

I. — DISPOSICIONES GENERALES

NORMAS

Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos (SEGINFODOC).

La Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa, tiene como objeto alcanzar la protección adecuada, proporcionada y razonable de la información del Ministerio de Defensa.

Para alcanzar dicho objetivo, la citada Orden Ministerial 76/2006, de 19 de mayo, establece unos principios básicos y unos criterios estratégicos comunes a todos los ámbitos del Departamento, y el desarrollo de un cuerpo normativo sobre Seguridad de la Información, enmarcando cada conjunto de normas en distintos niveles por la amplitud del aspecto tratado, ámbito de aplicación y obligatoriedad de cumplimiento.

El primer nivel de desarrollo se corresponde con una única norma que establece principios generales que abarca todo el ámbito de la Seguridad de la Información, y está constituido por la Política de Seguridad de la Información del Ministerio de Defensa.

El segundo nivel es un conjunto de normas que desarrollan y detallan la Política, abarcando un área, sub-área o aspecto determinado de la Seguridad de la Información, siendo su ámbito de aplicación todo el Departamento, y al que corresponde el presente documento.

Las normas para la aplicación de la Política de Seguridad de la información se recogen en la Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa. En esta instrucción se designa al Director General de Infraestructura como responsable de las Áreas de Seguridad de la Información en las Personas, en los Documentos, en los Sistemas de Información y Telecomunicaciones (SIT) y en las Instalaciones, atribuyéndole funciones corporativas en estas materias.

Las presentes normas de Seguridad de la Información en los Documentos establecen los requisitos exigidos en relación con los documentos para garantizar razonablemente el correcto manejo de la información contenida preservando su confidencialidad, integridad y disponibilidad.

Se establece por una parte, las medidas de seguridad a aplicar en los documentos que contienen información del Ministerio de Defensa en función de sus características físicas, y del tipo y grado de clasificación de la información a manejar, y por otro, se establece la estructura del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa.

El término documento engloba cualquier soporte portátil con capacidad para almacenar información, tal y como se recoge en la Orden Ministerial 76/2006, de 19 de mayo. Por ello, estas normas establecen los requisitos a aplicar a estos soportes portátiles, sea cual sea su naturaleza: soporte papel (como resultado de la materialización de la información contenida en un SIT o equivalente, mediante su impresión), o soporte informático (mediante su extracción a un dispositivo con capacidad de almacenamiento). Así mismo, estos requisitos deberán aplicarse durante todo su ciclo de vida, es decir, desde que se elabora o crea el documento hasta su destrucción, sin perjuicio de deber cumplir con otra regulación que le sea de aplicación, como por ejemplo, la relativa a la conservación de un documento en el Sistema Archivístico de la Defensa.

Los documentos electrónicos durante su elaboración, y almacenamiento y borrado en un SIT, serán regulados por lo dispuesto en las Normas de Seguridad de la información en los Sistemas de Información y Telecomunicaciones. Sin perjuicio de que le sea de aplicación lo dispuesto en estas normas cuando sean almacenados en un documento.

Se desarrolla también en estas normas, la estructura del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa que se compone de un Servicio Central Protección de Materias Clasificadas en el Nivel Corporativo, de los Servicios Generales de Protección de Materias Clasificadas y de los Servicios Locales de Protección de Materias Clasificadas en los ámbitos del Nivel Específico, dando así cumplimiento a los cometidos

que en esta materia se le encomiendan al Director de Seguridad de la Información en el apartado segundo de la Orden Ministerial 76/2006.

La disposición final primera de la Orden Ministerial 76/2006, de 19 de mayo, concede al Secretario de Estado de Defensa facultades para dictar disposiciones de desarrollo y ejecución de dicha orden ministerial.

En su virtud,

DISPONGO:

Artículo único. *Aprobación de las Normas de Seguridad de la Información en los Documentos del Ministerio de Defensa.*

Se aprueban las Normas de Seguridad de la Información en los Documentos del Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición final primera. *Desarrollo normativo.*

El desarrollo normativo de la Seguridad de la Información en los Documentos deberá cubrir, al menos, los siguientes aspectos:

En el Nivel Corporativo:

- procedimiento para la apertura, modificación y cierre de un Órgano de Control de la estructura del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa.
- procedimiento para el marcado de documentos.
- procedimiento para la destrucción de documentos.
- procedimiento para el transporte de documentos del Ministerio de Defensa.
- procedimiento de notificación y respuesta ante incidentes de seguridad en los documentos.
- procedimiento para la definición de un sistema de código identificativo para la gestión de los documentos clasificados.

En el Nivel Específico, cuando corresponda:

- procedimiento para la gestión de copias de trabajo.
- procedimiento para la gestión de mensajes clasificados.

Disposición final segunda. *Entrada en vigor.*

La presente instrucción entrará en vigor a los nueve meses desde su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 24 de junio 2013.—El Secretario de Estado de Defensa, Pedro Argüelles Salaverría.

Normas de seguridad de la información en los documentos del Ministerio de Defensa

