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.

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 265, de 2 de noviembre de 2016
Referencia: BOE-A-2016-10109

TEXTO CONSOLIDADO
Última modificación: sin modificaciones

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, prevé en su artículo 29 apartado 2 que el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Dichas instrucciones técnicas de seguridad son esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema.

Así, estas instrucciones técnicas de seguridad, enumeradas en la disposición adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; notificación de incidentes de Seguridad; auditoría de la Seguridad; conformidad con el Esquema Nacional de Seguridad; adquisición de Productos de Seguridad; criptología de empleo en el Esquema Nacional de Seguridad; interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad establece los criterios y procedimientos para la determinación de la conformidad con el Esquema Nacional de Seguridad y para la publicidad de dicha

conformidad, al objeto de poder dar adecuada respuesta al mandato del Capítulo VIII, Normas de conformidad, del Real Decreto 3/2010, de 8 de enero; así, determina los mecanismos de obtención y ulterior publicidad de las declaraciones de conformidad y los distintivos de seguridad de los que sean acreedores y que se hubieren obtenido respecto al cumplimiento del Esquema Nacional de Seguridad.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29 apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Conformidad con el Esquema Nacional de Seguridad», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 13 de octubre de 2016.

El Secretario de Estado de Administraciones Públicas,
Antonio Germán Beteta Barreda.

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

I. Objeto

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad tiene por objeto establecer los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.

II. Ámbito de aplicación

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en lo dispuesto en el artículo 3 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.

III. Procedimientos de determinación de la conformidad

III.1 En función de la categoría de los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, de acuerdo con el Anexo I del Real Decreto 3/2010, de 8 de enero, se define el procedimiento de determinación de la conformidad. Así los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, mientras que los sistemas de categoría MEDIA O ALTA precisarán de una auditoría formal para su certificación de la conformidad.

III.2 La declaración de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información con categoría BÁSICA se realizará mediante una autoevaluación que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el Esquema, al menos cada dos años. Dicha autoevaluación atenderá a lo dispuesto sobre auditoría en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 La certificación de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información 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 Esquema, al menos cada dos años. Dicha auditoría se realizará según lo dispuesto en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero.

III.4 Siendo obligatoria la auditoría formal para los sistemas de categoría MEDIA Y ALTA nada impide que un sistema de categoría BÁSICA se someta igualmente a una auditoria formal de certificación de la conformidad, siendo esta posibilidad siempre la deseable.

III.5 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.

IV. Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA y su publicidad

IV.1 La Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA o inferior será expedida por la propia entidad bajo cuya responsabilidad se encuentren dichos sistemas, y se completará mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la antedicha Declaración de Conformidad.

IV.2 Dicha Declaración de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos I y II respectivamente de la presente Instrucción Técnica de Seguridad.

IV.3 Para publicar la Declaración de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría BÁSICA o inferior bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Declaración de Conformidad que incluirá un enlace al documento de Declaración de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

V. Certificación de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría MEDIA o ALTA y su publicidad

V.1 La Certificación de Conformidad con el Esquema Nacional de Seguridad, de sistemas de categorías MEDIA o ALTA, será expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad.

V.2 Dicha Certificación de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos III y IV respectivamente de la presente Instrucción Técnica de Seguridad.

V.3 Para publicar la Certificación de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría MEDIA O ALTA bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Certificación de Conformidad que incluirá un enlace al documento de Certificación de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

VI. Requisitos de las entidades certificadoras

VI.1 Las entidades certificadoras a las que se refiere esta Instrucción Técnica deberán estar acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.

VI.2 Si la entidad certificadora de que se trate no dispusiere de la acreditación señalada, previamente a iniciar sus actividades, deberá remitir al Centro Criptológico Nacional, la aceptación por parte de la Entidad Nacional de Acreditación de haber solicitado la acreditación antedicha, pudiendo iniciar sus actividades de certificación de forma transitoria, disponiendo de 12 meses para obtener dicha acreditación, transcurridos los cuales sin haberla obtenido deberán cesar en sus actividades de certificación. El Centro Criptológico Nacional podrá requerir a la entidad certificadora solicitante cuanta información adicional considere necesaria que le permita verificar su adecuación y suficiencia.

VI.3 Transcurrido un año desde la entrada en vigor de la presente Instrucción Técnica de Seguridad, ya no será posible iniciar ningún proceso de certificación de la forma transitoria señalada en el punto anterior, exigiéndose a todas las entidades de certificación la acreditación recogida en el punto VI.1.

VI.4 Estarán exentas del cumplimiento de los requisitos señalados en los puntos anteriores del presente epígrafe 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.

VI.5 El Centro Criptológico Nacional 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 Esquema Nacional de Seguridad.

VII. Soluciones y servicios prestados por el sector privado

VII.1 Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

VIII.2 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 Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad.

VII.3 Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del Esquema Nacional de Seguridad sean realizados por operadores del sector privado, estos utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Instrucción Técnica de Seguridad, 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 electrónica del operador de que se trate.

VII.4 Además del Centro Criptológico Nacional y la Entidad Nacional de Acreditación, 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 Esquema Nacional de Seguridad 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.

ANEXO I

Contenido de la Declaración de Conformidad con el Esquema Nacional de Seguridad

Cada entidad u organismo declarante podrá disponer libremente de su propio formato de Declaración de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la entidad u organismo declarante.
– Identificación de la entidad u organismo declarante.
– Distintivo de Declaración de Conformidad de acuerdo al anexo II de esta Instrucción Técnica de Seguridad.
– Texto: “Declaración de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “Los sistemas de información reseñados, todos ellos de categoría BÁSICA, y los servicios que se relacionan, 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 en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de <>:”

– <>.

– Texto: “Fecha de declaración de conformidad inicial: <> de <> de <>”
– Texto: “Fecha de renovación de la declaración de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: <>.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la Declaración de Conformidad expedida.

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Declaración de conformidad.

ANEXO II

Distintivo de Declaración de Conformidad con el Esquema Nacional de Seguridad

En la medida de lo posible, los Distintivos de Declaración de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

Colores directos	CMYK	RGB	Hexadecimal
Pantone Orange 021C	C: 0	R: 235	FF6600
	M: 53	G: 111	
	Y: 100	B: 12	
	K: 0		

ANEXO III

Contenido de la Certificación de Conformidad con el Esquema Nacional de Seguridad

Cada Entidad Certificadora podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la Entidad Certificadora.
– Identificación de la Entidad Certificadora.
– Distintivo de Certificación de Conformidad de acuerdo al anexo IV de esta Instrucción Técnica de Seguridad.
– Texto: “Certificado de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “<> certifica que los sistemas de información reseñados, todos ellos de categoría <>, y los servicios que se relacionan, de <>, 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 electrónica, según se indica en el correspondiente Informe de Auditoría de <>:”

– <>.

– Texto: “Número de certificado: <>”.
– Texto: “Fecha de certificación de conformidad inicial: <> de <> de <>”.
– Texto: “Fecha de renovación de la certificación de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: Nombre y Apellidos del responsable competente de la Entidad Certificadora.

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

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Certificación de conformidad.

ANEXO IV

Distintivo de Conformidad con el Esquema Nacional de Seguridad

En la medida de lo posible, los Distintivos de Certificación de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

Colores directos	CMYK	RGB	Hexadecimal
Pantome 653C	C: 82	R: 55	336699
	M: 47	G: 99	
	Y: 11	B: 150	
	K: 0		