centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 802

ENS. Guía de auditorías de cumplimiento

Junio 2025

Edita:

CCN centro criptológico nacional

Fecha de Edición: junio 2025

La Agencia Estatal de Administración Digital del Ministerio para la Transformación Digital y de la Función Pública ha participado en la redacción y revisión de este documento.

ÍNDICE

1. INTRODUCCIÓN

1. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en cumplimiento de lo que dispone el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regula una de las piezas fundamentales que además vertebran lo que se ha dado en llamar la Administración Digital: **la seguridad de los sistemas de información** de las entidades del Sector Público, seguridad entendida como el conjunto de principios básicos y requisitos mínimos requeridos para una protección adecuada de la información tratada y los servicios prestados.

2. Los objetivos de seguridad, alcanzables siguiendo las disposiciones del ENS, no afectan únicamente a los sistemas de información del sector público, sino también a los pertenecientes al sector privado que le aporta soluciones o le presta servicios, según señala el artículo 2.3 del ENS. Para mayor abundamiento, cualquier organización puede decidir libremente cumplir con las disposiciones del ENS, aun cuando no se encuentre en su ámbito de aplicación, como marco o 'framework' de demostrada eficacia para la mejora de la seguridad de sus sistemas.

3. Por otro lado, la única garantía de que las medidas de seguridad aplicadas a los sistemas de información son acordes a los requerimientos de seguridad necesarios para cumplir los precitados principios básicos y requisitos mínimos que determina el ENS en función de la categoría del sistema, o de su postura de seguridad si se acoge a determinado Perfil de Cumplimiento Específico, es mediante la realización de auditorías.

4. El ENS es una norma jurídica certificable, lo que significa que para obtener la Certificación de Conformidad con el ENS debe superarse una auditoría de certificación. Se tratarán en esta guía dos tipos de auditoría: las internas de verificación, persiguiendo apoyar la mejora continua de la seguridad, junto a las externas de Certificación de la Conformidad respecto al ENS con el objetivo de sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado.

5. **La presente Guía desarrolla el proceso de realización de auditorías de cumplimiento respecto al ENS**, de acuerdo con lo que se dispone en el **artículo 31 del ENS** y en el Anexo III sobre auditorías de la seguridad, así como en la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y resoluciones posteriores que la sustituyan.

6. Esta guía también se irá armonizando con las guías **CCN-CERT IC-01/19 ENS. Criterios Generales de Auditoría y Certificación** y **CCN-STIC 809 Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento**, así como con la **ITS de Conformidad**, en base a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad y resoluciones posteriores que la sustituyan.

7. No obstante, en el hipotético caso de observarse inconsistencia o conflicto respecto a lo expresado en distintas guías de las mencionadas en el punto anterior, prevalecerá en primer lugar lo señalado en la guía **CCN-CERT IC-01/19 ENS. Criterios Generales de Auditoría y Certificación**, a no ser que el conflicto surja entre otras guías sin intervenir la IC-01/19, en cuyo caso se atenderá a la de más reciente publicación, en espera de que se vayan actualizando todas ellas y armonizando en su conjunto.

2. OBJETO DE LAS AUDITORÍAS DE CUMPLIMIENTO

8. Lo primero que debe considerarse es la diferencia existente entre una **auditoría de cumplimiento** y una **auditoría técnica**:

   - Una auditoría de cumplimiento verifica que se cumplan las disposiciones de determinada norma jurídica de obligado cumplimiento, como es en este caso el ENS; de una norma de adscripción voluntaria o estándar internacional, como son las normas ISO; o de alguna política interna de la organización, según corresponda. En cambio, una auditoría técnica en el contexto de la seguridad se orienta a evaluar la eficacia técnica de determinadas medidas implantadas en un sistema.
   - El equipo auditor que realiza una auditoría técnica (por ejemplo, un 'pentesting') interactúa directamente con el sistema, mientras que en una auditoría de cumplimiento el auditor entrevista al auditado y le solicita le muestre evidencias habitualmente interactivas (consultar un documento, acceder a una aplicación, visualizar determinados registros, etc.). En las auditorías de cumplimiento el auditor no interactúa con el sistema si no es a través de personal de la organización auditada, ya sea directamente en el ENS estándar, o a través del Portal de Gobernanza en las auditorías relacionadas con Perfiles de Cumplimiento Específicos, portal al que tienen acceso tanto el equipo auditor como los auditados.
   - En una auditoría de cumplimiento, se le puede solicitar al auditado que muestre el resultado de una o de diferentes auditorías técnicas realizada con anterioridad por un tercero, como puede ser el informe de un test de intrusión, de un análisis de vulnerabilidades, etc. A la inversa no es nada frecuente.

9. Como se ha visto en la introducción, las auditorías contempladas en esta guía, orientada a la seguridad de los sistemas de información, son la única forma de verificar el cumplimiento y la correcta implantación de los requisitos del ENS requeridos para garantizar la seguridad de uno o varios sistemas de información en el alcance.

10. Así, el objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados, es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

11. Ya sea en base a una auditoría del ENS *interna de verificación*, o *externa de Certificación de la Conformidad*, se dispone de la guía **CCN-STIC 808 ENS. Verificación del cumplimiento**, que proporciona los elementos necesarios para unificar los criterios de verificación de las medidas de seguridad que sean de aplicación del Anexo II del ENS, junto a lo señalado en su articulado relevante, siempre en armonía con el RD 311/2022.

12. Mención aparte merecen las auditorías de cumplimiento orientadas a organizaciones que se adscriben a determinado **Perfil de Cumplimiento Específico (PCE)** para alguno de sus sistemas de información. En ese caso la auditoría debe realizarse aplicando los criterios y procedimientos que se desarrollan en un anexo independiente de esta guía.

2.1. AUDITORÍAS DE CERTIFICACIÓN DE LA CONFORMIDAD

13. Si la auditoría de cumplimiento a realizar se orienta a la Certificación de la Conformidad con el ENS, entonces permite sustentar la confianza que merece el sistema de información certificado en relación al nivel de seguridad que tiene implantado.

14. Las auditorías de Certificación de la Conformidad con el ENS las pueden realizar los siguientes organismos de certificación:

    a. Una Entidad de Certificación (EC) del sector privado, acreditada por la Entidad Nacional de Acreditación (ENAC), pudiendo certificar a cualquier organización, salvo las limitaciones derivadas de alguna otra legislación aplicable.

    b. Un Órgano de Auditoría Técnica (OAT) del Sector Público, reconocido por el Centro Criptológico Nacional (CCN), pudiendo certificar al sector público en el ámbito de sus competencias y potestades administrativas, según se desarrolla en la guía **CCN-STIC 122 Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS**.

    c. En ocasiones excepcionales, el propio CCN.

15. En todos los casos, el organismo de certificación (que es como designaremos en esta guía tanto a ECs como a OATs) debe de demostrar, para obtener y mantener su acreditación, o su reconocimiento, que dispone de una eficaz gestión de riesgos respecto a la imparcialidad, en evitación de conflictos de interés, así como de la competencia técnica necesaria para la eficaz realización de las auditorías y demás etapas dentro del proceso de Certificación de la Conformidad con el ENS.

16. Según dispone el artículo 38 del ENS, la determinación de la conformidad de los sistemas de información en el ámbito de aplicación del ENS, para cualquier categoría o en base a cualquier Perfil de Cumplimiento Específico, se realizará mediante una auditoría de Certificación de la Conformidad con el ENS, al menos cada dos (2) años, o siempre que se hubieren realizado modificaciones sustanciales en el sistema de información de que se trate, que induzcan a pensar que las medidas adoptadas en el pasado pueden no ser válidas en la actualidad.

17. No obstante, para la determinación de la conformidad de los sistemas de información del ámbito de aplicación del ENS con categoría BÁSICA, como alternativa a la Certificación de Conformidad con el ENS, bastará con la ejecución de un procedimiento de autoevaluación al menos cada dos (2) años que, con carácter ordinario, manifieste el cumplimiento de los requerimientos contemplados en el ENS.

2.2. AUDITORÍAS INTERNAS DE VERIFICACIÓN

18. Dado que el ENS es un marco o '*framework*' de seguridad de la información, un sistema de información de categoría MEDIA o ALTA requiere disponer de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la gestión de su seguridad, como se determina en la medida de seguridad [op.pl.2] sobre arquitectura de seguridad. Bajo esta premisa, cabe decir que cualquier sistema de gestión está basado en la mejora continua, ya sea siguiendo el ciclo de Deming (PDCA) o cualquier otro método con el mismo fin.

19. En este sentido, el objetivo de la **auditoría de certificación de la conformidad** con el ENS es aportar la confianza de que el sistema de información ha sido auditado por un tercero independiente, imparcial y capacitado. Por otra parte, la finalidad de la **auditoría interna de verificación**, ya sea la que realice personal independiente de la propia organización, o bien la realicen 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.

20. Por todo ello, debe entenderse que la realización de auditorías internas de verificación es una actividad necesaria para sistemas de categorías MEDIA o ALTA, así como recomendable para 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, al menos con carácter bienal.

21. En consecuencia, es necesario para los sistemas de categoría MEDIA o ALTA, y conveniente para los de categoría BÁSICA, 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 de la Conformidad con el ENS consecutivas.

22. Las auditorías internas de verificación las puede realizar personal de la propia organización con la competencia necesaria o, en su caso, externalizarse en personal de otra organización con idénticos requisitos de competencia. En ambos casos, siempre que sea posible, se evitará que el referido personal haya tenido vinculación con el sistema de información (por ejemplo, participado en consultoría en los dos últimos años.

3. AUDITORÍAS EXTRAORDINARIAS

23. Con carácter extraordinario deberá realizarse una nueva auditoría, más allá de las regulares exigidas por el ENS, siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas, tal y como dispone el artículo 31 y el Anexo III del ENS.

24. El titular del sistema de información que ha cambiado deberá notificarlo sin demora indebida al organismo de certificación que le haya emitido la Certificación de Conformidad con el ENS vigente, si está certificado, el cual requerirá la información que estime necesaria, estudiará el caso y presentará, si corresponde, una propuesta de auditoría extraordinaria.

25. No es necesario que la auditoría extraordinaria sea completa, es decir, que verifique todas las medidas de seguridad que sean de aplicación al sistema, sino que podrá circunscribirse únicamente a lo relacionado con los cambios habidos en el sistema de información. En otras palabras, basta con auditar aquellas medidas, o incluso aquellos requisitos base o refuerzos obligatorios, susceptibles de haberse visto afectados por las modificaciones acaecidas en el sistema. Será el Auditor Jefe, en coordinación con el Responsable Técnico del organismo de certificación, quién determine qué requisitos deben auditarse y presente el correspondiente Plan de Auditoría.