ÍNDICE

- Título Preliminar: Disposiciones generales (Artículos 1 al 3).
- Título I: Seguridad de la Información en los Documentos
- Capítulo I. Principios generales (Artículos 4 al 6).
 - Capítulo II. Elaboración de documentos (Artículo 7).
 - Capítulo III. Marcado de documentos (Artículos 8 al 13).
 - Capítulo IV. Custodia y uso de documentos (Artículos 14 al 17).
 - Capítulo V. Almacenamiento de documentos (Artículos 18 al 20).
 - Capítulo VI. Copia, traducción y extracto de documentos (Artículos 21 al 26).
 - Capítulo VII. Directrices generales del transporte de documentos (Artículo 27).
 - Capítulo VIII. Transporte de documentos no clasificados (Artículo 28).
 - Capítulo IX. Transporte de documentos clasificados entre instalaciones del Ministerio de Defensa (Artículos 29 al 33).
 - Capítulo X. Transporte de documentos clasificados con destino ajeno al Ministerio de Defensa. (Artículos 34).
 - Capítulo XI. Borrado de información (Artículo 35).
 - Capítulo XII. Conservación o destrucción de documentos (Artículos 36 al 43).
 - Capítulo XIII. Registro, inventario y sistema de control de documentos clasificados (Artículos 44 al 45).
- Título II: Manejo de copias de trabajo y mensajes clasificados
- Capítulo I. Principios generales para el manejo de copias de trabajo y mensajes clasificados (Artículo 46).
 - Capítulo II. Copias de trabajo (Artículos 47 al 53).
 - Capítulo III. Mensajes clasificados (Artículos 54 al 59).
- Título III. Servicio de Protección de Materias Clasificadas del Ministerio de Defensa
- Capítulo I. Principios generales del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa (Artículos 60 al 62).
 - Capítulo II. Servicio Central de Protección de Materias Clasificadas del Ministerio de Defensa (Artículo 63).
 - Capítulo III. Servicio General de Protección de Materias Clasificadas del Ministerio de Defensa (Artículo 64).
 - Capítulo IV. Servicio Local de Protección de Materias Clasificadas del Ministerio de Defensa (Artículo 65).
- Título IV: Estructura funcional de la Seguridad de la Información en los Documentos
- Capítulo I. Nivel Corporativo de la Seguridad de la Información en los Documentos (Artículos 66 al 68).
 - Capítulo II. Nivel Específico de la Seguridad de la Información en los Documentos (Artículos 69 al 73).

TÍTULO PRELIMINAR

Disposiciones generalesArtículo 1. *Objeto.*

Estas normas tienen como objeto desarrollar la Política de Seguridad de la Información del Ministerio en la parte que afecta a los documentos. Para alcanzar dicho objetivo se establecen:

- a) Unas directrices comunes en materia de Seguridad de la Información en los Documentos en todo el ámbito del Ministerio, y
- b) la estructura funcional necesaria para su dirección, ejecución y control, incluyendo el Servicio de Protección de Materias Clasificadas del Ministerio de Defensa.

Artículo 2. *Ámbito de Aplicación.*

1. Afecta a todo el Departamento, y se aplicará a todos los documentos que contengan información del Ministerio de Defensa, entendiéndose por documento el concepto definido en la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa.

2. Las medidas de protección que deban acometerse para el tratamiento de la información de los documentos electrónicos en los Sistemas de Información y Telecomunicaciones quedan fuera de estas y serán recogidas en las normas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones. No obstante, cuando estos documentos electrónicos sean almacenados o archivados en un soporte portátil deberán atender lo dispuesto en estas normas.

3. Por la especial sensibilidad del Material de Cifra, éste requerirá la aplicación de medidas adicionales de seguridad más exigentes y podrá circular por canales específicos de distribución y custodia. En este sentido, estos documentos estarán sujetos a requisitos adicionales establecidos por los correspondientes Órganos de Control y de Distribución del Material de Cifra.

4. Los documentos de las empresas que contengan información del Ministerio de Defensa se regulan por el desarrollo normativo del Área de Seguridad de la Información en poder de las Empresas, según se establece en la Política de Seguridad de la Información.

5. Cualquier otra normativa interna que trate algún aspecto de la Seguridad de la Información del Ministerio en los documentos deberá emanar de la Política de la Seguridad de la Información, de sus normas de Aplicación y de lo establecido en estas normas.

Artículo 3. *Definiciones.*

A los efectos de estas normas se considera:

— Borrado de información: Acto por el cual se elimina la información que contiene un documento pero que no conlleva la destrucción del soporte portátil que la contiene.

— Cesión de información: Entrega de información que está bajo la custodia del que la cede, a un tercero. Entendiéndose por tercero, en este contexto, cualquier persona, órgano, organismo, estado, etc. ajeno al Ministerio de Defensa.

— Conservación de un documento: Acto por el cual se remite al Sistema Archivístico de la Defensa un documento para su conservación.

— Copia de trabajo: documento especial procedente de la realización de la copia de un documento, cuya validez temporal se prevé limitada para la que se establecen condiciones especiales que permiten por parte del custodio su manejo y destrucción una vez finalizada su validez temporal.

— Custodio: Persona u órgano responsable de la custodia de un documento. El custodio es a la vez usuario del documento. Sin embargo el usuario no es custodio del documento. La responsabilidad sobre la custodia de un documento al que tiene acceso un usuario es del custodio, no del usuario.

— Documento: Cualquier soporte portátil (papel o informático) con capacidad para contener información.

— Documento clasificado: Se considera documento clasificado, aquel que contiene información clasificada de alguno de los grados de clasificación definidos en la Política de Seguridad de la Información del Ministerio de Defensa. El grado de clasificación del documento será el grado más elevado de la información que contenga.

— Documento electrónico: Información elaborada de forma electrónica, empleando para ello un Sistema de Información y Telecomunicaciones (SIT), que puede ser archivada o almacenada en un SIT, o en un documento.

— Elaborador: El elaborador del documento es la persona que materializa la información en un soporte portátil.

— Marca: Distintivo, sello o etiqueta que se incorpora a un documento para indicar alguna característica relativa a la tipología, manejo, clasificación, y en su caso el grado y la naturaleza de la información que contiene.

— Mensaje clasificado: Documento clasificado que debe ser comunicado por parte del organismo originador a uno o varios destinatarios (receptor del mensaje) a través de los Centros de Comunicaciones (CECOM), u otros medios similares, que contiene información, que debe ser conocida por el receptor con la urgencia indicada en la prelación del mensaje y cuya validez temporal se prevé limitada.

