NORMAS

Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.

La evolución de la sociedad y las tecnologías de la información requiere a su vez, la actualización, modernización y adaptación al nuevo entorno tecnológico de la normativa en materia de seguridad de la información.

En el año 1968 se aprueba la primera norma del conjunto normativo actualmente en vigor y vinculante al Ministerio, sobre seguridad de la información, la Ley 9/1968, de 5 de abril, modificada por la Ley 48/1978, de 7 de octubre sobre secretos oficiales.

Esta Ley se promulgó con la intención de cubrir una laguna en nuestra legislación, que, al contrario de lo que ocurría en los estados caracterizados por la mayor libertad de información, no preveía una regulación de las medidas protectoras de los secretos oficiales. Para remediar esta situación, la Ley estableció un conjunto de medidas para evitar que transcendiese lo que debía permanecer secreto, además, de manera implícita, introducía los conceptos de confidencialidad de la información y necesidad de conocer.

Al siguiente año, la Ley fue desarrollada mediante el Decreto 242/1969, de 20 de febrero, el cual especificaba la necesidad de una unificación normativa internacional que aconsejaba utilizar las enseñanzas del derecho comparado, en especial el de las naciones industrializadas con mayor experiencia en la información tecnológica y reconocía la particularidad de las Fuerzas Armadas permitiendo a los departamentos ministeriales correspondientes la elaboración de normas específicas de régimen interior para el mejor cumplimiento de la alta misión que, por precepto legal, tiene encomendada.

Esta especificidad que el Decreto establecía condujo al desarrollo particular para el Ministerio de Defensa de la Ley y el Decreto sobre secretos oficiales, promulgándose la Orden Ministerial Comunicada 1/1982, de 25 de enero, por la que se aprueban las normas para la protección de la documentación y material clasificado. Estas normas introducían dos nuevos grados de protección bajo la denominación de materias objeto de reserva interna.

En ese mismo año se aprobó la Orden Ministerial Comunicada 12/1982, de 21 de octubre, del manual de seguridad industrial de las Fuerzas Armadas debido a la necesidad de regular las relaciones entre el Ministerio y las empresas, cuya colaboración cada vez más estrecha aumentaba la necesidad de compartir información clasificada.

Los avances en la tecnología de la información, han propiciado un proceso de cambio desde el período 1968-1982, pasando de un entorno de acceso a la información fundamentalmente selectivo y minoritario y en el que el papel era el formato preponderante tanto en almacenamiento como en transporte, al momento actual en donde el entorno de acceso a la información se caracteriza por su inmediatez y universalidad, siendo el formato electrónico el predominante.

Este nuevo entorno trae como consecuencia unos nuevos criterios de seguridad de la información, en donde se considera que para alcanzar un grado razonable de protección, además de preservar la confidencialidad de la información clasificada, se convierte en primordial, en la mayoría de los casos, preservar la integridad y la disponibilidad de la información, esté o no clasificada.

Con el objeto de regular las necesidades emergentes relativas a la protección de información, y con el fondo común de las tecnologías y de su evolución, durante los últimos años se han ido promulgando normas vinculantes al Ministerio, algunas veces por la necesidad de incluir en la jurisprudencia española directivas europeas y otras por iniciativa nacional.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, animada por la idea de implantar mecanismos cautelares que previniesen las violaciones de la privacidad resultantes del tratamiento de la información, limitaba el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal. Esta Ley se desarrollaría mediante el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal el cual determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

La citada Ley Orgánica 5/1992 sería actualizada por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, cuyo objeto es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas. El citado Real Decreto Ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Posteriormente, la Ley 59/2003, de 19 de diciembre, de firma electrónica, actualizaba a la vez el marco establecido en el Real Decreto–Ley 14/1999 mediante la incorporación de las modificaciones que aconsejaba la experiencia acumulada desde su entrada en vigor.

