GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

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

# ENS. Criterios Generales de Auditoría y Certificación


Marzo 2024

MINISTERIO DE DEFENSA

Edita:





Fecha de Edición: marzo de 2024

**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. OBJETO

1. La Disposición adicional segunda del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, señala que, para un mejor cumplimiento de lo establecido en el Real Decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

2. En este sentido, 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 dirigidos a las Entidades de Certificación (EC, en adelante), acreditadas por la Entidad Nacional de Acreditación (ENAC) y a los Órganos de Auditoría Técnica del Sector Público (OAT, en adelante), regulados en la Guía CCN-STIC 122[1]), de conformidad con lo señalado en el artículo 31 del precitado Real Decreto 311/2022, de 3 de mayo, sobre auditoría de la seguridad, y lo dispuesto en su normativa de desarrollo o complementaria, singularmente, las Instrucciones Técnicas de Seguridad y las Guías CCN-STIC que resulten de aplicación[2].

3. 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 recogido 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"*.

## 2. CRITERIOS GENERALES

4. Los sistemas de información comprendidos en el ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad serán objeto de una **auditoría regular ordinaria, al menos cada dos (2) años**, que verifique el cumplimiento de los requerimientos del ENS.

5. Con carácter inusual, deberá realizarse una auditoría **extraordinaria** siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La auditoría extraordinaria podrá circunscribirse a todo lo relacionado con los cambios habidos en el sistema de información, siempre que no haya transcurrido más de seis (6) meses desde la última auditoría de certificación ordinaria.

6. La realización de la auditoria extraordinaria no determinará la fecha de cómputo para el cálculo de los dos (2) años, establecidos para la realización de la siguiente auditoría regular ordinaria

[1] CCN-STIC 122 Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS

[2] De no señalarse lo contrario o deducirse lógicamente de ello, en tanto se encuentre vigente el periodo de 24 meses al que se refiere la Disposición transitoria única del Real Decreto 311/2022, de 3 de mayo, las referencias hechas en el presente documento al RD 311/2022 deben entenderse extensivas, mutatis mutandis, al desarrollo de las actividades derivadas de las auditorías realizadas conforme al RD 3/2010, de 8 de enero.

indicados en el párrafo anterior, sino que este plazo se mantendrá inmutable a no ser que la auditoría extraordinaria comprenda la totalidad de los requerimientos del ENS y, en consecuencia, sea equivalente a una auditoría ordinaria adelantada respecto al plazo establecido de dos (2) años.

7. Un cambio debido al incremento de la categoría del sistema de información que se certifica, o a una ampliación del alcance de dicha certificación, también podrá abordarse como una auditoría extraordinaria, siendo responsabilidad de la EC o del OAT determinar con rigor que requerimientos del ENS deben ser evaluados.

8. Con carácter extraordinario, deberá realizarse una **auditoría extraordinaria** siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos (2) años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

9. El plazo de dos (2) años señalado en los párrafos anteriores **podrá extenderse durante tres (3) meses** cuando concurran impedimentos de fuerza mayor no imputables a la organización titular del sistema o sistemas de información concernidos o a los recursos disponibles de la EC/OAT que la antedicha organización hubiere designado.

10. La auditoría se realizará en función de los niveles de seguridad de cada dimensión expresados en la Declaración de Aplicabilidad correspondiente y en la categoría de seguridad del sistema y, en su caso, los correspondientes al Perfil de Cumplimiento Específico sobre el que se realice la evaluación, según lo dispuesto en los Anexos I y III del RD 311/2022, de 3 de mayo, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

11. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normativa nacional e internacional aplicables a este tipo de actividades.

12. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del sistema o sistemas de información auditados con referencia al Real Decreto 311/2022, de 3 de mayo, identificando los hallazgos de cumplimiento e incumplimiento detectados y aportando las evidencias correspondientes. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

13. Los informes de auditoría serán presentados al Responsable del Sistema y al Responsable de la Seguridad de la entidad titular o responsable de los sistemas auditados. Estos informes serán analizados por el Responsable de la Seguridad, que presentará sus conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

14. Asimismo, los informes de auditoría podrán ser requeridos por los responsables de la entidad titular o responsable de los sistemas de información auditados que poseyeren competencias sobre seguridad de las tecnologías de la información, y por el CCN.

15. En el caso de sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el Responsable del Sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación, temporalidad que podrá extenderse en el tiempo contando siempre con la aprobación formal del órgano directivo responsable a estos efectos

16. Las EC/OAT 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 organizaciones del ámbito de aplicación del ENS (entidades del sector público y entidades privadas prestadoras de servicios competenciales a las anteriores) y, en consecuencia, en el aseguramiento del ejercicio de los derechos y libertades que la Constitución Española proclama y desarrolla el ordenamiento jurídico administrativo, entre otros..

17. Para ello, las EC/OAT 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.

18. Así pues, además de las previsiones que se deriven de la legislación vigente y de las Guías CCN-STIC del CCN que resulten de aplicación, las EC/OAT están obligadas a adoptar las cautelas y recomendaciones señaladas en los siguientes epígrafes.

## 2.1 EN RELACIÓN CON EL ALCANCE DE AUDITORÍA

19. Es necesario 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.

20. La redacción del ALCANCE de las Certificaciones de Conformidad con el ENS debe satisfacer los siguientes requisitos:

- Recoger, escrupulosamente, la información precisa y suficiente del sistema de información a auditar, incluyendo la funcionalidad de todos los servicios soportados por dicho sistema de información.
- Si los servicios soportados tienen un nombre comercial, puede incluirse en el Certificado de Conformidad con el ENS tal denominación, para lo que la EC/OAT deberá asegurarse de que todas las funcionalidades de dicho(s) servicio(s) han sido adecuadamente evaluadas conforme al ENS.
- Si existiera algún servicio que estuviera soportado por el sistema de información evaluado y que no hubiere sido objeto de evaluación, la EC/OAT deberá asegurarse de que la prestación de tal servicio no tiene impacto en la seguridad del sistema. Es decir, garantizar que un incidente de seguridad que tuviera su origen en tal servicio NO podría trasladarse al resto de los servicios soportados por el citado sistema de información.
- Es imperativo que la redacción del alcance NO INDUZCA A ERROR o a una MALA INTERPRETACIÓN a los destinatarios de las Certificaciones de Conformidad con el ENS, ni haga pensar que el alcance es mayor o distinto del que realmente ha sido evaluado.

- En relación con la evaluación de sistemas SaaS implantados en modo local, se recuerda la obligatoriedad de que la EC/OAT contemple, cuando proceda, lo dispuesto en la Guía CCN-STIC 858[3], incluyendo la evaluación del contenido de la preceptiva "Guía de relación entre cliente y proveedor" que allí se menciona.

21. Tanto los sistemas de información evaluados como 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 Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, con las precisiones que se contienen en el presente documento.

22. Asimismo, con el objetivo de ofrecer la debida transparencia en el cumplimiento del ENS y del resto de regulaciones concordantes, las Certificaciones de Conformidad con el ENS de aquellos sistemas de información que ofrezcan Servicios en la Nube o desde diferentes ubicaciones, expresarán, dentro de la mención a los servicios comprendidos en el alcance, la ubicación (continente o región, país y ciudad) de los CPD en los que se soportan dichos servicios, junto con una mención sobre los que hayan sido objeto de evaluación expresa por parte de la EC/OAT de que se trate.

23. Conviene recordar que, en cualquier caso, el alcance pactado con el cliente final será el que finalmente se evalúe (expresamente o por muestreo), debiendo ser el mismo que aparezca finalmente en la correspondiente Certificación de Conformidad con el ENS.

24. Por ejemplo, podría darse el caso de que un Prestador de Servicios en la Nube (CSP) o una organización dedicada al alquiler de espacio y equipos en sus Centros de Datos (*hosting*), no todos sus CPD estén comprendidos en el alcance ni, en consecuencia, se contemple su evaluación, aunque ésta sea muestral. Otro ejemplo sería el de un desarrollador de software con presencia en diferentes provincias españolas, y que únicamente persiga la evaluación de alguna de sus sedes, al considerar que cumplen con las medidas de seguridad apropiadas, dejando para una segunda fase el resto. En todos los casos planteados, y otros afines, es importante conocer las ubicaciones comprendidas en el alcance de la evaluación y la ulterior certificación, ya se trate de CPDs/Salas Técnicas o de sedes/oficinas desde donde se prestan servicios o se consideran relevantes para su prestación.

