
# GUÍA DE SEGURIDAD
# (CCN-STIC-806)

# ESQUEMA NACIONAL DE SEGURIDAD
# PLAN DE ADECUACIÓN


**ENERO 2011**

Edita:



NIPO: 075-11-053-3

Tirada: 1000 ejemplares
Fecha de Edición: enero de 2011
José Antonio Mañas ha participado en la redacción del documento.
El Ministerio de Política Territorial y Administración Pública ha financiado el desarrollo del presente documento y sus anexos.

# 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.

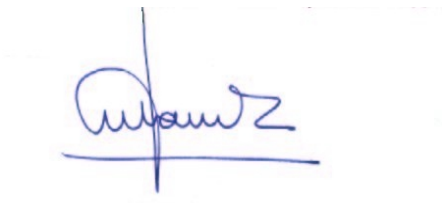
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Enero de 2011



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE

**1. INTRODUCCIÓN ..... 4**
**2. RESPONSABILIDAD ..... 4**
**3. CONTENIDO ..... 4**
3.1. LA POLÍTICA DE SEGURIDAD ..... 5
3.2. INFORMACIÓN QUE SE MANEJA, CON SU VALORACIÓN ..... 5
3.3. SERVICIOS QUE SE PRESTAN, CON SU VALORACIÓN ..... 5
3.4. DATOS DE CARÁCTER PERSONAL ..... 6
3.5. CATEGORÍA DEL SISTEMA ..... 6
3.6. ANÁLISIS DE RIESGOS ..... 6
3.7. DECLARACIÓN DE APLICABILIDAD DE LAS MEDIDAS DEL ANEXO II DEL ENS ..... 6
3.8. INSUFICIENCIAS DEL SISTEMA ..... 6
3.9. PLAN DE MEJORA DE LA SEGURIDAD ..... 7
**4. INTERCONEXIÓN DE SISTEMAS ..... 7**
**ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS ..... 8**
**ANEXO B. REFERENCIAS ..... 10**

# 1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. El Esquema Nacional de Seguridad, en su Disposición Transitoria sobre Adecuación de los Sistema, dice que
    1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.
    2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un **plan de adecuación** que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

       El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.
3. Esta guía propone un modelo genérico de Plan de Adecuación.

# 2. RESPONSABILIDAD

4. El plan de adecuación será elaborado por el Responsable de Seguridad del sistema.
5. Si el Responsable de Seguridad no está nombrado oficialmente, hará sus funciones, de forma temporal, quien la Dirección designe, anexándose al plan de adecuación su designación formal, que incluirá las funciones temporalmente asignadas y el periodo máximo de ejercicio de estas funciones con carácter temporal.

# 3. CONTENIDO

6. El plan de adecuación contendrá la siguiente información:
    1. la política de seguridad
    2. información que se maneja, con su valoración
    3. servicios que se prestan, con su valoración
    4. datos de carácter personal
    5. categoría del sistema
    6. análisis de riesgos
    7. declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
    8. insuficiencias del sistema *(gap analysis)*
    9. plan de mejora seguridad, incluyendo plazos estimados de ejecución
7. El plan de adecuación deberá estar aprobado por los órganos superiores competentes.

## 3.1. LA POLÍTICA DE SEGURIDAD

8. Si el organismo dispone de una Política de Seguridad conforme a lo que se pide en el Anexo II del ENS, sección [org.1], ésta se identificará y anexará al plan de adecuación.
9. Si se dispone de una Política de Seguridad, pero no satisface los requisitos del Anexo II, sección [org.1],
    1. se identificará la política de aplicación
    2. se anexará al plan de adecuación
    3. en el plan de mejora de la seguridad se hará constar cómo se planea adaptar la política a las exigencias del Anexo II
10. Si no se dispone de una Política de Seguridad, en el plan de mejora de la seguridad se hará constar cómo se planea desarrollar la política de acuerdo a las exigencias de Anexo II.

## 3.2. INFORMACIÓN QUE SE MANEJA, CON SU VALORACIÓN

11. Se hará constar una relación detallada de la información que se maneja, junto con su valoración según lo establecido en el Anexo I del Esquema Nacional de Seguridad.
12. Pueden darse varias causas que impidan alcanzar plenamente el objetivo propuesto en el párrafo anterior:
    - se carece de una Política de Seguridad, o esta es insuficiente
    - no está nombrado el responsable de alguna de las informaciones tratadas
    - no está aprobada formalmente la valoración de la información
13. En tales casos, la valoración la realizará y argumentará el Responsable de Seguridad, a su mejor criterio, dejando constancia de los motivos o razonamientos. Esta valoración sólo es vinculante para el organismo mientras no se disponga de la valoración formal. Deberá constar un plazo límite para disponer de la valoración formal.

## 3.3. SERVICIOS QUE SE PRESTAN, CON SU VALORACIÓN

14. Se hará constar una relación detallada de los servicios que se prestan, junto con su valoración según lo establecido en el Anexo I del Esquema Nacional de Seguridad.
15. Pueden darse varias causas que impidan alcanzar plenamente el objetivo propuesto en el párrafo anterior:
    - se carece de una Política de Seguridad, o esta es insuficiente
    - no está nombrado el responsable de alguno de los servicios prestados
    - no está aprobada formalmente la valoración de la información
16. En tales casos, la valoración la realizará y argumentará el Responsable de Seguridad, a su mejor criterio, dejando constancia de los motivos o razonamientos. Esta valoración sólo es vinculante para el organismo mientras no se disponga de la valoración formal. Deberá constar un plazo límite para disponer de la valoración formal.

