centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 809

Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento

Octubre 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-284-5

Fecha de Edición: octubre 2022

ÍNDICE

1. INTRODUCCIÓN

1. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en cumplimiento de lo que dispone el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regula una de las piezas fundamentales que 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. En los últimos años se han producido notables cambios en España y en la Unión Europea, incluidos la **progresiva transformación digital de nuestra sociedad**, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos.

3. Por otro lado, fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de **dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido**, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

4. En definitiva, la evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la **necesidad de mantener la conformidad** y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Las normas de conformidad se concretan en cuatro (4): Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

5. Sea como fuere, **es responsabilidad de las organizaciones** que el esfuerzo desarrollado en pos de un desenvolvimiento seguro de sus sistemas de información se publicite adecuadamente, trasladando a los ciudadanos la confianza de que se hallan ante unos servicios públicos eficaces y seguros.

6. Por todo ello, consciente de la necesidad de dar publicidad a las garantías adoptadas en el desenvolvimiento del sector Público y el desarrollo del procedimiento administrativo prestado por medios electrónicos, el artículo 38 del ENS señala:

   Artículo 38. Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.

   1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que

se puedan someter igualmente a una auditoria de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

7. La presente Guía articula el mecanismo de **Declaración y Certificación de Conformidad con el ENS**, determinando las condiciones para alcanzar aquel cumplimiento normativo. Además, tras varios años de experiencia en la implantación del Esquema Nacional de Seguridad, ha surgido la necesidad de introducir el concepto de **Aprobación Provisional de Conformidad** (APC) en el ENS, descrito y definido en la Guía *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*.

8. Así pues, persiguiendo su cumplimiento, se hace necesario señalar con precisión a los responsables públicos cuál debe ser el aspecto y el contenido de las **Declaraciones de Conformidad** y **Certificaciones de Conformidad**, mencionados en el citado artículo 38.2 del ENS, junto a los correspondientes **sellos o distintivos**, así como de las **aprobaciones provisionales de conformidad**, descritas en la Guía CCN-CERT IC-01/19, **y sus distintivos**. También, se ve necesario especificar quién puede solicitarlos, quién puede concederlos y cómo deben hacerse visibles en los espacios públicos tecnológicos de las organizaciones afectadas.

2. LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

2.1. CRITERIOS DE DETERMINACIÓN DE LA CONFORMIDAD

9. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad resulta de **aplicación a los sistemas de información de todo el sector público**, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma, incluyendo asimismo los sistemas de información de las entidades (públicas o privadas) que formen parte de la cadena de suministro en la prestación de servicios competenciales a las organizaciones públicas, en la medida que lo determine un previo análisis de riesgos.

10. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, el ENS será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

11. La conformidad con lo dispuesto en el ENS se alcanza satisfaciendo los mandatos contenidos en su texto articulado y mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II de la norma, previa

categorización de los sistemas a proteger.

12. Las Guías CCN STIC 802 (Guía de auditoría), 804 (Guía de implantación) y 808 (Verificación del cumplimiento de las medidas en el ENS), proporcionan los elementos necesarios para definir los criterios de determinación de la conformidad, así como la implantación y verificación de las medidas de seguridad, incluyendo el proceso de auditoría.

13. La determinación de la conformidad de los sistemas de información del ámbito de aplicación del ENS con categorías MEDIA o ALTA se realizará mediante un procedimiento de **auditoría formal** que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el ENS, **al menos cada dos (2) años**. Con carácter extraordinario, deberá realizarse dicha auditoría 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.

14. La organización titular del sistema de información deberá contar con procedimientos que permitan detectar las citadas modificaciones y comunicar esta circunstancia a la Entidad de Certificación (EC), o al Órgano de Auditoría Técnica del Sector Público (OAT), de que se trate. La ausencia de tal comunicación, cuando fuere necesaria, podrá suponer la retirada de la Certificación de Conformidad concedida.

15. Para la determinación de la conformidad de los sistemas de información del ámbito de aplicación del ENS con categoría BÁSICA bastará con la ejecución de un **procedimiento de autoevaluación** que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el ENS, **al menos cada dos (2) años**. Con carácter extraordinario, tal autoevaluación deberá realizarse 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.

16. El plazo de dos (2) años señalado en los párrafos anteriores **podrá extenderse durante tres (3) meses** cuando concurran impedimentos de fuerza mayor no imputables a la organización titular del sistema o sistemas de información concernidos.