26. Otra razón para requerirse una auditoría extraordinaria puede ser la intención de incrementar la categoría de un sistema de información ya certificado o pretender incrementar el alcance que abarca dicha certificación.

27. Cuando se realice una auditoría extraordinaria, salvo que ésta sea completa, es decir, que verifique todas y cada una de las medidas de seguridad que sean de aplicación, no se alterará la vigencia del nuevo certificado emitido respecto al que estaba vigente en el momento en que se realizó dicha auditoría extraordinaria.

28. Las auditorías extraordinarias únicamente serán posibles si están referidas al mismo Real Decreto del ENS. Dentro de ellas, las auditorías extraordinarias que no sean completas, únicamente podrán realizarse si no han transcurrido más de seis (6) meses desde la evaluación previa.

3.1. AUDITORÍA EXTRAORDINARIA POR INCREMENTO DE CATEGORÍA

29. El tránsito de una Certificación de Conformidad de categoría BÁSICA a otra de categoría MEDIA, o de categoría MEDIA a otra de categoría ALTA, siempre dentro del período de validez de la certificación vigente, implicará la realización de una auditoría extraordinaria.

30. La auditoría extraordinaria por incremento de categoría no será necesario que sea completa, sino que bastará con la exclusiva evaluación de aquellas medidas de seguridad del Anexo II del ENS, o de aquellos requisitos base y refuerzos obligatorios, que no hayan sido evaluados en la auditoría anterior.

31. La auditoría extraordinaria por incremento de categoría que no sea completa, únicamente podrá realizarse si, además de no haber transcurrido más de seis (6) meses desde la evaluación previa, se mantiene el alcance que fue evaluado para la categoría inferior y si no se han producido cambios relevantes en el sistema de información concernido.

3.2. AUDITORÍA EXTRAORDINARIA POR INCREMENTO DE ALCANCE

32. Para **incrementar el alcance** de una certificación existente, una posibilidad es esperar al vencimiento de la certificación y realizar la nueva auditoría regular con el nuevo alcance, o bien adelantar la fecha de dicha auditoría regular. En ambos casos la auditoría a realizar siempre será completa.

33. Otra posibilidad es realizar una auditoría extraordinaria, evaluando exclusivamente las medidas de seguridad en lo relativo a los activos que se incorporen al nuevo alcance más amplio. A modo de ejemplo, la medida de seguridad [org.1] Política de Seguridad es habitual que no se reevalúe en un incremento de alcance al ser común a todos los sistemas de la organización.

34. La auditoría extraordinaria por incremento de alcance no será necesario que sea completa, sino que bastará con la exclusiva evaluación de aquellas medidas de seguridad del Anexo II del ENS, o de aquellos requisitos base o refuerzos obligatorios, en lo correspondiente a la parte que no haya sido evaluada en la auditoría anterior, incluyendo asimismo aquellos requisitos ya evaluados, pero que puedan impactar en el nuevo alcance.

35. La auditoría extraordinaria por incremento de alcance que no sea completa, únicamente podrá realizarse si, además de no haber transcurrido más de seis (6) meses desde la evaluación previa, se mantiene la categoría del sistema que fue evaluado para el alcance anterior y si no se han producido cambios relevantes en el sistema de información concernido.

36. Respecto a la **reducción de alcance**, ésta no implica la realización de una auditoría extraordinaria siempre que se mantenga la categoría del sistema, sino únicamente el trámite administrativo de emitir un nuevo certificado con el nuevo alcance más reducido (debe ser un subconjunto del anterior) manteniendo el vencimiento y demás parámetros, salvo la fecha de emisión. La reducción de alcance puede realizarse en cualquier momento de la vigencia del certificado, siendo en la práctica un supuesto infrecuente.

4. SOBRE EL EQUIPO AUDITOR

37. Quienes constituyen el equipo auditor deben disponer de la competencia y la imparcialidad necesaria para que el informe de auditoría que emitan sea confiable.

38. En una **auditoría de Certificación de la Conformidad con el ENS**, cuyo objetivo principal es evidenciar la conformidad del sistema de información auditado, dicha confiabilidad es irrenunciable.

39. En una **auditoría interna de verificación**, cuyo objetivo es colaborar en la mejora continua del sistema, la confiabilidad es asimismo importante, aunque se puede permitir, únicamente en casos excepcionales y debidamente justificados, especialmente en aquellas organizaciones de reducidas dimensiones y que no dispongan de suficientes recursos propios para realizarlas y tengan dificultades para contratarlas externamente, minimizar el nivel de exigencia siempre que se evidencie la calidad y el cumplimiento de los objetivos de la auditoría. La precitada reducción en el nivel de exigencia no está permitida para auditorías internas de verificación a sistemas de información de categoría ALTA o MEDIA, pudiendo estudiarse para las realizadas a sistemas de categoría BÁSICA o a sistemas basados en algún Perfil de Cumplimiento Específico (PCE) cuyos requisitos no sean superiores en ningún caso a los establecidos para la categoría BÁSICA.

40. En el caso de los organismos de certificación, ya sean éstos una EC o un OAT, es la ENAC, o eventualmente el CCN, quienes verifican cada año su competencia e imparcialidad, así como que dispongan de los recursos suficientes para realizar las auditorías de Certificación de la Conformidad con el ENS con garantías, según se detalla en el apartado correspondiente de la guía **CCN-CERT IC-01/19 Criterios generales de auditoría y certificación**.

41. Para las auditorías internas de verificación, la comprobación de los conocimientos y, en su caso, la debida imparcialidad del equipo auditor, recaerá en la propia organización titular de los sistemas de información auditados, quien deberá verificar tales extremos en base a solicitar, por ejemplo, el CV del auditor y un extracto de su experiencia previa en la realización de auditorías del ENS y/o de otras normas de seguridad aplicadas sobre sistemas de información. Para las auditorías de Certificación de la Conformidad con el ENS, dicha verificación corresponde al organismo de certificación a quién se solicitan dichas auditorías.

42. Los integrantes del equipo auditor deberán haber firmado, antes de iniciarse la auditoría, las preceptivas cláusulas de confidencialidad, incluyendo las cláusulas derivadas de la legislación vigente sobre tratamiento de datos de carácter personal. En el ANEXO C de esta guía se incluye un modelo aplicable.

43. En el ANEXO A de esta guía se determinan los requisitos que deben cumplir los miembros del equipo auditor.

4.1. EQUIPO AUDITOR EXTERNO A LA ORGANIZACIÓN

44. El equipo auditor de un organismo de certificación, ya sea este una EC o un OAT, así como el de otra organización que ofrezca servicios de auditoría interna de verificación del ENS (aunque se trate de una sociedad unipersonal, o de un profesional autónomo o freelance), deberá estar compuesto por profesionales (Auditor Jefe, posibles auditores y, en su caso, expertos técnicos) que garanticen que se dispone de los conocimientos suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de la auditoría.

45. En este caso, además, será imprescindible la ausencia de conflicto de interés entre el personal del equipo auditor y la entidad auditada, exigiéndose que no haya tenido vinculación con el sistema de información a auditar (por ejemplo, participado en consultoría) durante, al menos, los dos últimos años.

46. Para asegurar la independencia objetiva del equipo auditor, las tareas de auditoría, ya sea esta interna de verificación o de Certificación de la Conformidad con el ENS, no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares, incluyendo recomendaciones particulares sobre productos o soluciones comerciales concretas, entre otras.

4.2. EQUIPO AUDITOR INTERNO DE LA ORGANIZACIÓN

47. En las auditorías internas de verificación, si el equipo auditor es interno, deberá procurarse que sea independiente de los sistemas de información o servicios que sean objeto de la auditoría. Por ejemplo, perteneciendo a otra área o departamento, de modo que se asegure su independencia y objetividad.

5. EL ALCANCE DE LA AUDITORÍA

48. El alcance de la auditoría debe estar claramente definido, documentado y consensuado entre el equipo auditor y el titular del sistema de información auditado, ya sea su objetivo la realización de una auditoría de Certificación de la Conformidad con el ENS o de una auditoría interna de verificación.

49. La realización de auditorías podrá ser requerida por la organización, a iniciativa de sus responsables con competencias sobre la seguridad del sistema de información objeto de éstas. Por lo tanto, es necesario establecer con claridad antes de concretar la realización de la auditoría, el objetivo, el alcance y el criterio de la misma.

50. Considerando que las redes de comunicaciones y sistemas, especialmente del Sector Público, tienen interconexiones con entidades públicas y privadas, la descripción detallada del alcance de la auditoría es esencial al ser necesario establecer claramente la extensión y el límite hasta dónde se audita.

51. Si parte del alcance está externalizado en los sistemas de información de otra organización, estando ya Certificados de Conformidad con el ENS de igual o superior categoría en toda esa parte, el equipo auditor, teniendo en cuenta criterios como la responsabilidad compartida o la necesidad de verificar ciertas medidas de seguridad (control de accesos, privilegios de cuentas, etc.) determinará para qué medidas es suficiente el certificado de Conformidad de la organización en la que esté externalizado parte de ese alcance y en cuáles será necesario realizar alguna comprobación.

52. Por el contrario, si la parte externalizada del alcance no está certificada, deberá ser evaluada, siempre teniendo en cuenta el apartado 'EN RELACIÓN CON LA UTILIZACIÓN DE SERVICIOS COMPARTIDOS' cuando éstos son ofrecidos por la Administración General del Estado (AGE) o, en su caso, por las Administraciones

Territoriales competentes, según consta en la guía **CCN-CERT IC-01/19 Criterios generales de auditoría y certificación**.

53. En el caso de grupos empresariales, conjunto de entidades vinculadas a determinado organismo público u otras formas de organizaciones más complejas, el alcance de la auditoría (siempre que sea global) debe reflejar qué servicios presta cada una de las organizaciones que constituyen el grupo de entre todos los servicios sustentados por los sistemas de información comunes, cuando los referidos servicios no sean los mismos para cada una de las organizaciones. Puede consultarse el Anexo C. Certificación de Conformidad con el ENS en organizaciones que incluyen diferentes entidades legales de la guía **CCN-CERT IC-01/19 Criterios Generales de Auditoría y Certificación**.

54. Las medidas de seguridad a auditar pueden ser de naturaleza diversa, comprendiéndose entre ellas las medidas de seguridad técnicas (físicas y lógicas) y no técnicas. Para facilitar su implantación y posteriores auditorías el ENS ha dividido las 73 medidas que constituyen su Anexo II en tres tipologías: marco organizativo, marco operacional y medidas de protección, subdividiéndose a su vez las dos últimas en grupos, como son el de planificación, control de acceso, etc. Por lo tanto, como parte de la definición del alcance de la auditoría, es necesario antes de comenzarla, identificar los elementos que entran dentro de ésta.

