

Guía de Seguridad de las TIC

CCN-STIC 809

DECLARACIÓN Y CERTIFICACIÓN DE CONFORMIDAD CON EL ENS Y DISTINTIVOS DE CUMPLIMIENTO



Marzo, 2018

Edita:



© Centro Criptológico Nacional, 2018

NIPO: 785-18-021-2

Fecha de Edición: Marzo, 2018

El Sr. Carlos Galán y ENAC han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

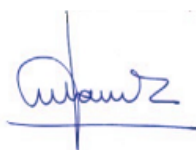
La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la formación clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.



Marzo, 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	1
2. LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD	2
2.1. CRITERIOS DE DETERMINACIÓN DE LA CONFORMIDAD	2
2.2. PROCEDIMIENTO DE DETERMINACIÓN DE LA CONFORMIDAD	3
3. PUBLICIDAD DE LA CONFORMIDAD	5
3.1. ESQUEMA DE DECLARACIÓN Y CERTIFICACIÓN DE LA CONFORMIDAD CON EL ENS5	
3.2. DECLARACIÓN DE CONFORMIDAD	7
3.3. CERTIFICACIÓN DE CONFORMIDAD.....	7
3.4. SOLUCIONES Y SERVICIOS PRESTADOS POR EL SECTOR PRIVADO	8
3.5. COMUNICACIÓN DE LAS CERTIFICACIONES DE CONFORMIDAD AL CENTRO CRIPTOLÓGICO NACIONAL Y SU PUBLICACIÓN	9

ANEXOS

ANEXO A. MODELOS DE DECLARACIÓN DE CONFORMIDAD Y DISTINTIVO	10
ANEXO B. MODELOS DE CERTIFICACIÓN DE CONFORMIDAD Y DISTINTIVO	11

1. INTRODUCCIÓN

1. El Real Decreto 3/2010, en cumplimiento de lo que dispuso en su momento la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios públicos (LAECSP) y de lo que recientemente ha recogido el texto de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), regula una de las piezas fundamentales que vertebran lo que se ha dado en llamar la Administración Electrónica: **la seguridad de los sistemas de información** de las Administraciones Públicas, seguridad entendida como el conjunto de principios básicos y requisitos mínimos requeridos para una protección adecuada de la información tratada y los servicios prestados por las entidades del sector público de su ámbito de aplicación.
2. Aquellos principios y requisitos configuraron en enero de 2010 una norma legal, de obligado cumplimiento para el sector público concernido: el **Esquema Nacional de Seguridad (ENS)**¹, cuya progresiva implantación ha venido propiciando la prestación de unos servicios públicos modernos y confiables. Los ciudadanos, profesionales y empresas españolas, beneficiarios últimos de lo exigido en el ENS, han observado en estos años una significativa mejora en la disponibilidad de los servicios prestados por vía electrónica, constatando el esfuerzo de los poderes públicos por dotar al tratamiento de la información de las debidas garantías de seguridad y legalidad que cualquier acto de las Administraciones públicas exige.
3. Muchas son ya, al cierre de la edición de esta Guía, las entidades públicas que han adaptado la seguridad de sus sistemas de información a lo dispuesto en el ENS. Otras, están en vías de lograrlo.
4. Sea como fuere, es responsabilidad de los organismos públicos 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.
5. Por otro lado, siendo cada vez más frecuente que las organizaciones y operadores económicos del sector privado participen en la prestación de servicios a las entidades públicas (a través, por ejemplo, de servicios en la nube), parece necesario extender el ámbito de la antedicha publicidad también a este sector.
6. Por todo ello, consciente de la necesidad de dar publicidad a las garantías adoptadas en el desenvolvimiento de las Administraciones Públicas y el desarrollo del procedimiento administrativo prestado por medios electrónicos, el artículo 41 del ENS señala:

Artículo 41. Publicación de conformidad.

