GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES QUE MANEJA INFORMACIÓN CLASIFICADA EN LA ADMINISTRACIÓN

POLÍTICA DE SEGURIDAD DE LAS TIC (CCN-STIC 001)

Junio 2016

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.03.27 19:03:21 +02'00'

© Centro Criptológico Nacional, 2016

NIPO: 002-16-004-5
Fecha de Edición: junio de 2016

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 (CNI), 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 (CCN) 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.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 (STIC) 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.

Junio de 2016

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. ANTECEDENTES 5
2. INTRODUCCIÓN 6
3. OBJETO 7
4. ALCANCE 7
5. CONCEPTOS GENERALES 8
5.1 INFORMACIÓN CLASIFICADA 8
5.2 SEGURIDAD DE LA INFORMACIÓN 10
6. PRINCIPIOS DE SEGURIDAD GENERALES 11
7. SEGURIDAD DEL ENTORNO DE OPERACIÓN 12
7.1 DE SEGURIDAD LIGADA AL PERSONAL 12
7.2 DE SEGURIDAD FÍSICA 13
7.3 DE SEGURIDAD DE LOS DOCUMENTOS 13
8. SEGURIDAD DE LAS TIC 13
8.1 PRINCIPIOS DE SEGURIDAD 13
8.2 MODOS SEGUROS DE OPERACIÓN 14
8.3 ACTIVIDADES DE SEGURIDAD EN EL CICLO DE VIDA 15
8.4 ACREDITACIÓN DE SEGURIDAD 16
8.5 SERVICIOS DE SEGURIDAD EN SISTEMAS ACREDITADOS 16
8.6 INTERCONEXIÓN DE SISTEMAS 17
8.7 FUNCIONES CRÍTICAS DE SEGURIDAD. GESTIÓN Y ADMINISTRACIÓN 17
8.7.1 GESTIÓN DE SEGURIDAD DE LAS TIC 17
8.7.2 ADMINISTRACIÓN DE SEGURIDAD DE LAS TIC 21
8.8 ASPECTOS GENERALES STIC 21
8.8.1 SOPORTES DE ALMACENAMIENTO EXTRAÍBLES 21
8.8.2 DISPOSITIVOS PORTÁTILES 22
8.8.3 RECURSOS DE PROPIEDAD PARTICULAR O DE CONTRATISTAS 22
9. SEGURIDAD CRIPTOLÓGICA 23
10. SEGURIDAD DE LAS EMANACIONES ELECTROMAGNÉTICAS 23
11. CERTIFICACIÓN DE SEGURIDAD 23
11.1 CERTIFICACIÓN FUNCIONAL 24
11.2 CERTIFICACIÓN CRIPTOLÓGICA 24
11.3 CERTIFICACIÓN TEMPEST 24
12. RESPONSABILIDADES 25
13. FORMACIÓN Y CONCIENCIACIÓN 26
13.1 FORMACIÓN 26
14. DESARROLLO NORMATIVO 26
ANEXO A: GUÍA DE EQUIVALENCIA ENTRE GRADOS DE CLASIFICACIÓN 28
ANEXO B: GLOSARIO DE TÉRMINOS Y ABREVIATURAS 28

1. ANTECEDENTES

1. La Ley 9/1968, de 5 de abril, sobre Secretos Oficiales (LSO), modificada por la Ley 48/1978, de 7 de octubre, y el Decreto 242/1969, de 20 de febrero, que la desarrolla, incluyen principios básicos de interés. Entre otros aspectos, establece que para transmitir información clasificada se deben utilizar medios de cifra adecuados y que la información clasificada debe ser protegida como tal, independientemente del soporte en el que se encuentre.

2. Por otra parte, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), establece el objetivo, el ámbito y las actividades de dicho Centro.

3. Según el artículo 4.e de esta Ley, una de sus funciones es la de *"Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro"*.

4. El artículo 4.f de la citada Ley señala asimismo que el CNI debe *"Velar por el cumplimiento de la normativa relativa a la información clasificada"*.

5. El Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN) asigna a este Centro las responsabilidades señaladas en los artículos 4.e. y 4.f. de la Ley 11/2002 aunque, en este último caso, exclusivamente en el ámbito de la normativa relativa a la protección de la información clasificada cuando es manejada por las Tecnologías de la Información y las Comunicaciones (TIC).

6. En concreto, las funciones que el Real Decreto asigna al CCN son:

    a) 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. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

    b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

    c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

    d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de

cifra, para procesar, almacenar o transmitir información de forma segura.

e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

7. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea el Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156, apartado 2 en similares términos

8. La Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

9. El Real Decreto 3/2010, de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad.

2. INTRODUCCIÓN

10. Los sistemas que manejan cualquier tipo de información en formato electrónico reciben indistintamente las denominaciones de *"Tecnologías de la Información y las Comunicaciones (TIC)"*, *"Tecnologías de la Información (TI)"*, *"Sistemas de Información"* o, en terminología inglesa, *"Communications and Information Systems (CIS)"*.

11. Estos conceptos quedan englobados en el término genérico *"Sistema"*, que se define como el conjunto de equipos y programas (hardware, firmware y software), métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información, y que está bajo la responsabilidad de una única autoridad.

12. El desarrollo de la llamada Sociedad de la Información implica que, cada vez más, la información se transmite, se procesa o se almacena en algún momento en un Sistema. Esto, unido al hecho de que los Sistemas son capaces de manejar mayor cantidad de información en menos tiempo, ha contribuido a conferir mayor importancia a la información propiamente dicha, que es considerada como un valor en sí misma.

13. Como tal valor, la información manejada en un Sistema puede estar sometida a distintos tipos de amenazas que conllevan un determinado nivel de riesgo. La implantación generalizada de las redes corporativas y el uso de Internet han contribuido a agravar esta situación.

14. Además, los equipos eléctricos y electrónicos, que componen un Sistema, pueden producir emisiones electromagnéticas no deseadas que detectadas y analizadas con los medios adecuados pueden llevar a la obtención de información (fenómeno TEMPEST).

15. Por todo ello, se hace necesario el establecimiento de unos principios básicos y la definición de unos requisitos mínimos de seguridad que permitan la adecuada protección de la información clasificada manejada en los sistemas de la Administración.

16. Tal y como establece la Autoridad Nacional para la Protección de la Información Clasificada, la *"Información Clasificada es cualquier información o material respecto de la cual se decida que **requiere protección contra su divulgación no autorizada** y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad" entendiéndose como información "todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma."*

3. OBJETO

17. Regular la política de seguridad de las tecnologías de la información que traten información clasificada en los sistemas de las Administraciones Públicas, mediante el establecimiento de principios básicos y la definición de requisitos mínimos para su adecuada protección.

18. A los sistemas de la Administración que manejen información sin clasificar les será de aplicación lo establecido en el Esquema Nacional de Seguridad (ENS), según establecen la Ley 39/2015, de 1 octubre, de Procedimiento Administrativo Común a las Administraciones Públicas y la Ley 40/2015, de 1 octubre, de Régimen Jurídico del Sector Público.