55. Es imprescindible que se defina, de forma previa al inicio de la auditoría, si existe alguna información que, por indicación del Responsable del Sistema, el Responsable de la Información, el Responsable del Servicio o el Responsable de la Seguridad, no estará accesible al equipo auditor, debiendo éste evaluar si ésta es una limitación para realizar la auditoría de acuerdo a lo previsto en el artículo 31 del ENS. Si es así, y se decide continuar con el proceso de auditoría, esta limitación debe reflejarse en el Informe de Auditoría.

6. METODOLOGÍA Y DESARROLLO DE UNA AUDITORÍA DE CUMPLIMIENTO

6.1. METODOLOGÍA

56. Las auditorías de cumplimiento, ya estén orientadas a la seguridad de los sistemas de las tecnologías de la información y las comunicaciones, o a evaluar otros aspectos, deben realizarse de una forma metodológica que permita identificar claramente:

- El objetivo, alcance y el criterio de la auditoría.
- Los recursos necesarios y apropiados para realizar la auditoría (especialmente el equipo auditor).
- Las debidas comunicaciones con los responsables de la organización que soliciten la auditoría.
- La determinación de aquellos requisitos de información que se consultarán previamente a la elaboración del plan de auditoría.
- El establecimiento de un Plan de Auditoría detallado con las actividades de auditoría previstas y quienes participarán en ellas.

- La presentación de los hallazgos de la auditoría, a medida que surjan, a las personas involucradas para su confirmación, de modo que puedan aportar nuevas evidencias clarificadoras ante su desacuerdo, sin esperar al informe final.
- La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del ENS.
- La confección, presentación y emisión formal del Informe de Auditoría.

57. La metodología aplicada debe permitir comprobar, a través de los registros y evidencias de auditoría, la consecución de estos pasos, las limitaciones que se hayan podido producir en el desarrollo de las tareas, y las actividades realizadas.

6.2. TIEMPOS DE AUDITORÍA

58. Según se establece en el apartado 'EN RELACIÓN CON EL TIEMPO DE AUDITORÍA' de la guía **CCN-CERT IC-01/19 Criterios generales de auditoría y certificación**, se deben determinar adecuadamente los tiempos necesarios para realizar las auditorías de cumplimiento, en sus diferentes fases, habitualmente agrupadas en tres conceptos diferenciados: estudio documental previo, auditoría material (ya sea presencial o remota) y otras actividades internas (elaboración del Plan de Auditoría, elaboración del Informe de Auditoría, revisión del posible PAC, etc.).

59. Para ello se observará, especialmente por parte de los organismos de certificación, determinados factores de cálculo que se desarrollan en la precitada guía IC-01/19, a la vez que el número de jornadas de auditoría resultantes puede ser objeto de incremento/decremento atendiendo a otros factores, que asimismo en ella se detallan, que en ningún caso influirán en más de un 20% respecto al cálculo inicial.

60. El número de jornadas total de auditoría 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 las medidas de seguridad (requisitos base y refuerzos obligatorios) que, en consecuencia, sea necesario auditar.

61. En organizaciones en las que a sus sistemas de información, por cualquier razón, se apliquen simultáneamente diferentes normas (como puede ser el RD 311/2022 y la norma ISO/IEC 27001:2022), nos encontraríamos ante una 'auditoría concurrente', denominada también 'auditoría combinada', en la que, en determinadas circunstancias, se podría apreciar un porcentaje de coincidencia elevado en la evaluación de determinadas medidas de seguridad, ya sean estas análogas en todo o en parte, en cuyo caso se podrá reducir la duración estimada para la auditoría concurrente de modo que sea hasta un 35% inferior a la suma de los tiempos de realización de ambas auditorías de cumplimiento por separado.

62. En la referida guía IC-01/19 se han establecido asimismo unos tiempos mínimos en función de la categoría del sistema evaluado. Ante la determinación de tiempos de auditoría anormales por parte de un organismo de certificación, el Centro Criptológico Nacional, en el ejercicio de sus competencias, podrá examinar las

circunstancias argumentadas para tal asignación, adoptando las medidas que, en derecho, procedan.

63. Si los tiempos de auditoría anormales corresponden a una auditoría interna de verificación, será el organismo de certificación quién en su auditoría de Certificación de la Conformidad con el ENS posterior los analice y, en su caso, determine una desviación al respecto.

6.3. FASES RELEVANTES EN UNA AUDITORÍA DE CUMPLIMIENTO

64. Distinguiremos una serie de fases en las auditorías de cumplimiento, al considerarse éstas un proceso en sí mismas. Las fases en las que se incide en esta guía son comunes, tanto a las auditorías internas de verificación, como a las auditorías de Certificación de la Conformidad con el ENS, aunque habrá otras fases en que difieran, como puede ser la revisión del expediente completo de certificación (incluyendo el informe de auditoría y el PAC) y la adopción de la decisión de certificar, o no, muy relevantes en un organismo de certificación.

65. Las fases que pueden identificarse, siempre partiendo de que se han suscrito los correspondientes acuerdos entre la organización auditora y la auditada, en el caso de diferir éstas, así como el que se disponga del conocimiento de la mínima información necesaria sobre el sistema de información a auditar (y su organización titular) para poder planificar y materializar eficazmente la auditoría, son:

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

    Las iremos analizando todas ellas en esta guía a lo largo de los apartados que siguen.

6.4. DESIGNACIÓN DEL EQUIPO AUDITOR

66. Debe designarse al equipo auditor que se encargará de materializar la auditoría partiendo de su objetivo, alcance y criterio. En todos los casos el equipo estará constituido, como mínimo, por un **Auditor Jefe**, que puede actuar en solitario, siendo éste el caso más frecuente.

67. Ante auditorías de cumplimiento de sistemas de información con un amplio alcance (por ejemplo, varias sedes, varios CPDs) y con un nivel de complejidad elevado, el Auditor Jefe se apoyará en uno o en varios **auditores**.

68. Debe tenerse asimismo en consideración que, en el desarrollo de la actividad auditora, el equipo auditor deberá revisar temas tecnológicos diversos, como los relacionados con la electrónica de red, sistemas abiertos o propietarios, mecanismos de cifrado, firma electrónica, gestión de documentos electrónicos,

planes de continuidad, seguridad de las comunicaciones, u otros de naturaleza análoga.

69. Es por esta razón que, una vez analizada la complejidad tecnológica, es posible que el Auditor Jefe considere necesaria la incorporación de **expertos técnicos** en determinadas materias. Entre estos expertos técnicos también es posible que sea necesario incluir profesionales con perfiles especializados tales como:

    - expertos con conocimientos jurídicos;
    - expertos en Procedimiento Administrativo;
    - expertos en Archivística, gestión documental y conservación a largo plazo;
    - Expertos tecnológicos (Blockchain, IA, etc.);
    - y otros que se estimen pertinentes en función del sistema auditado.

70. Los expertos estarán sujetos a las mismas reglas y deberes que el resto del equipo auditor (planificación, evidencias de auditoría, supervisión por el Auditor Jefe y cláusulas de confidencialidad y ausencia de conflictos de interés).

71. En cualquier caso, siempre la organización responsable del sistema de información auditado deberá conocer, con la debida antelación, quiénes constituirán el equipo auditor al efecto de poder recusar a alguno de sus miembros si se vislumbra riesgo a la imparcialidad ante un posible conflicto de interés debido a vinculaciones, tanto presentes, como a lo largo de los dos últimos años.

72. Como se ha mencionado en puntos anteriores, los componentes del equipo auditor deberán evidenciar, además de su imparcialidad, que poseen una formación suficiente en auditoría de sistemas de información, y en seguridad, sin obviar los requisitos más restrictivos que se requieren para ser cualificado como Auditor Jefe en un organismo de certificación, según se detalla en la guía **CCN-CERT IC-01/19 Criterios generales de auditoría y certificación**.

6.5. ESTUDIO DE LA DOCUMENTACIÓN DEL SISTEMA

73. Para la correcta realización de la auditoría de cumplimiento, de forma previa a la auditoría material debe realizarse asimismo el estudio de la documentación relevante del sistema por parte del equipo auditor. Para ello, la organización cuyo sistema de información será auditado, debe proporcionar al Auditor Jefe acceso a la misma, teniendo en consideración que todos los miembros del equipo auditor han suscrito una cláusula de confidencialidad.

74. Entre la información general del sistema a consultar, debe revisarse:

    - Documento que contenga una descripción lo más detallada posible del sistema a ser auditado.
    - Documento de valoración de los servicios soportados por el sistema, junto a la información que estos manejan, en las 5 dimensiones de la seguridad, suscrito por los responsables de la información y de los servicios.
    - Documento de categorización del sistema, suscrito por el Responsable de la Seguridad.

- Con independencia de que el sistema auditado sea de titularidad pública o privada, documento resultante de haber cumplimentado el informe de estado de la seguridad (INES).
- Declaración de Aplicabilidad, conteniendo las diferentes medidas de seguridad del Anexo II del ENS, con indicación de si éstas son de aplicación, o no, suscrita por el Responsable de la Seguridad. Si se han aplicado medidas compensatorias, desarrollo de las mismas según determina la guía **CCN-STIC 819 Medidas Compensatorias**.
- Relación de documentos del sistema incluyendo normas internas y procedimientos.
- Informe de la última auditoría interna de verificación realizada y, en su caso, externa de Certificación de la Conformidad con el ENS, así como el Plan de Acciones Correctivas (PAC) aportado o el registro que se disponga de seguimiento de las acciones correctivas derivadas de las auditorías.

75. Respecto a las diferentes medidas de seguridad que sean de aplicación en función de la categoría del sistema y/o de los niveles de seguridad de cada una de las dimensiones de la seguridad, así como su no aplicación por decisión justificada de la organización auditada, deberían consultarse asimismo los siguientes documentos, sin menoscabo de adicionar otros que pueda disponerse y se consideren relevantes. Concretamente:

- La Política de Seguridad de la Información (PSI) debidamente aprobada, así como Actas del Comité de Seguridad relevantes y, en su caso, documentos de aceptación de las personas designadas para los diferentes roles del ENS.
- Documento resumen del Análisis de Riesgos y Plan de Tratamiento de Riesgos (PTR) para aquellos evaluados como inaceptables. Documento o Acta de aprobación del umbral o apetito de riego, de las correspondientes acciones de tratamiento y de los riesgos residuales resultantes tras su aplicación.
- Mapas de arquitectura, líneas de defensa, cableado, sensores, alarmas, etc. Alguna de esta información, por motivos de seguridad, podría obviarse en el estudio documental y ser mostrada por la organización auditada durante la auditoría material.
- Procedimiento de compras o adquisiciones.
- Procedimiento de gestión de la capacidad e indicadores asociados a la monitorización.
- Normativa general de control de acceso. Normativa de acceso remoto.
- Procedimiento de altas y bajas de usuarios.
- Procedimiento de gestión de derechos de acceso.
- Inventario de activos. Relación de componentes certificados, de haberlos.
- Guías de bastionado (configuración de seguridad de las diferentes tipologías de activos). Evidencias de los bastionados realizados.
- Procedimiento de parches y actualizaciones de seguridad.
- Procedimiento de gestión de cambios.
- Procedimiento de protección frente a código dañino.

