GUÍA DE SEGURIDAD
(CCN-STIC-801)

ESQUEMA NACIONAL DE SEGURIDAD
RESPONSABILIDADES Y FUNCIONES

FEBRERO 2011

Edita:

NIPO: 075-11-053-3

Tirada: 1000 ejemplares
Fecha de Edición: febrero de 2011
Informática de la Comunidad de Madrid (ICM) ha participado en la redacción de 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.

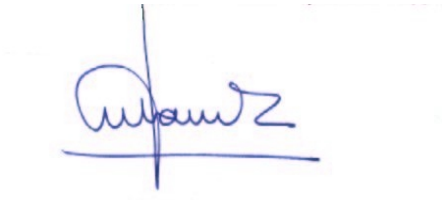
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Febrero de 2011



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

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 mantenimiento y gestión de la seguridad de los Sistemas de Información va íntimamente ligada al establecimiento de una Organización de Seguridad.
3. Dicha Organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas de información y la implantación de una estructura que las soporte.
4. En consonancia con el artículo 10 del Esquema Nacional de Seguridad,
    - En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
    - El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
    - La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
    - La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.
5. En esta guía, cuando se habla de “Seguridad”, se refiere a “Seguridad de la Información”, salvo que se indique algún ámbito específico.
6. En esta guía, cuando se habla de “Responsable de la Seguridad”, se refiere a “Responsable de la Seguridad de la Información”, salvo que se indique explícitamente algún ámbito específico.

2. OBJETO

7. El objeto de esta guía es crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los sistemas de información, así como proponer unas figuras o roles de seguridad que asuman dichas responsabilidades.
8. Es responsabilidad de cada Organismo establecer su propia Organización de Seguridad de acuerdo con sus necesidades y limitaciones.

3. ALCANCE

9. La estructura propuesta en este documento sirve como guía, pudiendo ser la implantación final diferente en cada Organización. No obstante, las responsabilidades definidas en esta norma deben ser cubiertas sea cual fuere la solución final adoptada.

4. ORGANIZACIÓN DE SEGURIDAD

10. Como norma general se encontrarán definidas las responsabilidades que se citan en los siguientes apartados. Hay que tener en cuenta que estas responsabilidades serán un modelo de referencia que servirá de orientación en el desarrollo de la estructura de seguridad de cualquier Organización, donde las necesidades de personal y recursos disponibles son determinantes.

11. La estructura propuesta diferencia 3 grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, la operación del sistema de información que se atiene a aquellos requisitos y la función de supervisión de acuerdo al principio básico del ENS "La seguridad como función diferenciada". La especificación de requisitos de seguridad corresponde a los responsables de la información y el servicio, junto con el responsable del fichero si hubiera datos de carácter personal. La operación corresponde al responsable del sistema. La supervisión corresponde al responsable de la seguridad.