— Órgano de control: Término designado para referirse de manera general a cualquier órgano del Servicio Central de Protección de Materias Clasificadas (SCPMC), de los Servicios Generales de Protección de Materias Clasificadas (SGPMC) y de los Servicios Locales de Protección de Materias Clasificadas (SLPMC).

— Soporte informático: Dispositivo portátil de almacenamiento que requiere de un Sistema de Información y Telecomunicaciones (SIT) para el manejo de la información que contiene

— Usuario: Persona a la que el custodio de la información de un Documento le permite el acceso a la misma.

— Zonas de Acceso Restringido (ZAR), Área Clase I ó Área Clase II: Instalación, o parte de ella, autorizada para manejar información clasificada CONFIDENCIAL o superior, según lo dispuesto en la Instrucción 95/2011, de 16 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información en las Instalaciones. Zonas de Seguridad: Instalación, o parte de ella, especialmente constituida para permitir el manejo de la información clasificada, según lo dispuesto en la Instrucción 95/2011, de 16 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información en las Instalaciones.

TÍTULO I

Seguridad de la Información en los Documentos

CAPÍTULO I

Principios generales

Artículo 4. *Principios generales de la Seguridad de la Información en los Documentos.*

1. La seguridad de la información en los documentos entiende de la protección de la información contenida en cualquier soporte portátil con capacidad para contener información. El manejo de la información que contiene un documento, se llevará a cabo según el grado de protección requerido, que vendrá determinado por los requisitos de confidencialidad, integridad y disponibilidad de la información que contienen, durante todo el ciclo de vida del documento, es decir, desde que se elabora hasta su destrucción, incluyendo su posible conservación en el Sistema Archivístico de la Defensa.

2. Para la correcta aplicación de las medidas de seguridad de la información en los documentos, se deberá tener en cuenta además de los requisitos definidos en estas normas, todas aquellas medidas de seguridad derivadas de la regulación nacional e internacional y que le sean de aplicación a los documentos, cuando sea necesario.

3. La protección de la información de los documentos, deberá adecuarse a la característica física del soporte que la contiene, ya sea papel o soporte informático portátil.

4. Aquellos documentos cuya naturaleza no sea papel, ni soporte informático: fichas, microfilms, etc. deberán ser tratados aplicando las medidas de seguridad más asimilables a su naturaleza, según corresponda en cada caso, bien las medidas aplicables a papel, bien las de soporte informático.

Artículo 5. Requisitos de seguridad de los documentos clasificados.

1. Los documentos clasificados, a lo largo de todo su ciclo de vida, siempre estarán asignados a un responsable (órgano o persona) de su custodia.

2. En caso de que un usuario reciba directamente un documento clasificado CONFIDENCIAL o superior, que no haya circulado a través de los correspondientes Órganos de Control, deberá informar a su correspondiente Órgano de Control para que se proceda al debido registro, control y custodia del mismo.

3. Todo documento clasificado deberá ser convenientemente marcado, indicando el grado de clasificación que le corresponde. El elaborador del documento es el responsable de aplicar la marca correspondiente, siendo el Órgano de Control al que pertenezca el elaborador, el responsable de comprobar el marcado correcto en relación con la información contenida, debiendo proceder a aplicar la marca correcta, cuando sea necesario.

4. Cuando se elabore un documento que contenga información clasificada y no clasificada, con el fin de facilitar su manejo y protección, se deberá, siempre y cuando sea posible, agrupar coherentemente la información en partes diferenciadas dentro del mismo documento, permitiendo así distinguir claramente los distintos tipos de información.

5. Existen documentos clasificados que requieren tratamientos especiales debido a su temporalidad. Este es el caso de los mensajes clasificados y las copias de trabajo.

Artículo 6. Medidas de seguridad de la información en los documentos.

1. La Seguridad de la Información en los Documentos está orientada a la protección de la información mediante la aplicación de medidas de seguridad a éstos durante todo su ciclo de vida: elaboración, utilización, almacenamiento, procesamiento, reproducción, acceso, transporte y destrucción, incluyendo su conservación con fines archivísticos, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de la información que contienen.

2. Las medidas de seguridad de la información están orientadas a disuadir, prevenir y detectar los incidentes de seguridad de la información en los Documentos y, en caso de incidente, minimizar los daños y adoptar las medidas adecuadas para evitar su repetición.

3. Las medidas de seguridad de la información en los documentos deben coordinarse con las del resto de áreas: Seguridad de la Información en las Personas, Seguridad de la Información en las Instalaciones, Seguridad de la Información en los Sistemas de Información y Telecomunicaciones y Seguridad de la Información en poder de las Empresas.

CAPÍTULO II

Elaboración de documentos

Artículo 7. Elaboración y elaborador de los documentos.

1. Se entiende por elaboración de un documento la materialización de la información del Ministerio de Defensa en un soporte con capacidad de almacenamiento, principalmente papel o soporte informático portátil.

2. El elaborador del documento es la persona que materializa la información en el soporte portátil. Esta persona, no tiene porqué coincidir con la persona que elabora la información que contiene dicho documento. Esta información puede haberse elaborado mediante el uso de un Sistema de Información. El elaborador del documento, en este caso, extrae la información a un determinado soporte, momento en el cual, dicho soporte es considerado como un documento.

3. El elaborador del documento, o en su defecto, el Órgano de Control del que depende es responsable de su debido marcado, cuando corresponda, según el grado de clasificación otorgado, la naturaleza de la información, el soporte utilizado o la temporalidad del mismo.

CAPÍTULO III

Marcado de documentos*Artículo 8. Directrices generales de marcado.*

1. El marcado de un documento elaborado por agregación de varios, corresponderá como mínimo con el grado de clasificación que tenga el componente con clasificación más alta. Se deberá revisar el producto final por si le correspondiese un grado de clasificación diferente del que tienen sus componentes. De igual forma, si tuviera cualquier otra marca especial, se deberán conservar estas.