25. Caso de que la organización prestadora de servicios a las entidades públicas, ya sea normativa interna o por disposiciones de normas jurídicas, tales como pueden la normativa sobre Protección de Infraestructuras Críticas o sobre Secretos Oficiales, considere que especificar la ubicación exacta de determinadas sedes o CPDs podría poner en riesgo su seguridad física, obviará la localización exacta y especificará únicamente la provincia, adicionando el municipio caso de existir duda entre diferentes ubicaciones en la misma provincia.

## 2.2 EN RELACIÓN CON LA COMPETENCIA TÉCNICA DE LA ENTIDAD DE CERTIFICACIÓN

26. 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,

[3] CCN-STIC 858 Implantación de sistemas SaaS en modo local (on-premise)

tomándose en consideración el importe y magnitud de los contratos, el número de certificados emitidos y las jornadas de auditor dedicadas a esta actividad.

27. En el caso de tratarse de entidades cuya reciente constitución no permita acreditar los referidos tres (3) años, ENAC, en base al dictamen previo del CCN, considerará la experiencia del personal relevante de la entidad en materia de auditoría, tal como su responsable técnico y el equipo auditor y revisor.

## 2.3 EN RELACIÓN CON LOS RECURSOS DE LA EC/OAT

28. La EC/OAT ha de mantener actualizada y a disposición del CCN 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.

29. Las EC/OAT deben disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación del ENS, conforme lo que indica la norma ISO/IEC 17065:2012, en todas las fases del proceso auditor: estudio documental previo, auditoría (remota/in situ) y redacción del Informe de Auditoría. En concreto, se exigirá disponer, al menos, de:

    - Un (1) Responsable Técnico, que podrá actuar en calidad de Jefe de equipo de auditorías (Auditor Jefe).
    - Tantos auditores jefes como equipos de auditoría o, lo que es lo mismo, como auditorías simultáneas pueda llegar a hacer la EC/OAT.
    - Un número suficiente de auditores para la correcta realización de las auditorías aceptadas contractualmente.
    - Al menos, un (1) revisor de los expedientes de auditoría, de conformidad con lo señalado en la norma ISO/IEC 17065:2012

30. Cada 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 preservando las evidencias obtenidas.

31. Siendo habitual la exclusiva participación del Auditor Jefe en muchas auditorías, será éste, conjuntamente con los Responsables de Operaciones de la EC/OAT, quienes previamente al inicio de cada auditoría decidirán si requiere apoyo de otros auditores o no.

32. 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 o internacional, cursos, seminarios o actividades formativas regladas o impartidas por entidades reconocidas, de calidad y adecuado número de horas formativas que permitan evidenciar la idoneidad y suficiencia de los conocimientos adquiridos.
    - Experiencia verificable de, al menos, 4 (cuatro) años, en la realización regular de auditorías de tecnologías de la información.

- Conocimiento 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 311/2022, demostrable por medio de cursos o seminarios sobre estas competencias, de calidad y alcance suficientes, que comprendan un mínimo de 20 horas de formación.
- Conocimientos de la legislación aplicable cuando la auditoría pueda requerir la evaluación de la conformidad de medidas derivadas del cumplimiento de otras normativas, tales como las de protección de datos, o el Esquema Nacional de Interoperabilidad, Identidad Electrónica, Firma Electrónica y Servicios de Confianza, entre otras.
- Al objeto de posibilitar una evaluación eficaz, las capacidades, formación y experiencia del personal encargado de la revisión de los expedientes de Auditoría deberán ser, al menos, las exigidas para el Auditor Jefe. Todo ello de acuerdo con el epígrafe 7.5 de la norma ISO/IEC 17065:2012 (usada para el procedimiento de acreditación de las Entidades de Certificación/Órganos de Auditoría Técnica del Sector Público del ENS).
- 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.
- Los miembros del equipo auditor deberán estar familiarizados con las Guías de Seguridad CCN-STIC aplicables a cada caso, y disponer de conocimientos en la administración de seguridad de sistemas operativos y aplicaciones, así como en infraestructuras de redes informáticas y mecanismos criptográficos.
- En ningún caso los integrantes del equipo auditor deben haber participado o ejercido responsabilidades previas a la auditoría en el sistema de información auditado, al menos durante los dos (2) años previos a la realización de la auditoría, o haber sido consultores para ese sistema en el proceso de implementación de los requisitos del ENS (RD 3/2010 o RD 311/2022).
- Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos y con anterioridad a la realización de la auditoría, deberán haber suscrito un acuerdo de confidencialidad con la EC/OAT.
- La EC/OAT 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.

## 2.4 EN RELACIÓN CON LA IMPARCIALIDAD E INDEPENDENCIA

33. Las EC/OAT deben asegurarse de que su organización, así como su personal involucrado, mantengan las preceptivas condiciones de imparcialidad e independencia respecto de la entidad cuyo sistema de información va a ser auditado, evitando los conflictos de interés, de conformidad con lo exigido en la ITS de Auditoría, en la ITS de Conformidad y en la ISO/IEC 17065.

34. Como prevención adicional, una EC debe demostrar imparcialidad frente a otras posibles organizaciones del mismo grupo empresarial al que pertenezca, si es el caso; así como un OAT debe demostrar imparcialidad respecto a otras áreas o unidades encuadradas en el mismo organismo que el propio OAT, por ejemplo, otra área que preste servicios de consultoría.

35. Ocasionalmente, podría darse el caso de que un organismo con al menos dos (2) áreas independientes, tuviera cada una de ellas un grupo actuando como OAT. En ese caso, cada OAT podría auditar a la otra área donde no estuviera encuadrado, en lo que podríamos denominar "**auditorías cruzadas"**, siempre que el análisis de riesgos frente a la imparcialidad y las posibles acciones de tratamiento asociadas dieran como resultado un valor de riesgo residual aceptable.

36. En cualquier caso, para garantizar la debida imparcialidad y ausencia de conflicto de interés en los OAT que desarrollen estas auditorías cruzadas, se podrá requerir la puesta a disposición del CCN de toda documentación relacionada con el proceso de auditoría que evidencie el riguroso mantenimiento de la antedicha imparcialidad, junto con la notificación del correspondiente Certificado de Conformidad con el ENS y el resumen de hallazgos de auditoría, documentación que incluirá necesariamente el Informe de Auditoría, y que podrá ampliarse con el programa o plan de auditoría, el análisis de riesgos para la imparcialidad o cualquier otra documentación que se estime necesaria relacionada con el proceso de auditoría.

37. Si el riesgo no puede ser mitigado, la EC/OAT deberá renunciar a realizar las evaluaciones/certificaciones afectadas por dicho riesgo inaceptable o, en caso de duda, realizar una consulta previa específica al CCN a través de la cuenta cocens@ccn.cni.es.

## 2.5 EN RELACIÓN CON LA OBLIGATORIEDAD DEL USO DE LAS GUÍAS CCN-STIC

38. Como señala la Disposición adicional segunda del RD 311/2022, de 3 de mayo, y para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

39. Con esta finalidad, las Guías CCN-STIC deben considerarse como "Mejores Prácticas[4]", 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.

40. Por tanto, no tratándose en puridad 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.

[4] 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.

41. 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 Observación, No Conformidad Menor o No Conformidad Mayor, atendiendo al impacto que su incumplimiento pudiera tener en la seguridad de dicho sistema de información.

## 2.6 EN RELACIÓN CON EL TIEMPO DE AUDITORÍA

42. La EC/OAT debe determinar adecuadamente los tiempos necesarios para realizar las Auditorías de Conformidad con el ENS, en sus diferentes fases: estudio documental previo, auditoría (remota/in situ) y redacción del Informe de Auditoría.

43. Para determinar los tiempos necesarios se observarán los siguientes factores:

- 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.
- 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.
  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 (p. ej. 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).
- 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.