Finalmente, se promulga la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y posteriormente el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, mediante los cuales, se encomienda al CNI, entre otras cosas, 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 y velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

Consecuentemente, en el Ministerio de Defensa se ha ido desarrollando una labor de actualización y modernización, al nuevo entorno tecnológico, de su normativa específica. Así, se han promulgado la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el manual de protección de materias clasificadas del Ministerio de Defensa en poder de las empresas; la Orden Ministerial Comunicada 44/2001, por la que se aprueba la normativa para la aplicación del manual de protección de materias clasificadas del Ministerio de Defensa en poder de las empresas y la Orden Ministerial 81/2001, de 20 de

abril, por la que se aprueban las normas de protección de contratos del Ministerio de Defensa, mediante las cuales se actualiza la normativa referente a seguridad industrial; la Orden DEF/315/2002, de 14 de febrero, por la que se aprueba el plan director de sistemas de información y telecomunicaciones y en la que se establecen cometidos y responsabilidades en materia de seguridad de la información en los sistemas de información y telecomunicaciones y la Orden Ministerial 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 y en la que se establece de manera explícita los conceptos de confidencialidad, integridad y disponibilidad.

A la normativa de Defensa anteriormente citada, hay que añadir la específica del Estado Mayor de la Defensa y de los Ejércitos, así como la derivada de la integración de España en foros y organizaciones internacionales, principalmente en la OTAN y en la Unión Europea sobre protección de la información, clasificada y no clasificada, de la organización.

De todo lo anteriormente expuesto, se deduce que, en la actualidad, la situación normativa de seguridad de la información en el Ministerio de Defensa es compleja, debido a la gran cantidad de normativa existente, a las diferentes procedencias, a la coexistencia de normativa obsoleta con normativa moderna y a la falta de un tronco común que facilite el desarrollo normativo coordinado.

La experiencia acumulada desde la entrada en vigor de la normativa citada, el deseo de conseguir una adecuada racionalización de la misma y la necesidad de afrontar el proceso de modernización, consecuencia de la evolución de las tecnologías de la información, hacen necesario establecer la política de seguridad de la información del Ministerio de Defensa como documento único del cual deberá emanar toda norma interna en materia de seguridad de la información del Ministerio, facilitando así, la necesaria coordinación en el desarrollo normativo posterior y de este modo alcanzar un conjunto normativo equilibrado, completo y con criterios unificados.

En su virtud, de acuerdo con lo dispuesto en el artículo 12 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado,

DISPONGO:

Primero. Aprobación.

Se aprueba la política de Seguridad de la Información del Ministerio de Defensa, cuyo texto se inserta a continuación.

Segundo. Dirección de la seguridad de la información del Ministerio de Defensa.

Se designa como Director de Seguridad de la Información del Ministerio de Defensa al Secretario de Estado de Defensa, y se le encomienda, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas.

Tercero. Protección de materias clasificadas.

Corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia (CNI) el velar por el cumplimiento de la normativa relativa a la protección de materias clasificadas.

Cuarto. Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

Se establece el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa, como órgano de coordinación de la seguridad de la información del Ministerio, cuya composición es la siguiente:

Presidente: el Secretario de Estado de Defensa.

Vocales:

El Secretario General del CNI.
El Jefe de Estado Mayor Conjunto de la Defensa.
El Segundo Jefe de Estado Mayor del Ejército.
El Segundo Jefe de Estado Mayor de la Armada.
El Segundo Jefe de Estado Mayor del Aire.
El Secretario General Técnico.
El Director General de Política de Defensa.
El Director General de Armamento y Material.
El Director General de Personal.
El Director General de Infraestructura.

Secretario: el Inspector General del Plan Director de Sistemas de Información y Telecomunicaciones.

Disposición adicional primera. Servicio de Protección de Materias Clasificadas del CNI.

El Centro Nacional de Inteligencia, por las especiales características de su misión y cometidos, creará su propio Servicio de Protección de Materias Clasificadas bajo la dependencia directa de su Secretario General.

Disposición adicional segunda. Información de la jurisdicción militar.

La información que pueda figurar en los distintos procedimientos de la jurisdicción militar se regirá exclusivamente por su normativa específica.

Disposición adicional tercera. Seguridad de la información procedente de organismos ajenos al Ministerio de Defensa.

La información suministrada al Ministerio de Defensa por organizaciones internacionales o países extranjeros tendrá el tratamiento y limitaciones concretas que impongan los convenios bilaterales o multilaterales en los que España sea parte y a cuyo amparo haya sido facilitada dicha información.