17. Siendo obligatoria la Auditoría en sistemas de categorías MEDIA o ALTA, nada impide que un sistema de categoría BÁSICA se someta igualmente a una Auditoría formal de verificación de conformidad, siendo esta posibilidad siempre la deseable.

18. Dado que el ENS es un *framework* de seguridad de la información, un sistema de información de categoría MEDIA y ALTA requiere disponer de un SGSI para la gestión de su seguridad, como se determina en la medida de seguridad [op.pl.2] 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 con el mismo fin.

19. En este sentido, el objetivo de la auditoría de certificación del ENS es aportar la confianza de que el sistema de información ha sido auditado por un tercero independiente, imparcial y capacitado. De otra parte, la finalidad de la auditoría interna 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 alanzarla.

20. Por todo ello, debe entenderse que la realización de auditorías internas es una actividad necesaria para sistemas de categorías MEDIA y ALTA, 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 de carácter bienal.

21. En consecuencia, es conveniente realizar auditorías internas anuales de seguimiento de las medidas de seguridad del Anexo II del ENS -especialmente, en los años que no haya que realizar auditorías de certificación-, asegurándose de que cada auditoría de seguimiento cubre el análisis de al menos el 50% de las medidas que le apliquen del Anexo II, y de que entre las dos auditorías internas del ciclo bienal se cubre el 100% de dichas medidas, resultando especialmente de aplicación en el caso de preverse auditorías de certificación iniciales o cualesquiera otras, a realizar sobre sistemas de categoría MEDIA o ALTA dentro del principio básico de mejora continua del proceso de seguridad que requiere todo SGSI.

2.2. PROCEDIMIENTO DE DETERMINACIÓN DE LA CONFORMIDAD

22. Como se desprende de lo contenido en el Anexo II del ENS, la conformidad con la norma de un sistema de información concreto pasa necesariamente por **adoptar y manifestar que se han implementado** las medidas de seguridad requeridas para tal sistema, atendiendo a su categoría (BÁSICA, MEDIA o ALTA), y asegurando que tales medidas **se mantienen a lo largo de todo el ciclo de vida del sistema.**

23. Esta constatación de conformidad, tanto inicial como periódica, queda claramente reflejada en el artículo 31 del ENS, cuando señala:

Artículo 31. Auditoría de la seguridad.

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

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

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

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

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

24. Por su parte, el Anexo III del ENS precisa el alcance de la verificación referida en el artículo anterior, **prescribiendo los dos (2) procedimientos** que se resumen en el cuadro siguiente:

Procedimiento de evaluación	Categoría de los Sistemas Afectados	Manifestación de Conformidad	Resultado de la evaluación	Análisis de la evaluación
AUTOEVALUACIÓN Realizada por el mismo personal que administra el sistema de información o aquel otro en quién hubiere delegado[1].	**BÁSICA**	**DECLARACIÓN DE CONFORMIDAD**	**Documento de autoevaluación,** indicando si cada medida de seguridad está implementada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.	Los documentos de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
AUDITORÍA FORMAL Realizada con las garantías metodológicas, de independencia, profesionalidad e imparcialidad	**MEDIA / ALTA**	**CERTIFICACIÓN DE CONFORMIDAD**	**Informe de auditoría,** es imperativo calificar adecuadamente, de conformidad con lo señalado en la ITS de Auditoría, las desviaciones halladas en las auditorías, distinguiendo entre No Conformidades Mayores,	Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras

[1] Como se ha dicho, nada impide que un sistema de categoría BÁSICA se someta igualmente a una Auditoría formal de verificación de conformidad, siendo esta posibilidad siempre la deseable.

requeridas.			No Conformidades Menores y Observaciones. Adicionalmente, el Informe de Auditoría podrá contener oportunidades de mejora que, a juicio del auditor, aporten valor a la auditoría y puedan contribuir a la mejora del sistema de gestión de la seguridad de los sistemas de información concernidos.	adecuadas.

3. PUBLICIDAD DE LA CONFORMIDAD

25. Alcanzada la conformidad con el ENS, y atendiendo a los dos (2) procedimientos señalados de Declaración y Certificación de la Conformidad, se describen seguidamente los contenidos de ambas manifestaciones de conformidad.

