

**GUÍA DE SEGURIDAD  
(CCN-STIC-805)**

**ESQUEMA NACIONAL DE SEGURIDAD  
POLÍTICA DE SEGURIDAD DE LA  
INFORMACIÓN**

Edita:



© Editor y Centro Criptológico Nacional, 2011  
NIPO: 075-11-053-3

Tirada: 1000 ejemplares

Fecha de Edición: septiembre de 2011

El Sr. José Antonio Mañas ha elaborado este documento.

El Ministerio de Política Territorial y Administración Pública ha financiado el 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 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.

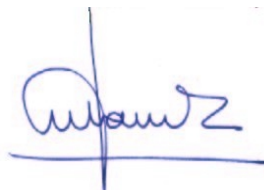
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Septiembre de 2011



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

**ÍNDICE**

<b>1. INTRODUCCIÓN.....</b>	<b>4</b>
<b>2. PRINCIPIOS DE SEGURIDAD .....</b>	<b>5</b>
<b>3. CONTENIDO .....</b>	<b>5</b>
3.1. MISIÓN DEL ORGANISMO .....	6
3.2. MARCO NORMATIVO.....	6
3.3. ORGANIZACIÓN DE LA SEGURIDAD.....	6
3.4. CONCIENCIACIÓN Y FORMACIÓN .....	6
3.5. GESTIÓN DE RIESGOS .....	6
3.6. PROCESO DE APROBACIÓN Y REVISIÓN.....	6
<b>4. DESARROLLO DE LA POLÍTICA DE SEGURIDAD .....</b>	<b>7</b>
<b>ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS.....</b>	<b>8</b>
<b>ANEXO B. REFERENCIAS.....</b>	<b>10</b>
<b>ANEXO C. EJEMPLO DE POLÍTICA.....</b>	<b>11</b>
<b>1. APROBACIÓN Y ENTRADA EN VIGOR .....</b>	<b>11</b>
<b>2. INTRODUCCIÓN.....</b>	<b>11</b>
2.1. PREVENCIÓN .....	11
2.2. DETECCIÓN.....	12
2.3. RESPUESTA.....	12
2.4. RECUPERACIÓN .....	12
<b>3. ALCANCE.....</b>	<b>12</b>
<b>4. MISIÓN .....</b>	<b>12</b>
<b>5. MARCO NORMATIVO.....</b>	<b>12</b>
<b>6. ORGANIZACIÓN DE LA SEGURIDAD .....</b>	<b>13</b>
6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES.....	13
6.2. ROLES: FUNCIONES Y RESPONSABILIDADES.....	13
6.3. PROCEDIMIENTOS DE DESIGNACIÓN .....	13
6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....	13
<b>7. DATOS DE CARÁCTER PERSONAL .....</b>	<b>13</b>
<b>8. GESTIÓN DE RIESGOS.....</b>	<b>13</b>
<b>9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>14</b>
<b>10. OBLIGACIONES DEL PERSONAL.....</b>	<b>14</b>
<b>11. TERCERAS PARTES .....</b>	<b>14</b>
<b>ANEXO D. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA .....</b>	<b>16</b>

## 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. La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa ‘seguridad de la información’ en una organización. El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.
3. En este documento se emplean las denominaciones ‘Política de Seguridad’ y ‘Política de Seguridad de la Información’ como términos equivalentes, excepto en donde se precisa explícitamente alguna diferencia significativa.
4. El Esquema Nacional de Seguridad (ENS) se refiere en varios puntos a la Política de Seguridad:
5. ENS. Artículo 11. Requisitos mínimos de seguridad:
  1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.
6. ENS. Artículo 12. Organización e implantación del proceso de seguridad

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.
7. ENS. Disposición transitoria. Adecuación de sistemas.
  3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.
8. ENS. Anexo II Medidas de Seguridad  
Marco organizativo [org]  
Política de seguridad [org.1]

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

  - a) Los objetivos o misión de la organización.
  - b) El marco legal y regulatorio en el que se desarrollarán las actividades.
  - c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
  - d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

- e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

9. Esta guía propone un modelo genérico de Política de Seguridad de la Información. El contenido se lista en la sección 3. La sección 4 da pautas para desarrollar dicho contenido. Y el Anexo C muestra un ejemplo que se puede tomar como base para particularizarlo a casos concretos.