4. ALCANCE

19. Esta Política es de obligado cumplimiento en todos los sistemas que manejen información clasificada nacional en la Administración o cedida por la Administración, como en el caso de empresas que trabajen para la misma en contratos, programas o actividades clasificadas.

20. También será de aplicación a todos aquellos sistemas propiedad de España y que manejen información clasificada de la Organización del Tratado del Atlántico Norte (OTAN), Unión Europea (UE) u otras organizaciones con las que nuestro país haya firmado un tratado o acuerdo de protección mutua de la información clasificada, a no ser que las estrategias de acreditación indiquen algo diferente.

5. CONCEPTOS GENERALES

5.1 INFORMACIÓN CLASIFICADA

21. Los artículos 23.1 y 105 b) de la Constitución establecen el principio de que una participación ciudadana responsable de los asuntos públicos exige una necesaria información, principio que sólo encuentra excepciones en los casos en que sea necesario proteger la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

22. El imperativo de proteger la seguridad y defensa del Estado conlleva la necesidad de restringir aquella información que, por su importancia, pudiera dar lugar a riesgo o perjuicio graves en el supuesto de ser divulgada o comunicada a personas no autorizadas.

23. Según la Ley 9/1968, de 5 de abril, la información puede ser clasificada con el grado de SECRETO o RESERVADO, siendo el primero de ellos superior al segundo, es decir, con unos requisitos de protección más estrictos debido a su mayor importancia.

24. Asimismo, dicha Ley señala que *"El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las materias clasificadas"*.

25. El Decreto 242/1969, de 20 de febrero, por el que se desarrolla lo dispuesto en la Ley anterior, específica para dichos grados de SECRETO y RESERVADO, entre otros, los siguientes aspectos:

    - Los responsables de la protección de las materias clasificadas deberán asegurar el adecuado tratamiento de las materias clasificadas y mantener el control o registro de dichas materias.
    - La posesión o uso de información o material clasificados estará limitado a lugares donde se disponga de instalaciones para su almacenaje y segura protección, y a los cuales no pueden tener acceso otras personas que no sean las que, de manera fehaciente, hayan sido autorizadas para ello.
    - La transmisión del material clasificado se hará *"… por medios de transmisión en forma cifrada"*.

26. El Acuerdo de Ministros, de 28 de noviembre de 1986, amplía esta protección a toda información derivada de los tratados y acuerdos internacionales válidamente celebrados por España que, una vez publicados oficialmente, se incorporan al ordenamiento jurídico español, en virtud de lo dispuesto en el artículo 96 de la Constitución.

27. Una de las consecuencias de lo anterior, tras la adhesión de España al Tratado del Atlántico Norte y a la Unión Europea y la consecuente adopción de las normas de seguridad de ambas organizaciones, es la ampliación de los grados de clasificación de la información a CONFIDENCIAL y DIFUSIÓN LIMITADA, en

orden decreciente y, a su vez, ambos inferiores a los ya existentes de SECRETO y RESERVADO.

28. Determinados Ministerios, en virtud de las especiales características de todo orden que concurren en el normal desenvolvimiento de su función y de lo dispuesto en el Decreto 242/1969, de 20 de febrero, también han introducido en su ámbito, mediante normativa interna, los grados de clasificación CONFIDENCIAL y DIFUSIÓN LIMITADA.

29. En aquellos departamentos ministeriales donde no exista una normativa específica para la protección de la información clasificada, emanada de la Ley de Secretos Oficiales y su Decreto de desarrollo aprobada por el Ministro responsable del departamento y publicada oficialmente, será de aplicación las Normas de Seguridad (NS) de la Autoridad Nacional para la protección de la Información Clasificada.

30. A los efectos de la aplicación de la presente Política de Seguridad de las TIC (Política STIC) y la normativa derivada, se considera información clasificada la etiquetada con alguno de los siguientes grados de clasificación, en orden decreciente de importancia:

- SECRETO
- RESERVADO
- CONFIDENCIAL
- DIFUSIÓN LIMITADA

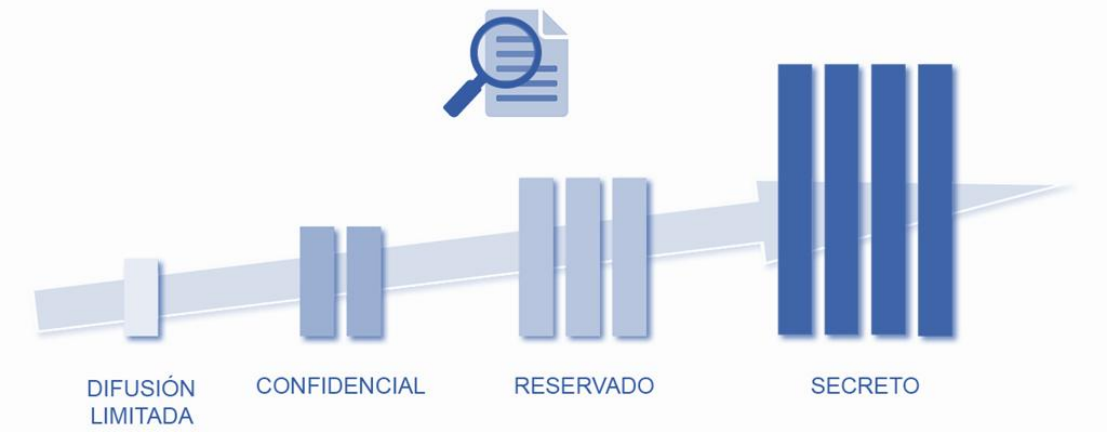

Figura 1.- Grados de clasificación de la información

31. En el Anexo A se encuentra, con carácter orientativo, una tabla de equivalencias entre los grados de clasificación de la información en lo que a medidas de protección se refiere.

32. Aquellos organismos que dispongan de información que, no pudiendo ser clasificada con ninguno de los grados anteriores, requiera cierta protección, por ser de carácter sensible o de uso interno, podrán regular mediante normativa

interna la introducción en su ámbito de la categoría SIN CLASIFICAR, pudiéndose marcar como USO OFICIAL/USO PÚBLICO.

5.2 SEGURIDAD DE LA INFORMACIÓN

33. La asignación de recursos para la protección de la información en los sistemas de las Administraciones Públicas requerirá la determinación previa de los activos a proteger.

34. La información clasificada, regulada por su normativa específica, constituye el activo más crítico en la Administración. Por lo tanto, para su tratamiento por los sistemas, requerirá la aplicación de las medidas de seguridad establecidas en la normativa correspondiente.

35. El resto de activos de información de las Administraciones Públicas, que no contengan información clasificada ni se refieran a actividades que desarrollen las administraciones en régimen de derecho privado, les serán de aplicación las medidas de seguridad establecidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Real Decreto 951/2015, de 23 de octubre, por el que se modifica el anterior.