La información suministrada al Ministerio de Defensa por otros órganos de las Administraciones Públicas, deberá protegerse de acuerdo con la normativa aplicable.

Disposición adicional cuarta. Seguridad de la información clasificada entregada a organismos ajenos al Ministerio de Defensa.

La entrega de información clasificada del Ministerio de Defensa a organizaciones internacionales o países extranjeros se realizará al amparo de los convenios bilaterales o multilaterales en los que España sea parte.

La entrega de información clasificada del Ministerio de Defensa a organismos de la Administraciones Públicas se realizará de acuerdo con la normativa aplicable.

Disposición transitoria única. Vigencia temporal de las disposiciones derogadas.

En tanto no se publiquen las normas de «Aplicación de la Política de Seguridad de la Información del Ministerio», «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», y «Seguridad de la Información en las Instalaciones», correspondientes al desarrollo normativo de segundo nivel de la política, se mantendrá la vigencia de las disposiciones derogadas en la disposición derogatoria única.

Disposición derogatoria única. Derogación normativa.

Quedan derogadas la Orden Ministerial Comunicada 1/1982, de 25 de enero, por la que se aprueban las normas para la protección de la documentación y material clasificado, y la Orden Ministerial 76/2002, de 18 de abril, por la que se aprueba la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.

Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido por la presente Orden Ministerial y documento que aprueba.

Disposición final primera. Facultad de desarrollo.

Se faculta al Secretario de Estado de Defensa a dictar las disposiciones oportunas, en el ámbito de sus competencias, para el desarrollo y ejecución de la presente Orden Ministerial.

Disposición final segunda. Entrada en vigor.

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 19 de mayo de 2006.

JOSE ANTONIO ALONSO SUAREZ

POLITICA DE SEGURIDAD DE LA INFORMACION DEL MINISTERIO DE DEFENSA

Primero. Objeto.

El objeto de esta política es alcanzar la protección adecuada, proporcionada y razonable de la Información del Ministerio de Defensa, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad.

Segundo. Definiciones.

A los efectos de la presente política, se considera:

Amenaza: evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales.

Auditoría: revisión e inspección independiente de las medidas de seguridad implantadas para valorar su idoneidad y eficacia, verificando y asegurando su conformidad con las políticas y los procedimientos establecidos y recomendando los cambios necesarios.

Confidencialidad: requisito básico de seguridad que garantiza que sólo las personas, entidades o procesos autorizados pueden acceder a la información.

Disponibilidad: requisito básico de seguridad que garantiza que se puede acceder a la información y a los recursos o servicios que la manejan, conforme a las especificaciones de los mismos.

Documento: cualquier soporte portátil con capacidad para contener información.

Habilitación personal de seguridad: certificación que establece que a la persona que la posee se le puede confiar información clasificada de un determinado grado y que está instruida en materia de seguridad de la información.

Información: todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

Información del Ministerio de Defensa: aquella que es generada de manera oficial por personal del departamento o por entidades ajenas que desarrollan trabajos para éste según los acuerdos correspondientes; y toda aquella que no se encuentre recogida en acuerdos nacionales o internacionales y que de forma específica se deposita en el Ministerio de Defensa para su tratamiento oficial.

Integridad: requisito básico de seguridad que garantiza que la información no pueda ser o no ha sido modificada o alterada por personas, entidades o procesos no autorizados.

Manejar información: elaborar, presentar, almacenar, procesar, transportar o destruir información.

Necesidad de conocer: determinación positiva por la que se confirma que un posible destinatario requiere el acceso a una determinada información para desempeñar servicios, tareas o cometidos oficiales.

Riesgo: la probabilidad o potencialidad de que una vulnerabilidad sea aprovechada por una amenaza, comprometiendo la confidencialidad, integridad y/o disponibilidad.

Sistema de Información y Telecomunicaciones: conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita manejar información.

Vulnerabilidad: debilidad, atributo o pérdida de control que permitiría o facilitaría la materialización de una amenaza.

Tercero. Alcance.

Esta política es de aplicación a la INFORMACION DEL MINISTERIO DE DEFENSA, con independencia del atributo que le afecte, la forma en la que se presente o el lugar en el que se encuentre.