3.1. ESQUEMA DE DECLARACIÓN Y CERTIFICACIÓN DE LA CONFORMIDAD CON EL ENS

26. La exhibición de una **Declaración de Conformidad**, de aplicación obligatoria a sistemas de información de categoría BÁSICA, o una **Certificación de Conformidad**, de aplicación obligatoria a sistemas de información de categorías MEDIA o ALTA y voluntaria en el caso de sistemas de información de categoría BASICA, y en su caso a través de los respectivos distintivos, son necesarios para mostrar, a todos los interesados, el compromiso de la entidad en cuestión con la seguridad de los sistemas, respecto de la información que trata o los servicios que presta.

27. En las comunidades autónomas con lengua cooficial se podrán expedir las declaraciones, certificaciones y sus respectivos **distintivos de conformidad en castellano o bien en texto bilingüe**. En este caso, se expedirán en un solo documento redactado en castellano y en la correspondiente lengua cooficial, en tipos de letra de igual rango, con las especificaciones y diligencias que sobre su texto se establecen en los anexos correspondientes.

28. Cuando se trate de sistemas de información de categoría MEDIA o ALTA, **el Centro Criptológico Nacional (CCN) y la Entidad Nacional de Acreditación (ENAC),** atendiendo a un procedimiento regulado, participarán en la acreditación de las **Entidades de Certificación del ENS**[2], a las que informarán sobre los requisitos que deben satisfacer y los criterios que deben adoptar para una adecuada evaluación de la conformidad respecto de las auditorías que desarrollen, por sí mismas o por terceros designados, autorizados o seleccionados por ellas[3].

29. La Certificación de Conformidad con el ENS a la que se refiere el punto anterior deberá ser expedida por una Entidad de Certificación que, en el momento de la expedición, esté acreditada por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas conforme a UNE-EN ISO/IEC 17065:2012 *Evaluación de la*

[2] 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 (BOE, Núm. 265, 2 de noviembre de 2016).

[3] ENAC, en el ejercicio de sus competencias, atenderá las denuncias, quejas, reclamaciones o sugerencias que pudieran transmitirle las Entidades de Certificación del ENS en relación con los procesos de certificación, abriendo la correspondiente investigación, si la naturaleza y gravedad de lo comunicado así lo aconsejan.

conformidad. Requisitos para organismos que certifican productos, procesos y servicios, para la certificación de sistemas de información del ámbito de aplicación del ENS.

30. Si no dispusiere de la acreditación señalada en el punto anterior, la Entidad de Certificación de que se trate no podrá expedir Certificaciones de Conformidad en tanto no alcance la citada acreditación. Previamente a iniciar sus actividades, deberá remitir al CCN la aceptación por parte de ENAC de haber solicitado la acreditación antedicha. El CCN podrá requerir al solicitante cuanta información adicional considere necesaria que le permita verificar su adecuación y suficiencia.

31. De acuerdo con lo indicado en la cláusula 4.2.6 e) de la norma UNE-EN ISO/IEC 17065:2012, la Entidad de Certificación, ni ninguna parte de la entidad legal a la que pertenezca, ni ninguna entidad bajo su control organizacional, podrán ofrecer ni suministrar consultoría o asistencia en el campo de los sistemas de gestión de seguridad de la información, sistemas de gobierno de la seguridad de la información, metodologías o herramientas asociadas (tales como ENS, ISO 27001, COBIT, Octave, MAGERIT, PILAR u otras realizaciones de naturaleza similar) ni auditorías internas sobre tales referentes.

32. Cualquier situación que ponga a la entidad de certificación en la necesidad de evaluar el producto de su propio trabajo es una amenaza inaceptable para la imparcialidad y la entidad de certificación debe tomar acciones para identificar y evitar tales situaciones.

33. La entidad de certificación no podrá certificar a una organización si en los dos (2) años anteriores a la solicitud de certificación la propia entidad de certificación, la entidad legal a la que pertenezca, así como alguna entidad bajo su control organizacional le hubiese prestado servicios o suministrado productos (al propio solicitante de la certificación o a sus proveedores en el área cubierta por la certificación de ENS) cuyo resultado tenga que ser usado por la entidad de certificación en su proceso de certificación. Este es el caso de actividades tales como la realización de análisis de riesgos, diseño o implantación de controles o medidas de seguridad o de continuidad de las operaciones.

34. En el caso de que la propia entidad de certificación, la entidad legal a la que pertenezca, así como alguna entidad bajo su control organizacional hayan suministrado a los clientes de la entidad de certificación productos o servicios, dentro del ámbito de la seguridad de la información, que no caigan en los descritos en el párrafo anterior, la entidad de certificación debe disponer de registros suficientes que demuestren la ausencia de impacto a la imparcialidad y que el resultado de las actividades previas no se usa en modo alguno en ninguna fase del proceso de certificación.