## 2. PRINCIPIOS DE SEGURIDAD

10. En la toma de decisiones en materia de seguridad se deben tener en cuenta los principios básicos enunciados en el Esquema Nacional de Seguridad. Esto es especialmente relevante cuando se elabora la Política de Seguridad de la Información, que establece el marco para el resto de los desarrollos normativos. El ENS establece los siguientes principios básicos:

Artículo 5. La seguridad como un proceso integral.

Artículo 6. Gestión de la seguridad basada en los riesgos.

Artículo 7. Prevención, reacción y recuperación.

Artículo 8. Líneas de defensa.

Artículo 9. Reevaluación periódica.

Artículo 10. La seguridad como función diferenciada.

## 3. CONTENIDO

11. Secciones típicas de una Política de Seguridad de la Información:

1. Misión u objetivos del organismo
2. Marco normativo
3. Organización de seguridad
  - Definición de comités y roles unipersonales
  - Funciones
  - Responsabilidades
  - Mecanismos de coordinación
  - Procedimientos de designación de personas
4. Concienciación y formación
5. Postura para la gestión de riesgos
  - Plan de análisis
  - Criterios de evaluación de riesgos
  - Directrices de tratamiento
  - Proceso de aceptación del riesgo residual

6. Proceso de revisión de la política de seguridad
12. Estos puntos se desarrollan a continuación.

### 3.1. MISIÓN DEL ORGANISMO

13. Se describirá la razón de la existencia de <el organismo> y los servicios que presta.

### 3.2. MARCO NORMATIVO

14. El objetivo es plasmar por escrito las responsabilidades que el organismo pueda tener por su naturaleza legal, por su obligación a atender normativa nacional o sectorial y por obligaciones contraídas con terceros, con indicación de las normas correspondientes.

### 3.3. ORGANIZACIÓN DE LA SEGURIDAD

15. Se debe describir cómo se coordina el organismo para atender a las necesidades de seguridad, tanto TIC como en otras materias y cómo se distribuye la información y se toman decisiones corporativas. La guía CCN-STIC 402 puede usarse como modelo.
16. Se deben describir los roles unipersonales en materia de seguridad de la información. En particular la figura del Responsable de Seguridad de la información, detallando sus funciones y responsabilidades.
17. Se debe determinar la estructura de seguridad teniendo en cuenta lo establecido en el Artículo 10 del ENS.
18. Cuando se traten datos de carácter personal, se hará mención explícita al Documento de Seguridad que refleja la postura de <el organismo> respecto de los mismos.

### 3.4. CONCIENCIACIÓN Y FORMACIÓN

19. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de <el organismo> y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

### 3.5. GESTIÓN DE RIESGOS

20. El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.
21. En esta sección se debe plasmar el compromiso de <el organismo> y la obligación de los responsables de los sistemas de realizar análisis de riesgos y atender a sus conclusiones.
22. El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente según lo establecido en el Artículo 9 del ENS.

### 3.6. PROCESO DE APROBACIÓN Y REVISIÓN

23. La Política de Seguridad de la Información es un documento que será aprobado formalmente por la Alta Dirección de la Organización y tendrá carácter imperativo sobre toda la organización.

24. Así mismo estará sujeto a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleto.
25. Por ello se establecerá un proceso organizativo que asegure que regularmente se revisa la oportunidad, idoneidad, completitud y precisión de lo que la Política establezca y sea sometido a aprobación formal por la Alta Dirección.
26. El proceso de elaboración y aprobación debe explicitarse en la misma Política.