- Procedimiento de gestión de incidentes. Evidencia del registro de incidentes de seguridad.
- Relación de los diferentes registros de actividad junto a su período de retención y tratamiento.
- Registro de proveedores en el alcance del ENS, con indicación de su POC de seguridad. Certificaciones o Declaraciones de Conformidad con el ENS de proveedores, así como otras certificaciones de seguridad.
- Registro de seguimiento de los Acuerdos de Nivel de Servicio (ANS/SLA) de proveedores.
- Relación de los posibles sistemas de proveedores interconectados con el propio sistema y su descripción y características.
- Bastionado o protección de servicios contratados en la Nube, de emplearse.
- Análisis de Impacto en los Servicios (BIA) con obtención de RTO y RPO.
- Si procede, Plan de Continuidad y Planes de Recuperación de Datos (DRP) asociados. Registros de pruebas periódicas.
- Métricas asociadas al grado de implantación de las medidas del anexo II del ENS, métricas relacionadas con la resolución de los incidentes de seguridad y métricas de asignación y uso de recursos en seguridad.
- Extracto de la Relación de Puestos de Trabajo (RPT) y Fichas descriptivas de los puestos de trabajo en el ámbito del ENS, incidiendo en responsabilidades y/o obligaciones respecto a la seguridad.
- Modelo de cláusulas de confidencialidad de empleados y acuerdos de confidencialidad suscritos con organizaciones proveedoras.
- Registro de acciones de concienciación y formación en seguridad realizadas y previstas.
- Normativa de uso de los medios puestos por la organización a disposición de los empleados. Por ejemplo, repositorios compartidos, correo electrónico, navegación web, equipos portátiles, impresoras, puesto de trabajo despejado, bloqueo de los terminales de los usuarios, etc.
- Normativa de uso de soportes (marcado, criptografía, transporte, custodia, borrado y destrucción).
- Metodología o normativa de desarrollo seguro, si procede.
- Normativa de realización de pruebas para la aceptación y puesta en servicio de aplicaciones.
- Normativa de calificación de la información.
- Política de firma electrónica.
- Normativa respecto a la revisión / eliminación de metadatos. Guía o procedimiento de verificación y borrado si no se dispone de herramientas automatizadas.
- Procedimiento de copias de seguridad.

6.6. PLAN DE AUDITORÍA

76. Tras el estudio de la documentación del sistema, el Auditor Jefe elabora el llamado Plan de Auditoría que consiste en la planificación detallada de la fase de auditoría material.

77. Los organismos de certificación antes de aceptar la realización de un proceso de certificación solicitan a la organización cuyo sistema de información será auditado que les cumplimente un formulario de toma de datos donde se recaba información detallada del sistema a ser auditado. Asimismo, muchas consultoras, antes de aceptar la realización de una auditoría interna de verificación en modalidad de prestación de servicios, también le hacen cumplimentar a su cliente un formulario de toma de datos. Si el formulario es completo, ya serviría como punto de partida para elaborar el Plan de Auditoría, aunque siempre es mejor acabar de concretarlo una vez estudiada la documentación detallada del sistema.

78. El Plan de Auditoría consta de al menos dos partes diferenciadas. Una parte donde se identifica el expediente de auditoría y se relaciona información identificativa de la evaluación: objetivo, criterio, detalle del alcance, fechas, organización titular del sistema, sedes y CPDs a ser auditados con su dirección, equipo auditor, etc.

79. Otra parte es el detalle cronológico, día a día, de las actividades y entrevistas a realizar por parte del equipo auditor en la auditoría material. Se pueden agrupar éstas por fechas de auditoría, siendo preferible concretar más, por ejemplo, mediante agrupaciones de medidas de seguridad del Anexo II y articulado relevante del ENS a lo largo de cada jornada de auditoría. Es importante incluir la reunión de apertura, tiempos de descanso y de almuerzo, posibles desplazamientos entre centros (si se producen éstos durante la jornada), la reunión final del equipo auditor, la reunión de cierre, etc.

80. Es habitual que cada fila en el cuerpo del Plan de Auditoría contenga la fecha, el intervalo horario, las iniciales del auditor que auditará esa parte, las medidas o el aspecto del sistema a ser auditado y el personal que será entrevistado. En auditorías mixtas es importante indicar si cada parte se auditará presencialmente o en remoto (on-line).

81. Como es sabido, las medidas de seguridad a auditar pueden ser de naturaleza diversa, habiéndolas de técnicas (físicas y lógicas) y no técnicas. Para facilitar su implantación y posteriores auditorías el ENS ha dividido las 73 medidas que constituyen su Anexo II en tres tipologías: marco organizativo, marco operacional y medidas de protección, subdividiéndose a su vez las dos últimas en grupos, como son el de planificación, control de acceso, etc. Por esta razón, hay auditores jefes que elaboran el plan de auditoría a nivel de grupos de medidas, asignándoles un intervalo temporal a cada grupo.

82. Este proceder no es el único posible, al no ser necesario auditar las medidas de seguridad del Anexo II correlativas, ni siquiera por orden de aparición de los grupos. Cada Auditor Jefe, de común acuerdo con la organización auditada, podrá decidir el orden y las agrupaciones más lógicas a nivel de medidas para cada auditoría y

contexto en el que ésta se desarrolle. Por ejemplo, un criterio es unificar las intervenciones de determinado personal crítico a ser auditado, agrupando las medidas concretas en que participará, aunque éstas no pertenezcan al mismo grupo, evitando un devenir de intervenciones puntuales que le impidan sus tareas habituales durante toda la extensión de la auditoría.

83. En relación al personal que será entrevistado, es frecuente que el Auditor Jefe no lo conozca en detalle en el momento de elaborar el Plan de Auditoría, por lo que una buena práctica consiste en facilitar una primera versión en texto editable para que el auditado anote qué personas participarán en cada una de las actividades de la auditoría en función de sus desempeños, competencias y disponibilidad.

84. También es posible que, en base a la disponibilidad del personal, el auditado solicite reorganizar la agenda de entrevistas, consensuando Auditor Jefe y auditado un nuevo Plan de Auditoría que una vez acordado será convertido en PDF, firmado por el Auditor Jefe y facilitado al auditado.

85. Debe procurarse siempre seguir el Plan de Auditoría durante la fase de auditoría material. No obstante, en ocasiones ocurren imponderables como el caso en que un entrevistado relevante deba atender a una urgencia y no pueda participar, o bien que sufra cualquier otra indisponibilidad insubsanable. Por ello, al inicio de cada jornada de auditoría, es una buena práctica revisar la parte del plan para esa jornada y si se adelantan imponderables que impidan su seguimiento, reestructurarlo de la mejor manera posible dentro de la propia jornada, o incluso intercambiando actividades con otra jornada posterior. En cualquier caso, no debe alterarse la duración total de la auditoría y al finalizar ésta es recomendable que el Auditor Jefe proporcione al auditado la nueva versión definitiva del Plan de Auditoría, para que pueda adjuntarse al expediente y quede constancia de cómo ha transcurrido realmente la misma.

6.7. REALIZACIÓN DE LA AUDITORÍA MATERIAL

6.7.1. DESARROLLO DE LA AUDITORÍA

86. La auditoría material se realizará siguiendo el Plan de Auditoría consensuado con el auditado. Si es en todo o en parte en remoto se recomienda establecer la conexión con margen suficiente para solventar problemas de acceso por parte de algún participante, siendo otra opción realizar una breve prueba de conexión con anterioridad. Es habitual emplear la plataforma de videoconferencia del propio auditado, aunque no necesario.

87. El equipo auditor no debe improvisar el detalle de la auditoría material, por lo que una buena sistemática es disponer de una plantilla del Cuaderno del Auditor, o directamente de una plantilla del Informe de Auditoría, según se organice, donde consten todos los requisitos base y refuerzos obligatorios a ser evaluados de cada una de las medidas de seguridad del Anexo II, así como requisitos destacables del articulado relevante el ENS.

88. Ya se trate de una auditoría interna de verificación, o de una auditoría de Certificación de la Conformidad con el ENS, se recomienda basarse en la guía **CCN-STIC 808 ENS. Verificación del cumplimiento**. Es importante destacar que los requisitos marcados en color gris en dicha guía se consideran nucleares, por lo que siempre deben ser evaluados por el equipo auditor.

89. Lo primero que se realiza es la **reunión de apertura** donde se presenta el equipo auditor, se refresca el alcance, objetivos y criterio de la auditoría y se confirma con todos los presentes el Plan de Auditoría. También se presenta una visión global del desarrollo previsto de la auditoría, se acuerda la logística entre centros y posibles medidas de Prevención de Riesgos Laborales (PRL) de haberlas, se recuerda la confidencialidad de la auditoría, se aportan comentarios relevantes respecto a la revisión documental realizada previamente, así como clarificaciones, ruegos y preguntas.

90. En el desarrollo de la auditoría material el auditor frecuentemente recurrirá al **muestreo**, por ejemplo, solicitando ver una muestra de incidentes de seguridad registrados, de cuentas de acceso de usuarios, de activos en el inventario, de peticiones de cambios en el sistema, de registros de autorizaciones solicitadas, etc. Es importante que se intente cubrir con el tamaño de la muestra las casuísticas más significativas, siempre procurando ajustarse a los tiempos previstos en el Plan de Auditoría. Será el equipo auditor quién elegirá la muestra y la consensuará con el auditado.

91. Un caso particular son las visitas a los CPDs, cuyo muestreo, caso de ser necesario, se realizará en base a la raíz cuadrada del número total de éstos, redondeado al entero superior. Es decir, si la organización auditada dispone en el alcance de ocho (8) CPDs, se auditará al menos tres (3) de ellos, auditándose otros tres en sucesivas auditorías que deban realizarse para acabar así visitándose todos. No obstante, este planteamiento es únicamente válido siempre que el conjunto total de CPDs sea homogéneo, es decir, que todos los CPDs sean de tamaño y características similares y, en el caso de estar externalizados en algún proveedor, que éste sea el mismo para todos ellos. Si no es así, la muestra debe recoger al menos dos elementos de cada una de las distintas tipologías (de existir), debiendo incrementarse si no se cumple esta condición a los efectos de que el muestreo aporte confianza sobre todo el sistema y no únicamente sobre la muestra auditada.