36. En función de la naturaleza de los activos, se pueden establecer los siguientes tipos de seguridad:

    - Seguridad de las personas.
    - Seguridad de las instalaciones, infraestructuras y plataformas.
    - Seguridad de las actividades.
    - Seguridad de la información.
    - Seguridad de las tecnologías de la información y las comunicaciones.

37. Se denomina Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) a la protección de la información almacenada, procesada o transmitida, por sistemas de las tecnologías de la información y las comunicaciones (sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información, así como la integridad y disponibilidad de los propios sistemas.

38. La Seguridad de las TIC, al objeto de conseguir una protección adecuada de la información, deberá considerar un conjunto equilibrado de medidas de seguridad de distinta naturaleza (física, de personal, documental, etc.) de acuerdo con la normativa específica aprobada por la Oficina Nacional de Seguridad (ONS).

39. Se denomina Política STIC al conjunto, formalizado en un documento aplicable, de elementos estratégicos, directivas, procedimientos, códigos de conducta, normas organizativas y técnicas, que tiene por objetivo la protección del (o de los) sistema(s) de información del Organismo.

6. PRINCIPIOS DE SEGURIDAD GENERALES

40. La Política STIC se apoya en los principios de seguridad establecidos para el tratamiento de la documentación y la información clasificada manejada en los sistemas y, en concreto, en los siguientes:

- Clasificación de la información.
- Habilitación/Autorización de seguridad.
- Necesidad de conocer.
- Compartimentación de la información.
- Imputabilidad.
- Equilibrio entre seguridad y eficacia o garantía razonable.
- Segregación de las funciones de administración, administración de seguridad y supervisión de seguridad.

41. Los principios de seguridad antes mencionados identifican los siguientes objetivos de seguridad para los sistemas TIC:

- Identificar y autenticar a las personas y controlar su acceso a la información manejada por un Sistema o a los recursos del mismo.
- Proporcionar confidencialidad a la información manejada por un Sistema.
- Proporcionar integridad a la información manejada por un Sistema o a los recursos del mismo.
- Mantener la disponibilidad de la información manejada por un Sistema o de los recursos del mismo.
- Garantizar la autenticidad de la información manejada por los sistemas.
- Emplear productos de seguridad que haya sido revisados, evaluados, recomendados y/o certificados por el Organismo de Certificación competente.
- Mantener la trazabilidad de las actuaciones realizadas.

Figura 2.- Principios de seguridad generales

42. Para un Sistema en concreto, los objetivos de seguridad a satisfacer se verificarán durante el procedimiento de Acreditación de Seguridad de las TIC.

43. Según el grado de clasificación de la información a proteger, el proceso de acreditación verificará que se cumplen los requisitos de seguridad establecidos en:

    - El entorno de operación
    - Los sistemas de las TIC
    - La criptología
    - Las emanaciones electromagnéticas (TEMPEST)

7. SEGURIDAD DEL ENTORNO DE OPERACIÓN

7.1 DE SEGURIDAD LIGADA AL PERSONAL

44. La seguridad deberá comprometer a todos los miembros de la Organización, existiendo unos claros responsables de velar por el cumplimiento de la propia Política STIC y de las normas que de ella se deriven.

45. La distribución de la información clasificada se llevará a cabo sobre los principios de necesidad de conocer y autorización.

46. Todo el personal que necesite acceder, o que por sus obligaciones pueda acceder, a información clasificada a través de un Sistema, deberá estar

convenientemente concienciado y formado en los distintos aspectos de seguridad y poseer la autorización correspondiente en su caso (Habilitación Personal de Seguridad). Para la categoría de DIFUSIÓN LIMITADA, no será necesaria la autorización expresa.

47. Cualquier infracción de seguridad que se produzca deberá comunicarse a la Autoridad correspondiente por el medio establecido a tal efecto.

7.2 DE SEGURIDAD FÍSICA

48. Aquellas áreas donde se pueda acceder a información clasificada deberán disponer de las medidas físicas de protección establecidas en la normativa vigente y del correspondiente documento, emitido por la Autoridad correspondiente, que certifique que el local cumple con dichas medidas.

7.3 DE SEGURIDAD DE LOS DOCUMENTOS

49. Los documentos impresos que contengan información clasificada, así como sus soportes informáticos, serán protegidos de acuerdo con la normativa vigente.

8. SEGURIDAD DE LAS TIC

8.1 PRINCIPIOS DE SEGURIDAD

50. Los principios necesarios para cumplir con los objetivos de seguridad en los sistemas clasificados son:

- **Análisis y Gestión del Riesgo.** Se realizarán aquellos procesos necesarios de análisis y gestión de riesgos que permitan determinar, reducir, eliminar, evitar o asumir los riesgos asociados al Sistema.
- **Mínima Funcionalidad.** Solo estarán disponibles las funciones, protocolos y servicios necesarios para cumplir con el requisito operacional o funcional del sistema.
- **Mínimo Privilegio.** Los usuarios de los sistemas que manejen información clasificada solo dispondrán de los privilegios y autorizaciones que se requieran para la realización de las obligaciones asociadas a su puesto de trabajo.
- **Nodo Autoprotegido.** Cada Sistema interconectado deberá, inicialmente, tratar al otro Sistema como un entorno no confiable y deberá implementar medidas que controlen el intercambio de información con el otro Sistema.
- **Defensa en Profundidad.** Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas, y en la máxima extensión, de manera que no haya una única línea (o componente) de defensa.

- **Control de Configuración.** Se debe mantener una configuración básica actualizada del equipamiento hardware y software en los sistemas clasificados. Se establecerá con carácter obligatorio la aplicación de configuraciones de seguridad en las diferentes tecnologías utilizadas en el Sistema.
- **Verificación de la Seguridad.** La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.
- **Monitorización, Vigilancia y Respuesta a Incidentes.** Se debe disponer de una capacidad de vigilancia y respuesta que permita la reacción oportuna y adecuada a cualquier incidente de seguridad.
- **Resiliencia.** Los sistemas tienen que tener la capacidad de soportar y recuperarse ante incidentes de seguridad.

8.2 MODOS SEGUROS DE OPERACIÓN

51. Los sistemas que manejen información clasificada deben funcionar de acuerdo con los Modos Seguros de Operación. Dichos modos vienen determinados por la autorización y necesidad de conocer de los usuarios, y por el mayor grado de clasificación de la información manejada en el Sistema.

52. Se pueden definir los siguientes modos seguros de operación:

- **Dedicado.** Es aquel modo en el que todo el personal con acceso al Sistema está autorizado para acceder al grado más elevado de clasificación de la información manejada en el Sistema, y además posee la misma necesidad de conocer.
    - La separación de los datos no es un requisito del Sistema.
- **Unificado al Nivel Superior.** Es aquel en el que las personas con acceso al Sistema:
    - Están autorizadas para acceder al grado más elevado de clasificación de la información manejada en el Sistema.
    - No todos tienen la misma necesidad de conocer.