35. Estarán exentas del cumplimiento de los requisitos señalados en los párrafos anteriores aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

36. El CCN mantendrá en su sede electrónica una relación actualizada de las Entidades de Certificación (EC), acreditadas o en vías de acreditación, para expedir Certificaciones de Conformidad con el ENS; Asimismo, constarán los Órganos de

Auditoría Técnica (OAT) reconocidos, o en vías de reconocimiento, para dicho fin.

37. En cuanto a los certificados caducados de las entidades (tanto del Sector Público como del Sector Privado), se prolongará la publicidad de los mismos en la página web del CCN, salvo situaciones excepcionales justificadas, durante dos (2) meses. Posteriormente, si no se ha recibido el nuevo Certificado, se procederá a su eliminación en dicha página.

38. Como se ha indicado, el detalle del procedimiento a que se refieren los párrafos anteriores, las condiciones requeridas para el otorgamiento de las acreditaciones, su alcance, verificación, mantenimiento periódico y publicidad de las entidades acreditadas, se especifican en la antedicha Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3.2. DECLARACIÓN DE CONFORMIDAD

39. Cuando se trate de sistemas de categoría BÁSICA, el titular del órgano superior de que se trate dará publicidad a la conformidad de los sistemas de información afectados mediante una **Declaración de Conformidad**, cuya estructura y contenido se detallan en el Anexo A de la presente Guía.

40. La Declaración de Conformidad con el ENS se expresará en un documento electrónico, en formato no editable, firmado electrónicamente por la propia organización bajo cuya responsabilidad se encuentre el sistema de información en cuestión o por quién en esta hubiere delegado.

41. La Declaración de Conformidad con el ENS podrá representarse mediante un Sello o **Distintivo de Declaración de Conformidad**, que será publicitado por la organización titular, o bajo cuya responsabilidad se encuentre el sistema de información en cuestión, siempre empleando los modelos de sellos o distintivos diseñados por el Centro Criptológico Nacional y descargables desde su página web.

42. El citado sello o Distintivo de Declaración de Conformidad será un documento electrónico, en formato no editable, que incluirá un enlace a la Declaración de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica o página web de la organización pública o privada, respectivamente, de que se trate.

3.3. CERTIFICACIÓN DE CONFORMIDAD

43. Cuando se trate de sistemas de categorías MEDIA o ALTA, y conforme a lo dispuesto en el Anexo III del ENS, el sistema de información deberá superar la correspondiente Auditoría.

44. El titular del órgano superior de que se trate dará publicidad a la conformidad de los sistemas de información afectados mediante la exhibición de una **Certificación de Conformidad.**

45. La Certificación de Conformidad con el ENS se expresará en un documento electrónico, en formato no editable, firmado electrónicamente por la Entidad Certificadora y debiendo contener, al menos, la información que se señala en la antedicha Instrucción Técnica de Seguridad de conformidad con el ENS y que se

refleja en el Anexo B a modo de ejemplo.

46. La Certificación de Conformidad con el ENS podrá representarse mediante un Sello o **Distintivo de Certificación de Conformidad**, que será expedido por la Entidad Certificadora de que se trate, siempre empleando los modelos de sellos o distintivos diseñados por el Centro Criptológico Nacional y descargables desde su página web, cuyo uso por parte de la entidad titular o usuaria del sistema de información en cuestión estará condicionado a la posesión de la antedicha Certificación de Conformidad.

47. El citado sello o Distintivo de Certificación de Conformidad será un documento electrónico, en formato no editable, firmado por la Entidad Certificadora, que incluirá un enlace que conduzca a la Certificación de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

3.4. COMUNICACIÓN DE LAS CERTIFICACIONES DE CONFORMIDAD AL CENTRO CRIPTOLÓGICO NACIONAL Y SU PUBLICACIÓN

48. Las Entidades de Certificación del ENS que hubieren expedido Certificaciones de Conformidad con el ENS, tanto a organizaciones del sector público como del privado, conforme al procedimiento descrito en esta Guía y a lo dispuesto en la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, comunicarán al Centro Criptológico Nacional la expedición de dichos Certificados de Conformidad dentro de los quince (15) días siguientes a la expedición del Certificado de que se trate, a través de la solución AMPARO, que el CCN pone a disposición de las Entidades de Certificación, adjuntando el correspondiente documento electrónico de Certificación de la Conformidad con el ENS, que habrá sido firmado/sellado electrónicamente por la Entidad de Certificación.