Cualquier norma interna que trate algún aspecto particular de la seguridad de la información del Ministerio debe emanar de esta política.

Cuarto. Información.

La información es un recurso de carácter estratégico para el Ministerio y, por tanto, debe garantizarse su protección. Esto no quiere decir que la protección de la información sea un fin en sí mismo, sino que debe ser protegida en la medida que el cumplimiento de la misión del Ministerio depende de ella.

La información es un concepto abstracto e intangible que se elabora, presenta, almacena, procesa, transporta o destruye (de ahora en adelante, maneja) mediante elementos tangibles. Estos elementos son: las personas, los documentos, los sistemas de información y telecomunicaciones, las instalaciones y las empresas. De acuerdo con ello, la protección de la información se realizará mediante la aplicación y supervisión de medidas de seguridad dirigidas a las personas, los documentos, los sistemas de información y telecomunicaciones, las instalaciones y las empresas.

Quinto. Seguridad de la información.

1. Conceptos generales.

La seguridad de la información del Ministerio se establece sobre la base de:

a. Visión estratégica unitaria.

b. Dirección única, que establezca normas y pautas comunes.

c. Agrupamiento de todos los recursos en entidades homogéneas que precisen de medidas de protección similares, de tal manera que se puedan delimitar responsabilidades y lograr una especialización de personal, normativa y recursos.

d. Establecimiento de un conjunto equilibrado y completo de medidas específicas de protección orientadas a alcanzar un grado de protección similar en cada grupo.

e. Acción coordinada e integrada de las medidas dimanantes de la política de seguridad aplicada a cada uno de dichos grupos.

f. Armonización con otros departamentos ministeriales u organizaciones nacionales e internacionales.

g. Un esquema funcional adecuado, que permita la dirección, ejecución, apoyo, y auditoría de las medidas de protección.

2. Principios básicos de la seguridad de la información.

Los principios básicos son directrices de obligado cumplimiento que hay que tener siempre presentes en cualquier actividad relacionada con la seguridad de la información. Se establecen los siguientes:

a. La seguridad de la información es responsabilidad de todos los miembros del Ministerio, los cuales deberán estar adecuadamente formados y concienciados para el satisfactorio cumplimiento de sus responsabilidades.

b. La seguridad de la información debe estar coordinada e integrada con el resto de la seguridad del Ministerio, con el fin de conformar un todo coherente y eficaz.

c. La seguridad de la información debe ir encaminada a preservar los requisitos básicos de seguridad durante todo el ciclo de vida de la información, en cualquier medio o formato que se emplee y en cualquier lugar donde se encuentre, dentro o fuera del Ministerio.

d. La seguridad de la información debe ser periódicamente evaluada.

e. Las medidas de protección deben aplicarse en proporción a los daños que produciría la pérdida de alguno de los requisitos básicos de seguridad.

f. Las medidas y procedimientos que se implanten para la protección de la información deben acatar lo establecido en la legislación vigente vinculante al Ministerio, tanto a nivel nacional como internacional.

Sexto. Clasificación de la información.

1. Conceptos generales.

Se consideran «materias clasificadas» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado. Estas «materias clasificadas» serán exclusivamente las que, de acuerdo con la Ley 9/68, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre secretos oficiales, se definen posteriormente como SECRETO y RESERVADO en el apartado 2, «Grados de clasificación».

Se consideran «materias objeto de reserva interna» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pudiera afectar a la seguridad del Ministerio de Defensa, amenazar sus intereses o dificultar el cumplimiento de su misión. Estas materias son las que posteriormente se definen como CONFIDENCIAL y DIFUSIÓN LIMITADA en el apartado 2, «Grados de clasificación».

A efectos de la presente política, las «materias clasificadas» y las «materias objeto de reserva interna» quedan englobadas en el concepto general de «información clasificada».

La clasificación es el acto formal mediante el cual, a una determinada información, se le asigna un grado en atención a las medidas de seguridad que requiere frente a la pérdida de confidencialidad. Se emplea para poner en conocimiento del receptor o depositario de la información la necesidad de protegerla y el grado de protección requerido.

La reclasificación es la asignación de un nuevo grado de clasificación a una información clasificada.