  La necesidad de conocer se garantiza por medio de procesos informales, que hacen que el Sistema realice la separación de datos de una de manera fiable, disponga de un control de accesos selectivo a la información conforme a la diferente necesidad de conocer y cumpla con lo establecido en la normativa de seguridad vigente y en sus políticas correspondientes fundamentalmente por medios procedimentales.
- **Compartimentado.** Es aquel en el que las personas con acceso al Sistema:
    - Están autorizadas para acceder al grado más elevado de clasificación de la información manejada en el Sistema,

- No todos tienen la misma necesidad de conocer,

La necesidad de conocer se garantiza por medio de una autorización formal para acceder a la información manejada en el Sistema, y se materializa, además de en una gestión centralizada formal para el control de accesos, en el uso de herramientas y mecanismos adicionales que refuercen globalmente el cumplimiento de las políticas y la normativa de seguridad.

- **Multinivel.** Es aquel modo en el que un Sistema maneja información con diferentes grados de clasificación.
  - Permite el acceso selectivo y simultáneo a dicha información al personal autorizado con diferentes grados de clasificación y distintas necesidades de conocer.
  - El Sistema realiza de manera fiable la completa separación de los datos y el control del acceso selectivo.
  - Este modo de operación no es de aplicación para los sistemas acreditados para manejar información DIFUSIÓN LIMITADA, o equivalente.

8.3 ACTIVIDADES DE SEGURIDAD EN EL CICLO DE VIDA

53. La seguridad tiene un tratamiento diferente durante todo el ciclo de vida del Sistema: determinación de la necesidad, diseño, desarrollo, implantación, operación, mantenimiento y retirada.

54. Los aspectos de seguridad pueden limitar el número de soluciones que se puedan implementar en el diseño y desarrollo del Sistema. Los requerimientos de seguridad afectan a la operación, el mantenimiento, el personal y a los costes asociados a la solución seleccionada.

55. Con objeto de reducir las amenazas y vulnerabilidades en los sistemas TIC, la seguridad se tratará desde la fase de diseño donde se seleccionarán las salvaguardas que limiten los riesgos e identificando la necesidad de productos STIC (equipos de cifra, herramientas y productos de seguridad, etc.). La introducción de salvaguardas con el Sistema en operación normalmente es más costosa y menos efectiva.

56. Por ello, el análisis y gestión de riesgos de seguridad estará presente en el proceso de desarrollo del Sistema. Esta actividad será realizada coordinadamente por los responsables de diseño y operación con el propósito de asegurar que se cumplen los requisitos mínimos de protección para la información clasificada de que se trate, utilizando la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) y sus herramientas de apoyo.

8.4 ACREDITACIÓN DE SEGURIDAD

57. La Acreditación es la autorización otorgada a un Sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su Concepto de Operación (CO).

58. Todos los sistemas que requieran manejar información clasificada en la Administración deberán ser previamente acreditados, de acuerdo con el procedimiento que, para tal fin, apruebe la Autoridad de Acreditación de Seguridad (AAS)[1].

59. El Secretario de Estado Director del Centro Nacional de Inteligencia en virtud del artículo 4, apartados e y f, de la Ley 11/2002, de 6 de mayo, es Autoridad de Acreditación de Seguridad (AAS).

60. El procedimiento de acreditación de seguridad, entre otros requisitos, confirmará que las medidas de seguridad, que satisfacen los requisitos STIC, se encuentran en operación en los sistemas antes de manejar información clasificada.

8.5 SERVICIOS DE SEGURIDAD EN SISTEMAS ACREDITADOS

61. Todos los sistemas que manejen información clasificada deberán disponer de un conjunto equilibrado de servicios de seguridad de las TIC que permitan alcanzar los objetivos necesarios para proteger dicha información. Conforme al grado de clasificación de la información que cada Sistema maneja y su modo de operación, estos servicios de seguridad permitirán lo siguiente:

    - Identificar y autenticar al personal con acceso autorizado.
    - Controlar los accesos a la información en base al principio de "*la necesidad de conocer*".
    - Verificar la integridad y autenticidad de la información, así como la integridad de los elementos del Sistema.
    - Mantener la integridad y autenticidad de la información, así como la integridad de los elementos del Sistema.
    - Mantener la disponibilidad requerida para la información y los elementos del Sistema.
    - Garantizar y verificar el funcionamiento de los mecanismos de seguridad del Sistema.
    - Registrar y auditar la actividad de los usuarios del Sistema.
    - Controlar las conexiones y los enlaces de los Sistemas.

[1] Véase Guía CCN-STIC-101 Acreditación de Sistemas de las TIC que manejan Información Clasificada

- Monitorizar y vigilar los registros de actividad de las diferentes tecnologías, así como el tráfico de red con el fin de detectar ataques.
- Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información, o a la integridad y disponibilidad del Sistema que la maneja.

8.6 INTERCONEXIÓN DE SISTEMAS

62. Con anterioridad a la acreditación de la interconexión de sistemas, éstos deberán estar acreditados siempre que manejen información clasificada. Un Sistema que no esté acreditado, se considerará como un Sistema o red de acceso público a los efectos de su interconexión con otros Sistemas.
63. La AAS establecerá los criterios, condiciones y requisitos de interconexión en la normativa correspondiente.
64. En la documentación de seguridad correspondiente a cada interconexión debe reflejarse:
    - Los flujos de información.
    - Los métodos de interconexión y servicios.
    - Los riesgos de seguridad específicos.
    - La arquitectura de seguridad.
    - Los requisitos de seguridad adicionales.
    - Los procedimientos empleados.

8.7 FUNCIONES CRÍTICAS DE SEGURIDAD. GESTIÓN Y ADMINISTRACIÓN

8.7.1 GESTIÓN DE SEGURIDAD DE LAS TIC

65. El término gestión de la seguridad describe el proceso que asegura la confidencialidad, integridad y disponibilidad de los activos de una organización, información, datos y servicios de las TIC.
66. Para gestionar la seguridad adecuadamente hay que establecer cuatro procesos fundamentales que conjuntamente contribuyen a cubrir el programa completo de la gestión de la seguridad. En la figura siguiente se muestra la interacción que estos procesos tienen entre sí.

Figura 3.- Procesos en la gestión completa de la seguridad

8.7.1.1 POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN

67. La política de seguridad es única para todos los sistemas de la organización. Los sistemas que manejen información clasificada tendrán como referencia el presente documento y la normativa derivada.

8.7.1.2 GESTIÓN DE RIESGOS DE SEGURIDAD

68. Cada organismo que desarrolle e implante sistemas que manejen información clasificada realizará la correspondiente gestión de riesgos de acuerdo a los criterios proporcionados por la Autoridad de Acreditación de Seguridad.

69. La gestión de riesgos de seguridad deberá permitir mantener un entorno controlado minimizando los riesgos hasta niveles asumibles.

70. La reducción de los niveles de riesgo exige el despliegue de controles de seguridad, por lo que será necesario establecer un equilibrio entre los niveles de seguridad y el coste de las medidas de seguridad a desplegar (riesgo residual).