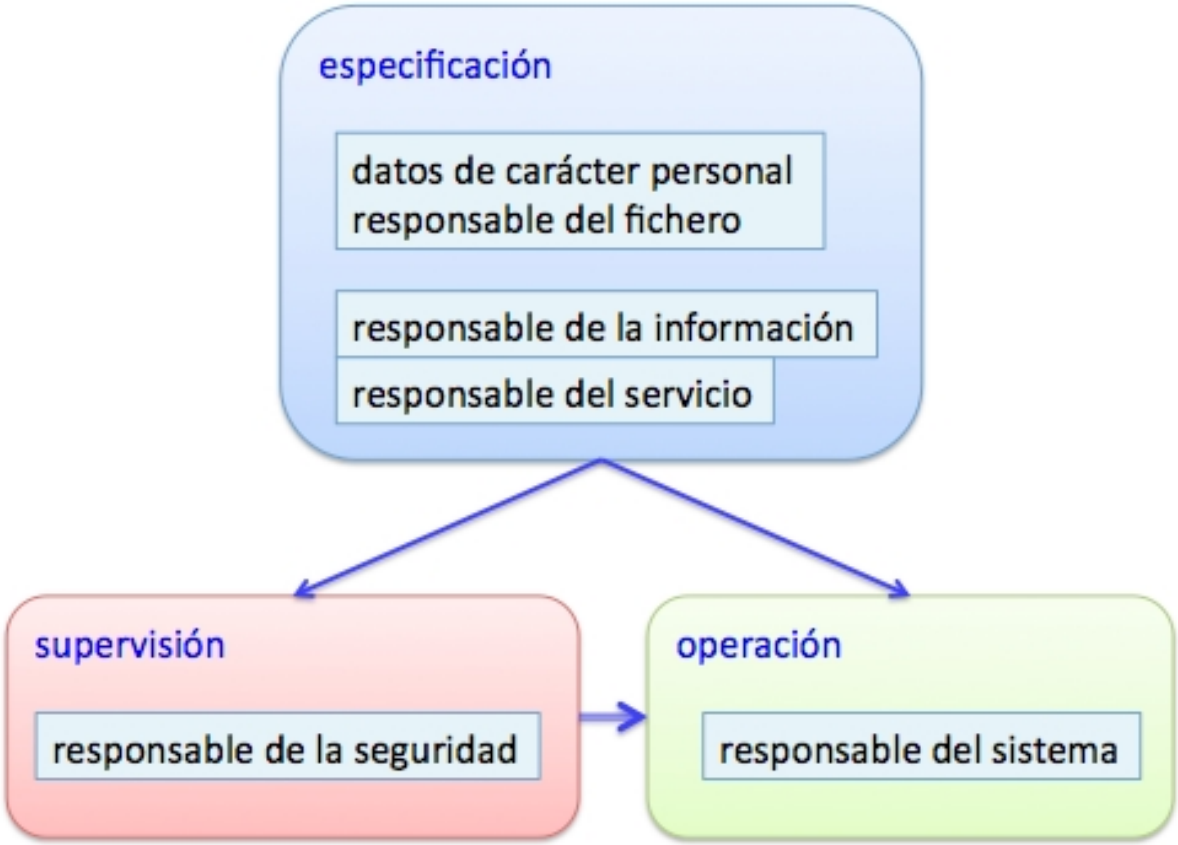


Ilustración 1 – Responsables

12. Puede que exista por encima de todos ellos un Comité de Seguridad Corporativa (sus funcionen se exponen más adelante).

13. Puede que exista un Comité de Seguridad de la Información que aúne las responsabilidades sobre información y servicios. Sus funciones se exponen más adelante.

14. A menudo pueden distinguirse 3 niveles en el organigrama de una organización:

- Nivel 1 – Órganos de Gobierno: alta dirección, que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de que se alcancen.
- Nivel 2 – Dirección Ejecutiva: gerencias, que entienden qué hace cada departamento y cómo los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.
- Nivel 3: Operacional, que se centra en una actividad concreta y controla cómo se hacen las cosas.

15. El Responsable de la Información estará en el nivel 1.
16. El Responsable de la Seguridad estará en el nivel 2.
17. El Responsable del Sistema estará en el nivel 3.
18. El Responsable del Servicio, cuando sea diferente del Responsable de la Información, estará en el nivel 1 o en el nivel 2 dependiendo del organigrama de la organización.
19. Cuando exista un Comité de Seguridad Corporativa, estará en el nivel 1.
20. Cuando existe un Comité de Seguridad de la Información, estará en el nivel 1.

<table>
<tr><th>nivel</th><th>opción A</th><th>opción B</th></tr>
<tr><td rowspan="3">1 - gobierno</td><td colspan="2">comité de seguridad corporativa</td></tr>
<tr><td rowspan="2">comité de seguridad de la información</td><td>responsable de la información</td></tr>
<tr><td>responsable del servicio</td></tr>
<tr><td>2 - ejecutivo</td><td colspan="2">responsable de la seguridad</td></tr>
<tr><td>3 - operaciones</td><td colspan="2">responsable del sistema</td></tr>
</table>

21. En los siguientes párrafos se describen las funciones del Responsable de la Información y del Responsable del Servicio, sin perjuicio de que estas responsabilidades puedan ser unipersonales o verse asumidas en el Comité de Seguridad de la Información.
22. Las estructuras de dependencia mencionadas en esta guía se limitan a la materia de seguridad de la información, independientemente de otras dependencias propias de la organización.
23. Cuando haya órganos colegiados, estos se constituirán de acuerdo con lo previsto en el Capítulo II, Título II, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas, y del Procedimiento Administrativo Común, y del Capítulo IV del Título II, de la Ley 6/1967, de 14 de abril, de organización y funcionamiento de la Administración General del Estado.

4.1. SEGREGACIÓN

24. El artículo 10 del Esquema Nacional de Seguridad recoge el principio de “La seguridad como función diferenciada”. Este principio exige que el Responsable de la Seguridad sea independiente del Responsable del Sistema.

4.2. RESOLUCIÓN DE CONFLICTOS

25. De acuerdo con el Principio de Jerarquía que rige en las administraciones públicas españolas, en caso de conflicto este deberá ser resuelto por el superior jerárquico.

26. Esto debería concretarse para el caso de cada organización, acorde con la normativa que sea de aplicación. El mecanismo concreto debe figurar en la Política de Seguridad.

5. RESPONSABLES ESENCIALES

27. La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

28. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

29. En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos. Una misma persona puede aunar varias responsabilidades.

5.1. EL RESPONSABLE DE LA INFORMACIÓN

30. El Responsable de la Información *(information owner)* es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

31. El ENS asigna al 'Responsable de la Información' la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

32. El Responsable de la Información puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa. Ver Comités.

33. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

34. La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

5.2. EL RESPONSABLE DEL SERVICIO

35. El ENS asigna al 'Responsable del Servicio' la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

36. El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa. Ver Comités.

37. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

38. La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

39. La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

5.3. RESPONSABILIDADES UNIFICADAS

40. Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido

- cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio
- cuando la prestación del servicio no depende de la unidad que es Responsable de la Información

6. EL RESPONSABLE DE LA SEGURIDAD

41. Persona designada por la Dirección, según procedimiento descrito en su Política de Seguridad.

42. Responsabilidades:

a. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.

b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

c. Además, ver Anexo A: Tareas.

43. Otras denominaciones

- NIST: *Computer Security Program Manager* [SP 800-12]
- NIST: *Chief Information Security Officer* [SP 800-53]
- Unión Europea: Autoridad INFOSEC (ASTIC) [2001/264/CE]
- CCN: Autoridad de Seguridad de las Tecnologías de la Información y Comunicación (ASTIC) [CCN-STIC 201]
- Ministerio de Defensa: Autoridad INFOSEC (AI) [OM 76/2002]

6.1. CISO VS CSO

44. La figura descrita se denomina en ciertos ámbitos CISO (Chief Information Security Officer). Y en ciertas organizaciones se habla del CSO (Chief Security Officer). Los siguientes párrafos intentan ordenar un poco estos roles a título meramente informativo.