49. El Centro Criptológico Nacional mantendrá en su página web una relación de las organizaciones públicas o privadas que hubieren obtenido Certificaciones de Conformidad, con expresión de los sistemas de información certificados, los servicios sustentados o soportados en tales sistemas y las fechas de expedición y expiración de las Certificaciones.

50. Por último, entendiendo que los Informes de Autoevaluación o Auditoría podrían contener información o datos sensibles, de naturaleza personal, comercial o institucional y/o encontrarse protegidos por distintas regulaciones, la facultad que la ITS de Conformidad con el ENS confiere a las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado titulares de una Declaración o Certificación de Conformidad para solicitar a tales operadores dichos Informes de Autoevaluación o Auditoría, se instrumentalizará dirigiendo tal solicitud y su necesidad a la cuenta de correo electrónico cocens@ccn.cni.es del Centro Criptológico Nacional, que valorará la petición y resolverá en consecuencia, dando cuenta de ello a la entidad peticionaria y a la Entidad de Certificación responsable de la emisión de la antedicha Certificación de Conformidad con el ENS.

4. LA APROBACIÓN PROVISIONAL DE CONFORMIDAD CON EL ENS

51. Tal y como se recoge en la Guía *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*, podrá expedirse excepcionalmente una **Aprobación Provisional de Conformidad (APC)** para sistemas de información con **categorías BÁSICA o MEDIA.**

52. La Aprobación Provisional de Conformidad (APC), **será emitida por el Centro Criptológico Nacional,** a petición **del Órgano de Auditoría Técnica del Sector Público (OAT, en adelante, y regulado en la Guía CCN-STIC 122) o la Entidad de Certificación**.

53. La APC se expresará en un documento electrónico, en formato no editable, firmado electrónicamente por el Centro Criptológico Nacional y debiendo contener, al menos, la información detallada en la citada Guía CCN-CERT IC-01/19, y que cuyo formato se muestra en el Anexo C del presente documento.

54. La Aprobación Provisional de Conformidad con el ENS podrá representarse mediante un **Distintivo de Aprobación Provisional de Conformidad**, que será **expedido por el Centro Criptológico Nacional**.

55. El citado **Distintivo de Aprobación Provisional de Conformidad** será un documento electrónico, en formato no editable, **emitido por el CCN**, que incluirá un enlace que conduzca a la Aprobación Provisional de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica o página web de la organización pública o privada, respectivamente, de que se trate.

56. No se publicitarán en la página web del CCN las organizaciones que estén en posesión de una Aprobación Provisional de Conformidad hasta que hayan completado el Plan de Acciones Correctivas, resultado del proceso de Auditoría, y obtenido la Certificación de Conformidad con el ENS correspondiente; en cuyo caso, la Entidad de Certificación de que se trate, continuará con el proceso descrito en el apartado 3.5 del presente documento.

5. CONSEJO DE CERTIFICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD (CoCENS)

5.1. JUSTIFICACIÓN

57. La expedición de las Certificaciones de Conformidad con el Esquema Nacional de Seguridad (ENS), tal y como se encuentra regulada en la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, exige el concurso coordinado de diferentes actores y elementos.

58. En primer lugar, entre los actores, es necesario contemplar a la Entidad Nacional de Acreditación (ENAC), organismo encargado de acreditar a las Entidades de Certificación que realizan las preceptivas auditorías de conformidad a las que se refiere el RD 311/2022 (ENS). Todo ello sin perder de vista la responsabilidad que el ordenamiento jurídico confiere a las Administraciones Públicas co-responsables del ENS (y, en su consecuencia, de su esquema de certificación): el Ministerio de Política Territorial y Función Pública y el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia, encuadrado en el Ministerio de Defensa.

59. Por otro lado, el adecuado despliegue de la Certificación de Conformidad con el

ENS exige también disponer de una contrastada normativa para la acreditación de las Entidades de Certificación (sustentada en la norma internacional *UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios*) y una no menos rigurosa metodología para la Auditoría de Sistemas de Información, tal y como la describe el propio ENS, la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información y las Guías CCN-STIC publicadas sobre la materia.