92. En auditorías de renovación de la Certificación de la Conformidad con el ENS, teniendo en cuenta los mismos condicionantes que en el punto anterior, se podrá aplicar un factor reductor del 20%, es decir, multiplicar por 0,8 el valor obtenido de la raíz cuadrada del número total de CPDs.

93. Este criterio muestral asimismo podrá ser aplicable a las diferentes sedes de una organización, considerando que, si determinadas de ellas proporcionan o participan de forma exclusiva en la prestación de determinados servicios del sistema de información, deberán auditarse siempre, por lo que se incorporarán al muestreo elegido.

94. Los miembros del equipo auditor se basarán para la evaluación en hechos probados y verificados (evidencias objetivas). Su comparativa con el criterio de auditoría (en este caso el RD 311/2022, de 3 de mayo, por el que se regula el ENS) determinará, entre otros, de una parte, los hallazgos de cumplimiento, y de otra, los de incumplimiento, que, tras la revisión de todos ellos, podrán derivar en conformidad, en desviaciones o en recomendaciones. Las desviaciones, las recomendaciones del equipo auditor y los puntos fuertes (dentro de la conformidad) se desarrollan en un apartado posterior.

95. Para la obtención de evidencias, que sustenten los hallazgos de auditoría, el equipo auditor se podrá basar en entrevistas al personal (propio del auditado y colaboradores externos), observaciones directas (ubicaciones, dispositivos, aplicaciones, registros, etc.) así como en información documentada.

96. Es importante que, durante la auditoría material, el equipo auditor recoja o referencie información suficiente para evidenciar no solo las desviaciones, sino la conformidad, de modo que no queden dudas del rigor con el que se ha desarrollado la auditoría.

97. Una buena práctica es, al final de cada jornada, emplear unos pocos minutos para una reunión de seguimiento en la que se pongan de manifiesto las desviaciones halladas a lo largo del día. No obstante, se recuerda que el equipo auditor debe actuar con transparencia, expresando la posible desviación nada más detectarse ésta para dar opción al auditado a esclarecer la situación aportando, si procede, nuevas evidencias que demuestren que se trataba de un posible malentendido, o aceptándola sin ninguna duda.

6.7.2. RESPECTO A LAS EVIDENCIAS RECOGIDAS

98. El equipo auditor, en el diseño de sus comprobaciones, no debe limitarse a la revisión de documentos, ya que el objetivo de la auditoría es obtener **evidencias objetivas y eficaces** para evaluar y sustentar si, **en la práctica**, las medidas de seguridad auditadas son adecuadas para proteger la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad, según corresponda, de los servicios sustentados y la información tratada, almacenada o transmitida por el sistema auditado.

99. En esta línea, se comprobará que lo que se documenta en normas internas, procedimientos e instrucciones operativas, describe a tenor literal cómo se está llevando realmente en la práctica.

100. En el apartado 'propuesta de evidencias' al principio de cada tabla asociada a los artículos relevantes del ENS y a las 73 medidas de seguridad de su Anexo II, en la guía **CCN-STIC-808 ENS. Verificación del cumplimiento**, se sugieren posibles evidencias a ser requeridas por el auditor.

101. Las descripciones detalladas de los hallazgos de auditoría es preferible registrarlos en el cuaderno del auditor, de modo que puedan ser fácilmente reproducibles y verificables por la organización cuyo sistema de información ha sido auditado

cuando posteriormente se presenten en el Informe de Auditoría. Para ello, siempre que sea posible, se concretará:

- En las aplicaciones: su nombre o identificación, su versión, la opción seleccionada, el resultado obtenido, etc.
- En los paneles de control: su identificación, el equipo o equipos que gestionan, su versión, la gráfica o tabla seleccionada, etc.
- En los registros: su nombre o identificación, su versión y fecha, el número de registro (pestaña, fila y/o columna, si se trata de una hoja Excel), Etc.
- En los documentos escritos: nombre o identificación, versión y fecha de la última modificación, apartado que se ha consultado, etc.
- En las entrevistas: las iniciales del entrevistado, su cargo en la organización, la fecha y hora de la entrevista, etc.

102. El equipo auditor, adicionalmente, recogerá durante la auditoría aquellas evidencias que considera refuerzan la descripción realizada de los hallazgos. Para ello se solicitará siempre autorización al auditado, diferenciándose si la auditoría es presencial de la que transcurre en remoto.

103. En las auditorías presenciales, se solicitará al auditado que recoja (tal vez en una carpeta) la colección de evidencias digitales (por ejemplo, los pantallazos que el auditor le vaya indicando respecto a todo aquello que se le muestra), facilitándoselos por algún medio seguro al finalizar cada jornada de auditoría. En inspecciones oculares, por ejemplo, para verificar [mp.eq.1] puesto de trabajo despejado, tal vez una fotografía tomada por el propio auditado a indicación del auditor.

104. En las auditorías en remoto el auditor podría técnicamente, en cualquier momento durante la auditoría, tomar una captura de pantalla de todo aquello que le muestra el auditado, por lo que será necesario clarificar antes, o al menos al principio de la auditoría, que se solicitará autorización previamente a la captura de cualquier información.

6.8. REUNIÓN DE CIERRE Y DICTAMEN DE LA AUDITORÍA

105. La reunión de cierre, o de final de la auditoría, se preparará habitualmente entre 30 minutos y una hora antes de iniciarse la misma, en una reunión privada del equipo auditor. Ambas reuniones (la de preparación y la de cierre) constarán claramente identificadas en el Plan de Auditoría.

106. La reunión de cierre la dirige el Auditor Jefe y pueden asistir quienes la organización estime conveniente, a ser posible los roles relevantes del ENS y representantes de la Dirección.

107. En cuanto a los aspectos a tratar en la reunión de cierre, lo habitual es comenzar agradeciendo el desarrollo y nivel de colaboración en la auditoría por parte de los auditados, siempre que haya sido así, recordar el criterio, objetivo y alcance de la auditoría, comentar sobre el modelo de Informe de Auditoría que se proporcionará y en qué plazo, recordar que la auditoría es por muestreo y que puede que existan

otras desviaciones que en esta evaluación no se hayan detectado, recordar la confidencialidad de la información recabada o de aquella de la que se haya tenido conocimiento por parte del equipo auditor, indicar el resultado de la auditoría recordando los tres (3) posibles, definir los diferentes tipos de desviaciones exponiendo las halladas durante la auditoría, explicar cómo actuar en caso de discrepancias, cómo deberá presentarse el posible PAC, clarificaciones, ruegos y preguntas y despedida.

108. En relación al dictamen, o resultado final de la auditoría, éste será uno de los tres (3) siguientes:

- **FAVORABLE**: cuando no se evidencie ninguna desviación, ya sea "No Conformidad Mayor" o "No Conformidad Menor".
- **FAVORABLE CON NO CONFORMIDADES**: cuando se evidencien desviaciones, ya sean "No Conformidades Menores" y/o "No Conformidades Mayores". En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un PAC sobre tales desviaciones para su evaluación por parte del Auditor Jefe.
- **DESFAVORABLE**: Cuando exista un número significativo de No Conformidades Mayores y menores cuya solución, a juicio del Auditor Jefe, no pueda evidenciarse a través de un PAC y requiera la comprobación in-situ de su correcta implantación a través de una auditoría extraordinaria, circunscrita a tales desviaciones encontradas, a realizar en un plazo inferior a seis meses.

109. El Auditor Jefe indicará durante la reunión de cierre que las desviaciones expuestas son provisionales hasta la emisión del Informe de Auditoría definitivo, pudiendo estas variar.

110. Es una práctica común, aunque no obligatoria, entregar inmediatamente tras la reunión de cierre un documento provisional relacionando las No Conformidades Mayores y menores, donde conste claramente visible un texto que denote la provisionalidad del documento, su finalidad meramente orientativa y su prescripción una vez se emita el Informe de Auditoría definitivo.

6.9. INFORME DE AUDITORÍA

111. El Informe de Auditoría debe ser emitido en el tiempo acordado. Si se demora por causa de fuerza mayor, el retraso debe ser comunicado a la organización auditada.

112. El informe estará fechado y firmado electrónicamente por el Auditor Jefe mediante un certificado cualificado. A partir de la fecha de remisión al auditado del Informe de Auditoría se inicia el cómputo de los plazos para que el auditado presente el PAC o, en su caso, realice una auditoría extraordinaria circunscrita a las desviaciones encontradas, especialmente si se trata de una auditoría de Certificación de la Conformidad con el ENS.

113. El Informe de Auditoría contendrá como mínimo:

- La fecha de emisión del informe y su versión.

- La organización cuyo sistema de información se ha auditado.
- El criterio de auditoría, alcance detallado y objetivo (si es auditoría interna de verificación o de Certificación del Cumplimiento con el ENS).
- Una breve descripción de la organización, el contexto en el que opera y de los sistemas de información auditados.
- El nombre y firma del Auditor Jefe.
- El resto de miembros del equipo auditor, incluyendo los posibles expertos técnicos.
- La relación de personal del auditado que ha participado en la auditoría: nombre y desempeño (incluyendo organización a la que pertenece, de ser externo).
- Breve descripción de la metodología empleada para realizar la auditoría.
- Relación de documentos revisados durante el estudio documental.
- Indicación de si ha habido alguna limitación en la realización de la auditoría, que impida al equipo auditor formarse una opinión sobre determinados aspectos de la auditoría, incluidas las medidas de seguridad.
- Una sección a modo de informe ejecutivo resumiendo los puntos fuertes, las desviaciones (resumen de las no conformidades Mayores y menores), las recomendaciones del auditor (Observaciones y Oportunidades de Mejora), e incluyendo un resumen general del grado de cumplimiento.
- Las recomendaciones en ningún caso deberán ser cerradas, sino sugerencias generales de las distintas alternativas posibles a considerar por los responsables de la seguridad de la organización auditada. Es importante evitar su excesivo desarrollo ya que podrían ser consideradas como labor de consultoría generándose un conflicto de interés ante su incompatibilidad con la auditoría.
- Todas las desviaciones de la auditoría estarán siempre basadas en la existencia de un riesgo para la seguridad y sustentadas debidamente en evidencias, o bien relacionadas con un incumplimiento fehaciente y preciso de los requisitos base o de los refuerzos obligatorios del ENS.
- La descripción de los detalles y evidencias que permiten llegar a las conclusiones del informe se intercalarán agrupadas en cada apartado correspondiente a cada una de las medidas que sean de aplicación del Anexo II, o que correspondan a los artículos relevantes del ENS. Otra opción será que el Informe de Auditoría contenga descripciones detalladas que se vinculen a un documento independiente conteniendo todas las evidencias (pantallazos de aplicaciones, fotografías, fragmentos de documento, etc.), claramente referenciadas. La clasificación de los distintos tipos de hallazgos se desarrolla en el apartado 'CLASIFICACIÓN DE LOS HALLAZGOS DE AUDITORÍA' más adelante en esta misma guía.
- En el caso de que las evidencias de conformidad y no conformidad sean recogidas en un documento independiente, tal documento deberá estar vinculado indubitadamente con el Informe de Auditoría, asimismo fechado y firmado, expresándose tal vínculo, de modo que no queden dudas de que ambos documentos constituyen en su conjunto el Informe de Auditoría completo.