45. Al CSO se le requiere una 'visión de negocio'; es decir, que comprenda los riesgos que afronta la Organización y cómo tratarlos. Para ello debe entender la misión y los objetivos últimos de la Organización y cerciorarse de que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos. Entre otras cosas, debe comprender las necesidades normativas, la gestión de la reputación de la Organización y las expectativas de los usuarios. Al CSO a veces se le denomina Responsable de Seguridad Corporativa. Véase la sección dedicada a Comités más adelante.

46. La existencia de un CSO permite enmarcar las decisiones de seguridad de la información, tanto tecnológicas como operacionales, en un marco más amplio de referencia y asegurar la continuidad de las actividades frente a cualquier incidente de seguridad. No obstante, la figura del CSO sólo aparece en organizaciones grandes con una estructura directiva compleja.

47. El rol del CISO suele ser más centrado en aspectos de seguridad de la información. Al CISO se le exige que tenga una cierta formación técnica, siendo al menos capaz de entender los problemas y las soluciones tecnológicas y traducirlas al lenguaje de la Dirección (lo que veces se denomina 'en términos de negocio').

48. Cuando existen CSO y CISO, el CISO reporta al CSO y el CSO a la Dirección. Véase la sección dedicada a Comités más adelante.

49. En organizaciones pequeñas es frecuente que coincidan ambas responsabilidades en una misma persona, que a veces adopta un nombre, a veces el otro.

6.2. DELEGACIÓN DE FUNCIONES

50. En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, cada Organización podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

51. La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

52. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

53. Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

7. ESTRUCTURA OPERACIONAL DEL SISTEMA

7.1. EL RESPONSABLE DEL SISTEMA

54. Persona designada por la Dirección. La persona designada figurará en la documentación de seguridad del sistema de información.

55. Responsabilidades:

    a. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

    b. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

    c. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

    d. El Responsable del Sistema puede ***acordar*** la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

    e. Además, ver Anexo A: Tareas.

56. Otras denominaciones

    - NIST: *Program and Functional Managers / Application Owners* [SP 800-12]
    - NIST: *Information System Owner* [SP 800-53]
    - Unión Europea: Autoridad Operativa del Sistema de Tecnología de la Información (AOSTI) [2001/264/CE]
    - CCN: Autoridad Operacional del Sistema de las Tecnologías de la Información y Comunicación (AOSTIC) [CCN-STIC 201]
    - Ministerio de Defensa: Autoridad Operacional del Sistema (AOS) [OM 76/2002]

7.1.1. DELEGACIÓN DE FUNCIONES

57. En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada Organización podrá designar cuantos Responsables de Sistema Delegados considere necesarios.

58. La designación corresponde al Responsable del Sistema. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

59. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información. Es habitual que se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

60. Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reportan.

7.2. SEGURIDAD FÍSICA

61. Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el ENS en materia de seguridad física de forma análoga a lo establecido en los puntos anteriores.

62. El Responsable de la Seguridad Física implantará las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

7.3. GESTIÓN DEL PERSONAL

63. Los responsables de gestión del personal se ajustarán a lo establecido por el ENS en materia de personal de forma análoga a lo establecido en los puntos anteriores.

64. Los responsables de personal implantarán las medidas de seguridad que les competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informarán a éste de su grado de implantación, eficacia e incidentes.

8. EL ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA (ASS)

65. La persona designada figurará en la documentación de seguridad del Sistema de información. Según las circunstancias, el ASS puede depender del Responsable del Sistema o del Responsable de la Seguridad. Ver las siguientes sub-secciones.

66. Funciones:

    a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

    b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.

    c. La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

    d. La aplicación de los Procedimientos Operativos de Seguridad.

    e. Aprobar los cambios en la configuración vigente del Sistema de Información.

    f. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

    g. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

    h. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

    i. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

j. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

k. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

l. Además, ver Anexo A: Tareas.

67. En emplazamientos donde se encuentren ubicados varios sistemas de información, la función de ASS de cada uno de ellos podría recaer en la misma persona.

68. Otras denominaciones

- NIST: *Security Officer* [SP 800-12]
- Unión Europea: Agente de Seguridad INFOSEC [2001/264/CE]
- CCN: Administrador de Seguridad del Sistema (ASS) [CCN-STIC-201]
- Ministerio de Defensa: Administrador de Seguridad del Sistema (ASS) [OM 76/2002]

8.1. DEPENDENCIA FUNCIONAL DEL RESPONSABLE DEL SISTEMA

69. El ASS puede depender del Responsable del Sistema.

Ilustración 2 - El ASS depende del Responsable del Sistema

70. Cuando el ASS depende del Responsable del Sistema,

- la persona será designada por la Dirección a propuesta del Responsable del Sistema.
- el ASS reportará al Responsable del Sistema

71. Esta arquitectura es clásica y prima las funciones de operatividad, a veces en detrimento de las funciones de seguridad. Cuando se aplique, las actividades de auditoría deben incidir especialmente en garantizar un buen alineamiento entre los requisitos establecidos por el Responsable de la Seguridad y las actuaciones del Administrador de la Seguridad.