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los

¹ De conformidad con lo dispuesto en el art. 42 del ENS, que exige su actualización permanente, atendiendo al progreso de los servicios de Administración electrónica, la evolución tecnológica y los nuevos estándares internacionales en materia de seguridad y auditoría de sistemas, se ha publicado recientemente el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

7. Finalmente, conforme a lo recogido en el Plan de Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas (PSSIAP), en su calidad de Plan Derivado del Plan Nacional de Ciberseguridad, y dando respuesta a lo señalado en la Línea de Acción 2 de la Estrategia de Ciberseguridad Nacional, la presente Guía articula el correspondiente **Esquema de Declaración y Certificación de Conformidad con el ENS**, determinando las condiciones para alcanzar aquel cumplimiento normativo.
8. El PSSIAP, como consecuencia de las acciones de verificación del estado de implantación del ENS, recogió el mandato del artículo 41 del ENS y propuso la creación de un distintivo que, además de dar respuesta a las exigencias legales de publicidad recogidas en el RD 3/2010, sirviera también para incentivar a aquellos organismos que, de manera verificable, hubieren alcanzado la conformidad con la implantación del ENS en alguno de sus sistemas de información.
9. 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 distintivos de seguridad** mencionados en el citado artículo 41 del ENS, quién puede solicitarlos, quién puede concederlos y cómo deben hacerse visibles en los espacios públicos tecnológicos de los organismos afectados o en los privados de los operadores económicos concernidos.

2. LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

2.1. CRITERIOS DE DETERMINACIÓN DE LA CONFORMIDAD

10. El ENS, en su condición de norma legal y tal como se recoge en su artículo 3, resulta de obligado cumplimiento para todos los sistemas de su ámbito de aplicación², sin más excepciones que los sistemas que tratan la información clasificada regulada en la Ley 9/1968, de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.
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

² Ámbito de aplicación subjetivo regulado en el art. 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

cumplimiento de los requerimientos contemplados en el ENS, al menos cada dos años. Con carácter extraordinario, tal auditoría deberá realizarse siempre que se produzcan modificaciones significativas en el sistema considerado que pudieran repercutir en las medidas de seguridad que deban adoptarse, tal y como disponen el artículo 34 y el Anexo III del ENS

14. 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 años. Con carácter extraordinario, tal autoevaluación deberá realizarse siempre que se produzcan modificaciones significativas en el sistema considerado, que pudieran repercutir en las medidas de seguridad que deban adoptarse, tal y como disponen el artículo 34 y el Anexo III del ENS.
15. 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.

2.2. PROCEDIMIENTO DE DETERMINACIÓN DE LA CONFORMIDAD

16. Como se desprende de lo contenido en el Anexo I del ENS, la conformidad con la norma de un sistema de información concreto pasa necesariamente por **adoptar y manifestar que se han implantado** 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**.
17. Esta constatación de conformidad, tanto inicial como periódica, queda claramente reflejada en el artículo 34 del ENS, cuando señala:

Artículo 34. Auditoría de la seguridad.

1. *Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad. Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría 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.*
2. *Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.*
3. *En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.*
4. *En la realización de esta auditoría se utilizarán los criterios, métodos de*

trabajo y de conducta, generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. *El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. 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.*
 6. *Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.*
 7. *En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.*
 8. *Los informes de auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las tecnologías de la información.*
18. Por su parte, el Anexo III del ENS precisa el alcance de la verificación referida en el artículo anterior, prescribiendo los dos procedimientos que se resumen en el cuadro siguiente:

Procedimiento de verificación	Categoría de los Sistemas Afectados	Manifestación de Conformidad	Resultado de la verificación	Análisis de la verificación
AUTOEVALUACIÓN realizada por el mismo personal que administra el sistema de información o aquel otro en quién hubiere delegado.	BÁSICA	DECLARACIÓN DE CONFORMIDAD	Documento de autoevaluación , indicando si cada medida de seguridad está implantada 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	MEDIA / ALTA	CERTIFICACIÓN DE	Informe de auditoría , dictaminando sobre el grado de cumplimiento con el ENS,	Los informes de auditoría serán analizados por el

con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.		CONFORMIDAD	identificando sus deficiencias y sugiriendo, en su caso, posibles medidas correctoras o complementarias y las recomendaciones que se consideren oportunas. Deberá incluir o referenciar 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.	responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
--	--	--------------------	---	--

3. PUBLICIDAD DE LA CONFORMIDAD

19. Alcanzada la conformidad con el ENS, y atendiendo a los dos 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

20. 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 BÁSICA-, 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.
21. 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.
22. 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 ENS³**, 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 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, Miércoles 2 de noviembre de 2016).