114. En la sección correspondiente al resumen o informe ejecutivo, dentro del Informe de Auditoría, no se incluirán términos o acrónimos técnicos, ya que dicho apartado del informe podrá ser leído por directores y gerentes, o terceros, que no tengan el conocimiento específico adecuado. Tampoco se deberán incluir nombres de personas concretas, solo funciones o puestos desempeñados y, en el caso de considerarse, únicamente sus iniciales.

115. El Informe de Auditoría, dado que puede poner de manifiesto debilidades de los sistemas de la organización, incorporará en la cabecera o en el pie de todas las páginas la marca de '**USO OFICIAL**' acompañada preferiblemente de la frase "*este informe puede contener información sensible para la organización*" o equivalente.

116. En relación a la sensibilidad del Informe de Auditoría, se proporcionará este de forma segura, se conservará con las convenientes medidas de seguridad y se limitará su difusión únicamente a quienes tengan necesidad de conocer.

117. El equipo auditor no entregará ni concederá acceso al informe de auditoría a terceros distintos de la organización cuyo sistema de información se ha auditado, salvo por imperativo legal o mandato judicial. No obstante, el informe de auditoría podrá ser requerido por el CCN en los términos previstos en el artículo 31 del ENS.

6.10. PLAN DE ACCIONES CORRECTIVAS

118. Ante un dictamen 'FAVORABLE CON NO CONFORMIDADES' en el Informe de Auditoría, la organización cuyo sistema de información ha sido auditado dispone de un mes de plazo para presentar un PAC que trate y resuelva las desviaciones halladas, que será evaluado a criterio del Auditor Jefe.

119. Algunos organismos de certificación consideran el mes de agosto inhábil, por lo que, si la fecha límite para presentar el PAC coincide a lo largo de dicho mes, pasa al mismo día de septiembre. Tal circunstancia constará en su metodología o proceso de certificación documentado.

120. Es de apreciar que el Auditor Jefe, tal vez acompañando al Informe de Auditoría, entregue a la organización cuyo sistema se ha auditado un documento con orientaciones sobre la presentación adecuada del PAC y/o un modelo de plantilla o formato recomendado para su presentación.

121. En cualquier caso, para cada desviación, como mínimo en el PAC se relacionará la misma, se identificará la causa raíz que la ha originado, se detallará la acción correctiva que se haya implantado para subsanar la desviación y para, atacando la causa raíz, evitar futuras ocurrencias.

122. En las auditorías de Certificación de la Conformidad con el ENS, si en el plazo de un mes, a contar desde la fecha del Informe de Auditoría, a la organización auditada no le ha sido posible presentar el PAC, o éste no solventa de forma adecuada las desviaciones, o bien si el dictamen de la auditoría ha sido 'DESFAVORABLE', la organización dispondrá de un plazo no superior a seis (6) meses desde la precitada fecha del Informe de Auditoría para someterse a una Auditoría Extraordinaria, exclusivamente sobre las desviaciones halladas. Dicha auditoría extraordinaria no

admite un nuevo PAC, por lo que de no superarse con dictamen "FAVORABLE", deberá repetirse el proceso de certificación completo.

123. Adicionalmente en las auditorías de Certificación de la Conformidad con el ENS, en el caso de un sistema con la certificación vigente sobre el que se detecten '**No Conformidades Mayores**' en la auditoría de certificación, durante el período de resolución de las mismas el Certificado de Conformidad quedará **en suspenso**. En caso de no cerrar las 'No Conformidades Mayores' en un plazo de seis meses contado a partir de la fecha del informe de auditoría, el Certificado de Conformidad quedaría revocado y la organización auditada deberá eliminar el Distintivo de Conformidad para ese sistema de información de su portal web y/o de su sede electrónica, hasta su próxima recertificación.

6.10.1. EVALUACIÓN DEL PAC

124. En las auditorías internas de verificación el Auditor Jefe no suele evaluar el PAC, aunque podría hacerse si así se acuerda con la organización auditada. No obstante, en las auditorías de certificación de la conformidad, realizadas por un OAT o una EC, el Auditor Jefe evaluará el PAC siempre que se entregue en plazo (30 días desde la fecha del Informe de Auditoría). Para ello dispondrá de un formulario al efecto donde, además de la fecha del informe de auditoría y de recepción del PAC, de los datos identificativos de la organización cuyo sistema de información se certifica, la identificación del propio PAC y la del Informe de Auditoría vinculado, para cada desviación (No Conformidad Mayor o Menor) hallada, indicará:

- El texto de la desviación según consta en el informe de auditoría.
- La acción correctiva inmediata propuesta por el auditado.
- La causa raíz de la desviación identificada por el auditado.
- La acción correctiva a futuro que, solventando la causa raíz según el auditado, evitará vuelva a reproducirse la desviación más adelante en el tiempo.
- La evaluación del Auditor Jefe para cada desviación, por ejemplo, señalando si es ACEPTADA o RECHAZADA, en cuyo caso se expondrá el motivo del rechazo.

125. Debe tenerse en consideración que, tras la evaluación del PAC favorablemente por parte del Auditor Jefe de la EC, o del OAT, así se hará constar en el formulario que el Auditor Jefe suscribirá y adjuntará al expediente. A continuación, el Revisor de Expedientes de la EC, o del OAT, revisará el expediente completo y caso de encontrarlo correcto lo plasmará asimismo en un documento que suscribirá, notificándolo a continuación al Comité de Certificación, o a quién se haya designado para adoptar la decisión de certificar, quedando constancia de dicha decisión en un documento al efecto, siendo la fecha en que ésta decisión se adopte (caso de ser favorable) la que constará en el certificado de conformidad con el ENS que se emita.

7. CLASIFICACIÓN DE LOS HALLAZGOS DE AUDITORÍA

126. Ya se ha mencionado en apartados anteriores que los hallazgos de auditoría, claramente evidenciados, se dividen en desviaciones (No Conformidades Mayores y menores), recomendaciones del equipo auditor (Observaciones y Oportunidades de Mejora) y puntos fuertes.

7.1. DESVIACIONES

127. Se considera la existencia de una '**No Conformidad menor**':

- Ante un incumplimiento parcial de algún artículo del ENS y/o el incumplimiento parcial de alguna medida de seguridad del Anexo II (el incumplimiento de algún requisito base o refuerzo obligatorio), siempre que sea de aplicación en función de la categorización del sistema.
- Cuando, sin afectar significativamente a la capacidad del sistema de protección para lograr los resultados previstos, los requisitos podrían satisfacerse de forma manifiestamente mejorable, o se aprecian incoherencias entre requisitos que deberían estar alineados.

128. Una 'No Conformidad menor', por sí sola, no debe poner de manifiesto un grave riesgo respecto a la seguridad del sistema de información que se está auditando, en cuyo caso debería plantearse clasificarla como 'No Conformidad Mayor'.

129. Se considera la existencia de una '**No Conformidad Mayor**':

- Cuando se detecten fallos o ausencias significativas referidas a artículos y preceptos esenciales del ENS, como son los relativos a la valoración y categorización del sistema, a la elaboración de la Declaración de Aplicabilidad o a la falta de designación de algún rol básico del ENS como lo es, por ejemplo, el de Responsable de la Seguridad, o la carencia de Política de la Seguridad de la Información.
- Ante la ausencia o implantación inadecuada de un número significativo de las medidas contenidas en cualquier grupo del Marco Operacional (Planificación, Control de accesos, Explotación, Recursos externos, Servicios en la Nube, Continuidad del servicio, Monitorización del sistema) o en las Medidas de Protección (Protección de las instalaciones e infraestructuras, Gestión del personal, Protección de los equipos, protección de las comunicaciones, Protección de los soportes de información, Protección de las aplicaciones informáticas, Protección de la información, Protección de los servicios) que, consideradas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo considerado.
- 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 se evidencie un número significativo de no conformidades menores asociadas al mismo requisito.

- Cuando el número, o la significación, de las 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.

130. Para facilitar la identificación y el posterior tratamiento de las desviaciones de una auditoría y la verificación de su solución, será posible agrupar las 'No Conformidades menores', respetando las siguientes reglas:

- en una sola 'No Conformidad menor', si dichos hallazgos están referidos a una única medida del anexo II del ENS.
- 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.

7.2. RECOMENDACIONES

131. Se considera la existencia de una **Observación** cuando se encuentren evidencias de una debilidad, una vulnerabilidad o determinada situación que, sin comprometer actualmente al sistema de información, ni al posible sistema de gestión de la seguridad de la información asociado, a juicio del Auditor Jefe pueda acabar derivando en el transcurrir del tiempo en una No Conformidad o en un problema de seguridad.

132. Se considerará la existencia de una **Oportunidad de Mejora** cuando de forma completamente subjetiva por parte del auditor, en base a su experiencia profesional y a las mejores prácticas, considera que algún aspecto de la seguridad del sistema con un enfoque distinto sería más eficaz o más eficiente. El auditor debe ser muy escueto al redactar las oportunidades de mejora para que no puedan ser consideradas consultoría encubierta.

133. Las respuestas a las recomendaciones no es obligado incorporarlas al PAC, aunque pueda hacerse de forma voluntaria. No obstante, es muy recomendable que sean analizadas por la organización auditada, persiguiendo siempre la mejora continua, y aplicar al sistema, o planificar, las acciones de mejora derivadas que se consideren. Es una práctica habitual durante las auditorías de certificación de la conformidad con el ENS solicitar a la organización auditada información sobre las observaciones reportadas en el informe anterior (además de las desviaciones) y ver cómo éstas se han tratado.

7.3. PUNTOS FUERTES

134. Un Punto Fuerte se refleja en el Informe de Auditoría, a juicio del Auditor Jefe en base a su experiencia, para poner de manifiesto aquellos aspectos del sistema,

referentes a la seguridad, que sobresalen de la media por su eficacia y eficiencia respecto a la seguridad del sistema de información auditado.