72. Es posible segregar las funciones del ASS de forma que haya 2 personas diferentes, una encargada del aseguramiento de la prestación del servicio (esta persona dependería funcionalmente del Responsable del Sistema) y otra persona encargada de la protección de la información (esta dependiendo del Responsable de la Seguridad).

8.2. DEPENDENCIA FUNCIONAL DEL RESPONSABLE DE LA SEGURIDAD

73. El ASS puede depender del Responsable de la Seguridad.

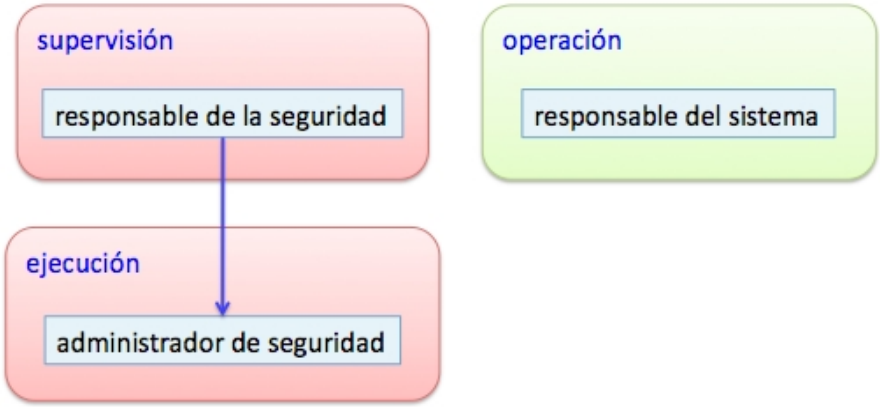


Ilustración 3 - El ASS depende del Responsable de la Seguridad

74. Cuando el ASS depende del Responsable de la Seguridad,

- la persona será designada por la Dirección a propuesta del Responsable de la Seguridad
- el ASS reportará al Responsable de la Seguridad

75. Esta arquitectura es frecuente en sistemas donde la seguridad de la información es más importante que la prestación de los servicios. Cuando se aplique, hay que asegurar que las funciones de explotación no se ven ralentizadas por las actividades del ASS, estableciendo canales y foros de coordinación operativa.

76. Es posible segregar las funciones del ASS de forma que haya 2 personas diferentes, una encargada del aseguramiento de la prestación del servicio (esta persona dependería funcionalmente del Responsable del Sistema) y otra persona encargada de la protección de la información (esta dependiendo del Responsable de la Seguridad).

77. Cuando existe un ASS que reporta al Responsable de Seguridad, son funciones típicas las siguientes:

- monitorización del estado de seguridad del sistema, analizando la información proporcionada por la herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica instalados en el sistema
- supervisión de que todo el equipamiento se ajusta a lo autorizado
- supervisión de las actividades de los administradores del sistema: actuaciones y aplicación de los procedimientos de seguridad establecidos
- supervisión de que las actividades de los usuarios del sistema están conformes a lo que cada uno está autorizado
- cuando existe un sistema separado de gestión de privilegios, el ASS puede encargarse de las actuaciones relativas a la implantación y mantenimiento de las autorizaciones concedidas a los usuarios del sistema

8.3. DELEGACIÓN DE FUNCIONES

78. En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de ASS, se podrán designar Administradores de Seguridad del Sistema Delegados (ASS-D).

79. Los ASS-D serán responsables, en su ámbito, de aquellas acciones que delegue el ASS relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

80. El ASS-D será designado a solicitud del ASS, del que dependerá funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del sistema de información.

9. COMITÉS

81. Algunas responsabilidades pueden instrumentarse por medio de comités, que se articularán y funcionarán como órganos colegiados de acuerdo con la normativa administrativa. Estos comités facilitan la armonía de las diferentes partes de la organización.

82. Son habituales los siguientes:

- Comité de Seguridad de la Información, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.
- Comité de Seguridad Corporativa, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, cabiendo destacar los aspectos de seguridad patrimonial (seguridad de las instalaciones) y planes de contingencia.

83. Nótese que el Comité de Seguridad Corporativa está por encima, coordinando las actividades del Comité de Seguridad de la Información.

84. Las siguientes secciones apuntan las responsabilidades que se atribuyen típicamente a estos comités, cuando existen.

9.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

85. El Comité de Seguridad de la Información coordina la seguridad de la información a nivel de organización. La seguridad de la información necesita estar coordinada:

- Es conveniente coordinarla para racionalizar el gasto.
- Es necesario coordinarla para evitar disfunciones que permitan fallas de seguridad al ofrecer el Sistema puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.

86. El Comité de Seguridad de la Información estará formado por el Responsable de Seguridad de la Información y por representantes de las áreas de la Organización afectadas. La composición se determinará en la Política de Seguridad de la Información de la Organización.

87. Son funciones típicas del Comité de Seguridad de la Información:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.

- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

88. El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

89. El Responsable de la seguridad de la información del sistema (Responsable de la Seguridad en el ENS) es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.

- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

90. Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

9.2. COMITÉ DE SEGURIDAD CORPORATIVA

91. La seguridad de la información es una más de las áreas de seguridad de una organización. En grandes Organizaciones aparece un Comité de Seguridad Corporativa con su propio Secretario, el responsable de seguridad corporativa (CSO). El Responsable de Seguridad de la Información (CISO) queda como miembro del Comité de Seguridad Corporativa junto con otros responsables de otras áreas, tales como:

- Responsables de la seguridad de instalaciones y áreas (seguridad física).
- Responsables de la seguridad de la información.
- Responsables de seguridad industrial.
- Responsables de seguridad operacional.
- etc.

92. Son funciones típicas del comité de seguridad corporativa:

- Coordinar todas las funciones de seguridad de la Organización.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación sin fisuras en el caso de que deban ser activados.
- Elaborar la Política de Seguridad Corporativa, que será aprobada por la Alta Dirección.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los responsables de seguridad se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Atender a las inquietudes de la Alta Dirección y transmitírselas a los Responsables de Seguridad pertinentes. De estos últimos, recabar respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.
- Recabar de los Responsables de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes, se consolidan y resumen para la Alta Dirección.
- Coordinar y da respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.

9.2.1. RESPONSABLE DE SEGURIDAD CORPORATIVA (CSO)

93. Actúa como Secretario del Comité de Seguridad Corporativa.

94. Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.

95. Escucha las inquietudes de la Alta Dirección y de los responsables de seguridad y las incorpora al orden del día para su discusión en las reuniones del Comité de Seguridad Corporativa.

96. Es responsable, junto con los diferentes Responsables de Seguridad, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad Corporativa y proponiendo las medidas oportunas de adecuación al nuevo marco.

97. Es el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad Corporativa. Estas decisiones serán respuesta a propuestas de los responsables de seguridad, velando por la unidad de acción y la coordinación de actuaciones, en general y en especial en caso de incidencias que tengan repercusión fuera de la Organización y en caso de desastres.

98. En caso de desastre se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización.

10. NOMBRAMIENTOS

99. La Dirección de la Organización nombra

- al Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información)
- al Responsable del Servicio; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información)
- al Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando existan, a los comités de seguridad de la información y seguridad corporativa
- al Responsable del Sistema, que, en materia de seguridad, debe reportar al Responsable de la Seguridad

100. El procedimiento de nombramiento de los responsables mencionados en el párrafo anterior debe constar en la Política de Seguridad de la Información de la Organización. El nombramiento debe ser formal. La designación será unipersonal cuando las responsabilidades recaigan en personas. Los Responsables de la Información y del Servicio pueden ser órganos colegiados; el Responsable de la Seguridad conviene que sea unipersonal.

101. La Dirección de la Organización designa a la persona Responsable del Sistema

- a propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información
- a propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio

- directamente cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados

102. La Dirección de la Organización designa al Administrador de Seguridad del Sistema a propuesta del responsable del mismo (ver opciones de dependencia en la sección dedicada al ASS). Es muy recomendable que el nombramiento del Administrador de Seguridad sea formal y conste en la documentación de seguridad del sistema, reconociendo que sus funciones no son coyunturales, sino esenciales para cumplir las exigencias en materia de seguridad. No es nada recomendable que las funciones de esta persona se diluyan y sean realizadas por cualquier operador del sistema.

11. REPORTES

103. El administrador de seguridad reporta al Responsable del Sistema o al Responsable de la Seguridad, según sea su dependencia funcional:

- incidentes relativos a la seguridad del sistema
- acciones de configuración, actualización o corrección

104. El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

105. El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

106. El Responsable del Sistema reporta al Responsable de la Seguridad:

- actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema
- resumen consolidado de los incidentes de seguridad

107. Cuando el ASS dependa del Responsable del Sistema, éste informará al Responsable de la Seguridad: de la eficacia de las medidas de protección que se deben implantar, además de un resumen consolidado de los incidentes de seguridad.

108. Cuando el ASS dependa del Responsable de la Seguridad, éste proporcionará al Responsable del Sistema un resumen consolidado de los incidentes de seguridad.

109. El Responsable de la Seguridad informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

110. El Responsable de la Seguridad informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

111. Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta a dicho comité como secretario:

- resumen consolidado de actuaciones en materia de seguridad
- resumen consolidado de incidentes relativos a la seguridad de la información

- estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto

112. Cuando exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informa a dicho comité como miembro, según lo acordado en el Comité de Seguridad de la Información.

113. Cuando no exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informa a la Dirección de la Organización, según lo acordado en el Comité de Seguridad de la Información.

114. Cuando no exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta directamente a la Dirección de la Organización:

- resumen consolidado de actuaciones en materia de seguridad
- resumen consolidado de incidentes relativos a la seguridad de la información
- estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto

12. GESTIÓN DE LOS RIESGOS

115. La gestión de los riesgos son tareas que deben realizarse de manera continua sobre los sistemas de información y orientar todas las demás actividades, de acuerdo a los principios (b) “Gestión de riesgos” y (e) “Reevaluación periódica”:

- ver Artículo 6 del ENS, “Gestión de la seguridad basada en los riesgos”
- ver Artículo 9 del ENS, “Reevaluación periódica”

116. La forma de realizar el análisis de riesgos se detalla en el Anexo II, [op.pl.1] “Análisis de riesgos”, estableciendo una proporcionalidad entre el nivel de detalle del análisis y la categoría del sistema de información.

