GUÍA DE SEGURIDAD
(CCN-STIC-809)

DECLARACIÓN DE CONFORMIDAD DEL ESQUEMA NACIONAL DE SEGURIDAD (BORRADOR)

29 JULIO 2010

Edita:

NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: julio de 2010
José María Molina ha participado en la redacción del documento.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (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, 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 información 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 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.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad 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 las comunicaciones 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.

Julio de 2010

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN....4
2. CONSIDERACIONES CONJUNTAS DE ADECUACIÓN Y CONFORMIDAD....4
3. DECLARACIÓN DE CONFORMIDAD....4
3.1. CONTENIDO. 4
3.2. IDENTIFICACIÓN DEL DECLARANTE....5
3.3. OBJETO DE LA DECLARACIÓN.....5
3.4. BASE Y FINALIDAD DE LA DECLARACIÓN DE CONFORMIDAD....5
3.5. LUGAR, FECHA Y FIRMA DE LA DECLARACIÓN....6
4. MECANISMO DE CONTROL....6
5. DISTINTIVO DE SEGURIDAD....6
6. MODELO DE DECLARACIÓN DE CONFORMIDAD 6

1. INTRODUCCIÓN

1. La presente Guía tiene por objeto dar pautas generales para la aplicación de lo dispuesto en el artículo 41 del Esquema Nacional de Seguridad, sin perjuicio de la particularización de cada organismo.
2. 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 dedica su capítulo VIII a las normas de conformidad. El artículo 41 preceptúa que los órganos y entidades de derecho público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

2. CONSIDERACIONES CONJUNTAS DE ADECUACIÓN Y CONFORMIDAD.

3. De acuerdo con lo dispuesto en la disposición transitoria del Real Decreto 2/2010, de 8 de enero, los sistemas existentes a su entrada en vigor dispondrán de doce meses para adecuarse al Esquema Nacional de Seguridad, de forma que puedan cumplir lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio.
4. Cuando existan motivos fundados para entender que a la finalización del periodo de tiempo señalado no se haya producido la adecuación indicada, debido a la existencia de causas que lo impidan, los órganos superiores competentes dispondrán lo necesario para elaborar un plan de adecuación de acuerdo con lo establecido en la Guía CCN-STIC 806, en el que, entre otros aspectos, se señale de forma clara y concisa, los plazos de ejecución que, en ningún caso, serán superiores a cuarenta y ocho meses desde la entrada en vigor del Real Decreto indicado.
5. Una vez finalizado el periodo inicial de doce meses, el 30 de enero de 2011 se publicará la declaración de conformidad o, en su caso, el plan de adecuación, en los términos señalados en las Guías correspondientes.

3. DECLARACIÓN DE CONFORMIDAD

6. Los órganos y entidades de derecho público darán publicidad a la conformidad de sus sistemas respecto al cumplimiento del Esquema Nacional de Seguridad, de acuerdo con lo dispuesto en el Capítulo VIII del Real Decreto 3/2010, de 8 de enero, mediante declaraciones escritas, publicadas en las correspondientes sedes electrónicas y situadas en lugar de fácil acceso para los usuarios.

3.1 CONTENIDO.

7. El contenido de la declaración de conformidad constará de tres cuerpos. En el primer cuerpo se identificará el declarante, en el segundo se indicará el contenido de la declaración y, en el tercero, se señalará en base a qué se declara la conformidad y con qué finalidad.

3.2. IDENTIFICACIÓN DEL DECLARANTE.

8. El órgano o entidad de derecho público titular del sistema, que se declara conforme, se identificará de forma inequívoca en la declaración escrita, señalando grupos operativos, departamentos o Administración a la que pertenece, o los datos que fuesen necesarios para proporcionar la identificación indubitada del organismo público a que se refiere, mediante la denominación con la que aparece en la norma que aprueba la estructura orgánica a la que está adscrito.

3.3. OBJETO DE LA DECLARACIÓN.

9. El contenido de la declaración de conformidad ha de describir de forma inequívoca el objeto de la misma, identificar de forma fidedigna el sistema o sistemas, y servicios a los que se refiere, e indicar que ha superado el plan de adecuación para lograrlo, en su caso.

10. a) La descripción del objeto se hará mediante la manifestación expresa que el sistema cumple los requerimientos establecidos en el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regulado por Real Decreto 3/2010, de 8 de enero y, especialmente, lo dispuesto en los artículos 38, 39 y 40, de forma que recoja constancia expresa de lo siguiente:

    - Que las sedes y registros electrónicos, así como el acceso electrónico de los ciudadanos a los mismos y a los servicios que proporcionan, cumplen las exigencias de seguridad del ENS.
    - Que las especificaciones de seguridad están incluidas en el ciclo de vida de los servicios y sistemas, acompañadas del correspondiente procedimiento de control.
    - Que existe mecanismo de control para garantizar el cumplimiento del ENS, establecido por el órgano o entidad de derecho público que efectúa la declaración.