23. La Certificación de Conformidad con el ENS a la que se refiere el punto anterior deberá ser expedida por una Entidad Certificadora 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 conformidad. Requisitos para organismos que certifican productos, procesos y servicios*, para la certificación de sistemas de información del ámbito de aplicación del ENS.
24. Si no dispusiere de la acreditación señalada en el punto anterior, la Entidad Certificadora de que se trate, 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.
25. De acuerdo con lo indicado en la cláusula 4.2.6 e) de la norma UNE-EN ISO/IEC 17065:2012, la Entidad Certificadora, 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 (ENS, ISO 27000, COBIT, Octave u otros de naturaleza similar) ni auditoría interna sobre tales sistemas de gestión.
26. Cualquier situación que ponga a la entidad certificadora en la necesidad de evaluar el producto de su propio trabajo es una amenaza inaceptable para la imparcialidad y la entidad certificadora debe tomar acciones para identificar y evitar tales situaciones.
27. La entidad certificadora no podrá certificar a una organización si en los dos años anteriores a la solicitud de certificación la propia entidad certificadora, 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.
28. En el caso de que la propia entidad certificadora, 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.
29. El CCN mantendrá en su sede electrónica una relación actualizada de las Entidades de Certificación, acreditadas o en vías de acreditación, para expedir Certificaciones de Conformidad con el ENS.
30. 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.

31. Como se ha dicho, 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 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, conforme a lo dispuesto en el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010.

3.2. DECLARACIÓN DE CONFORMIDAD

32. 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.
33. La Declaración de Conformidad con el ENS se expresará en un documento electrónico, en formato no editable, firmado electrónicamente por la propia entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión o por quién en esta hubiere delegado.
34. La Declaración de Conformidad con el ENS podrá representarse mediante un **Distintivo de Declaración de Conformidad**, que será generado por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, y cuyo uso por parte de la entidad pública titular o usuaria del sistema de información en cuestión estará condicionado a la antedicha Declaración de Conformidad con el ENS.
35. El citado 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 entidad pública o privada, respectivamente, de que se trate.

3.3. CERTIFICACIÓN DE CONFORMIDAD

36. 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.
37. 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**.
38. 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.
39. La Certificación de Conformidad con el ENS podrá representarse mediante un **Distintivo de Certificación de Conformidad**, que será expedido por la Entidad

Certificadora de que se trate, y cuyo uso por parte de la entidad pública titular o usuaria del sistema de información en cuestión estará condicionado a la posesión de la antedicha Certificación de Conformidad.

40. El citado 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. SOLUCIONES Y SERVICIOS PRESTADOS POR EL SECTOR PRIVADO

41. Como hemos señalado con anterioridad, es muy frecuente que las organizaciones del sector privado participen en la provisión de soluciones tecnológicas o en la prestación de servicios a las entidades públicas (a través, por ejemplo, de servicios en la nube).
42. Cuando las organizaciones del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del ENS, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el ENS (cuando se trate de sistemas de categoría BÁSICA) o la Certificación de Conformidad con el ENS (obligatoriamente, cuando se trate de sistemas de categorías MEDIA o ALTA, y de aplicación voluntaria en el caso de sistemas de categoría BÁSICA), utilizando los mismos procedimientos que los exigidos para las entidades públicas.
43. Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en esta Guía.
44. Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del ENS sean realizados por organizaciones del sector privado, estas utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Guía, sustituyendo las referencias a las entidades públicas por las correspondientes a las entidades privadas. Análogamente, los Distintivos de Conformidad, cuando se exhiban por parte de dichos operadores privados, deberán enlazar con las correspondientes Declaraciones o Certificaciones de Conformidad, que permanecerán siempre accesibles en la página web del operador de que se trate.
45. Además del Centro Criptológico Nacional, las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el ENS podrán solicitar en todo momento a tales operadores los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones.