117. Véase el Anexo A: Tareas, donde se muestran escenarios posibles de asignación de tareas relativas a la gestión de riesgos.

118. El Responsable de la Información es el propietario de los riesgos sobre la información.

119. El Responsable del Servicio es el propietario de los riesgos sobre los servicios.

120. El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

121. **Indicadores de riesgo.** En sistemas de información de categoría alta se recomienda que se establezcan indicadores del estado de los riesgos críticos (*KRI – Key Risk Indicators*). Estos indicadores:

- son propuestos por el Responsable de la Seguridad;
- su definición es acordada por el Responsable de la Seguridad y el propietario del riesgo; la definición indicará exactamente:
  - en qué medidas se basan,
  - cuál es el algoritmo de cálculo,
  - la periodicidad de evaluación y

- los umbrales de aviso y alarma (atención urgente)

- se le presentan al responsable correspondiente
  - rutinariamente, con la periodicidad establecida,
  - puntualmente, por demanda del propietario del riesgo medido,
  - y extraordinariamente cuando se supera un umbral de riesgo
- estos indicadores estarán a disposición de los auditores

122. La responsabilidad de monitorizar un riesgo recae en su propietario, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

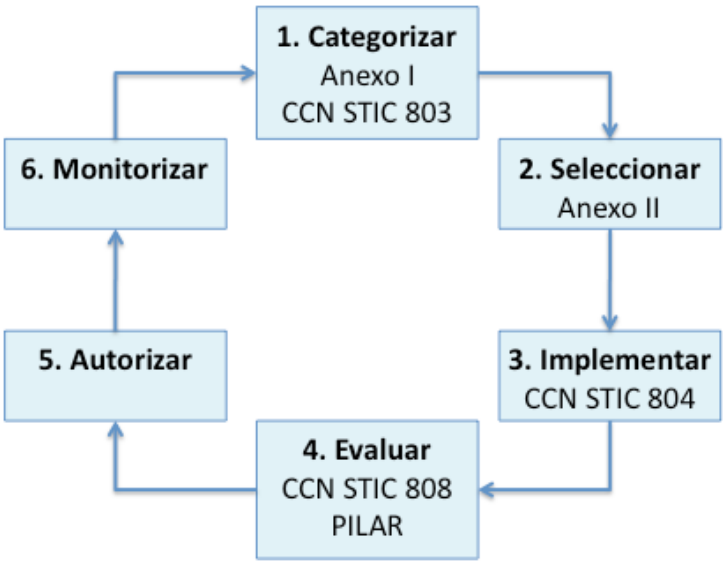


Ilustración 4 - Proceso de Gestión de Riesgos

123. Paso 1 – Categorizar el sistema de información
   - el Responsable de la Información manejada establece los niveles requeridos (ver Anexo I del ENS y guía CCN-STIC 803)
   - el responsable de los servicios prestados establece los niveles requeridos (ver Anexo I del ENS y guía CCN-STIC 803)
   - se deduce automáticamente la categoría del sistema de información (ver Anexo I del ENS)
124. Paso 2 – Seleccionar medidas de seguridad
   - el responsable de la seguridad realiza el pertinente análisis de riesgos
   - el responsable de la seguridad determina la Declaración de Aplicabilidad, teniendo en cuenta los mínimos requeridos por el Anexo II del ENS y las medidas adicionales que se estimen oportunas
125. Paso 3 – Implantar las medidas de seguridad

- el Administrador de Seguridad del Sistema (ASS) se encarga de aplicar las medidas acordadas
  (ver guía CCN STIC 804)

126. Paso 4 – Evaluar la seguridad del sistema de información

- corresponde al sistema de gestión que se emplee, pudiendo recurrir a auditorías externas cuando sea pertinente
  (ver guía CCN STIC 802)
- se evalúa el riesgo residual

127. Paso 5 – Autorización para operar

- el Responsable de la Información acepta el riesgo residual sobre la información que le compete
- el Responsable del Servicio acepta el riesgo residual sobre los servicios que le competen
- puede ser necesario un plan de mejora de la seguridad para atender a los riesgos que no son aceptables, regresando al paso 2

128. Paso 6 – Monitorizar

- el Administrador de Seguridad del Sistema (ASS) recopila información sobre el desempeño del sistema de información en materia de seguridad
- el Responsable de la Seguridad monitoriza que el sistema de información se comporta dentro de los márgenes aceptados de riesgo
- los responsables de la información y de los servicios son informados de desviaciones significativas del riesgo sobre los activos de los que son propietarios; si la desviación es elevada, el Responsable del Sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo

13. CONCURRENCIA CON EL RD 1720/2007

129. Existen numerosos puntos de concurrencia entre el Esquema Nacional de Seguridad y el Reglamento de Protección de Datos de Carácter Personal. En algunos puntos hay coincidencia, y en otros diferencias.

130. El RD 1720/2007 de Protección de Datos de Carácter Personal, identifica varios responsables y encargados, pormenorizando las funciones y tareas que cada uno debe realizar. Los siguientes párrafos muestran cómo conviven con las tareas y funciones marcadas por el Esquema Nacional de Seguridad.

131. Todos los roles determinados en uno y otro ordenamiento deberán ser identificados y estar formalmente asignados, sin perjuicio de que algunas figuras puedan concurrir en la misma persona, según de desarrolla a continuación.

132. RD 1720/2007. Artículo 5. Definiciones.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

l) Responsable de la Seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

133. Habitualmente, en la administración pública, el Responsable del Fichero es una persona jurídica, el organismo titular del mismo.

134. En cierta medida pueden coincidir las figuras de “Responsable de la Información” con el “Responsable del Fichero”. Hay que tener en cuenta que la determinación del carácter personal de los datos viene regulada por la normativa y matizada por una amplia jurisprudencia, acotando el margen de discrecionalidad del Responsable de la Información. En todo caso, el Responsable de la Información que se maneja estará supeditado al responsable del fichero.

135. El Responsable del Sistema debe aunar los requisitos sobre los datos de carácter personal que se manejen en el sistema de información de su competencia, tanto si son propios de la Organización, como si son datos cedidos por un tercero.

136. No cabe esperar que se produzcan conflictos entre los responsables de la información, y de los servicios por una parte, y los responsables del fichero y del tratamiento por otra. En caso de discrepancia, los datos de carácter personal constituyen un objeto protegido de mayor rango y marcarán la pauta a seguir.

137. La figura del “Responsable de la Seguridad” aparece en ambas normativas con un papel muy similar como persona que vela porque los sistemas de información efectivamente respondan a los requisitos establecidos. Las organizaciones harán bien en hacer coincidir estas responsabilidades en una única figura, recopilando todas las funciones en la Política de Seguridad.

138. No cabe esperar que se produzcan conflictos entre las obligaciones del Responsable de la Seguridad derivadas de una u otra normativa, pues siempre deberá cumplirse la mayor de las exigencias derivadas de uno u otro.

ANEXO A. TAREAS

En la tabla se usan las siguientes abreviaturas:

CSI – Comité de Seguridad de la Información

RINFO – Responsable de la Información

RSERV – Responsable del Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable del Sistema

ASS – Administrador de la Seguridad del Sistema

tarea	**responsable**
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba : Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG

Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

Respuesta a incidentes de seguridad de la información:

- ASS: Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- ASS: Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- ASS: Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- ASS: Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- ASS: Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- ASS: Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.
- RSEG: Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.
- RSIS: Planificar la implantación de las salvaguardas en el sistema.
- Comité de Seguridad: Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.
- RSIS: Ejecutar el plan de seguridad aprobado.

A.1. MATRIZ RACI

Como toda esta guía, la matriz que se expone a continuación es orientativa y cada organismo deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un equipo.

	rol	descripción
R	**Responsible**	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	**Accountable**	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	**Consulted**	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	**Informed**	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
determinación de la categoría del sistema		I	I	A/R	I	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
medidas de seguridad adicionales				A/R	C	
configuración de seguridad		I	I	A	C	R
aceptación del riesgo residual (1)		A	A	R	I	
documentación de seguridad (3)				A	C	I
política de seguridad	A			R	C	
normativa de seguridad (3)				A	C	I
procedimientos de seguridad (3)				C	A	I
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				(2)	(2)	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad (3)				A	C	
planes de concienciación y formación (3)				A	C	

planes de continuidad (3)				C	A	
suspensión temporal del servicio	A	C	C	C	R	
seguridad en el ciclo de vida (3)				C	A	

(1) Aparecen dos A porque la aceptación del riesgo residual debe ser coordinada entre ambas responsabilidades. Esta coordinación es muy sencilla si las responsabilidades se aúnan en un Comité de Seguridad de la Información.

(2) Las tareas que realiza el ASS involucran al los Responsables del Sistema y de la Seguridad. Uno deberá ser el responsable (A) y el otro deberá ser consultado (C). La determinación de quién hace cada papel dependerá de a quién reporta el ASS, pudiendo existir diferentes ASS para diferentes funciones, pero siempre con una línea clara de dependencia de uno u otro responsable.

- cuando el ASS depende del RSIS

Tarea	RINFO	RSERV	RSEG	RSIS	ASS
implantación de las medidas de seguridad	I	I	C	A	R
supervisión de las medidas de seguridad	I	I	C	A	R

- cuando el ASS depende del RSEG, dependiendo de la distribución de funciones, una posible matriz sería la siguiente:

Tarea	RINFO	RSERV	RSEG	RSIS	ASS
implantación de las medidas de seguridad	I	I	C	A	R
gestión de autorizaciones	I	I	A	C	R
supervisión de las medidas de seguridad	I	I	A	C	R

(3) Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, en cada organismo se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

ANEXO B. EQUIVALENCIAS ENTRE ESTRUCTURAS STIC

B.1. UNIÓN EUROPEA

Se indica la correspondencia entre las figuras descritas en esta guía y las establecidas en la Unión Europea en la directiva 2001/264/CE.

Unión Europea	Esquema Nacional de Seguridad
Autoridad INFOSEC (ASTIC)	Responsable de la Seguridad
Autoridad Operativa del Sistema de Tecnologías de Información (AOSTI)	Responsable del Sistema
Agente de Seguridad INFOSEC	Administrador de Seguridad del Sistema

B.2. MINISTERIO DE DEFENSA

Se indica la correspondencia entre las figuras descritas en esta guía y las establecidas en la Política de Seguridad del Ministerio de Defensa [OM 76/2002].