2. En el caso de que algún soporte por sus características físicas de tamaño, no pueda marcarse, se deberá incorporar una etiqueta en el soporte. Si esto tampoco fuese posible, se deberán aplicar los controles necesarios que garanticen la misma efectividad que el empleo de una marca.

Artículo 9. Marcado de documentos no clasificados.

1. Los documentos no clasificados del Ministerio de Defensa se clasificarán como documentos de USO OFICIAL o de USO PÚBLICO, según sea la información que manejen: información de USO OFICIAL o de USO PÚBLICO.

2. Todo documento no clasificado que contenga información del Ministerio de Defensa de USO OFICIAL deberán marcarse con la correspondiente marca de «USO OFICIAL».

3. Todo documento no clasificado que contenga información del Ministerio de Defensa de USO PÚBLICO, en el caso de que el elaborador así lo decida, podrá marcarlo con su correspondiente marca de «USO PÚBLICO».

Artículo 10. Marcado de documentos clasificados.

Todo documento clasificado deberá estar debidamente marcado con una marca acorde al grado de clasificación de la información que contienen: «DIFUSIÓN LIMITADA», «CONFIDENCIAL», «RESERVADO» o «SECRETO».

Artículo 11. Marcas especiales.

1. En el caso de que la información del documento tenga alguna otra característica especial que por razones de seguridad deba ser especificada, se incluirá junto con la marca relativa al grado de clasificación.

2. Se incluirán como marcas especiales aquellas que especifiquen la naturaleza de la información que lo requiera (por ejemplo, relativas a criptografía, o a inteligencia de señales), su alcance (por ejemplo, distribuible a terceros, distribuible por internet), su temporalidad (por ejemplo, copia de trabajo), o si se trata de una copia, traducción o extracto o si no está clasificado separado del anexo, etc.

Artículo 12. Marcado de las copias, traducciones y extractos.

1. Todas las copias, traducciones y extractos de documentos clasificados deberán quedar perfectamente identificadas, de forma unívoca y exclusiva. Para ello, se marcará el documento con la marca COPIA, TRADUCCIÓN o EXTRACTO, la referencia del documento original y su grado de clasificación, según corresponda. Para las copias se añadirá a la referencia del Documento original una numeración sucesiva que indique el número de copias que se han realizado de ese documento (copia 1 de ..., para la primera, copia 2 de ..., para la segunda, etc.), según los criterios que para tal fin indique el Jefe de Seguridad de la información de cada ámbito.

2. Las copias, traducciones y extractos de documentos no clasificados de USO PÚBLICO no requieren ser marcadas, salvo que el documento original disponga de la correspondiente marca. En este caso, la copia, traducción o extracto deberá llevar la misma marca.

3. Las copias, traducciones y extractos de documentos no clasificados de USO OFICIAL deben ser marcadas, con la misma marca que lleve el original.

Artículo 13. *Directrices específicas para el mercado de documentos en papel.*

Además de las directrices generales, para los documentos en papel debe tenerse en cuenta los siguientes requisitos:

- a) Cuando en un documento existan secciones, capítulos, anexos, apéndices, o cualquier otra parte que contengan información con diferentes grados de clasificación, se deberá marcar cada uno de ellos con su marca específica. Incluso, cuando se considere necesario por parte del elaborador, podrán marcarse los distintos párrafos de un documento.
- b) Todas y cada una de las páginas o partes divisibles de un documento irán numeradas y deberán llevar la marca con el grado de clasificación máximo de la información que contienen, en la parte superior e inferior, centrada con respecto a los laterales, de tal forma que no pueda quedar oculta por dobleces, grapas, etc.
- c) En los planos, esquemas, esbozos, diseños, croquis, bocetos, diagramas, mapas o similares, la marca se colocará en la carátula o parte identificativa del mismo y en los lugares en que se permita su mayor visibilidad.
- d) Cuando en un documento clasificado se incluyan páginas en blanco, éstas deberán reflejar su condición con una referencia del tipo: «Página en blanco.»
- e) Los mensajes o escritos de remisión que acompañen a documentos clasificados, y no contengan en ellos información clasificada, aunque lleven la clasificación que les corresponda por agregación, se deberá incluir una marca de que el citado escrito no constituye información clasificada cuando se separe de los anexos.

CAPÍTULO IV

Custodia y uso de documentos

Artículo 14. *Directrices generales para la custodia y uso de documentos.*

1. Todos los documentos clasificados así como los no clasificados de USO OFICIAL deberán tener asignado a un custodio (órgano o persona) que será el responsable de la custodia del propio documento. Dicho custodio será responsable de la protección y vigilancia del documento, garantizando en todo momento la confidencialidad, integridad y disponibilidad de la información que contienen.

2. Para poder manejar documentos de USO OFICIAL y clasificados de DIFUSIÓN LIMITADA, se deberá contar con la «necesidad de conocer» y haber sido previamente instruido en el manejo de información del Ministerio de Defensa.

3. Para poder manejar documentos clasificados CONFIDENCIAL o superior, además de cumplir con la necesidad de conocer y con la instrucción previa, se requerirá tener en vigor la Habilitación Personal de Seguridad (HPS) acorde al grado de clasificación de la información que se requiere manejar.

4. Los documentos no clasificados de USO PÚBLICO, por su propia naturaleza, no requieren disponer de un custodio de los mismos. Todo aquel que maneje un documento de USO PÚBLICO, se considera como usuario del mismo.

5. Todo aquel que requiera el acceso a un documento clasificado o no clasificado de USO OFICIAL deberá solicitárselo al custodio correspondiente. El custodio podrá permitir el acceso a dicho documento siempre que existan garantías constatadas de que el usuario está debidamente autorizado y cumple los requisitos de acceso al mismo. Los usuarios, por el simple hecho de serlo no podrán autorizar a otros usuarios el acceso al Documento que ellos manejan.