60. En este sentido, las Guías CCN-STIC deben considerarse como "Mejores Prácticas[4]", que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones, principios, etc., que podrían influir en el desarrollo legislativo pudiendo asimismo ser utilizadas como referentes específicos en la actuación judicial o arbitral.

61. Por tanto, no tratándose exactamente de normas imperativas, su cumplimiento no resulta obligatorio, aunque su inobservancia, caso de producirse algún incidente que pueda poner en riesgo la seguridad de los sistemas de información concernidos, podría derivar en responsabilidad.

62. La complejidad para mantener un adecuado equilibrio entre las obligaciones de servicio de las organizaciones del sector público y privado junto las funciones de las entidades de certificación y los OAT del Sector Público, además de la permanente evolución internacional de los esquemas de certificación y reconocimiento mutuo, hacen que sea necesario constituir un órgano que, incorporando a todas las partes concernidas, ayude a la adecuada implantación del ENS y, en su consecuencia, a la mejor y más garante prestación de los servicios públicos, objetivos últimos del ENS.

63. Por todo lo anterior, y persiguiendo los propósitos antedichos, el presente texto crea y ordena el **Consejo de Certificación del ENS (CoCENS),** en los términos que seguidamente se describen.

5.2. TÉRMINOS DE REFERENCIA DEL CONSEJO DE CERTIFICACIÓN DEL ENS

64. Sin perjuicio de una eventual formalización jurídica del **Consejo de Certificación del ENS (CoCENS),** se describen seguidamente sus caracteres principales.

Naturaleza	El Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS) se constituye como un órgano colegiado, regulado por lo dispuesto en la Sección 3ª del Capítulo II del Título Preliminar, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por lo establecido en la presente disposición.
Composición	1. Corresponde al Director del Centro Criptológico Nacional (CCN) la presidencia del Consejo de Certificación del ENS. 2. Serán miembros permanentes del Consejo de Certificación del ENS, los siguientes: a) El Jefe del Área de Normativa y Servicios de Ciberseguridad del Centro Criptológico Nacional, que podrá asumir la presidencia del Consejo de Certificación del ENS por delegación del Director del CCN. b) Un representante del Ministerio de Política Territorial y Función Pública, con categoría de Subdirector General o Subdirector Adjunto, y cuyo nombramiento y asistencia solicitará el CCN.

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

	c) El Director Técnico de la Entidad Nacional de Acreditación (ENAC), o en quién este delegue, y cuyo nombramiento y asistencia solicitará el CCN. 3. Serán miembros no permanentes del Consejo de Certificación del ENS, los siguientes: a) Un representante de cada OAT del Sector Público o Entidad de Certificación del ENS acreditada. b) Especialistas externos, de los sectores público, privado y/o académico que, por razón de su experiencia o vinculación con la Certificación del ENS puedan ser llamados a las reuniones del Consejo.
Fines	Corresponde al Consejo de Certificación del ENS: a) Velar por la adecuada implantación de la Certificación del ENS, adoptando las medidas que, en Derecho, correspondan. b) Alentar los procesos de Certificación de la Conformidad con el ENS. c) Proponer para su análisis y, en su caso, redactar y publicar Normas, Informes, Criterios o Buenas Prácticas en materia de Certificación de la Conformidad con el ENS. d) Asesorar a las partes implicadas respecto de los métodos, procedimientos, herramientas y criterios en materia de Certificación de la Conformidad con el ENS y, en general, con su implantación, orientando su gestión al mejor servicio del sector público y la mayor y mejor colaboración con el sector privado, fabricantes y suministradores de productos o servicios. e) Asesorar a las partes implicadas en la identificación de otros esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para los sectores público y privado. f) Informar a sus Departamentos constituyentes y al Consejo Nacional de Ciberseguridad sobre el grado de implantación de la certificación de Conformidad con el Esquema Nacional de Seguridad
Atribuciones	Las atribuciones del Consejo de Certificación del ENS son: a) Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas. b) Estar permanentemente informado de la relación de OAT del sector público y Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas. c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados. d) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Consejo, a las que su presidente, deberá dar cumplida respuesta.
Periodicidad de las reuniones y adopción de acuerdos	1. El Consejo de Certificación del ENS se reunirá, como mínimo, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones. 2. Las reuniones se convocarán por su presidencia, a su iniciativa o por mayoría de sus miembros permanentes. 3. Las decisiones se adoptarán por consenso de sus miembros permanentes.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL