auditada será notificada y podrá trabajar en el Plan de Acciones Correctivas (PAC) a través de un asistente en el Portal de Gobernanza.
39. Las evidencias de la corrección de las No Conformidades detectadas durante la auditoría y reflejadas en el informe de auditoría deberán incorporase a las medidas correspondientes en el Portal de Gobernanza, como ficheros y documentos adicionales, sin modificar la información auditada previamente.
40. Una vez resueltas las No Conformidades reflejadas en el informe de auditoría, y habiéndose respetado los plazos establecidos de presentación del PAC, se notificará al equipo auditor a través del Portal de Gobernanza para la revisión y análisis de las evidencias de la corrección incorporadas al sistema.

4.8. DECISIÓN DE CERTIFICACIÓN Y EMISIÓN DEL CERTIFICADO

41. Siempre que se trate de una auditoría de Certificación de la Conformidad y una vez la auditoría haya finalizado y se determine que ésta no es DESFAVORABLE y, en su caso, se han solventado las posibles No Conformidades mediante un PAC, se podrá generar el Certificado de Conformidad, tras la confirmación de los datos sobre la organización auditada que constan en el Portal de Gobernanza.

42. Ante un dictamen «DESFAVORABLE», la entidad titular del sistema de información auditado, en un plazo no superior a seis meses desde la fecha de emisión del Informe de Auditoría, deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre los hallazgos de no conformidad evidenciados que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.
43. Este proceso se realizará siguiendo los procedimientos de toma de decisión de certificación establecidos en la EC/OAT.
44. Una vez generado el Certificado de Conformidad, se procederá a la notificación para su publicación de acuerdo con lo establecido en la CCN-STIC-809 Declaración y Certificación Conformidad ENS.