71. La gestión de riesgos de seguridad se desarrolla de forma cíclica. El ciclo de vida del proceso consta de cuatro fases:

    - Fase 1: Evaluación del riesgo. Identificar y priorizar los riesgos.
    - Fase 2: Selección de controles de seguridad.
    - Fase 3: Despliegue de los controles seleccionados.
    - Fase 4: Medir la efectividad del programa. Analizar la efectividad del proceso de gestión de riesgos de seguridad y verificar que los controles están proporcionando el grado de protección esperado.

Figura4.- Ciclo de vida del proceso de gestión de la seguridad

8.7.1.3 MONITORIZACIÓN DE SEGURIDAD

72. El objetivo general es la recolección, presentación y almacenamiento de registros para detectar anomalías que afecten a la protección de los sistemas y la seguridad de la información que manejan. Se examinarán los registros que se determinen en los sistemas con herramientas de correlación y minería de datos, y se desplegarán sistemas de detección/prevención de intrusos o detección de anomalías.

73. La monitorización de la seguridad es un proceso continuo que se observa en los sistemas e identifica los intentos de comprometer la seguridad de la organización.

74. En los sistemas de la Administración que manejan información clasificada, la actividad de monitorización será responsabilidad de la Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC) en su ámbito de actuación.

8.7.1.4 CAPACIDAD DE RESPUESTA A INCIDENTES DE SEGURIDAD

75. El proceso de respuesta a incidentes define la forma en la que son comunicados los incidentes de seguridad y las actividades derivadas.

76. Los objetivos del proceso son:

    - Desarrollar una efectiva y oportuna reacción ante determinados incidentes y subsanar cualquier daño que se haya producido. El objetivo es reducir el impacto sobre la actividad de la organización y sobre los usuarios.
    - Minimizar la posibilidad de ocurrencia de un incidente de seguridad. Para ello, tras un análisis profundo que determine exactamente las causas de

éste, se recomendarán la introducción o modificación de los controles de seguridad necesarios.

77. El proceso de respuesta a incidentes debe asegurar que todos los miembros de la organización sean completamente conscientes de las acciones a tomar cuando ocurra un incidente de seguridad.

78. El resultado de la evaluación de los incidentes de seguridad debe realimentar los procesos de generación de Políticas de Seguridad y de Análisis de Riesgos para intentar minimizar el riesgo de nuevos incidentes.

79. La respuesta a incidentes es una tarea compartida entre las siguientes autoridades:

- **AOSTIC.** Realizará la monitorización del Sistema. Proporcionará el primer nivel de respuesta a incidentes de seguridad.
- **AAS/AAS-D.** Deberá recibir información de los incidentes de seguridad según su criticidad.

80. El objetivo de los Equipos de la Respuesta a Incidentes de Seguridad es responder a las amenazas de forma oportuna y efectiva con objeto de minimizar cualquier impacto contra la confidencialidad, integridad o disponibilidad.

81. Esta actividad es conveniente centralizarla al más alto nivel posible y evitar duplicidad de esfuerzos. Asimismo, es necesaria la cooperación de todos los usuarios para asegurar que los incidentes son comunicados, resueltos y se toman las acciones preventivas para evitar que se vuelvan a reproducir.

82. El CCN-CERT, como CERT Gubernamental Nacional, y de acuerdo a diferente normativa, tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Por este motivo, proporcionará la respuesta a incidentes de seguridad en un segundo nivel. En su caso, centralizará la capacidad conjunta de monitorización, a través de su Sistema de Alerta Temprana (SAT).

83. La respuesta a incidentes de seguridad y su clasificación se desarrolla en la normativa correspondiente[2]. En el caso de incidentes con peligrosidad ALTA, MUY ALTA y/o CRÍTICA es obligatoria la notificación urgente al CCN-CERT según los plazos establecidos.

8.7.1.5 AUDITORÍA/INSPECCIÓN DE SEGURIDAD

84. La auditoría/inspección de seguridad es una actividad periódica que trata de verificar que todos los sistemas cumplen con las políticas de seguridad establecidas. El objetivo es evaluar cualquier deficiencia o no cumplimiento de

[2] Véase Guía CCN-STIC-817 de Gestión de Ciberincidentes en donde se recoge la clasificación y peligrosidad de los mismos.

las políticas de seguridad e identificar y proponer las medidas correctoras apropiadas.

85. En los sistemas que manejan información clasificada, la actividad de auditoría/inspección será responsabilidad de la AAS/AAS-D y sus organismos de apoyo siendo un procedimiento único para toda la organización.

8.7.2 ADMINISTRACIÓN DE SEGURIDAD DE LAS TIC

86. La administración de seguridad es el proceso necesario para mantener un entorno seguro en los sistemas de las TIC.

87. La administración de seguridad está relacionada con todos los aspectos de seguridad necesarios y entre ellos los siguientes:

- **Control de acceso.** Determinar los permisos de acceso adecuados para cada usuario de la organización.
- **Seguridad de aplicaciones.** Controlar los permisos y las acciones que los usuarios pueden ejecutar dentro de los sistemas de la organización, así como las configuraciones de seguridad de las aplicaciones utilizadas.
- **Seguridad de los sistemas operativos.** Configurar de forma segura los sistemas operativos y garantizar el soporte y mantenimiento de los mismos. Un sistema operativo inseguro puede comprometer a todos los sistemas y servicios que dependen de éste.
- **Seguridad del hardware.** Asegurar el hardware (servidores, estaciones de trabajo, equipos portátiles, sistemas y/o soportes de respaldo, dispositivos de almacenamiento removibles, tarjetas inteligentes, dispositivos de impresión, etc.) dentro y fuera del entorno seguro.
- **Seguridad de la red.** Asegurar la infraestructura de la red para evitar el acceso no autorizado a la información, así como su manipulación.

8.8 ASPECTOS GENERALES STIC

8.8.1 SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

88. Se deberán establecer procedimientos que permitan identificar, controlar, registrar y proteger los soportes de almacenamiento extraíbles (DVD, CD, discos duros, disquetes, discos USB, tarjetas de memoria u otros de naturaleza análoga) que contengan información clasificada, de acuerdo al grado de clasificación de dicha información.

89. Las marcas o etiquetas (en adelante marcas) empleadas para la identificación de estos soportes de almacenamiento deberán reflejar el mayor grado de clasificación de la información que contienen y adaptarse en lo posible a las características físicas de los mismos.

90. Se llevará a cabo un inventario anual de los soportes que hayan almacenado información clasificada de acuerdo a lo establecido en las Normas de la Autoridad Nacional de Seguridad y se establecerán controles periódicos para comprobar su presencia, así como su contenido.

91. Los soportes que hayan almacenado información clasificada de grado SECRETO o RESERVADO, o equivalente, en cuanto a medidas de seguridad, no podrán ser desclasificados ni reutilizados en sistemas de diferente grado de clasificación. Una vez finalizado su ciclo de vida debe procederse a su destrucción según el procedimiento establecido.