La desclasificación es el acto formal mediante el cual se anula de manera expresa la clasificación de una información. Este acto formal no será necesario si la autoridad que otorgó la clasificación señaló un plazo de duración de ésta, o las circunstancias que lo condicionen.

La propuesta de clasificación es el documento por el que se somete, a la autoridad facultada para clasificar, la propuesta de asignación de grado de clasificación a informaciones individuales o agrupadas en un conjunto, así como su vigencia, de acuerdo con el procedimiento de reclasificación que regulará la variación temporal del grado asignado.

La diligencia de clasificación es el documento por el que la autoridad facultada aprueba la propuesta de clasificación de la información.

La guía de clasificación es el documento que recoge los datos relevantes de la información clasificada (los grados de clasificación asignados a la misma, las vigencias de las clasificaciones, las autoridades facultadas que la han clasificado, etc.), y que sirve de referencia para el marcado de los documentos.

2. Grados de clasificación.

SECRETO (S): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello pudiera dar lugar a riesgos o perjuicios de la seguridad y defensa del Estado.

RESERVADO (R): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a la seguridad y defensa del Estado.

CONFIDENCIAL (C): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.

DIFUSION LIMITADA (DL): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

3. Autoridades y órganos facultados para clasificar.

La facultad para clasificar de SECRETO o RESERVADO corresponde a las autoridades y órganos establecidos en el artículo cuatro de la Ley 9/1968, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre sobre secretos oficiales, no pudiendo ser transferida ni delegada.

La facultad para clasificar de CONFIDENCIAL o DIFUSION LIMITADA, corresponde, en el ámbito de su competencia, a las siguientes autoridades:

Ministro de Defensa.
Jefe del Estado Mayor de la Defensa.
Secretario de Estado de Defensa.
Secretario de Estado Director del CNI.
Subsecretario de Defensa.
Secretario General de Política de Defensa.
Jefe del Estado Mayor del Ejército.
Jefe del Estado Mayor de la Armada.
Jefe del Estado Mayor del Ejército del Aire.

Estas autoridades pueden delegar oficialmente dicha atribución.

4. Información no clasificada.

Dependiendo de su ámbito de distribución, podrá ser:

Información de USO OFICIAL: información cuya distribución esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo.

Información de USO PUBLICO: información cuya distribución NO esté limitada.

Séptimo. Areas de la seguridad de la información.

La seguridad de la información se divide en áreas, atendiendo al elemento tangible que hace uso de ella, ya sea elaborándola, presentándola, almacenándola, procesándola, transportándola o destruyéndola. De este modo tendremos:

Seguridad de la Información en las Personas.
Seguridad de la Información en los Documentos.
Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.
Seguridad de la Información en las Instalaciones.
Seguridad de la Información en poder de las Empresas.

1. Seguridad de la Información en las Personas (SEGINFOPER).

Entiende de los requisitos exigidos a las personas con el objeto de garantizar razonablemente el correcto uso de la información por éstas.

Se podrá autorizar el acceso a información clasificada de grado CONFIDENCIAL o superior siempre y cuando, en la persona, concurran las dos condiciones siguientes:

Disponer de habilitación personal de seguridad con el grado correspondiente, y

Tener necesidad de conocer dicha información para el desempeño de sus cometidos oficiales.

Para el acceso a información DIFUSION LIMITADA o inferior, no se requerirá habilitación personal de seguridad específica. Se permitirá el acceso cuando la persona sea conocedora de sus responsabilidades, y tenga necesidad de conocer dicha información para el desempeño de sus cometidos oficiales.

2. Seguridad de la Información en los Documentos (SEGINFODOC).

Entiende de las medidas de protección aplicables a los documentos durante todo su ciclo de vida, es decir, durante su elaboración, almacenamiento, transporte o destrucción, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que contienen.

Todo documento que contenga información clasificada llevará, de forma clara y visible, un distintivo, marca, sello o etiqueta (de ahora en adelante marca) que indique el grado de clasificación que se le ha asignado. Será preciso adaptar la correspondiente marca a las características físicas de los soportes, con objeto de que pueda reconocerse con toda claridad.