11. b) La identificación del sistema se efectuará mediante su descripción de forma que pueda ser reconocido indubitadamente y, contendrá, al menos, los siguientes datos:

    - Nombre del sistema.
    - Objeto.
    - Servicios que presta.

12. c) Los servicios se identificarán con nombres comprensibles para los ciudadanos, con indicación genérica de la información que maneja.

13. d) El plan de adecuación, en su caso, se identificará de acuerdo con lo establecido en la Guía CCN-STIC 806.

3.4. BASE Y FINALIDAD DE LA DECLARACIÓN DE CONFORMIDAD.

14. La base por la que se declara la conformidad con los requisitos esenciales del ENS, es la superación en conformidad de la evaluación efectuada, realizada por el Responsable de Seguridad, mediante la elaboración de un dictamen técnico en el que se señale, de forma expresa, que el sistema a que se refiere es conforme al Esquema Nacional de Seguridad, con indicación que la declaración de conformidad se realiza de acuerdo con lo

establecido en el Capítulo VIII del Real Decreto 3/2010, de 8 de enero, y la presente Guía.

3.5. LUGAR, FECHA Y FIRMA DE LA DECLARACIÓN.

15. La declaración de conformidad contendrá expresión del lugar y fecha de la emisión de la misma.
16. El lugar se expresará mediante indicación de la ciudad, la provincia entre paréntesis, en el caso que la ciudad no sea capital de la misma y, de igual modo, España.
17. Asimismo se ha de firmar por el titular del organismo emisor de la declaración de conformidad, que ha de ser identificado con su nombre, dos apellidos y cargo que ostenta.

4. MECANISMO DE CONTROL.

18. Los mecanismo de control a los que se refiere el artículo 41, son los instrumentos mediante los que se garantiza que la declaración de conformidad mantiene su vigencia durante el transcurso del tiempo.
19. Podrían consistir en una evaluación anual de los parámetros que acreditan la conformidad de un sistema al Esquema Nacional de Seguridad, realizada por el Responsable de Seguridad y plasmado en un informe técnico bajo su firma, u otro mecanismo análogo que consiga la misma finalidad.

5. DISTINTIVOS DE SEGURIDAD.

20. La publicidad de los distintivos de seguridad a los que sean acreedores los sistemas o los órganos o entidades de derecho público respecto a los mismos, reunirán los requisitos establecidos para la declaración de conformidad, referidas al distintivo de seguridad correspondiente, añadiendo, de forma clara, los datos relativos a la entidad que los emite y el ámbito al que se refiere.
21. Entre estos distintivos se incluirán certificaciones de accesibilidad, interoperabilidad, menciones de calidad de cualesquiera de las Administraciones públicas (estatal, autonómica y local), de organizaciones internacionales o de organismos privados.

6. MODELO DE DECLARACIÓN DE CONFORMIDAD.

22. El modelo recomendado para efectuar la declaración de conformidad es el siguiente:

"DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Nombre del declarante:……..

(identificación del órgano o entidad de derecho público que la formula)

Dirección postal……

Dirección electrónica……

En cumplimiento de lo dispuesto en el artículo 41 del Real Decreto 372010, de 8 de enero, declara bajo su exclusiva responsabilidad la conformidad del Sistema…….
al que se refiere este documento, con el Esquema Nacional de Seguridad regulado en el citado real decreto.

Información adicional:

1) Las sedes y registros electrónicos, así como el acceso electrónico de los ciudadanos a los mismos y a los servicios que estos proporcionan, cumplen las exigencias de seguridad del Esquema Nacional de Seguridad.

2) Las especificaciones de seguridad están incluidas en el ciclo de vida de los servicios y sistemas, acompañadas del correspondiente procedimiento de control.

3) El mecanismo de control establecido por…… que efectúa la declaración de garantía de cumplimiento del ENS, consiste en…….

4) Otros avales de seguridad:……
……
……
……

En ……a……de……de…….

Persona que lo firma:……
Cargo que ostenta:…….
Firma:……..”

ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Para más información sobre términos y abreviaturas empleados en el Esquema Nacional de Seguridad se recomienda consultar la guía de seguridad CCN-STIC-800 “ESQUEMA NACIONAL DE SEGURIDAD GLOSARIO DE TÉRMINOS Y ABREVIATURAS”.