44. 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;<br>• Infraestructura compleja, involucrando varias dependencias o ubicaciones;<br>• 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;<br>• 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;<br>• Sistemas de Información que soportan Servicios de escasa complejidad tecnológica;<br>• Equipos de usuarios sometidos a un mismo control organizacional, desarrollando las mismas tareas;<br>• Conocimiento previo de la organización y del sistema auditado. (Por ejemplo, si el sistema ya ha sido certificado previamente con el ENS);<br>• 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);<br>• Elevada madurez del sistema de gestión de seguridad de la información. |

45. En todo caso, **los factores de incremento o decremento no podrán suponer en su conjunto una variación mayor de un 20% respecto al cálculo inicial de jornadas de auditoría**.

46. El número de jornadas total de auditoría (estudio documental previo, auditoría en modo remoto/in situ, redacción del Informe de Auditoría y, eventualmente, la evaluación del Plan de Acciones Correctivas), se determinará atendiendo a la categoría de seguridad del sistema de información, habiendo considerado los niveles de seguridad de cada dimensión reflejados en la correspondiente Declaración de Aplicabilidad y los controles que, en consecuencia, sea necesario auditar.

47. La experiencia ha evidenciado que unos tiempos de auditoría razonables deben atender 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, 1,5 jornada.<br>• Categoría MEDIA: mínimo, 2,5 jornadas.<br>• Categoría ALTA: mínimo, 3,5 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. |

48. En determinados supuestos, como los que suceden al combinar la evaluación del RD 311/2022, de 3 de mayo, con la norma ISO/IEC 27001:2022, nos encontraríamos ante una "auditoría concurrente" en donde, en determinadas circunstancias, se podría apreciar un porcentaje de coincidencia mayor del 50% en la evaluación de controles análogos o parcialmente análogos, en cuyo caso no se puede entrar a valorar el tiempo de reducción total en una evaluación conjunta ENS-ISO/IEC 27001.

49. No obstante, con las versiones de 2022 de ambas normas (ENS-ISO/IEC 27001) se podría analizar lo que en una auditoría concurrente significara un mayor decremento, que es algo que deberá

considerar cada EC/OAT en base a su propio criterio, estableciéndose en todo caso que la reducción no podrá suponer más de un 35% en el tiempo total de auditoría.

50. Ante la determinación de tiempos de auditoría anormales por parte de la EC/OAT, **el Centro Criptológico Nacional, en el ejercicio de sus competencias, podrá examinar las circunstancias argumentadas por la EC/OAT para tal asignación**, adoptando las medidas que, en derecho, procedan.

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

51. 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.

52. 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, la existencia del Registro de Actividades de Tratamiento, etc.

53. 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.

54. 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, siempre que sean enunciativas y no se desarrollen exhaustivamente, de tal forma que pudiera llegar a considerarse consultoría encubierta.

55. 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 311/2022 y/o el incumplimiento total de un conjunto de medidas/controles pertenecientes a un dominio de su 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 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 de información de que se trate 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 311/2022 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 pueden satisfacerse de forma manifiestamente mejorable o se aprecian incoherencias entre requisitos que deberían estar alineados.

56. Para facilitar la identificación y el posterior tratamiento de los hallazgos de una auditoría y la verificación de su solución:
    - Será posible agrupar varias No Conformidades menores en una sola No Conformidad menor, si dichos hallazgos están referidos a una única medida.
    - Cuando las No Conformidades menores estén referidas a varias medidas dentro de un mismo grupo de medidas (por ejemplo: [op.pl.*], [op.acc.*], [op.exp.*], [mp.if.*], [mp.eq.*], etc.), su posible agrupación se calificará como No Conformidad Mayor.
    - No podrán agruparse No Conformidades menores que se refieran a distintos grupos de medidas, como tampoco podrán agruparse No Conformidades Mayores, en ningún caso.
57. 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, sino, asimismo, 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.
58. Respecto del **Plan de Acciones Correctivas**, es necesario verificar que todas las No Conformidades (mayores o menores) se han corregido. No obstante, en caso de que la entidad auditada precise de un tiempo mayor de un mes 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.
59. El **Centro Criptológico Nacional se reserva el derecho de acompañar a las EC/OAT** en las auditorías que estas realicen.

## 2.8 RESUMEN DE LOS HALLAZGOS DE AUDITORÍA

60. Las EC/OAT 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 las disposiciones del RD 311/2022 afectadas, ya sean los artículos o las medidas de su Anexo II.

61. 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 EC/OAT 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.

## 2.9 AUDITORÍAS DE CERTIFICACIÓN REALIZADAS EN MODO REMOTO

62. 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, puedan desarrollarse, total o parcialmente, usando determinados medios telemáticos que puedan complementar o, incluso, sustituir a las tradicionales actividades auditoras presenciales.

63. Como disponen el art. 31 y el Anexo III del RD 311/2022 (y desarrolla 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.

64. Por todo ello conviene incidir en consecuencia, que es responsabilidad de la EC/OAT obtener todas aquellas evidencias que le permitan emitir un dictamen de auditoría con el adecuado nivel de garantía y confiabilidad.

65. 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.

66. Así las cosas, y sin prejuzgar otras situaciones más complejas, 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 EC/OAT, 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.

67. 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), …

68. En estos casos, será el Auditor Jefe asignado quien determinará 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 tecnologías digitales.

69. 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.

70. Por consiguiente, **será posible realizar inspecciones en modo remoto durante las Auditorías de Certificación del ENS** (iniciales o no, 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 EC/OAT** 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.

71. 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.

## 2.10 EN RELACIÓN CON LA UTILIZACIÓN DE SERVICIOS COMPARTIDOS

72. 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 sistemas de información externos que posean la Certificación de Conformidad con el ENS o puedan ser auditados y certificados en tal sentido).

73. 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 no se encuentra comprendida en tal alcance.

74. No obstante, cuanto tales servicios compartidos logren la Certificación de Conformidad, la EC/OAT podrá generar un nuevo Certificado de Conformidad, eliminando la precisión anterior.

## 2.11 EN RELACIÓN CON LAS CERTIFICACIONES Y DISTINTIVOS DE CONFORMIDAD

75. 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.

76. En las Certificaciones de Conformidad expedidas, las EC/OAT 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.

77. 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.

78. La presencia de los Distintivos de Conformidad con el ENS (ya sean Declaraciones de Conformidad 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. 38 del RD 311/2022, de 3 de mayo, obligación que el mismo RD extiende al resto de entidades del ámbito de aplicación de tal norma, incluyendo el sector privado.

79. 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 públicos ofrecidos por medios electrónicos y satisfaciendo los requisitos de transparencia que la gestión de tales servicios exige.

80. 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. 38).

81. Por todo ello, es necesario que, cuando entre las funciones de las EC/OAT se encuentre el seguimiento de que los Distintivos de Conformidad con el ENS expedidos a sus clientes se exhiben adecuadamente, atendiendo a lo dispuesto en la ITS de Conformidad con el ENS, la EC/OAT deberá disponer de una sistemática de actividades periódicas de vigilancia en el que se

indiquen los mecanismos para verificar, al menos semestralmente, su adecuado cumplimiento, y los procedimientos de monitorización y reporte de incidencias previstos.

82. Se establece el plazo de un (1) mes para que el cliente resuelva los incumplimientos detectados en el uso de los Distintivos de Conformidad.

83. Si el incumplimiento se apreciara una vez concluida la auditoría de certificación y expedida la Certificación de Conformidad con el ENS, la EC/OAT expedidora instará a su cliente a solventar tal situación, que, de no ser resuelta, se pondrá en conocimiento del CCN.

84. Cuando el incumplimiento en la adecuada exhibición del Distintivo de Conformidad fuera imputable a un proveedor de la entidad auditada, la EC/OAT deberá instar a su cliente a poner remedio a esta anómala situación que, de no resolverse satisfactoriamente, obligará a la EC/OAT a poner este extremo en conocimiento del CCN, que procederá en consecuencia, conforme a derecho.

85. Asimismo, las Certificaciones de Conformidad expedidas para sistemas de información de organizaciones del sector privado que sean susceptibles de prestar sus servicios desde diferentes ubicaciones, detallarán en dicho certificado las ubicaciones desde las que se prestan los servicios que ampara la Certificación, así como dónde se encuentran situados los CPD con la infraestructura necesaria, quedando implícitamente excluidas las ubicaciones y los CPDs que no consten en el certificado. Dicha localización está sujeta a las matizaciones contempladas en el apartado sobre el alcance de la certificación, en esta misma guía, buscando un equilibrio entre la transparencia y la seguridad física de las ubicaciones.

86. El Anexo A del presente documento detalla el **contenido** que deben poseer las Certificaciones de Conformidad con el ENS, así como otras precisiones relevantes.

## 2.12 EN RELACIÓN CON LA PUESTA A DISPOSICIÓN DEL INFORME DE AUDITORÍA

87. El Distintivo de Conformidad con el ENS, electrónicamente enlazado con la Declaración o la Certificación de Conformidad de la que trae causa, resulta evidencia suficiente para demostrar que el proceso de Autoevaluación o Auditoría de Certificación, respectivamente, a la que se refiera, 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.

88. 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 encontrarse 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 CCN, que valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y a la EC/OAT responsable de la emisión de la antedicha Certificación de Conformidad con el ENS.

## 2.13 EN RELACIÓN CON EL PERÍODO DE VALIDEZ DE LAS CERTIFICACIONES DE CONFORMIDAD CON EL ENS EN SITUACIONES EXCEPCIONALES

89. 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 EC/OAT y sus clientes, el CCN podrá, en el ejercicio de sus competencias, prolongar la vigencia de los Certificados de Conformidad mediante la oportuna comunicación en su página web.

90. La vigencia 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 que permita facilitar el restablecimiento paulatino de las relaciones entre las EC/OAT y sus clientes. Por tanto, la vigencia de los certificados afectados se incrementará en un tiempo determinado por el que haya durado la situación excepcional, que será comunicado formalmente por el CCN.

91. Una vez haya concluido el paréntesis citado, se reactivarán los períodos y plazos para obtener las Certificaciones de Conformidad correspondientes.

92. Si las circunstancias así lo aconsejaran, el CCN podría ampliar el plazo anterior o, en su caso, iniciar un nuevo período de suspensión temporal de la vigencia de las antedichas Certificaciones.

93. 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 EC/OAT podrán solicitar un 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.

94. De conformidad con las competencias del CCN y lo recogido en esta Guía, se permitirá a las EC/OAT solicitar al CCN la extensión de la vigencia de las Certificaciones de Conformidad desde el Portal de Gobernanza (https://gobernanza.ccn-cert.cni.es/) justificando las razones de la solicitud, que se estudiarán en cada caso para conceder las debidas autorizaciones.

95. De esta manera, la entidad interesada podrá solicitar a una EC/OAT, a través de un simple formulario, la ampliación de validez de cualquiera de sus certificados de conformidad. De este modo, dicha EC/OAT gestionará las solicitudes para comprobar las mismas y remitirlas/notificarlas al CCN para que se pueda valorar la viabilidad de la concesión del período de extensión de la vigencia de los certificados recogidos en la solicitud.

## 2.14 EN RELACIÓN CON EL USO DE CERTIFICADOS ELECTRÓNICOS CUALIFICADOS

96. Para facilitar la identificación de las personas y organizaciones involucradas en las preceptivas auditorías del ENS, la emisión de las correspondientes Declaraciones o Certificaciones de Conformidad y con el propósito de satisfacer los requisitos de identificación y firma recogidos en las leyes 39/2015, 40/2015, ambas de 1 de octubre, y sus normas de desarrollo:

    - Los Informes de Auditoría que la EC/OAT entregue a su cliente deberán, al menos, estar firmados electrónicamente por el Auditor Jefe, usando un certificado electrónico cualificado de firma electrónica, según se encuentra regulado en el Reglamento (UE) 910/2014, de Identidad Electrónica y Servicios de Confianza (Reglamento eIDAS).

- Los Certificados de Conformidad con el ENS que la EC/OAT entregue a su cliente deberán estar firmados electrónicamente por la persona designada por la EC/OAT para su firma, usando un certificado electrónico cualificado de firma electrónica de representante, según se encuentra regulado en el Reglamento (UE) 910/2014, de Identidad Electrónica y Servicios de Confianza (Reglamento eIDAS).
- Alternativamente, podrán ser sellados electrónicamente por la EC/OAT usando un certificado electrónico cualificado de sello electrónico, según se encuentra regulado en la antedicha norma europea.

## 2.15 EN RELACIÓN CON EL TRÁNSITO DE UNA CERTIFICACIÓN DE CONFORMIDAD DE UNA CATEGORÍA A OTRA SUPERIOR

97. El tránsito de una Certificación de Conformidad de categoría BÁSICA a otra de categoría MEDIA, o de categoría MEDIA a otra de categoría ALTA, con la exclusiva evaluación de aquellas medidas que no hayan sido evaluadas en la auditoría anterior, podrá ser posible si concurren las siguientes circunstancias:

    - El proceso de realización de la nueva auditoría para la categoría superior, incluyendo la evaluación del Plan de Acciones Correctivas, debe realizarse, íntegramente, dentro del período de validez de la Declaración o Certificación de Conformidad vigente.
    - El alcance del sistema de información que pretende elevarse de categoría debe ser exactamente el mismo que el que fue evaluado para la categoría inferior, garantizándose que no se hayan producido cambios en el sistema de información concernido, y, en todo caso, solo podrá realizarse si no han transcurrido más de seis (6) meses desde la evaluación previa.
    - Se deberá mantener la fecha de la Declaración o Certificación de Conformidad con la que se expidió el certificado precedente, lo que supone que el período de validez de la nueva Certificación será coincidente con el expresado en la Declaración o Certificación anterior.

## 2.16 EN RELACIÓN CON LAS EVALUACIONES QUE CONTEMPLEN UN AUMENTO DE ALCANCE DE LOS SISTEMAS DE INFORMACIÓN

98. Si una evaluación contemplara un aumento del alcance del sistema de información en cuestión, la posibilidad de evaluar exclusivamente las medidas correspondientes a dicho nuevo alcance solo será posible en sistemas previamente certificados contra el mismo Real Decreto, siguiéndose el siguiente protocolo:

    - Es condición “sine qua non” que dicha evaluación debe realizarse antes de cumplidos los seis (6) meses desde que el sistema en cuestión obtuvo la certificación anterior, lo que posibilita que la evaluación solo necesite hacerse sobre las medidas no evaluadas. Transcurridos dichos seis (6) meses, la auditoría será completa.
    - No es posible acometer lo descrito en el punto anterior si lo pretendido es un aumento de alcance que persiga la certificación respecto al RD 311/2022 partiendo de otra del RD 3/2010. En estos casos, la auditoría será completa.

- Se deberá mantener la fecha de la Declaración o Certificación de Conformidad con la que se expidió el certificado precedente, lo que supone que el período de validez de la nueva Certificación será coincidente con el expresado en la Declaración o Certificación anterior.

## 2.17 OBLIGACIONES DE LAS EC/OAT

99. Mantener a disposición del CCN los Informes de Auditoría resultantes de las evaluaciones realizadas, que, de conformidad con lo dispuesto en el RD 311/2022, podrá verificar su contenido e idoneidad.

100. Mantener una permanente vigilancia respecto de las últimas versiones de las Guías CCN-STIC (especialmente esta guía y las comprendidas en la serie 800) que resulten aplicables en cada situación, atendiendo prioritariamente a las Instrucciones Técnicas de Seguridad, parte del ordenamiento jurídico aplicable.

101. Comunicar al CCN cualquier circunstancia que pueda impedir o limitar la calidad de los trabajos de las EC/OAT o la imparcialidad requerida.

102. Realizar la comunicación de la expedición de las Certificaciones de Conformidad con el ENS **dentro de los quince (15) días siguientes a la expedición del Certificado**, a través de la solución AMPARO, asegurándose de que el número de total de medidas incluidas en los certificados se corresponde con la Declaración de Aplicabilidad usada en la auditoría.

103. No todas las organizaciones titulares de sistemas de información con la misma categoría y mismos niveles de seguridad para cada una de sus dimensiones deberán exhibir necesariamente el mismo número de medidas. La confirmación de las medidas aplicables por el equipo auditor es importante, puesto que la antedicha Declaración de Aplicabilidad podrá tener, en relación con las medidas teóricas de aplicación al sistema de información en función de su categoría y niveles en cada dimensión, un número menor de medidas si las excluidas no aplicaran y ello estuviere debidamente justificado, o un número mayor de medidas que podrían añadirse voluntariamente al objeto de mitigar riesgos particulares que se derivaran del preceptivo análisis de riesgos.

104. Asegurarse de que las Auditorías se planifican con tiempo suficiente con respecto a la fecha de caducidad del certificado teniendo en cuenta que los Certificados caducados se eliminarán del repositorio del CCN coincidiendo con la fecha de finalización de su vigencia.

## 2.18 APROBACIÓN PROVISIONAL DE CONFORMIDAD

105. El CCN, con carácter excepcional, podrá expedir 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 del sistema de información auditado.
- 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.

106. La **Aprobación Provisional de Conformidad (APC), que será emitida por el Centro Criptológico Nacional a petición de la EC/OAT**, identificará las condiciones de aplicación de la APC al caso concreto, incluyendo la evaluación de las posibles medidas de mitigación del riesgo o reducción de determinadas funcionalidades, las acciones pendientes para completar el proceso y el marco temporal de validez.

107. 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 que así lo aconsejen.

108. Habiéndose corregido durante el período de validez de la APC las desviaciones detectadas, la EC/OAT de que se trate podrá expedir el correspondiente Certificado de Conformidad en el ENS.

109. En caso de que las desviaciones halladas no hubiesen sido adecuadamente corregidas en el plazo antedicho, el CCN, a propuesta de la EC/OAT de que se trate, podrá retirar la Aprobación Provisional de Conformidad concedida.

110. 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 EC/OAT 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.

111. Por otro lado, la EC/OAT 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.

112. Tras un informe de auditoría no desfavorable, el CCN 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.

113. En estos casos y, tras la emisión de la APC, la EC/OAT 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.

## 2.19 AUDITORÍAS INTERNAS DE CUMPLIMIENTO DEL ENS

114. Si bien el objetivo de la Auditoría de Certificación del ENS es aportar la confianza de que el sistema de información ha sido auditado por un tercero independiente, imparcial y capacitado, la finalidad de la auditoría interna realizada por miembros de la propia organización o por auditores externos en modalidad de prestación de servicios, es la mejora del sistema, ya que se busca confirmar la eficacia del sistema de gestión u obtener información que permita alcanzarla.

115. Pese a que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad no prescribe explícitamente la realización obligatoria de auditorías internas, denominadas en algunos casos auditorías de primera parte, el artículo 27 de dicho cuerpo legal exige la **aplicación de los criterios y métodos reconocidos en la práctica nacional e**

**internacional relativos a la gestión de la seguridad de las tecnologías de la información**; exigencia que, trayendo causa del objeto del ENS, expresado en su artículo 1, se concreta igualmente en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, cuando se hace referencia al grado de confianza en las revisiones de la Dirección y en las auditorías internas del auditado.

116. Por otro lado, un sistema de información de categoría MEDIA y ALTA requiere disponer de un SGSI para la gestión de su seguridad, como se determina en la medida de seguridad [op.pl.2] *arquitectura de seguridad*, dando cabida a cualquier sistema de gestión basado en la mejora continua, ya sea siguiendo el ciclo de Deming (PDCA) o cualquier otro con el mismo fin.

117. Por todo ello, la realización de auditorías internas constituye una actividad fundamental para sistemas de categorías MEDIA y ALTA, y recomendable para los sistemas de categoría BÁSICA, puesto que constituyen la mejor forma de demostrar que el sistema es capaz de ir mejorando, todo ello con independencia de la realización de las preceptivas Auditorías de Certificación.

118. En consecuencia, **es conveniente o necesario -atendiendo a la categoría de seguridad del sistema auditado- realizar auditorías internas anuales de seguimiento, al menos de las medidas de seguridad del Anexo II del ENS implantadas,** actividad auditora que podrá desplegarse a lo largo del tiempo que media entre dos Auditorías de Certificación consecutivas.

119. La ausencia de una auditoría interna o sus elementos documentales esenciales, tales como su Plan de Auditoría, el correspondiente Informe de Auditoría, la no idoneidad del equipo auditor (por falta de formación, competencia o capacidad, o claro conflicto de interés, fundamentalmente), o no elaborar y abordar un Plan de Acciones Correctivas (PAC) respecto a las desviaciones a las que hubiere lugar, a juicio todo ello de la EC/OAT, será tipificada, en el caso de sistemas de información de categorías MEDIA o ALTA, como una **Observación** en el Informe de Auditoría que genere la EC/OAT, desviación que, de persistir, derivará en una **No Conformidad Mayor** en la siguiente Auditoría de Certificación y que provocará que el dictamen global de la auditoría sea, en consecuencia, **DESFAVORABLE**.

120. Así pues, ante un dictamen **DESFAVORABLE**, se requerirá la realización una auditoría extraordinaria de las reguladas en la ITS de Auditoría de la Seguridad, **limitada únicamente a las No Conformidades detectadas, incluyendo la desviación correspondiente a la ausencia de auditoría interna,** en el plazo no mayor de seis (6) meses, a concretar entre la organización auditada y la EC/OAT.

121. Llegado el caso de realizar una **auditoría extraordinaria**, la subsanación de la desviación relativa a la ausencia de auditoría interna exigirá de la organización auditada la presentación del correspondiente **Plan de Auditoría** y el **Informe de Auditoría** y, en su caso, del registro de gestión de las posibles desviaciones encontradas en dicha auditoría interna.

## 2.20 GESTIÓN DEL PROGRAMA DE AUDITORÍAS DEL ENS

122. Las diferentes auditorías de cumplimiento del ENS que deban realizarse a un mismo sistema de información, deben quedar claramente establecidas, planificadas y mantenidas en un **programa de auditoría**, el cual incluirá la frecuencia, métodos, responsabilidades, requisitos de planificación e informes derivados.

123. Deberán armonizarse en dicho programa de auditoría, tanto las auditorías de tercera parte (o de certificación) con las de primera parte (o internas), de modo que **las auditorías internas se realicen antes de cada nueva auditoría de certificación,** en la que se verificará cómo se han materializado aquellas, sus hallazgos y el proceso de planificación y corrección de las desviaciones, en su caso.

124. Para cada auditoría interna, la organización deberá definir el **alcance** de la misma, que deberá ser, al menos, la **evaluación de las medidas de seguridad aplicables del Anexo II del ENS**, en función de los niveles de seguridad, la categoría del sistema y las posibles exclusiones justificadas.

125. Si las auditorías internas se realizaran dentro de cada año natural que media entre dos (2) auditorías de certificación consecutivas, cada una de tales auditorías podría contemplar la evaluación de la mitad de los requisitos exigibles, de forma que en su conjunto abarquen la totalidad de ellos. No obstante, si circunstancias especiales o sobrevenidas (por ejemplo, modificación del sistema de información, etc.) justificaran la realización de una única auditoría interna, deberán evaluarse en ella la totalidad de los requisitos exigibles.

126. Para la materialización de las auditorías internas, la organización debe seleccionar **auditores con la suficiente competencia, experiencia e imparcialidad**, conservando el currículo de los mismos, bajo el principio de quien audita no debería de haber participado en el plan de adecuación, en la implantación del sistema de información auditado, salvo que se establezcan mecanismos de imparcialidad razonables y eficaces.

127. El resultado de las auditorías internas, como el Informe de Auditoría y el posible Plan de Acciones Correctivas (PAC), debe quedar documentado y remitirse para su análisis y eventuales acciones al Comité de Seguridad, al Responsable de la seguridad y al Responsable del Sistema, así como estar a disposición del auditor jefe de la siguiente Auditoría de Certificación que se realice.

128. La auditoría interna deberá ser específica respecto al RD 311/2022 del ENS, no siendo aceptables auditorías internas únicamente orientadas a otras normas o estándares. No obstante, sí que es admisible una auditoría interna del ENS concurrente entre un estándar internacional de seguridad de la información, como la norma ISO/IEC 27001 en su versión vigente, de modo que en su conjunto el alcance abarque todas las disposiciones evaluables del ENS de forma efectiva.