El responsable de aplicar la marca correspondiente, siguiendo los criterios de la guía de clasificación de la información, será el generador del documento.

Se podrán habilitar marcas especiales que especifiquen el ámbito abarcado, una distribución específica basada en el principio de la necesidad de conocer, o una categoría especial que precise de requisitos de seguridad suplementarios.

La aplicación de marcas para establecer una distribución específica basada en el principio de la necesidad de conocer deberá ser cuidadosa y no limitar la necesidad de compartir esa información.

3. Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT).

Entiende de las medidas de protección aplicables en los sistemas de información y telecomunicaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que manejan.

Previamente a que un sistema comience a manejar información del Ministerio deberá estar autorizado por la autoridad facultada para ello, de acuerdo con el desarrollo normativo de la presente política.

La autorización otorgada a un sistema le permite manejar información del Ministerio en unas determinadas condiciones de confidencialidad, integridad y disponibilidad. Dicha autorización se ajustará al procedimiento que para tal fin apruebe el Director de Seguridad de la Información del Ministerio.

4. Seguridad de la Información en las Instalaciones (SEGINFOINS).

Entiende de las medidas de protección aplicables a las instalaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información.

Previamente a que en una instalación se maneje información clasificada de grado CONFIDENCIAL o superior, deberá estar autorizada por la autoridad facultada para ello de acuerdo al desarrollo normativo de la presente política.

La autorización otorgada a una instalación permite albergar recursos o manejar información del Ministerio en su interior en unas determinadas condiciones de confidencialidad, integridad y disponibilidad. Dicha autorización se ajustará al procedimiento que para tal fin elabore y apruebe el Director de Seguridad de la Información del Ministerio.

5. Seguridad de la Información en poder de las Empresas (SEGINFOEMP).

Entiende de las medidas de protección dirigidas a las empresas y aplicables por ellas, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Ministerio manejada por éstas, como consecuencia de su participación en programas, proyectos o contratos del Ministerio.

Octavo. Desarrollo normativo.

Se desarrollará el correspondiente cuerpo normativo sobre seguridad de la información, enmarcando cada conjunto de normas en distintos niveles por amplitud del aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

Cada norma de un nivel determinado debe fundamentarse en norma o normas de nivel superior.

1. Primer nivel normativo.

Una única norma que establece principios generales abarcando todo el ámbito de la seguridad de la información. Está constituido por el presente documento de «Política de Seguridad de la Información del Ministerio de Defensa».

Su ámbito de aplicación es todo el departamento.

2. Segundo nivel normativo.

Conjunto de normas que desarrollan y detallan la política, abarcando un área, subárea o aspecto determinado de la seguridad de la información.

Su ámbito de aplicación será todo el departamento y la autoridad responsable de su aprobación es el Director de Seguridad de la Información del Ministerio.

El desarrollo normativo de segundo nivel de la seguridad de la información incluirá, al menos, las siguientes normas:

Aplicación de la Política de Seguridad de la Información del Ministerio.

Seguridad de la Información en las Personas.

Seguridad de la Información en los Documentos.

Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.

Seguridad de la Información en las Instalaciones.

Seguridad de la Información en poder de las Empresas: recogido en la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el manual de protección de las materias clasificadas del Ministerio de Defensa en poder de las empresas, la Orden Ministerial Comunicada 44/2001, por la que se aprueba la normativa para la aplicación del citado manual, y la Orden Ministerial 81/2001, de 20 de abril, por la que se aprueban las normas de protección de contratos del Ministerio de Defensa.

3. Tercer nivel normativo.

Conjunto de normas que desarrollan y detallan la normativa de nivel 2.

Está constituido por:

Normas de carácter eminentemente técnico: directrices en las que predominan las disposiciones técnicas o explicativas, para el cumplimiento de uno o varios servicios o aspectos de seguridad.

Normas de carácter eminentemente procedimental: directrices generales que se deben seguir o a las que se deben ajustar las conductas, tareas o actividades de las personas y organizaciones en relación con la protección de la información.

Dependiendo del aspecto tratado, su aplicación podrá ser a todo el departamento, un ámbito específico o un sistema determinado.

La responsabilidad de la aprobación de las normas de este nivel dependerá de su ámbito de aplicación.