Ministerio de Defensa	Esquema Nacional de Seguridad
Autoridad INFOSEC (AI)	Responsable de la Seguridad
Autoridad Operacional del Sistema (AOS)	Responsable del Sistema
Administrador de Seguridad del Sistema (ASS)	Administrador de Seguridad del Sistema

B.3. AUTORIDAD NACIONAL DE SEGURIDAD

Se indica la correspondencia entre las figuras descritas en esta guía y las establecidas para la Autoridad Nacional de Seguridad [CCN-STIC 201].

Autoridad Nacional de Seguridad	Esquema Nacional de Seguridad
Autoridad de Seguridad de las Tecnologías de la Información y Comunicación (ASTIC)	Responsable de la Seguridad
Autoridad Operacional del Sistema de las Tecnologías de la Información y Comunicación (AOSTIC)	Responsable del Sistema
Administrador de Seguridad del Sistema (ASS)	Administrador de Seguridad del Sistema

B.4. SP 800-53

Se indican la correspondencia entre las figuras descritas en esta guía y las establecidas en la guía 800-53, 'Recommended Security Controls for Federal Information Systems and Organizations', del NIST.

800-53	Esquema Nacional de Seguridad
Authorizing Official	Función asumida por el Responsable de la Seguridad, si bien el riesgo residual debe ser aceptado por los responsables de la información y de los servicios.
Information owner	Responsable de la Información
Chief Information Security Officer (CISO) Senior (Agency) Information Security Officer (SAISO)	Responsable de la Seguridad
Information System Owner (or Program Manager)	Responsable del Sistema
Information System Security Officer (ISSO)	Administrador del Seguridad del Sistema

ANEXO C. ESTRUCTURA MÍNIMA

En organismos de pequeña dimensión, los roles y responsabilidades identificadas en esta guía pueden reducirse a la siguiente estructura mínima reducida a 2 roles:

Dirección: una figura integrando las siguientes funciones:

- responsable del fichero (si hay datos de carácter personal)
- responsable de la información
- responsable del servicio
- responsable de la seguridad

Operación: una figura, reportando a Dirección, e integrando las siguientes funciones:

- responsable del sistema
- administrador de seguridad

ANEXO D. ESTRUCTURA INTERMEDIA

En organismos de dimensión intermedia, los roles y responsabilidades identificadas en esta guía pueden reducirse a la siguiente estructura reducida a 3 roles:

Dirección: una figura integrando las siguientes funciones:

- responsable del fichero (si hay datos de carácter personal)
- responsable de la información
- responsable del servicio

Supervisión: una figura, reportando a Dirección

- responsable de la seguridad

Operación: una figura, reportando a Dirección, e integrando las siguientes funciones:

- responsable del sistema
- administrador de seguridad

ANEXO E. ESTRUCTURA DE MÁXIMOS

Suele ser muy eficaz la fórmula de disponer de un Comité de Seguridad de la Información que aúne las siguientes responsabilidades:

- responsabilidades derivadas del tratamiento de datos de carácter personal
- responsables de servicios, para todos los servicios prestados dentro del marco de la ley 11/2007
- responsables de información, para todas las informaciones manejadas por los servicios prestados dentro del marco de la ley 11/2007

ANEXO F. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Administrador de Seguridad del Sistema (ASS)

Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.

Information System Security Officer (IISO). Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. CNSS Inst. 4009, Adapted

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.

Dueño del riesgo

Persona o entidad que tiene la responsabilidad y la autoridad para gestionar los riesgos. ISO Guía 73.

Risk owner. Person or entity with the accountability and authority to manage the risk. ISO Guide 73.

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.

Procedimientos Operativos de Seguridad (POS)

Los POS definen los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal. Los POS se elaborarán bajo la responsabilidad del Responsable del Sistema. Adaptada de 2001/264/CE.

Propietario del riesgo

Ver ‘dueño del riesgo’.

Propietario del sistema

Ver ‘responsable del sistema’.

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 la 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.

Seguridad de los sistemas de información

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. CNSS Int. 4009.

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.

Sistema TIC

Sistema de información que emplea tecnologías de la información y de las comunicaciones.

ABREVIATURAS

ASS	Administrador de Seguridad del Sistema
CCN	Centro Criptológico Nacional
CSI	Comité de Seguridad de la Información
ENS	Esquema Nacional de Seguridad
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSO	Information System Security Offices (ISSO)
POS	Procedimientos Operativos de Seguridad
RINFO	Responsable de la Información
RSEG	Responsable de la Seguridad
RSERV	Responsable del Servicio
RSIS	Responsable del Sistema
STIC	Seguridad TIC
TIC	Tecnologías de la Información y las Comunicaciones

ANEXO G. REFERENCIAS

2001/264/CE

Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.

CCN-STIC-201

Organización y Gestión para la Seguridad de las TIC

CCN-STIC-402

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

CCN-STIC-802

Guía de Auditoría. Junio 2010.

CCN-STIC-803

Valoración de los Sistemas. 2010.

CCN-STIC-804

ENS - Guía de Implantación. 2010.

CNSS Inst. 4009

National Information Assurance (IA) Glossary. April 2010.

FIPS 200

Minimum Security Requirements for Federal Information and Information Systems. March 2006.

ISO Guide 73

Risk management — Vocabulary. 2009.

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.

OM 76/2002

Orden Ministerial número 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones. BOE de 29 de abril de 2002.

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.

SP 800-12

An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. October 1995.

SP 800-53

Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 3. August 2009.

SP 800-100

Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100. October 2006.