92. Los soportes que hayan almacenado información clasificada con un grado de clasificación CONFIDENCIAL, o inferior, si podrán ser reutilizados en otros sistemas con independencia del grado de clasificación una vez se haya procedido a su borrado seguro y desclasificación. De no poder borrarse de forma segura, se procederá a su destrucción según el procedimiento establecido.

8.8.2 DISPOSITIVOS PORTÁTILES

93. La Autoridad Operativa del Sistema establecerá procedimientos para la identificación, control, registro y protección de todos aquellos dispositivos portátiles (tabletas, agendas electrónicas, teléfonos inteligentes, etc.) que manejen información clasificada, operando de forma aislada o en red, de acuerdo al grado de clasificación de dicha información.

8.8.3 RECURSOS DE PROPIEDAD PARTICULAR O DE CONTRATISTAS

94. Con carácter general no se podrán utilizar medios de propiedad particular (personales o de servicios externalizados) con capacidad de almacenamiento y/o procesamiento de información (dispositivos portátiles, soportes de almacenamiento extraíbles, software, hardware, etc.) para el manejo de información clasificada CONFIDENCIAL o superior. En situaciones excepcionales, la Autoridad de Acreditación de Seguridad (AAS) o la Autoridad Delegada de Acreditación de Seguridad (AAS-D) podrán autorizar dicha utilización.

95. La simple introducción de medios informáticos distintos de los acreditados en las zonas de seguridad en las que se encuentre un Sistema que maneje información clasificada CONFIDENCIAL o superior, deberá contar con la autorización expresa de la Autoridad Operativa de dicho Sistema.

96. Los sistemas propiedad de contratistas que vayan a manejar información clasificada deberán ser acreditados siguiendo los mismos procedimientos y aplicando la misma normativa que para los sistemas de la Administración. Como exención de lo anterior, la Autoridad Operativa podrá autorizar aquel equipamiento que se utilice exclusivamente para diagnóstico y mantenimiento del Sistema.

9. SEGURIDAD CRIPTOLÓGICA

97. Los Sistemas que manejen información clasificada DIFUSIÓN LIMITADA o superior, y utilicen mecanismos de cifra para su protección, deberán hacer uso de productos de cifra aprobados de acuerdo al grado de clasificación de la información a proteger[3].

98. Aquellos organismos en los que se requiera el empleo de material de cifra para la protección de la información clasificada CONFIDENCIAL o superior, deberán tener establecida una estructura para el control y el registro de todo el material de cifra utilizado y disponer del personal con la formación adecuada, según lo que establezca la normativa correspondiente.

99. La Autoridad de Certificación Criptológica (ACC) deberá autorizar expresamente el empleo de otro material de cifra. El procedimiento para solicitar dicha autorización viene descrito en la guía CCN-STIC-003.

100. La selección, desarrollo, adquisición, operación, mantenimiento, modificación y retirada del servicio del equipamiento criptológico para manejar información clasificada se regulará mediante la normativa correspondiente.

10. SEGURIDAD DE LAS EMANACIONES ELECTROMAGNÉTICAS

101. La seguridad de las emanaciones es el conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.

102. Los sistemas que manejen información clasificada CONFIDENCIAL o superior, requerirán el uso de equipos con certificación TEMPEST o clasificación de zona (ZONING) de los locales y plataformas donde se ubican dichos equipos, según lo establecido en la normativa correspondiente. En el caso de certificaciones TEMPEST, la AAS/AAS-D podrá autorizar el empleo de equipos con certificaciones emitidas por las autoridades competentes de otras naciones.

103. Los requisitos TEMPEST de equipos, locales y plataformas se deben tener en cuenta durante las fases de selección, desarrollo, operación, mantenimiento y, en su caso, en la fase de modificación y actualización.

11. CERTIFICACIÓN DE SEGURIDAD

104. La certificación de la seguridad es la determinación, realizada mediante un proceso metodológico de evaluación tanto analítico como práctico, de la conformidad de las propiedades de seguridad de un producto o sistema con unos criterios pre-establecidos.

[3] El catálogo de dichos productos está disponible en la guía CCN-STIC-103.

105. Según los criterios en los que se base el proceso de evaluación, es decir, según los aspectos de seguridad que se evalúen, la certificación del producto o sistema de las TIC podrá ser funcional, criptológica y TEMPEST.

106. Para la acreditación de un Sistema se recomienda la utilización de, al menos, sistemas operativos y dispositivos de protección de perímetro certificados respecto a perfiles de protección autorizados por la AAS/AAS-D. En cualquier caso, será obligatorio disponer de una configuración de seguridad según las guías CCN-STIC en vigor.

11.1 CERTIFICACIÓN FUNCIONAL

107. La certificación funcional tiene como objetivo la confirmación de que las funciones de seguridad de un producto o sistema son ciertas y están correctamente implementadas y además, contrarrestan efectivamente a las amenazas a la vez que satisfacen los objetivos de seguridad descritos en su declaración de seguridad.

108. Este proceso de certificación, realizado por el Centro Criptológico Nacional (CCN) como Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, viene regulado por la Orden de Presidencia OPRE 2740/2007, de 19 de septiembre, y por los procedimientos del Esquema publicados en su página web (http://oc.ccn.cni.es).

109. La evaluación de seguridad será realizada por un laboratorio independiente, acreditado en el Esquema y capacitado técnicamente para tal fin, siguiendo una metodología pública como puede ser Common Criteria, ISO/IEC 15408 o ITSEC (Information Technology Security Evalulation Criteria) u otras que reconozca el Organismo de Certificación.

11.2 CERTIFICACIÓN CRIPTOLÓGICA

110. El Centro Criptológico Nacional (CCN) es el Organismo responsable de la elaboración del Catálogo de Productos con Certificación Criptológica que incluye los productos capaces de proteger la información clasificada nacional.

111. De esta forma, tendrá la consideración de equipo o sistema de cifra nacional con certificación criptológica aquel equipo de cifra que haya superado favorablemente la evaluación criptológica y obtenido dicha certificación por parte del CCN.

11.3 CERTIFICACIÓN TEMPEST

112. Todos los equipos que procesan información clasificada CONFIDENCIAL, o superior, pueden requerir del correspondiente certificado TEMPEST si así se

determina como resultado de los estudios de posible ubicación dentro de las instalaciones o plataforma.

113. Las instalaciones y plataformas, en las que se ubiquen sistemas de las TIC que manejen información clasificada CONFIDENCIAL, o superior, deberán disponer del correspondiente certificado de que la instalación o local cumple con las medidas TEMPEST necesarias.

114. Los equipos certificados TEMPEST y los equipos clasificados para un ZONING determinado figuran en la Lista de Productos con Certificación TEMPEST.

115. El CCN, como autoridad de certificación de seguridad TIC en el ámbito EMSEC (Seguridad de las Emanaciones), tiene entre otras misiones, el desarrollo de normativa Nacional en este campo, la evaluación y certificación de equipos, sistemas e instalaciones, así como la participación y asesoramiento en diferentes foros, actuando en todos ellos como Autoridad TEMPEST Nacional (NTA).