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

46. Las Entidades de Certificación del ENS que hubieren expedido Certificaciones de Conformidad con el ENS, tanto a entidades del sector público como del privado, conforme al procedimiento descrito en esta Guía y a lo dispuesto en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, comunicarán al Centro Criptológico Nacional la expedición de dichos Certificados de Conformidad dentro de los siete días siguientes a la expedición del Certificado de que se trate, a través de la dirección de correo electrónico certificaciones809ens@ccn-cert.cni.es, adjuntando el correspondiente documento electrónico de Certificación de la Conformidad con el ENS, que habrá sido firmado/sellado electrónicamente por la Entidad de Certificación. Dicha comunicación es igualmente exigible cuando se trate de suspensiones o retiradas de Certificados de Conformidad previos.
47. El Centro Criptológico Nacional mantendrá en su página web una relación de las entidades 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.

ANEXO A. MODELOS DE DECLARACIÓN DE CONFORMIDAD Y DISTINTIVO

Logotipo de la Entidad Pública declarante Identificación inequívoca de la Unidad del declarante dirección		
DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD		
Los sistemas de información y los servicios prestados, de categoría BÁSICA, han superado un proceso de autoevaluación conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de <<fecha>> para:		
1.	Denominación Sistema de Información 1 y servicios prestados	
2.	Denominación Sistema de Información 2 y servicios prestados	
...	...	
Fecha de declaración de conformidad inicial: <<día>> de <<mes>> de <<año>>" Fecha de renovación de la declaración de conformidad: <<día>> de <<mes>> de <<año>>" En Localidad, a día de mes de año.		
Fdo. Nombre y Apellidos del titular del Órgano Superior de que se trate Administración Pública de que se trate		

Nota: Los textos señalados en letra *cursiva* deben ser adaptados a cada caso.

A efectos de dar cumplimiento a lo dispuesto en el artículo 41 del ENS, los **Distintivos referidos a las Declaraciones de Conformidad con el ENS** que se exhibirán en la sede electrónica del organismo en cuestión, poseerán el aspecto y contenido que se muestra en la figura siguiente y un enlace a la Declaración de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica del organismo de que se trate.

Colores directos: Pantone Orange 021C



CMYK

C:0

Y:100

K:0

RGB

R:235

M:53

B:12

HEXADECIMAL

FF6600

G:111

ANEXO B. MODELOS DE CERTIFICACIÓN DE CONFORMIDAD Y DISTINTIVO

A modo de ejemplo, se incluye seguidamente el aspecto que podría tener una Certificación de Conformidad con el ENS.

Logotipo
de la
Entidad Certificadora
con marca de
certificación acreditada

CERTIFICACIÓN DE
CONFORMIDAD CON EL

 Esquema Nacional de
Seguridad
 Categoría MEDIA
 RD 3/2010

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

“<<Entidad Certificadora>>” certifica que los sistemas de información reseñados, todos ellos de categoría <<señalar categoría máxima aplicable (BÁSICA, MEDIA o ALTA)>> y los servicios que se relacionan, de << Entidad [pública o privada], dirección postal>>.

han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración, según se indica en el correspondiente Informe de Auditoría de <<fecha>> para:

<<enumerar los sistemas de información y los servicios objeto de la certificación>>.

Fecha de certificación de conformidad inicial: <<día>> de <<mes>> de <<año>>.

Fecha de renovación de la certificación de conformidad: <<día>> de <<mes>> de <<año>>.

Número de certificado: <<número de certificado>>.

Fecha<<Localidad (la que corresponda)>>, <<día>> de <<mes>> de <<año>>”.

Firma: <<Nombre y Apellidos del responsable competente de la Entidad Certificadora>>.

Firma del responsable de la Entidad Certificadora:

Nombre completo /razón social de la Entidad Certificadora y pág. web.
 Dirección postal/ electrónica.
 Código Postal. Provincia. País.

A efectos de dar cumplimiento a lo dispuesto en el artículo 41 del ENS, los **Distintivos de Conformidad referidos a las Certificaciones de Conformidad con el ENS**, que se exhibirán en la sede electrónica del organismo en cuestión, poseerán el aspecto y contenido que se muestra en la figura siguiente, incluyendo la categoría del sistema certificado (BASICA, MEDIA o ALTA) y un enlace a la Certificación de Conformidad anterior, que también permanecerá accesible a través de la sede electrónica del organismo de que se trate.



Colores directos

Pantone 653C

CMYK

M: 47

Y: 11

Y: 11

K: 0

RGB

R: 55

G: 99

B: 150

HEXADECIMAL

336699