135. Su función es incentivar la mejora continua en seguridad, resaltando los esfuerzos realizados en base a los resultados obtenidos.

8. ANEXO A. REQUISITOS PARA EL EQUIPO AUDITOR

136. Los requisitos del equipo auditor diferirán según se trate de una auditoría de cumplimiento orientada a la Certificación de Conformidad con el ENS, o de una auditoría interna de verificación.

8.1. REQUISITOS PARA UN ORGANISMO DE CERTIFICACIÓN

137. Los organismos de certificación, según se detalla en el apartado 'EN RELACIÓN CON LOS RECURSOS DE LA EC/OAT' de la guía **CCN-CERT IC-01/19 Criterios generales de auditoría y certificación**, deben disponer de personal cualificado y suficiente para la realización de las Auditorías de Certificación de la Conformidad con el ENS, conforme a lo que indica la norma ISO/IEC 17065:2012, en todas las fases del proceso de auditoría, como son algunas de ellas el estudio documental previo, la auditoría material (remota/in situ) y la redacción del Informe de Auditoría. En concreto, se exigirá disponer, al menos, de:

- Un (1) Responsable Técnico, que podrá actuar en calidad de Auditor Jefe.
- Tantos auditores jefes como equipos de auditoría o, lo que es lo mismo, como auditorías simultáneas pueda llegar a hacer el organismo de certificación.
- 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.

138. El Auditor Jefe debe 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 (ENI), Identidad Electrónica, Firma Electrónica y Servicios de Confianza, entre otras.

139. 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 auditoría. No obstante, 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, tratándose el ENS de un marco o 'framework' de seguridad.

8.2. REQUISITOS PARA QUIENES REALIZAN AUDITORÍAS INTERNAS

140. En relación a las auditorías internas de verificación, especialmente cuando éstas se externalizan, la organización auditada deberá verificar que se le evidencie la competencia del Auditor Jefe, por ejemplo, mediante la aportación de su CV y la relación de auditorías equivalentes en las que ha participado. Dicha evidencia se conservará junto al resto de documentación de la auditoría. Deberá disponer y acreditar buenos conocimientos sobre el ENS, sobre seguridad de los sistemas de información, sobre Protección de Datos, etc.

141. Si el Auditor Jefe se apoya en otros miembros del equipo auditor (otros auditores o expertos técnicos), también estos deberán evidenciar su competencia y experiencia en el área de responsabilidad que le haya sido asignada.

9. ANEXO B. CONCURRENCIA ENTRE AUDITORÍAS DEL ENS Y AUDITORÍAS DE PROTECCIÓN DE DATOS

142. El ENS únicamente contempla la Protección de Datos de forma explícita en alguna de sus disposiciones:

- Artículo 3. Sistemas de información que traten datos personales.
- Artículo 12. Política de seguridad y requisitos mínimos de seguridad.
- Medida de seguridad [mp.info.1] Datos personales, de su Anexo II.

Sin menoscabo de lo señalado en la Disposición adicional primera de la LOPD-GDD que determina la aplicación de las medidas de seguridad que correspondan de las previstas en el Anexo II, a los tratamientos de datos personales por parte del sector público y de sus proveedores relevantes en el ámbito del ENS.

143. Como consecuencia, aunque se verifique determinados aspectos relevantes durante la auditoría, el objeto y alcance establecidos para el ENS son mucho más amplios que el objeto de la protección de datos de carácter personal.

144. Cuando el sistema auditado trate datos personales, se tendrá en cuenta lo previsto en la legislación vigente, especialmente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD), entre otras normas jurídicas.

145. Si durante la realización de la auditoría orientada exclusivamente al cumplimiento del ENS (sea interna de verificación o de certificación de la conformidad), se identificase algún incumplimiento manifiesto de dicha legislación de protección de datos personales, es obligación del equipo auditor comunicarlo, e incluirlo en el informe de auditoría.

146. El ENS difiere de una auditoría exclusiva de protección de datos personales, por lo que debe destinársele en el Plan de Auditoría únicamente el tiempo que corresponde para evaluar lo más relevante. Si la organización auditada dispone de una auditoría previa de protección de datos, el auditor del ENS la solicitará y, en su caso, incidirá en aquellos aspectos que considere de la misma.

147. Si se establece previamente la realización concurrente de ambas auditorías (del ENS y de protección de datos personales), la duración de la misma no debe actuar en detrimento de la adecuada realización de ambas. Lo deseable es que cada una disponga de sus jornadas específicas en el Plan de Auditoría, aunque sean consecutivas en el tiempo.

10. ANEXO C. MODELO DE ACUERDO DE CONFIENCIALIDAD Y AUSENCIA DE CONFLICTO DE INTERÉS

148. Los organismos de certificación del ENS ya disponen de su propio modelo de acuerdo de confidencialidad y ausencia de conflicto de interés (un único documento o dos de específicos), diferenciando en ocasiones las funciones de su Responsable Técnico, de su Revisor de Expedientes, de los miembros de su equipo auditor y del resto de desempeños vinculados con su actividad de certificación.

149. El modelo aquí incluido es generalista y orientativo ante las múltiples casuísticas que pueden darse. Las responsabilidades derivadas de su aplicación, en relación a los diferentes involucrados en cualquier desempeño en la auditoría, corresponden tanto a la organización responsable del equipo de auditoría (o auditor independiente, según el caso), como a la del sistema de información auditado.

10.1. ACUERDO DE CONFIDENCIALIDAD

[NOMBRE Y APELLIDOS] con DNI [NIF], en calidad de Auditor Jefe, Auditor o Experto Técnico integrante del equipo de auditoría de [NOMBRE DE LA ORGANIZACIÓN QUE AUDITA], se compromete a no difundir información alguna, ya sea verbalmente o por escrito, que pueda conocer o a la tenga acceso durante la realización de la auditoría de cumplimiento [INDICAR SI ES INTERNA DE VERIFICACIÓN o DE CERTIFICACIÓN DE LA CONFORMIDAD] que le ha sido asignada, correspondiente al Esquema Nacional de Seguridad (ENS). Es indiferente que la referida información esté relacionada, o no, con la organización auditada y/o sus sistemas de información, mientras no sea calificada por su titular como pública.

Quedarán asimismo incluidos en este deber de secreto los contenidos a los que se tenga acceso, que hayan sido confeccionados por quien suscribe este acuerdo o por cualquier otro miembro del equipo auditor, como pueden ser auditores jefes, auditores o expertos técnicos, en sus preceptivos documentos de trabajo, informes y, en general, con motivo de su desempeño profesional relacionado con la auditoría asignada.

Todo ello sin menoscabo de aquellos casos en los que le sea legalmente requerido, siempre previa notificación a la organización auditada. En este sentido están instruidos todos los integrantes del equipo auditor y demás personal vinculado con la organización que auditará.

Una copia de los documentos de trabajo que se elaboren para la realización de la auditoría podrá ser custodiada por el auditor o experto técnico, como evidencia del trabajo realizado, adoptando las adecuadas medidas de seguridad que se determinen por la organización a la que pertenece, hasta que se le requiera su destrucción o devolución.

Asimismo, quién suscribe se compromete a tratar cualquier dato personal recabado durante el proceso de auditoría cumpliendo la legislación vigente en cuanto a tratamiento de datos de carácter personal, conforme a las instrucciones del responsable del tratamiento, y a no aplicarlos o utilizarlos con finalidad distinta a la que figure en este acuerdo, ni a comunicarlos, ni siquiera para su conservación, a otras personas u

organizaciones que no estén previstas contractualmente o en los documentos de normativa interna o procedimientos debidamente aprobados de la organización que audita.

Las tareas a realizar en la auditoría no conllevan, necesariamente en sí mismas, el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios, es posible que se acceda a datos de carácter personal (por ejemplo, en alguna documentación revisada o evidencia recabada).

Quién suscribe declara conocer la legislación vigente en materia de protección de datos, estando cualquier integrante del equipo auditor instruido en estos requisitos. Por lo tanto, en caso de tener lugar acceso a datos personales como consecuencia de los servicios a prestar, el Auditor Jefe, Auditor o Experto Técnico se compromete a observar los requisitos establecidos en la legislación vigente.

10.2. DECLARACIÓN DE AUSENCIA DE CONFLICTO DE INTERÉS

[NOMBRE Y APELLIDOS] con DNI [NIF], en calidad de Auditor Jefe, Auditor o Experto Técnico integrante del equipo de auditoría de [NOMBRE DE LA ORGANIZACIÓN QUE AUDITA], declara que antes de iniciar la auditoría de cumplimiento respecto al ENS que le ha sido asignada, ha comprobado que no está sujeto a ninguna asociación o vinculación previa o actual por su parte con el sistema de información auditado, o por parte de su empleador en el caso de personal externo a la organización que audita, comprometiéndose a comunicarlo a quién corresponda, para que pueda evaluarse y, en su caso, designarse a un nuevo auditor o experto técnico desvinculado y que, por tanto, se preserve la independencia de la auditoría.

Por asociación o vinculación previa se entenderá la comprendida durante los dos años anteriores (730 días naturales) a su designación como auditor respecto a la organización auditada, siempre que haya existido relación con el sistema de información a auditar, ya sea como empleado, colaborador externo, o en calidad de asesor o consultor interno o externo. Únicamente no se considerará que atenta a la independencia si la actividad profesional se ha circunscrito exclusivamente a realizar auditorías [DE CERTIFICACIÓN, EN EL CASO DE PERTENECER A UN ORGANISMO DE CERTIFICACIÓN] al auditado, ya sea desde la propia organización que audita, o desde otra.

Asimismo, quién suscribe declara que las tareas como auditor o experto técnico no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares, tales como implantación, configuración o modificación de aplicaciones relacionadas con el sistema auditado, redacción de documentos requeridos por el ENS o procedimientos de actuación, así como recomendaciones particulares sobre productos o soluciones comerciales concretas, entre otros.

En consecuencia, el abajo firmante se compromete a revelar toda situación que conozca le pueda presentar a él, o a la organización que audita, un conflicto de intereses, o le despierte dudas razonables.

150. Este documento será firmado por todos los miembros del equipo auditor que han sido designados para realizar una auditoría de cumplimiento, con independencia del momento de su designación.

151. Otra opción posible consiste en que los miembros del equipo auditor de una organización concreta especializada, entre otras actividades, en la realización de auditorías internas de verificación, o que forme parte de un organismo de certificación, ya sea personal fijo o contratado en modalidad de prestación de servicios, en el momento de la contratación suscriban un acuerdo de confidencialidad genérico que abarque cualquier auditoría que realicen con la organización, al igual que una declaración de imparcialidad genérica que les obligue, para cualquier auditoría que les sea asignada, a notificar si se produce algún conflicto de interés.