6. El custodio del Documento podrá permitir a un determinado usuario actuar como custodio, cuando existan razones justificadas, esté garantizada la seguridad de la información y el nuevo custodio conozca sus responsabilidades.

7. El custodio, que tenga necesidad de conocer, será considerado adicionalmente como usuario, teniendo no solo responsabilidad sobre la custodia sino también sobre su uso.

Artículo 15. *Uso y custodia de documentos no clasificados.*

1. El usuario o custodio de documentos no clasificados de USO PÚBLICO podrá manejar estos documentos tanto en las instalaciones del Ministerio de Defensa, como

fuera de ellas, no estando su distribución limitada, sin necesidad de aplicar medidas de seguridad específicas.

2. En las instalaciones del Ministerio de Defensa, los documentos no clasificados de USO OFICIAL pueden usarse libremente sin necesidad de aplicar ninguna medida de protección adicional. Podrán almacenarse en cualquier Instalación del Ministerio de Defensa, no siendo necesario guardarlos bajo llave, aunque debe evitarse que puedan ser accesibles por personal no autorizado.

3. Los documentos no clasificados de USO OFICIAL, que deban salir de la Instalación en la que se encuentren, seguirán estando bajo la responsabilidad de su custodio quién deberá protegerlos de accesos indebidos.

Artículo 16. Uso y Custodia de documentos clasificados DIFUSIÓN LIMITADA.

1. Los documentos clasificados DIFUSIÓN LIMITADA sólo podrán manejarse en aquellas instalaciones que estén debidamente autorizadas, es decir, sólo se podrá hacer uso de ellos en Zonas de Seguridad.

2. Estos documentos podrán manejarse en cualquier instalación designada como Zona de Seguridad. Deberán permanecer bajo llave siempre que estén desatendidos, es decir que no estén siendo usados por el usuario.

3. Los documentos clasificados DIFUSIÓN LIMITADA que deban salir de su correspondiente Zona de Seguridad, lo harán bajo la responsabilidad de su custodio.

4. Siempre que sea posible, se recomienda que su transporte se haga a través del correspondiente Órgano de Control, aunque se permite que sea el propio custodio el que gestione el transporte de estos documentos, pudiéndolos transportar directamente él.

Artículo 17. Uso y custodia de documentos clasificados CONFIDENCIAL o superior.

1. Los documentos clasificados CONFIDENCIAL o superior estarán bajo la custodia de los Órganos de Control, que permitirán el manejo de dichos documentos sólo a los usuarios debidamente autorizados. Estos usuarios se convierten en custodios del documento, durante todo el tiempo que le sea permitido su manejo.

2. Estos documentos deberán ser manejados en áreas autorizadas como ZAR, Área Clase I ó Área Clase II.

3. Excepcionalmente, el Jefe de Seguridad de la Información de cada ámbito específico o en quién él delegue formalmente, podrá autorizar por un plazo determinado, cuando sea estrictamente necesario, que un usuario, bajo su responsabilidad, con custodia directa y en horario laboral pueda quedarse con un documento clasificado CONFIDENCIAL o RESERVADO. En todos los casos, se informará al custodio de sus responsabilidades y obligaciones durante su custodia para garantizar la confidencialidad, integridad y disponibilidad de la información que contiene el documento que obra en su poder. Entre otras, se le informará expresamente de la prohibición de realizar cualquier tipo de copia del documento, y de la obligatoriedad de que devuelva el documento, en caso de que deba ausentarse de la ZAR en la que se encuentra.

4. No se permitirá que los documentos clasificados SECRETO queden en posesión del custodio fuera de una ZAR.

5. Cuando por razones justificadas sea necesario que un custodio asista a una reunión o actividad clasificada en la que se requiera manejar un documento clasificado, el Jefe de Seguridad de la Información del ámbito, o en quién él delegue formalmente, podrá autorizar que dicho custodio transporte personalmente el documento clasificado CONFIDENCIAL o RESERVADO, informando a su Órgano de Control y asegurando en todo momento la confidencialidad, integridad y disponibilidad de la información que tiene en custodia.

6. En el caso de que sea necesario que el custodio necesite manejar un documento clasificado SECRETO en una ZAR distinta a la suya habitual o acudir a una reunión con un documento clasificado de SECRETO deberá solicitar a su Órgano de Control correspondiente el transporte del mismo. En ningún caso, podrá hacerlo él directamente. Serán los Órganos de Control los que se encarguen del envío de los documentos clasificados SECRETO mediante el transporte a los Órganos de Control de los destinatarios.

CAPÍTULO V

Almacenamiento de documentos

Artículo 18. *Almacenamiento de documentos.*

El almacenamiento de documentos entiende de las medidas de protección necesarias para la guarda y control de los documentos del Ministerio de Defensa por parte de los custodios.

Artículo 19. *Almacenamiento de documentos no clasificados.*

Los documentos no clasificados no requieren de ningún requisito específico para su almacenamiento.

Artículo 20. *Requisitos generales para el almacenamiento de documentos clasificados.*

1. Los documentos clasificados deberán almacenarse por separado, de cualquier otro documento que contenga cualquier otro tipo de información clasificada (OTAN, UE, etc.). De forma que se garantice, en todo caso, que el acceso a un tipo de información no conlleva el acceso al resto de tipos de información. Los documentos clasificados con un determinado grado de clasificación podrán almacenarse con otros documentos de grado superior, siempre que se preserven las medidas de seguridad derivadas de la protección de los documentos de mayor grado. Se deberá garantizar en todo caso que el acceso a un documento clasificado no conlleve el acceso a un documento clasificado de mayor grado.

2. Estos contenedores deberán disponer de las medidas de seguridad necesarias para garantizar que solo el personal autorizado para el acceso a un documento, es el que accede al mismo. Será por tanto necesario, controlar el acceso a los documentos, no dejarlos desatendidos, ni accesibles por terceros no autorizados.