129. Cuando se seleccione el equipo auditor, es muy importante considerar la imparcialidad y ausencia de conflictos de interés del mismo respecto al sistema de información a auditar. Esta cautela afecta tanto si el equipo auditor es interno de la propia organización, como si es externo contratado en modalidad de prestación de servicios.

130. Si la auditoría interna se externaliza en la misma organización que ha colaborado en la implantación del sistema de información y/o en su gestión y gobernanza, el equipo auditor no deberá tener ningún miembro en común con los consultores que han colaborado con dicho sistema, evidenciando la ausencia de conflictos de interés. Caso de ser personal interno, tampoco puede este haber colaborado en la implantación ni en la gestión del sistema.

131. En relación al equipo auditor, éste debe contar con formación y experiencia razonable y demostrable en auditorías internas de seguridad de la información, así como formación especializada en el ENS.

## 2.21 AUDITORÍAS CONTRA PERFILES DE CUMPLIMIENTO ESPECÍFICO

132. Como dispone el Real Decreto 311/2022, de 3 de mayo, en virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se crean los Perfiles de Cumplimiento Específico (PCE), que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

133. El CCN, en el ejercicio de sus competencias y de conformidad con el antedicho cuerpo legal, ha iniciado el proceso de creación y validación de varios Perfiles de Cumplimiento Específico, los cuales han sido publicados en otras tantas Guías de Seguridad CCN-STIC.

134. Al objeto de posibilitar la implantación práctica de los PCE, las EC/OAT acreditadas por ENAC o reconocidas por el CCN, respectivamente, para la realización de evaluaciones de conformidad con el ENS, podrán dar comienzo a sus actividades de evaluación contra los Perfiles de Cumplimiento Específico publicados.

## 2.22 INFORME NACIONAL DE ESTADO DE SEGURIDAD (INES)

135. Todas las organizaciones titulares de sistemas de información públicas, comprendidas en el ámbito de aplicación del ENS (Real Decreto 311/2022, de 3 de mayo) comunicarán, al menos con carácter anual, el estado de las principales variables de seguridad de aquellos sistemas de información que se encuentren bajo su responsabilidad, a través de la cumplimentación del formulario INES.

136. Asimismo, a partir del 5 de mayo de 2024, también las organizaciones del sector privado comprendidas en el antedicho ámbito de aplicación deberán haber cumplimentado el formulario INES.

137. En cualquiera de ambos casos, la no observancia del señalado requisito será considerada una No Conformidad y así será recogida en el correspondiente Informe de Auditoría.

# 3. ENTRADA EN VIGOR

138. Los requisitos expresados en la presente Guía serán plenamente exigibles a su fecha de publicación en la página web del ENS (https://ens.ccn.cni.es/es/certificacion/cocens) o así se determine en una reunión del CoCENS.

[Las exigencias señaladas en los párrafos del 118 al 121 entrarán en vigor el 05.05.2024 coincidiendo con el fin del periodo transitorio de adecuación al RD 311/2022, de 3 de mayo]

[Las exigencias señaladas en el Anexo B, párrafos del 143 al 159, entrarán en vigor el 05.11.2024]

[Las exigencias señaladas en el Anexo C, párrafos del 160 al 178, entrarán en vigor el 05.11.2024]

# ANEXO A. CERTIFICACIÓN DE CONFORMIDAD CON EL ENS

## 1. CONTENIDO DE LA CERTIFICACIÓN DE CONFORMIDAD CON EL ENS ENTRADA EN VIGOR

139. Cada EC/OAT podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema Nacional de Seguridad, y que, en todo caso, deberá mostrar el contenido siguiente[5]:

- Logotipo de la EC/OAT.
- Identificación de la EC/OAT.
- Distintivo de Certificación de Conformidad con el ENS, conforme a lo recogido en los anexos de la Guía CCN-STIC 809.
- Marca de Certificación Acreditada ISO 17065, incorporando el número de acreditación (en caso de Entidades de Certificación acreditadas por ENAC).
- Texto: "Certificado de Conformidad con el Esquema Nacional de Seguridad".
- Texto: "<<EC/OAT>> certifica que el sistema o sistemas de información evaluado(s), todos ellos de categoría <<señalar categoría aplicable: BÁSICA, MEDIA o ALTA>>, y los servicios que se relacionan, de <<Entidad titular [pública o privada] del sistema o sistemas de información evaluado(s), dirección postal>>, han sido auditados y encontrados conforme con las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, según se detalla en el correspondiente Informe de Auditoría de <<dd.mm.aaaa>>:"

  Podrá aparecer, eventualmente: "<<El sistema o sistemas de información evaluado(s) que soporta(n) la tramitación de los servicios descritos en el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (CCN-STIC xxx). >>"
- <<enumerar los sistemas de información auditados y los servicios comprendidos en el alcance de la Certificación, incluyendo, si lo poseen, el nombre o marca con la que se comercializan tales servicios, e incluyendo la ubicación geográfica (dirección postal completa) de los Centros de Proceso de Datos en los que se encuentren los servidores, infraestructuras técnicas centrales y sistemas de back-up de los sistemas de información implicados en la prestación de los servicios comprendidos en el alcance de la Certificación, ya sean propios o de terceros[6]; y, atendiendo a la Declaración de Aplicabilidad en cuestión, el cuadro de los niveles de seguridad auditados para cada una de las cinco (5) dimensiones de seguridad y el número de medidas de seguridad implementadas, de la forma:

[5] Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la certificación expedida.

[6] Si, en casos muy excepcionales y por razones justificadas, la entidad titular de los sistemas de información implicados en la prestación de los servicios comprendidos en el alcance de la Certificación, exhibiera razones que aconsejaran no publicar alguna de las referidas direcciones, la EC/OAT podría omitir tal información en el contenido de la Certificación, comprometiéndose en cualquier caso a revelarla al Centro Criptológico Nacional, quien determinará la posibilidad o no de suministrar dicha información a un usuario legitimado que así lo solicite y que, a juicio del CCN, posea motivos justificados.

| CATEGORÍA DEL SISTEMA | DIMENSIONES DE SEGURIDAD | | | | | MEDIDAS |
|---|---|---|---|---|---|---|
| | C | I | T | A | D | Total de Medidas |
| BÁSICA<br>MEDIA<br>ALTA | n/a<br>Bajo<br>Medio<br>Alto | n/a<br>Bajo<br>Medio<br>Alto | n/a<br>Bajo<br>Medio<br>Alto | n/a<br>Bajo<br>Medio<br>Alto | n/a<br>Bajo<br>Medio<br>Alto | -- |

- Texto: "Número de certificado: <<número de certificado propio de la EC/OAT>>".
- Texto: "Fecha de concesión: <<día>> de <<mes>> de <<año>>". (correspondiente a la fecha en la que se expide la actual Certificación y que se utilizará para señalar el momento inicial para el computo de los dos (2) años señalados por la norma).
- Texto: "Fecha de expiración: <<día>> de <<mes>> de <<año>>". (correspondiente a la fecha hasta la que se mantiene vigente la Certificación, que, en condiciones de normalidad, no podrá ser superior a dos (2) años respecto de la fecha anterior).
- Texto: "Fecha inicial de certificación: <<día>> de <<mes>> de <<año>>. (correspondiente a la fecha en que dicho sistema obtuvo por primera vez la Certificación de Conformidad con el ENS). "Categoría de seguridad:" <<BÁSICA>> o <<MEDIA>> o <<ALTA>>" (correspondiente a la que tenía el sistema en aquel momento).
- Texto: "Emitido en <<ciudad>>, a <<día>> de <<mes>> de <<año>>". (correspondiendo dicha fecha a aquella en la que se emite el certificado. Debería coincidir con la "Fecha de expedición de la presente Certificación de Conformidad").
- (Firma): Nombre, Apellidos y cargo de la persona competente de la EC/OAT (el documento deberá estar firmado con firma electrónica cualificada de persona física representante de persona jurídica (de la EC/OAT) o sello electrónico cualificado.
- A pie de página podrá aparecer, eventualmente: "Certificación de acuerdo a lo establecido en el Modelo µCeENS - Guía CCN-STIC xxx"

140. La guía de seguridad CCN-STIC 809 podrá ofrecer modelos ilustrativos de la Certificación de Conformidad con el ENS, alienados con lo recogido en el presente documento.