#### **4. DESARROLLO DE LA POLÍTICA DE SEGURIDAD**

27. Aparte de esta guía, se puede encontrar ayuda en numerosas guías y libros, así como recurrir a servicios profesionales para la elaboración de la Política. Existen incluso programas que generan borradores automáticamente.
28. El texto será claro en los objetivos que se persiguen y evitar referencias a soluciones tecnológicas concretas, de tal forma que la evolución tecnológica no requiera la revisión de la política. Antes bien, la Política debe garantizar que se mantiene la posición de la organización en materia de seguridad independientemente de los recursos que se empleen en cada momento para optimizar criterios funcionales y económicos.
29. Aunque el texto deba revisarse regularmente, estas revisiones tendrán por lo general un carácter marcadamente continuista, limitándose a mejorar expresiones ambiguas, mejorar la claridad y atajar situaciones no previstas que se han ocurrido en la utilización del sistema. No se puede cambiar de política alegremente; pero si se debe ir adaptando continuamente a la realidad.



## 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.

### **Gestión de incidentes**

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas. ENS.

### **Gestión de riesgos**

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. ENS.

### **Incidente de seguridad**

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS.

### **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.

### **Principios básicos de seguridad**

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios. 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-to-day 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

CCN	Centro Criptológico Nacional
CERT	Computer Emergency Reaction Team
ENS	Esquema Nacional de Seguridad
STIC	Seguridad TIC
TIC	Tecnologías de la Información y las Comunicaciones

## **ANEXO B. REFERENCIAS**

### **CCN-STIC-402**

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

### **CCN-STIC-801**

ENS - Responsables y Funciones. 2010.

### **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.

## ANEXO C. EJEMPLO DE POLÍTICA

### 1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día <día> de <mes> de <año> por <órgano que la aprueba>.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día <día> de <mes> de <año> por <órgano que lo aprobó>.

### 2. INTRODUCCIÓN

<El organismo> depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

#### 2.1. PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

## 2.2. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

## 2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

## 2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

## 3. ALCANCE

Esta política se aplica a todos los sistemas TIC de <el organismo> y a todos los miembros de la organización, sin excepciones.

## 4. MISIÓN

Describir los objetivos de servicio del organismo

## 5. MARCO NORMATIVO

Listar leyes, reglamentos y otra normativa, nacional o internacional, a la que el organismo esté sujeto.

## 6. ORGANIZACIÓN DE LA SEGURIDAD

### 6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

La guía CCN-STIC 402 puede usarse como modelo.

El Comité de Seguridad TIC estará formado por <...>. Aquí aparecen cargos corporativos y designaciones de departamentos dentro del organismo cuando proceda.

El Secretario del Comité de Seguridad TIC será <...> y tendrá como funciones <...>.

El Comité de Seguridad TIC reportará a <...>.

El Comité de Seguridad TIC tendrá las siguientes funciones: <...>.

### 6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

La guía CCN-STIC 801 puede usarse como modelo, en particular concretando las funciones y responsabilidades del Responsable de Seguridad de la Información y su relación con el Comité de Seguridad TIC.

Cuando proceda, se detallará el nombramiento de Responsables Delegados de Seguridad y las funciones que les son delegadas.

Se detallarán igualmente las funciones de los Responsables de Sistemas.

### 6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por <órgano que no nombra> a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

### 6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por <órgano que la aprueba> y difundida para que la conozcan todas las partes afectadas.

## 7. DATOS DE CARÁCTER PERSONAL

<El organismo> trata datos de carácter personal. El <documento de seguridad>, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de <el organismo> se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

## 8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año

- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

## 9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de <el organismo> en diferentes materias:

- *Listar referencias a otras políticas en materia de seguridad.*

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet

URL

e impresa en

LOCALIZACIÓN

## 10. OBLIGACIONES DEL PERSONAL

Todos los miembros de <el organismo> tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de <el organismo> atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de <el organismo>, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 11. TERCERAS PARTES

Cuando <el organismo> preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se

establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando <el organismo> utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.



## ANEXO D. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA

Tomado de la guía NIST SP 800-100, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- normas de seguridad (*security standards*)
- guías de seguridad (*security guides*)
- procedimientos de seguridad (*security procedures*)

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos [operativos] de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.