## 3.4. DATOS DE CARÁCTER PERSONAL

17. Si el sistema maneja datos de carácter personal, el plan de adecuación incluirá una relación detallada de dichos datos. Bastará una referencia al Documento de Seguridad requerido por el RD 1720 de 2007.

## 3.5. CATEGORÍA DEL SISTEMA

18. El Responsable de Seguridad llevará a cabo los pasos descritos en el Anexo I para establecer la categoría del sistema.
19. Si lo considera oportuno, puede fragmentar el sistema en varios sub-sistemas a fin de acotar las exigencias de medidas de protección y, en última instancia, reducir los recursos necesarios.

## 3.6. ANÁLISIS DE RIESGOS

20. El plan de adecuación incorporará un análisis de riesgos, según lo descrito en el Anexo II, sección [op.pl.1] para la categoría establecida para el sistema.
21. En el análisis de riesgos se valorarán las salvaguardas presentes en la fecha de aprobación del plan de adecuación.

## 3.7. DECLARACIÓN DE APLICABILIDAD DE LAS MEDIDAS DEL ANEXO II DEL ENS

22. Vistas las exigencias del Anexo II del ENS y las exigencias derivadas de los datos de carácter personal, el Responsable de Seguridad elaborará una relación de las medidas que son de aplicación al sistema (o a cada sub-sistema, si se ha recurrido a una fragmentación como se describe en la sección anterior).
23. Habitualmente se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.
24. Cuando una medida requerida por el Anexo II en función de la valoración del sistema no vaya se consideré aplicable, esta no-aplicabilidad debe estar motivada.
25. Cuando se recurra a medidas alternativas, se indicará el motivo, así como las medidas que sustituye.
26. Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado. Téngase en cuenta que tanto el ENS como la reglamentación de protección de datos de carácter personal, establecen una serie de medidas mínimas que deben ampliarse cuando sea prudente hacerlo.

## 3.8. INSUFICIENCIAS DEL SISTEMA

27. Pueden detectarse insuficiencias en el sistema por varias vías:
    - Incumplimiento formal de las medidas de seguridad exigidas en el Anexo II para la valoración del sistema
    - Incumplimiento formal de las medidas de seguridad exigidas por el RD 1720/1997 para los datos de carácter personal tratados por el sistema
    - Existencia de riesgos no asumibles por el organismo.

28. Formalmente, los riesgos residuales deben ser aceptados por los responsables de la información y servicios afectados. Si no están designados o si la aceptación del riesgo no es formal, el Responsable de Seguridad tomará la decisión a su mejor criterio, indicando las circunstancias que le llevan a ello y motivando sus decisiones de aceptación o no del riesgo residual.

### 3.9. PLAN DE MEJORA DE LA SEGURIDAD

29. El plan de mejora de la seguridad constará de una serie de actuaciones destinadas a subsanar las insuficiencias detectadas.
30. Cada actuación prevista incluirá
    - las insuficiencias que subsana
    - el plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación, así como los principales hitos intermedios
    - una estimación del coste que supondrá
31. Las fechas de inicio pueden limitarse al año en que se prevé acometer la actuación.
32. La fecha de terminación se puede calcular en función del tiempo que se ha estimado para ejecutar la actuación.
33. El coste puede ser estimativo o basarse en ofertas ya disponibles.

## 4. INTERCONEXIÓN DE SISTEMAS

1. Cuando un sistema maneja información de terceros o presta servicios a terceros, la valoración de la información y los servicios será la determinada por dicho tercero.
2. Para la realización del plan de adecuación, se requiere conocer la valoración realizada por los responsables del otro sistema. Si se carece de dicha valoración, el Responsable de Seguridad establecerá unos valores a su mejor criterio y los hará constar como “compromiso de prestación de servicios”. Si en el futuro los responsables del otro sistema elevan las exigencias en materia de seguridad, se recurrirá a la realización de un “plan de adecuación incremental” que contemple las actuaciones encaminadas a subsanar las insuficiencias derivadas del nuevo escenario.
3. Cuando un sistema utiliza sistemas de terceros para manejar información o para prestar servicios, la valoración propia será impuesta al tercero que colabora, que la tendrá en cuenta en su propio plan. Si el prestatario está sujeto al cumplimiento del Esquema Nacional de Seguridad, incorporará estos requisitos a su propio plan de adecuación o a su propia declaración de conformidad.

# ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

**Análisis de riesgos**

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

**Datos de carácter personal**

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

**Información**

Caso concreto de un cierto tipo de información.

**Information.** An instance of an information type. FIPS 199.

**Política de seguridad**

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. ENS.

**Responsable de la información**

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

**Information Owner.** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

**Responsable de la seguridad**

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

The **Computer Security Program Manager** (and support staff) directs the organization's day-today management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

**Information systems security manager (ISSM).** Individual responsible for a program, organization, system, or enclave’s information assurance program. CNSS Inst. 4009.

**Responsable del servicio**

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

**Responsable del sistema**

Persona que se encarga de la explotación del sistema de información.

**Information System Owner (or Program Manager).** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted

**Servicio**

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

**Sistema de información**

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

**Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

# ABREVIATURAS

| | |
|---|---|
| ENS | Esquema Nacional de Seguridad |

# ANEXO B. REFERENCIAS

**Ley 11/2007**

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.

**Ley 15/1999**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.

**RD 1720/2007**

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

**RD 3/2010**

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. BOE de 29 de enero de 2010.