3. Los documentos clasificados de DIFUSIÓN LIMITADA deberán ser almacenados en instalaciones autorizadas como Zonas de Seguridad.

4. Los documentos clasificados CONFIDENCIAL o superior deberán ser almacenados en áreas autorizadas como ZAR, Área Clase I ó Área Clase II, preferentemente en los correspondientes Órganos de Control.

5. El Jefe de Seguridad de la Información podrá instar a aplicar medidas adicionales de seguridad, cuando lo estime oportuno, con objeto de garantizar la preservación de la necesidad de conocer de la información de estos documentos.

CAPÍTULO VI

Copia, traducción y extractos de documentos

Artículo 21. *Directrices generales de copia, traducción y extractos.*

1. Se entenderá por copia de un documento, el hecho por el que se duplica la información que éste contiene en otro documento. La duplicación parcial será considerada extracción.

2. Los documentos resultado del proceso de copia, traducción y/o extracción serán manejados siguiendo los mismos principios de seguridad que los utilizados para los documentos originales de los que se ha obtenido la información.

Artículo 22. *Copias, traducciones y extractos de documentos de no clasificados.*

Las copias, traducciones o extractos de documentos de USO PÚBLICO y de USO OFICIAL podrán llevarse a cabo directamente por el usuario que lo maneje y no requieren ningún tipo de protección especial.

Artículo 23. *Copias, traducciones y extractos de documentos clasificados DIFUSIÓN LIMITADA.*

1. Las copias, traducciones o extractos de documentos clasificados DIFUSIÓN LIMITADA, podrán ser realizados por el custodio siempre que se asegure su control,

de forma que no se produzcan accesos no autorizados a las mismas. No obstante, se recomienda que siempre que sea posible se realicen a través del Órgano de Control correspondiente.

2. El Jefe de Seguridad de la información de cada ámbito podrá establecer, cuando estime oportuno, la obligatoriedad de que las copias, traducciones y extractos de documentos clasificados DIFUSIÓN LIMITADA se realicen a través de los correspondientes Órganos de Control

Artículo 24. Copias, traducciones y extractos de documentos clasificados CONFIDENCIAL.

Las copias, traducciones o extractos de documentos clasificados CONFIDENCIAL deberán realizarse a través de los Órganos de Control correspondientes, con objeto de asegurar que toda copia, extracto o traducción se registra convenientemente y se le asigna el número de documento oportuno.

Artículo 25. Copias, traducciones y extractos de documentos clasificados RESERVADO.

Las copias, traducciones o extractos de documentos clasificados RESERVADO se deberán realizar a través de los Órganos de Control correspondientes, recomendándose que éstas se realicen por el Órgano de Control del elaborador del documento objeto de copia, siempre que sea posible. Se deberá registrar convenientemente y asignarle el número de documento oportuno.

Artículo 26. Copias, traducciones y extractos de documentos clasificados SECRETO.

Como regla general, los documentos clasificados SECRETO no podrán ser reproducidos, traducidos o extractados. En caso de necesitarse copias extras de un documento determinado sólo podrán ser realizadas por el Servicio Central o, General correspondiente o por el Órgano de Control elaborador o destinatario del documento. En éste último caso el destinatario deberá haber sido previamente autorizado por el elaborador del documento. Las copias, traducciones o extractos, se deberán registrar convenientemente y asignarle el número de documento oportuno.

CAPÍTULO VII

Directrices generales de transporte

Artículo 27. Directrices generales del transporte de documentos.

1. Se entiende por transporte de documentos el hecho por el cual se envía un documento de una instalación a otra. El transporte de documentos podrá realizarse por alguno de los siguientes medios, de acuerdo a los requisitos que se establezcan para cada grado de clasificación y cada transporte:

- a) Correo autorizado (también denominado valija conducida).
- b) Valija militar (estafeta militar) o gubernamental, no conducida.
- c) Servicio de correo comercial autorizado y servicio de Correos.
- d) Transporte personal o en mano.

2. El Jefe de Seguridad de la Información del ámbito podrá ampliar o restringir los requisitos de uso, o prohibir el uso de alguno de estos medios, cuando lo estime oportuno.

3. El custodio será el responsable de que se use el medio de transporte más adecuado al grado de clasificación del documento que debe ser transportado.

4. Los documentos deberán ser empaquetados y/o precintados de forma que se impida la observación del contenido de los mismos y que permita identificar cualquier manipulación que pueda ocurrir durante el transporte.

CAPÍTULO VIII

Transporte de documentos no clasificados

Artículo 28. *Transporte de documentos no clasificados.*

1. El transporte de documentos no clasificados podrá hacerlo directamente en mano, el custodio, el usuario o un tercero.

2. Por regla general, los documentos de USO OFICIAL deben ser transportados ocultando la información que contienen, para impedir la observación del contenido de los mismos. Durante el transporte de estos documentos no se debe consultar la información que contienen en lugares no autorizadas (espacios públicos, transportes, etc.).

3. Los documentos de USO PÚBLICO pueden ser transportados sin necesidad de ocultar su información y pueden ser consultados en lugares públicos.

CAPÍTULO IX

Transporte de documentos clasificados entre Instalaciones del Ministerio de Defensa

Artículo 29. *Consideraciones generales.*

El transporte de documentos clasificados entre instalaciones del Ministerio de Defensa entiende de los envíos de documentos clasificados que se inicien y recepcionen en Instalaciones del Ministerio de Defensa, ubicadas tanto en el territorio nacional como fuera del mismo.

Artículo 30. *Transporte de documentos clasificados DIFUSIÓN LIMITADA.*

Los documentos clasificados como DIFUSIÓN LIMITADA pueden ser transportados directamente, en mano, por su custodio, o un tercero. No obstante, siempre que sea posible se recomienda que dichos documentos circulen a través de los Órganos de Control correspondientes del emisor y del destinatario.