116. La norma TEMPEST (CCN-STIC-210) es de aplicación para la información clasificada con el grado CONFIDENCIAL o superior. Por tanto, afecta a equipos, sistemas e instalaciones, tanto fijas como móviles en las que se genera o procesa esta información.

12. RESPONSABILIDADES

117. Para conseguir una seguridad efectiva y completa en los sistemas clasificados es imprescindible que se delimiten las funciones y se definan las responsabilidades de quienes los utilizan y gestionan.

118. En los sistemas clasificados se determinarán una serie de autoridades y responsables relacionados con la seguridad de los sistemas a lo largo de su ciclo de vida. En cada organización deberán existir las siguientes estructuras:

- Estructura STIC Nacional.
- Estructura STIC de la organización.
- Estructura de control de material de cifra de la organización.
- Estructura de operación del Sistema.

119. Estructura STIC Nacional. Estructura común a todos los sistemas y a todos los organismos en la que existirán las siguientes Autoridades:

- Autoridad de Acreditación de Seguridad (AAS).
- Autoridad de Certificación de la Seguridad de las Tecnologías de la Información (ACSTI).
- Autoridad de Certificación Criptológica (ACC).
- Autoridad de Certificación de la Seguridad de las Emanaciones TEMPEST (ACT).

- Esta estructura podrá contar con una Autoridad de Acreditación de Seguridad Delegada (AAS-D). La AAS/AAS-D mantendrá un registro de sistemas acreditados para manejar información clasificada.

120. Estructura de control de material de cifra de la organización. En el caso de que una organización tenga material de cifra, deberá tener una estructura de control para garantizar la seguridad, custodia y control/inventario del material de cifra de la organización.

121. Estructura de Operación del Sistema. Estructura establecida en todos los sistemas clasificados y existirán, en su caso, las siguientes Autoridades:

    - Autoridad Operativa del Sistema de las TIC (AOSTIC).

    En la normativa correspondiente se desarrollarán las diferentes estructuras.

13. FORMACIÓN Y CONCIENCIACIÓN

13.1 FORMACIÓN

122. El Centro Criptológico Nacional establecerá un plan de formación anual que incluirá los cursos de especialización necesarios para la aplicación de la presente Política[4].

123. El plan de formación se compone de:

    - **Cursos Informativos y de Concienciación de Seguridad.** Se componen de seminarios generales de concienciación, seminarios temáticos y cursos generales sobre seguridad de las TIC.
    - **Cursos Básicos de Seguridad.** Cursos de iniciación en las funcionalidades de seguridad de las diferentes tecnologías.
    - **Cursos Específicos de Gestión de Seguridad.** Cursos que capaciten al personal de los diferentes organismos a realizar la función de Gestión de Seguridad y todos los procesos y actividades asociadas.
    - **Cursos de Especialización de Seguridad.** Cursos que capaciten al personal técnico en el empleo y aplicación de configuraciones de seguridad de las diferentes tecnologías de los Sistemas.

124. Las AOSTIC podrán elaborar y mantener el plan de formación y especialización para la aplicación de la presente Política en sus respectivos ámbitos.

14. DESARROLLO NORMATIVO

125. El desarrollo normativo de la Política STIC se desglosará en los siguientes tipos de documentos:

    - Procedimientos.

[4] El CCN ofrece tanto cursos presenciales como online (https://www.ccn-cert.cni.es/cursos.html)

- Normas.
- Instrucciones Técnicas.
- Guías.

126. Los **Procedimientos STIC** (Serie CCN-STIC-100) establecerán el marco común de actuación en los procesos de acreditación y certificación de las TIC, así como en cualquier otro proceso relacionado con la seguridad de las TIC. Estos procedimientos serán sancionados y publicados por la AAS/AAS-D.

127. Las **Normas STIC** (Serie CCN-STIC-200) constituyen la reglamentación que debe seguirse, o a la que deben ajustarse las conductas, tareas o actividades de las personas y organizaciones en relación con la protección de la información clasificada cuando es manejada por un Sistema. Establecerán las directrices para la redacción de la documentación de seguridad, para la realización de análisis de riesgos o para cualquier otra actividad que se considere necesaria en relación con la seguridad de las TIC.

128. Las **Instrucciones Técnicas STIC** (Serie CCN-STIC-300) atenderán a un objetivo de seguridad específico. Establecerán los requisitos de seguridad generales o específicos a implantar en los sistemas.

129. Las **Guías STIC** son recomendaciones o informaciones relativas a temas concretos STIC y establecerán las configuraciones mínimas de seguridad de los diferentes elementos de un Sistema, recomendaciones de uso o de otro tipo.

130. A efectos del presente documento, las series documentales 000, 100, 200 y 300 son de obligado cumplimiento.

ANEXO A: GUÍA DE EQUIVALENCIA ENTRE GRADOS DE CLASIFICACIÓN

La siguiente tabla es meramente orientativa y no tiene ningún carácter normativo. Pretende representar las equivalencias entre los grados de clasificación de la información **en lo que a medidas de protección** se refiere.

Nacional	UNIÓN EUROPEA	OTAN	ENS
SECRETO	TRES SECRET UE /UE TOP SECRET	COSMIC TOP SECRET (CTS)	
RESERVADO	SECRET UE / UE SECRET	NATO SECRET (NS)	
CONFIDENCIAL	CONFIDENTIEL UE / EU CONFIDENTIAL	NATO CONFIDENTIAL (NC)	CATEGORÍA ALTA
DIFUSIÓN LIMITADA	RESTREINT EU / EU RESTRICTED	NATO RESTRICTED (NR)	CATEGORÍA MEDIA
SIN CLASIFICAR **USO OFICIAL** **USO PÚBLICO**	EU SENSITIVE INFORMATION (EUSI) LIMITE PUBLIC	NATO UNCLASSIFIDED (UN) COMMERCIAL-MEDIAL-PERSONAL-PUBLIC- OPEN SOURCE	CATEGORÍA BÁSICA

Tabla 1.- Guía de equivalencias entre grados de clasificación de la información

ANEXO B: GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acreditación — La Acreditación es la autorización otorgada a un Sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su Concepto de Operación (CO).

Activos — Son los recursos del Sistema, o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Amenaza — Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un Sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio Sistema.