**Nota importante**: debe tenerse en cuenta que las subsiguientes certificaciones a la primera de ellas (a las que, informalmente, suele denominarse "renovaciones") deben preverse con suficiente antelación. Salvo en las circunstancias excepcionales o de fuerza mayor que el CCN determine oportunamente, si la Certificación de Conformidad con el ENS se expidiera vencido el plazo de vigencia de la Certificación anterior, se perderá la antigüedad y desaparecerá de la nueva Certificación la "Fecha inicial de certificación".

141. En el caso de que no todas las actividades certificadas dentro del alcance de certificación se presten en todos los centros, se deberá identificar de forma inequívoca la actividad desarrollada en cada centro.

142. En las comunidades autónomas con lengua cooficial se podrán expedir las declaraciones y certificaciones de conformidad y sus respectivos distintivos de conformidad en castellano o bien

en texto bilingüe. En este caso, se expedirán en un solo documento redactado en castellano y en la correspondiente lengua cooficial, en tipos de letra de igual rango, con las especificaciones y diligencias que sobre su texto se establecen en los anexos correspondientes (este criterio también será aplicable en el caso de que se deba emitir el certificado en otros idiomas, como inglés o francés).

# ANEXO B. AUDITORÍA EN ORGANIZACIONES CON MÚLTIPLES EMPLAZAMIENTOS

## 1. INTRODUCCIÓN

143. Este anexo recoge las peculiaridades que habrán de tenerse en cuenta para la realización de auditorías de conformidad con el ENS sobre sistemas de información que se encuentren distribuidos en varios emplazamientos de una misma organización, todos ellos sometidos a la regulación de un mismo sistema de gestión de seguridad de la información.

144. Este anexo:

- No aplica a organizaciones con múltiples emplazamientos donde se utilicen distintos sistemas de gestión, o donde cada emplazamiento deba considerarse como una única organización y auditarse en consecuencia.
- No debe utilizarse en situaciones donde pudieran asociarse o agruparse varias organizaciones o personas jurídicas distintas en torno a otra organización (por ejemplo, una empresa de consultoría o una organización artificial), aunque todas ellas se encuentren sometidas al mismo sistema de gestión.

145. A continuación, se hace referencia a definiciones para tener en cuenta:

- **Emplazamiento**: cada una de las localizaciones físicas o virtuales desde las que la organización presta los servicios soportados por los sistemas de información a certificar.
- **Organización con múltiples emplazamientos**: una organización que tiene implantados los sistemas de información susceptibles de ser certificados según el ENS y que comprende una serie de emplazamientos desde los que se ofrecen los servicios soportados por dichos sistemas, en su totalidad o parcialmente.
- **Función central**: la función que es responsable y controla de forma centralizada el sistema de gestión y los sistemas de la información de la organización de que se trate.
- **Sub-alcance**: alcance de los servicios prestados desde un emplazamiento concreto y soportados por los sistemas de información que se pretende certificar.

**Nota importante**: el alcance de un emplazamiento en concreto podría ser el mismo o solo una parte que el alcance completo de la organización con múltiples emplazamientos.

## 2. APLICACIÓN

146. Cualquier emplazamiento puede ofrecer total o parcialmente los servicios soportados por los sistemas de información a certificar y los diferentes emplazamientos de la organización pueden pertenecer a la misma entidad legal o no, tal y como se desarrolla en el Anexo C del presente documento.

147. , La auditoría de conformidad con el ENS deberá evidenciar, con la precisión exigible a una evaluación muestral, que los sistemas de información implantados en la organización son capaces de lograr los resultados previstos para cada uno de los emplazamientos involucrados, y

que todos ellos, de forma conjunta, son capaces de prestar los servicios expresados en el alcance de la Certificación de Conformidad con el ENS.

148. En el caso de que una organización posea un número considerable de emplazamientos desde los que se ofrezcan servicios muy similares, y estén soportados por los mismos sistemas de información que se pretenden certificar, podrá aplicarse un procedimiento de muestreo razonable y adecuado, según se señala en el epígrafe 2.7 del presente documento. En todo caso, el procedimiento de muestreo no podrá ser aplicable cuando:

    - Los emplazamientos ofrezcan servicios significativamente diferentes en relación con el alcance global que deba aparecer en la Certificación de Conformidad con el ENS, aunque estén soportados por los mismos sistemas de información.
    - El cliente solicita que cada emplazamiento sea auditado.

149. Entre estos dos (2) casos extremos, hay muchas organizaciones con múltiples emplazamientos donde una parte de los emplazamientos ofrecen servicios similares, mientras que otros emplazamientos están dedicados a la prestación de servicios muy específicos que no se realizan en ningún otro lugar de la organización. Al igual que con cualquier proceso de muestreo, el adecuado muestreo entre emplazamientos se limita solo a aquellos emplazamientos que están prestando servicios similares, los cuales son parte del alcance de la organización, y siempre sobre la base de los mismos sistemas de información.

150. El número mínimo de emplazamientos a visitar por auditoría es:

    - **Auditoría inicial**: el tamaño de la muestra debe ser la raíz cuadrada del número de emplazamientos: ($y = \sqrt{x}$), redondeado al entero inmediato superior, donde y = número de emplazamientos a ser muestreados y x= el total número de emplazamientos.
    - **Auditoría de renovación o posteriores**: el tamaño de la muestra debería ser el mismo que en una auditoría inicial. Sin embargo, cuando el sistema haya demostrado ser eficaz durante un ciclo de certificación y a criterio del Responsable Técnico de la EC/OAT, según analice las circunstancias, el tamaño de la muestra podría reducirse a $y = 0{,}8\sqrt{x}$ redondeado al entero inmediato superior. Este criterio se aplicará siempre y cuando no se hayan producido modificaciones en alcance de la certificación y la categoría.

151. Ante situaciones muy específicas, se deberá exponer la situación al CCN quién la analizará y decidirá al respecto.

## 3. REQUISITOS A CUMPLIR POR UNA ORGANIZACIÓN CON MÚLTIPLES EMPLAZAMIENTOS PARA LA CERTIFICACIÓN

152. La organización debe identificar su función central. La función central deberá tener autoridad organizativa para definir, establecer y mantener los procesos de seguridad en toda la organización con un sistema único de gestión. El sistema de gestión único de la organización debe estar sujeto a una revisión centralizada por el Comité de Seguridad y todos los emplazamientos deben estar sujetos al programa de auditoría interna de la organización.

153. La función central será responsable de garantizar que se recojan y analicen los datos de todos los emplazamientos y deberá poder demostrar su autoridad y capacidad para iniciar los cambios organizativos necesarios en relación con, entre otros aspectos:

- Documentación del ENS y cambios en el ENS.
- Revisión de la gestión.
- Reclamaciones.
- Evaluación de las acciones correctivas.
- Planificación de Auditorías internas y evaluación de los resultados.
- Los requisitos legales y reglamentarios aplicables.

## 4. NO CONFORMIDADES Y CERTIFICACIÓN

154. Cuando se encuentren no conformidades, tal y como se definen en ISO/IEC 17065, en cualquier emplazamiento individual, ya sea a través de la auditoría interna de la organización o por la auditoría de certificación, se llevará a cabo una investigación para determinar si otros emplazamientos pudieran estar afectados por la misma desviación.

155. Por lo tanto, la EC/OAT deberá exigir que la organización revise las no conformidades, realizando un análisis de extensión de las mismas, para determinar si indican o no una deficiencia general de los sistemas de información aplicable a otros emplazamientos. Si se determina que así es, se deben realizar acciones correctivas y ser verificadas en toda la organización, incluyendo los emplazamientos individuales afectados. Si no es así, la organización deberá poder demostrar a la EC/OAT la justificación para limitar la aplicación de su acción correctiva.

156. La EC/OAT deberá exigir las pruebas de estas acciones y, si lo considera necesario, modificar el plan de muestreo hasta que quede constancia de que el control se ha restablecido.

157. En el momento del proceso de toma de decisiones, si un emplazamiento presenta una No Conformidad Mayor, se denegará la certificación a toda la organización, incluyendo a todos los emplazamientos, hasta que se adopten medidas correctivas satisfactorias.