Artículo 31. *Transporte de documentos clasificados CONFIDENCIAL y RESERVADO.*

El transporte de documentos clasificados CONFIDENCIAL y/o RESERVADO deberá llevarse a cabo a través de los Órganos de Control correspondientes del emisor y del destinatario. Estos Órganos de Control deberán anotar adecuadamente la entrada y/o salida del documento y actualizar el registro existente.

Artículo 32. *Transporte de documentos clasificados SECRETO.*

El transporte de documentos clasificados SECRETO deberá llevarse a cabo a través del SCPMC o de los SGPMC, correspondientes.

Artículo 33. *Reglas generales para el transporte de documentos clasificados CONFIDENCIAL o superior entre Órganos de Control.*

1. Para el transporte de estos documentos, se deberán empaquetar y precintar de tal forma que se impida la observación del contenido de los mismos y que permita identificar cualquier manipulación que pueda ocurrir durante el transporte, facilitando su trazabilidad.

2. Previamente a su remisión, se anotará en el Órgano de Control correspondiente, la salida del documento y sus datos de identificación.

3. Como evidencia del transporte realizado se utilizarán recibos de entrega y recepción tanto en el Órgano de Control emisor, que será quién lo remita, como en el Órgano de Control destino, que una vez cumplimentado se lo devolverá al emisor. Los receptores de los documentos, deberán inspeccionar detenidamente los envíos recibidos para detectar cualquier posible manipulación. En el caso de que detecten alguna incidencia o anomalía en el transporte deberán anotarlo en el recibo de entrega y recepción.

4. El uso de recibos no eximirá a los Órganos de Control remitente y destinatario de la anotación de los movimientos en los registros de entrada y salida respectivos, ni de la actualización de los registros correspondientes.

CAPÍTULO X

Transporte de documentos clasificados con destino externo al Ministerio de Defensa

Artículo 34. *Consideraciones generales.*

1. El transporte de documentos clasificados con destino externo al Departamento entiende de las medidas a aplicar para el envío de documentos clasificados desde una instalación del Ministerio de Defensa hacia cualquier organismo, órgano, persona o estado, ajenos al Ministerio de Defensa.

2. Este tipo de transporte será considerado como cesión de información y deberá realizarse según el mandato legal o acuerdo de protección correspondiente, que deberá haberse establecido previo al envío del documento.

3. El transporte de documentos clasificados DIFUSIÓN LIMITADA y CONFIDENCIAL se hará desde el Órgano de Control del emisor quién deberá verificar que el receptor del documento dispone de los mecanismos necesarios para proteger debidamente la información de los documentos clasificados entregados.

4. El transporte de documentos clasificados RESERVADO se hará a través del SGPMC, o del SCPMC, según corresponda. No está permitido que se envíen estos documentos a través de los Órganos de Control subordinados.

5. El transporte de documentos clasificados SECRETO se hará exclusivamente a través del SCPMC, no permitiéndose realizar este transporte a los Servicios Generales ni a los Servicios Locales.

CAPÍTULO XI

Borrado de información

Artículo 35. *Consideraciones generales.*

1. El borrado de la información de documentos sólo aplica a documentos en soporte informático con capacidad de re-escritura, en los que se elimina la información que contienen, sin necesidad de que el documento sea destruido.

2. Dependiendo del tipo de herramientas que se utilice para la eliminación de la información, el borrado puede considerarse:

a) Reversible o no seguro: Se emplean herramientas informáticas estándares (formateado del documento, supresión del archivo, etc.). Estas herramientas permiten la recuperación de la información.

b) Irreversible o seguro: Se utilizan herramientas que impiden la recuperación de la información que contenían.

3. En todos los casos, previo a que el documento pueda ser reutilizable y contener otra información, se deberán eliminar las marcas o etiquetas que tengan y que estuvieran asociadas a la información que contenían anteriormente.

CAPÍTULO XII

Conservación o destrucción de documentos

Artículo 36. *Documentos innecesarios.*

1. Con el fin de evitar la acumulación de documentos innecesarios en los ámbitos, el Jefe de Seguridad de la Información de cada ámbito periódicamente solicitará la revisión de los documentos existentes, al menos con carácter anual, para proceder a la destrucción

de aquellos que puedan eliminarse o enviarlos al Sistema Archivístico de la Defensa, según proceda.

2. En ningún caso se podrán destruir documentos originales en tanto subsista en ellos valor probatorio de derechos y obligaciones de las personas físicas o jurídicas o no hayan transcurrido los plazos que la legislación establezca para su conservación.

Artículo 37. Conservación de documentos.

Los documentos que deban ser transferidos para su conservación se remitirán al Sistema Archivístico de la Defensa, según la normativa vigente.

Artículo 38. Destrucción de documentos.

1. La destrucción de documentos conlleva la destrucción del propio soporte, y por tanto, la eliminación irreversible de la información.

2. Sólo podrán destruirse aquellos documentos innecesarios para el ámbito que no deban ser transferidos al Sistema Archivístico de la Defensa.

3. El Jefe de Seguridad de la información deberá proveer los controles necesarios para garantizar que se pueda proceder a la destrucción del mismo.

Artículo 39. Destrucción de documentos no clasificados.

1. Los documentos no clasificados podrán ser destruidos directamente por el usuario o por el custodio de los mismos.

2. La información de estos documentos podrá ser borrada, en lugar de destruir el propio documento, en el caso de que se trate de soportes informáticos con capacidad de re-escritura, pudiéndose emplear para ello tanto el borrado reversible o irreversible.

Artículo 40. Destrucción de documentos clasificados DIFUSIÓN LIMITADA.