Análisis de riesgos — Es el proceso por el cual se identifican y valoran los riesgos

Autenticidad — Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente

	de la que proceden los datos.
Autoridad de Acreditación de Seguridad (AAS)	Autoridad responsable de conceder la autorización a un Sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.
Autoridad de Certificación Criptológica (ACC)	Autoridad responsable de la evaluación y certificación de productos y Sistemas (de tecnologías de la información y telecomunicaciones) que incorporen mecanismos criptológicos.
Autoridad de Acreditación de Seguridad Delegada (AAS-D)	Autoridad en la que ha delegado la Acreditación la AAS, y que es responsable de la aplicación de la normativa de acreditación vigente.
Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC)	Autoridad responsable del desarrollo, la operación y mantenimiento del Sistema durante su ciclo de vida, de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.
Certificación de seguridad	La certificación es la determinación positiva de que un producto o sistema tiene capacidad para proteger la información según un nivel de seguridad y de acuerdo a unos criterios establecidos en el procedimiento o metodología de evaluación correspondiente
Clase I	Zona en la que se maneja y almacena información clasificada de tal forma que la entrada a la zona supone, a todos los efectos, el acceso a dicha información, por lo que sólo puede acceder personal debidamente habilitado y autorizado. Este tipo de zona precisa: - Un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas. - Un sistema de control de entrada que admita exclusivamente a aquellas personas debidamente habilitadas y específicamente autorizadas para acceder a dicha área. - Que las personas que accedan a la zona sean informadas previamente del tipo y grado de clasificación de la información a la que da acceso la entrada.
Clase II	Zona en la que se maneja y almacena información clasificada de tal forma que pueda estar protegida del acceso de personas no autorizadas mediante controles establecidos internamente, por lo que se podrá admitir la entrada a personal visitante debidamente controlado.

	Este tipo de zona precisa: - Un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas. - Un sistema de control de entrada que sólo permite el acceso sin escolta a aquellas personas con habilitación de seguridad y con autorización específica para acceder a la zona. A todas las demás personas se les proporcionará escolta o controles equivalentes a fin de evitar el acceso no autorizado a la información clasificada y la entrada, no controlada, a las zonas sujetas a inspección de seguridad técnica.
Confidencialidad	Cualidad o condición de la información que asegura que ésta no es conocida por individuos, entidades o procesos no autorizados.
Concepto de Operación	Declaración expresa que se realiza sobre el objeto o función de un Sistema o de una interconexión, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación…), las entradas y salidas de información y las amenazas a las que estará sometido. Es responsabilidad de la Autoridad Operativa del Sistema de las Tecnologías de la Información (AOSTIC).
Disponibilidad	Cualidad o condición de la información que permite, a las personas o procesos autorizados, acceder a ella cuando se requiera de acuerdo a los requisitos establecidos.
Gestión de la Seguridad	Proceso que asegura la confidencialidad, integridad y disponibilidad de los activos de una organización, información, datos y servicios de TI.
Gestión del riesgo	Proceso, que se basa en los resultados de la evaluación del riesgo, consistente en seleccionar las salvaguardas.
Habilitación Personal de Seguridad (HPS)	Documento que acredita que una persona determinada cumple los criterios necesarios para acceder a Información Clasificada. Esta habilitación la concede, deniega o retira la Autoridad Delegada.
Habilitación de Seguridad de Empresa (HSEM)	La determinación positiva por la que la Autoridad Nacional reconoce formalmente la capacidad y fiabilidad de un contratista para generar y acceder a Información Clasificada hasta un determinado grado, sin que pueda

	manejarla o almacenarla en sus propias instalaciones
Habilitación de Seguridad de Establecimiento (HSES)	La determinación positiva por la que la Autoridad Nacional reconoce formalmente la capacidad y fiabilidad de un contratista poseedor de una HSEM para manejar y almacenar Información Clasificada hasta un determinado grado en aquellas de sus propias instalaciones habilitadas al efecto
Impacto	Consecuencia sobre un activo de la materialización de una amenaza.
Integridad	Cualidad o condición de la información que garantiza que no ha sido modificada por personas no autorizadas.
Interconexión	Se produce una interconexión entre Sistemas, cuando existe una conexión y se habilitan flujos de información entre los mismos, con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes Autoridades Operativas de los Sistemas de las Tecnologías de la Información y las Comunicaciones (AOSTIC) o una combinación de las anteriores.
Oficina Nacional de Seguridad (ONS)	Órgano de trabajo del Director del CNI para auxiliarle en el cumplimiento de sus cometidos relacionados con la protección de la Información Clasificada. Tiene por misión fundamental la de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de Tratados o Acuerdos internacionales suscritos por España (artículo 4 f de la Ley 11/2002, de 6 de mayo, Reguladora del CNI).
Política de Seguridad de las TIC (Política STIC)	Conjunto formalizado en un documento aplicable, de elementos estratégicos, directivas, procedimientos, códigos de conducta, normas organizacionales y técnicas, que tiene por objetivo la protección del (o de los) sistema(s) de información del organismo.
Procedimientos Operativos de Seguridad (POS).	Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. En su caso será la descripción de la aplicación de la DRS correspondiente
Resiliencia	Es la capacidad que tiene un Sistema de soportar y recuperarse ante incidentes de seguridad.
Riesgo	Es la posibilidad de que se materialice una amenaza

	sobre un activo, ocasionando una pérdida en la Organización.
Riesgo residual	Es el riesgo resultante de la aplicación de contramedidas y, por tanto, constituye el riesgo a asumir.
Salvaguardas (contramedidas)	Procedimiento o mecanismo tecnológico que reduce el riesgo.
Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC)	Protección de la información almacenada, procesada o transmitida, por Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.
Seguridad de las Emanaciones o Seguridad TEMPEST	Conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.
Sistema de las Tecnologías de la Información y las Comunicaciones (Sistema)	Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única Autoridad.
TEMPEST	Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
Vulnerabilidad	Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.
ZONING	Término que hace referencia a la clasificación de zona de los locales y plataformas donde se ubican equipos TEMPEST.

AAS	Autoridad de Acreditación de Seguridad
AAS-D	Autoridad de Acreditación de Seguridad Delegada
ACC	Autoridad de Certificación Criptológica

ACSTI	Autoridad de Certificación de la Seguridad de las Tecnologías de la Información
ACT	Autoridad De Certificación de la Seguridad de las Emanaciones TEMPEST
AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones
CCN	Centro Criptológico Nacional
CD	Compact Disk
CERT	Computer Emergency Response Team
CIS	Communications and Information Systems
CNI	Centro Nacional de Inteligencia
CO	Concepto de Operación
CTS	COSMIC TOP SECRET
DVD	Digital Video Disk
	Digital Versatile Disk
ENS	Esquema Nacional de Seguridad
EUSI	EU Sensitive Information
IEC	International Electrotechnical Commission
ISO	International Organization for Standarization
ITSEC	Information Technology Security Evaluation Criteria
LSO	Ley de Secretos Oficiales
MAGERIT	Metodología de Análisis y Gestión De Riesgos de los Sistemas de Información
NC	NATO CONFIDENCIAL
NR	NATO RESTRICTED
NS	Normas de Seguridad
	NATO SECRET
NU	NATO UNCLASSIFIED
ONS	Oficina Nacional de Seguridad
OPRE	Orden de Presidencia
OTAN	Organización del Tratado del Atlántico Norte
RD	Real Decreto
Sistema	Sistema de las Tecnologías de la Información y las

	Comunicaciones
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea
USB	Universal Serial Bus