158. No será admisible que, para superar el obstáculo planteado por la existencia de una no conformidad en un único emplazamiento, que la organización intente excluir del alcance el emplazamiento "problemático" durante el proceso de certificación.

159. La Certificación de Conformidad con el ENS que finalmente pueda expedirse, recogerá, para información de sus destinatarios, todos los emplazamientos auditados.

# ANEXO C. CERTIFICACIÓN DE CONFORMIDAD CON EL ENS EN ORGANIZACIONES QUE INCLUYEN DIFERENTES ENTIDADES LEGALES

## 1. INTRODUCCIÓN

160. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece, entre sus principios básicos, que el objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

161. A lo largo de dicho Real Decreto y en el resto de las normas jurídicas y guías que lo desarrollan, se refiere, de forma recurrente, a los sistemas de información implantados en las organizaciones dentro de su ámbito de aplicación. Así pues, las EC/OAT certifican los sistemas de información de una organización. Las organizaciones pueden pertenecer tanto al sector público como al sector privado (si prestan servicios competenciales al sector público).

162. Durante el proceso de certificación es imprescindible el asegurar que la certificación se concede a una única organización perfectamente identificada. En este sentido, la definición de "Organización" que aparece en la norma ISO 9000:2015 permite gran flexibilidad en su interpretación:

> *"Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos".*

**Nota importante**: el concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, asociación, organización, organización benéfica o institución, o una parte o combinación de ésta, ya estén constituidas o no, públicas o privadas.

163. Dicha flexibilidad, sin embargo, no debería traducirse en indefinición a la hora de identificar a la organización o relacionar dicha organización con los sistemas de información implantados en la misma que se pretenden certificar.

164. Generalmente, las EC/OAT certifican los sistemas de información (sobre los que se prestan determinados servicios) implantados en una organización que coincide con una entidad pública, con una empresa o con parte de esa entidad pública o de esa empresa. En ese caso, la organización cliente es la propia entidad pública/empresa o departamento de esta (tal y como se define en la cláusula 3.1 ISO/IEC 17065) y, además, coincide con el cliente con el cual la entidad firma el acuerdo de certificación (cláusula 4.1.2 ISO/IEC 17065) y que necesariamente debe tener personalidad jurídica para poder contratar.

165. Sin embargo, en otros casos, la identificación de la organización cliente no es obvia, por ejemplo, cuando la certificación se solicita para un grupo de empresas que actúa como una única organización que es responsable de los sistemas de información o cuando dentro de una única organización hay, por razones legales o fiscales, varias entidades legales que han implantado dichos sistemas de información, pero que actúan, en términos del ámbito de aplicación del ENS, como una única organización.

166. En cualquier caso, debe quedar claro que la certificación alcanza a los sistemas de información implantados en una organización, siendo posible que dicha organización sea parte de una

entidad jurídica (un departamento, una unidad de producción, un emplazamiento concreto, un órgano administrativo, etc.) o, por el contrario, comprenda más de una entidad jurídica.

167. Por todo ello y con el fin de cumplir con lo establecido en la norma ISO/IEC 17065 la EC/OAT, antes de admitir una solicitud de certificación, debe:

    1. **Identificar la organización que tiene implantados los sistemas de información a certificar**. Para ello, la EC/OAT debe identificar de manera inequívoca los limites competenciales de la organización que tiene implantados los sistemas de información a certificar y a sus máximos responsables. La cláusula 7.2 ISO/IEC 17065 hace referencia a información necesaria de la organización. Este proceso debe asegurar también que la organización, una vez se han evaluado satisfactoriamente los sistemas de información concernidos, pueda ser identificada posteriormente de manera inequívoca en el certificado. Esto puede ser especialmente complicado cuando la organización abarca a varias entidades, pero no dispone de un nombre o una identificación única.

       Sin embargo, en algunos casos, la mera identificación de una entidad legal o bien de un conjunto de ellas no tiene por qué asegurar una relación biunívoca de la organización con los sistemas de información a certificar.

    2. **Identificar a su cliente**. Entendido como aquella organización o persona (física o jurídica) responsable ante la EC/OAT de asegurar que se cumplen los requisitos de certificación y con el que firma el acuerdo de certificación (cláusula 4.1.2 ISO/IEC 17065). La EC/OAT deberá asegurarse de que su cliente tiene capacidad legal para obligar a la organización que tiene implantados los sistemas de información y debe asegurarse de que el compromiso de cumplir con los requisitos de certificación, o las partes de este compromiso que correspondan, son adecuadamente transmitidas, con acuerdos legalmente ejecutables, a las entidades que fueran a ser incluidas en el certificado.

       También debe quedar claro en el contrato que la solicitud se realiza en nombre de la organización que tiene implantados los sistemas de información y que, por tanto, puede ser esta, y no el cliente con el que se firma el contrato, a la única a la que se haga referencia en el certificado.

    3. Asegurarse de que en **la organización se han implantado los sistemas de información** que se pretenden certificar y que constituirán el alcance de la eventual Certificación de la Conformidad con el ENS.

168. La EC/OAT debe conservar registros que justifiquen sus decisiones tomadas durante la etapa de revisión de la solicitud, en relación con los tres (3) apartados anteriores.

## 2. EVALUACIÓN

169. Una vez que la EC/OAT haya identificado a la organización cliente, el proceso de certificación debe seguir lo establecido en la norma ISO/IEC 17065 y, en el caso de que la organización cliente esté formada por varias entidades legales usuarias del sistema de información de que se trate, sean o no propietarias del mismo, se deberán evaluar todos los extremos necesarios, incluyendo tanto las medidas comunes como las medidas privativas y exigibles a cada entidad en concreto y comprobar que todas ellas satisfacen, en la parte que le corresponde a cada una de ellas, los

requisitos del ENS (por ejemplo, disponer de una Política de seguridad común o una Normativa Interna común, etc.).

# 3. EMISIÓN DE CERTIFICADOS

170. El proceso de certificación debe seguir el proceso normal establecido en la norma ISO/IEC 17065 y, una vez terminado, deberá concluir con un Certificado de Conformidad con el ENS en el que se identifique a la Organización identificada que es la que tiene implantados los sistemas de información certificados, incluyendo la relación de servicios que presta a través de dichos sistemas de información.

171. Esta Organización podría incluir tanto a la organización propietaria del sistema de información, como a otras entidades legales que, aunque no sean propietarias del sistema de información en cuestión, estén utilizando dicho sistema de información, incluyendo la relación de servicios que cada una de ellas presta en base a dicho sistema de información. Deberá evitarse, en cualquier caso, que pueda entenderse que alguna de dichas entidades legales tiene implantados sistemas de información certificados de manera independiente.

172. También podría incluirse, a título meramente informativo, la denominación del Grupo Empresarial al que, en su caso, pertenecieran las entidades referidas.

## 3.1 DOCUMENTOS DE CERTIFICACIÓN

173. El documento de certificación deberá reflejar los emplazamientos cubiertos por la certificación de múltiples emplazamientos, indicando los servicios prestados desde cada uno de ellos y que son soportados por los sistemas de información certificados.

174. Los documentos de certificación deberán contener el nombre y la dirección de todos los emplazamientos, que reflejen la organización a la que refieren los documentos de certificación.

175. El alcance u otra referencia en estos documentos deben dejar claro que los servicios soportados por los sistemas de información certificados son prestados por los emplazamientos enumerados. Sin embargo, si los servicios de un emplazamiento solo incluyen un subconjunto del alcance de la organización, el documento de certificación debe incluir el sub-alcance del emplazamiento.

176. Cuando se emitan documentos de certificación para un emplazamiento, éstos deben incluir:

- los servicios prestados por ese emplazamiento específico que están cubiertos por esta certificación;
- trazabilidad con el certificado principal, p. e. un código; y
- una declaración que diga que "la validez de este certificado depende de la validez del certificado principal".

177. Bajo ninguna circunstancia, este documento de certificación puede emitirse al nombre del emplazamiento o sugerir que este emplazamiento está certificado, ni debe incluir una declaración de conformidad de los servicios prestados por el emplazamiento.

178. Si alguno de los emplazamientos no cumple con las disposiciones necesarias para la certificación, se retirará el documento de certificación en su totalidad.