11. ANEXO D. BIBLIOGRAFÍA DE REFERENCIA

152. En la realización de las auditorías de cumplimiento se utilizarán, además de los requisitos determinados por esta guía, los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a las auditorías

153. A continuación, se incluyen referencias bibliográficas que pueden ayudar a los auditores en su desempeño profesional, sin tratarse en ningún caso de una relación exhaustiva, estando además supeditadas al desarrollo legislativo y a la aparición de nuevas versiones de los documentos:

11.1. NORMAS JURÍDICAS

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD).
- En su caso, Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- En su caso, Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2) y especialmente su transposición al Ordenamiento Jurídico Español.
- ITS de Auditoría de la Seguridad de los Sistemas de Información por la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.
- ITS de Conformidad con el ENS por la Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.
- ITS de Informe del Estado de la Seguridad por la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.
- ITS de Notificación de Incidentes de Seguridad por la Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública.

11.2. ESTÁNDARES NACIONALES E INTERNACIONALES

- **ISO 19011:2018** Directrices para la auditoría de los sistemas de gestión.
- **ISO/IEC 17065:2012** Requisitos para organismos que certifican productos, procesos y servicios.
- **ISO/IEC 27006-1:2024** Requirements for bodies providing audit and certification of information security management systems.

- **MAGERIT – versión 3**. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- **ISO31000:2018** Gestión del riesgo – Directrices.

11.3. GUÍAS DEL CCN RELACIONADAS CON AUDITORÍA

- **CCN-CERT IC-01/19** ENS. Criterios Generales de Auditoría y Certificación.
- **CCN-STIC-122** Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS.
- **CCN-STIC-802** ENS. Auditorías de cumplimiento.
- **CCN-STIC-808** ENS. Verificación del cumplimiento.
- **CCN-STIC-808** Anexo Independiente en Excel.
- **CCN-STIC-809** Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento.
- **CCN-STIC-819** Medidas Compensatorias.

11.4. OTROS DOCUMENTOS

154. Hay diferentes organizaciones internacionales dedicadas a la auditoría, que elaboran diferentes documentos relacionados con esta actividad:

- Normas Globales de Auditoría Interna. **The Institute of Internal Auditors** (www.theiia.org)
- **Information Systems Audit and Control Association (ISACA)** (www.isaca.org) Esta entidad pone a disposición de los auditores de sistemas de información, distintos estándares, directrices y procedimientos de auditoría que pueden ser de utilidad para los auditores, ya que la mayoría de ellos tienen en cuenta aspectos relacionados con la seguridad.

12. ANEXO E. GLOSARIO DE TÉRMINOS

Alcance de la auditoría:

Extensión y límites de una auditoría. Puede especificar los sistemas de información que serán auditados (incluyendo todos o alguno de los servicios que sustentan), las ubicaciones a ser auditadas (por ejemplo, determinadas sedes y/o centros de trabajo, CPDs, …), el ámbito geográfico (por ejemplo, los países o poblaciones incluidas en la auditoría, especialmente tratándose de organizaciones multinacionales), y cualesquiera otros aspectos que puedan acotar sin indeterminaciones la auditoría. En cualquier caso, el alcance no debe inducir a error haciendo creer que es mayor o distinto del que realmente ha sido evaluado.

Auditado:

Organización que es auditada en su totalidad, o en parte (por ejemplo, alguno de sus sistemas de información). A la organización o persona que solicita una auditoría se le designa asimismo como *cliente de la auditoría*.

Auditor:

Persona que lleva a cabo una auditoría. Debe ser un profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma imparcial (sin conflictos de interés).

Auditor externo:

Auditor independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar, al menos en los últimos dos (2) años.

Auditor interno:

Suele pertenecer a una unidad independiente dentro de la organización a la que pertenecen los sistemas de información objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión respecto a los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad habitualmente reporta al nivel jerárquico más alto dentro de la organización.

Auditoría:

Proceso sistemático, independiente y documentado para obtener *evidencias objetivas* y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los *criterios de auditoría.*

Auditoría combinada:

Auditoría llevada a cabo conjuntamente a un único auditado respecto a dos o más sistemas de gestión. Por ejemplo, auditar conjuntamente un sistema de información respecto al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y a la norma ISO/IEC 27001:2022 sobre Sistemas de Gestión de seguridad de la Información.

Auditoría externa:

Las auditorías externas incluyen auditorías de segunda y tercera parte.
Las auditorías de segunda parte se llevan a cabo por partes que tienen interés en la organización, como por ejemplo un cliente que audita a su proveedor.
Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes, como son los organismos de certificación (Entidades de Certificación acreditadas por la ENAC u Órganos de Auditoría Técnica de la Administración reconocidos por el CCN).

Auditoría interna:

Las auditorías internas, denominadas asimismo como auditorías de primera parte, se realizan por la propia organización, o en su nombre, para confirmar, por ejemplo, la eficacia del sistema de gestión aplicado sobre un sistema de información, o para obtener información útil para su mejora.
Las auditorías internas pueden constituir la base para una autodeclaración de conformidad de una organización, únicamente posible para sistemas de información de categoría BÁSICA del ENS.

Competencia:

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

Comprobación:

Verificar, confirmar la veracidad o exactitud de algo. En el contexto de esta guía son verificaciones del establecimiento de las medidas de seguridad, junto a su eficacia, así como de la documentación de políticas, normas internas, procedimientos, instrucciones operativas, etc., junto a la comprobación de que lo indicado en ellas coincida con lo efectivamente llevado a la práctica por la organización, dentro de los requerimientos establecidos por el ENS como criterio de auditoría.

Conclusiones de la auditoría (Dictamen):

Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los *hallazgos de la auditoría*.

Conformidad:

Cumplimiento de un *requisito*.

Criterios de auditoría:

Conjunto de *requisitos* usados como referencia frente a la cual se compara la evidencia objetiva. Los requisitos pueden ser disposiciones legales (determinada norma jurídica), estándares internacionales (como determinada norma ISO), obligaciones contractuales, etc.

Desempeño:

Resultado medible que se puede relacionar con hallazgos cuantitativos o cualitativos en relación con la gestión de actividades, procesos, productos, servicios, sistemas u organizaciones.

Eficacia:

Grado en el que se realizan las actividades planificadas y se logran los resultados previstos. En otras palabras, capacidad para lograr el efecto que se desea o espera.

Se complementa con la *eficiencia* que consiste en logarlos objetivos propuestos empleando el mínimo de recursos posible.

La conjunción de *eficacia* y *eficiencia* se suele denominar *efectividad*.

Equipo auditor:

Una o más personas que llevan a cabo una auditoría con el apoyo, si es necesario, de *expertos técnicos*. El equipo auditor puede incluir auditores en formación.

Evidencia de la auditoría:

Registros, declaraciones de hechos, o cualquier otra información que es pertinente para los *criterios de auditoría* y que es verificable.

Evidencia objetiva:

Datos que respaldan la existencia o veracidad de algo. La evidencia objetiva puede obtenerse por medio de la observación, medición o por otros métodos.

Experto técnico:

Persona que aporta conocimientos o experiencia específicos al *equipo auditor*. El conocimiento o pericia específicos se relacionan con la organización, la actividad, el proceso, el producto, el servicio, la disciplina a auditar, la tecnología, o el idioma o la cultura.

Guía:

Persona designada por el auditado para asistir al equipo auditor. Suele encargarse de reservar salas, contactar con los diferentes participantes en la auditoría para que estén disponibles en el momento que se les requiere siguiendo el Plan de Auditoría, coordinar las visitas a otros centros, etc.

Hallazgo de auditoría:

Resultados de la evaluación de la *evidencia de la auditoría* recopilada frente a los *criterios de auditoría*. Los hallazgos de auditoría indican conformidad o no conformidad. Asimismo, pueden conducir a la identificación de riesgos, oportunidades para la mejora o al registro de buenas prácticas. Si los *criterios de auditoría* se seleccionan entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoria se denomina cumplimiento o no cumplimiento (incumplimiento).

Imparcialidad:

Ausencia de objetividad.

Informe de Auditoría:

Es el entregable que se facilita al auditado una vez finalizada la fase de auditoría material. En el informe el Auditor Jefe refleja los resultados de las tareas realizadas, poniendo de manifiesto los *hallazgos de auditoría* con el resultado final o dictamen de la auditoría.

No Conformidad:

Incumplimiento de un *requisito*. Puede ser una No Conformidad Mayor o una No Conformidad menor. Al conjunto de todas ellas se les denomina *desviaciones*.

Objetivos de la auditoría:

Los objetivos definen qué se pretende lograr con la auditoría. Pueden ser evaluar a la organización respecto al grado de *conformidad* con los *criterios de auditoría*, evaluar si es tenida en cuenta por la organización aquella legislación relevante que le obliga, hacer un seguimiento de las desviaciones halladas en auditorías anteriores, la mejora continua de un sistema, etc.

Observador:

Persona que acompaña al equipo auditor, pero que no tiene una participación activa durante la auditoría. Asiste a solicitud del auditado o el auditor. Puede corresponderse, por ejemplo, con un representante del CCN, personal de algún OAT en proceso de reconocimiento, etc.

Organismo de certificación:

Organismo de evaluación de la conformidad de tercera parte que opera esquemas de certificación. Un organismo de certificación puede ser gubernamental o no gubernamental.

Plan de auditoría:

Descripción de las actividades y de los detalles acordados de una auditoría, establecidos de forma cronológica. En el plan de la auditoría también se

incluye la asignación de tareas a los miembros del equipo auditor, fechas de realización de las tareas, y recursos necesarios para desarrollar la auditoría. También el personal de la organización auditada que participará.

Proceso:

Conjunto de actividades mutuamente relacionadas que utiliza las entradas para proporcionar un resultado previsto.

Programa de auditoría:

Acuerdos para un conjunto de una o más auditorías, planificadas para un período de tiempo determinado y dirigidas hacia un propósito específico.

Requisito:

Necesidad o expectativa establecida, generalmente implícita u obligatoria.

155. La mayoría de entradas en este glosario se han reproducido a partir de la norma **ISO 19011:2018 Directrices para la auditoría de los sistemas de gestión**. No obstante, algunas de ellas se han ampliado o adaptado al objeto de esta guía, junto a la adición de otras definiciones que se ha considerado, por ejemplo, de la norma **ISO 17065:2012 Requisitos para organismos que certifican productos, procesos y servicios**. No se trata de una relación exhaustiva.