1. La destrucción de documentos clasificados (originales y/o copias, traducciones o extractos) DIFUSIÓN LIMITADA podrá ser hecha directamente por el usuario o por el custodio si así lo estima oportuno, aunque siempre que sea posible se deberá realizar su destrucción a través del Órgano de Control correspondiente. Cuando el documento esté registrado e inventariado en su correspondiente Órgano de Control, el custodio deberá informarle para que proceda a la actualización del registro e inventario.

2. La información de estos documentos podrá ser borrada, en lugar de destruir el propio documento, en el caso de que se trate de soportes informáticos con capacidad de re-escritura, empleando herramientas que garanticen el borrado irreversible.

3. El Jefe de Seguridad de la información de cada ámbito podrá establecer, cuando estime oportuno, la obligatoriedad de que la destrucción de documentos clasificados DIFUSIÓN LIMITADA se realice siempre en el correspondiente Órgano de Control.

Artículo 41. Destrucción de documentos clasificados CONFIDENCIAL.

1. La destrucción de documentos clasificados CONFIDENCIAL (originales y/o copias, traducciones o extractos) sólo puede realizarse bajo control del Órgano de Control correspondiente.

2. La información de estos documentos podrá ser borrada, en lugar de destruir el propio documento, en el caso de que se trate de soportes informáticos con capacidad de re-escritura, empleando herramientas que garanticen el borrado irreversible.

3. La destrucción o borrado de un documento clasificado CONFIDENCIAL conllevará en todo caso el levantamiento de un acta en el que se registre la acción realizada.

4. Las actas de destrucción o borrado de los documentos clasificados CONFIDENCIAL se conservarán por los Órganos de Control responsables de la destrucción durante un periodo mínimo de tres (3) años.

Artículo 42. Destrucción de documentos clasificados RESERVADO.

1. La destrucción de documentos clasificados RESERVADO (originales y/o copias, traducciones o extractos) sólo puede realizarse por el Órgano de Control correspondiente.

2. Una vez destruido el documento, se levantará acta, que deberá ir firmada por el responsable del Órgano de Control que realice su destrucción y por una persona, preferiblemente ajena al Órgano de Control, que actuará como testigo del acto y que deberá disponer de la HPS correspondiente, al menos al grado de clasificación del documento que se va a destruir.

3. Los Órganos de Control responsables de la destrucción conservarán durante un mínimo de cinco (5) años el acta de destrucción y las hojas de registro e inventario.

Artículo 43. Destrucción de documentos clasificados SECRETO.

1. Los documentos clasificados SECRETO (originales y/o copias, traducciones o extractos) únicamente pueden ser destruidos bajo control del Servicio Central o el Servicio General de Protección de Materias Clasificadas del Ámbito correspondiente.

2. Una vez destruido el documento, se levantará acta, que deberá ir firmada por el Responsable del Órgano de Control, que realice su destrucción y por una persona ajena al Órgano de Control que actuará como testigo del acto y que deberá disponer de la HPS correspondiente, al menos al grado de clasificación del documento que se va a destruir.

3. Los Órganos de Control responsables de la destrucción conservarán durante un mínimo de diez (10) años el acta de destrucción y las hojas de registro e inventario.

CAPÍTULO XIII

Registro, inventario y sistema de control de documentos clasificados

Artículo 44. Directrices generales del registro e inventario de documentos en los Órganos de Control.

1. Los documentos, originales y/o copias, traducción o extractos, de USO PÚBLICO y de USO OFICIAL no requieren ser registrados, ni inventariados por los Órganos de Control.

2. Los documentos, originales y/o copias, traducción o extractos, clasificados DIFUSIÓN LIMITADA en el caso de que éstos sean remitidos para su gestión a un Órgano de Control, deberán ser registrados e inventariados por el Órgano de Control que los maneje.

3. Los documentos, originales y/o copias, traducción o extractos, clasificados CONFIDENCIAL o superior, deberán ser registrados e inventariados por el Órgano de Control. Deberán conservarse los registros e inventarios de estos documentos clasificados por un plazo superior a la vigencia de los documentos que contienen inventariados y/o registrados, de forma que se garantice la localización y trazabilidad de dichos documentos.

4. Será necesario disponer para los documentos, originales y/o copias, traducción o extractos, clasificados RESERVADO y SECRETO de un registro de control de acceso, hoja de acceso o similar, que permita conocer quién tiene la custodia y/o uso del documento clasificado.

5. El DSIDEF podrá solicitar la información total o parcial de estos registros, cuando lo considere oportuno.

Artículo 45. Sistema de control de los documentos de los Órganos de Control.

1. El DSIDEF dispondrá de los mecanismos necesarios para conocer y controlar los documentos existentes en todos los Órganos de Control del Ministerio de Defensa.

2. El responsable del área de Seguridad de la Información en los Documentos, representando al DSIDEF, podrá solicitar a los Jefes de Seguridad de la Información de cada ámbito, la información contenida en los registros e inventarios de sus Órganos de Control.

3. El Jefe de Seguridad de la Información de cada ámbito podrán solicitar a sus correspondientes responsables de los Órganos de Control la información contenida en sus registros e inventarios.

4. El Jefe de Seguridad de la Información de cada ámbito deberá remitir al Responsable del área de Seguridad de la Información en los documentos, la información que se le requiera relativa al control de los documentos que manejan los Órganos de Control bajo su dependencia, para su inclusión en el Informe Anual de Seguridad de la Información del Ministerio de Defensa, al menos, con carácter anual y siempre que le sea requerido.

TÍTULO II

Manejo de mensajes clasificados y copias de trabajo

CAPÍTULO I

Principios Generales para el manejo de copias de trabajo y mensajes clasificados

Artículo 46. *Principios generales para el manejo de copias de trabajo y mensajes clasificados.*

1. Las copias de trabajo y mensajes clasificados son documentos especiales, con carácter temporal breve, a los que se les permite un posible trato diferenciado del resto de documentos clasificados, en cuanto a su registro e inventario y su destrucción.

2. No se permite la elaboración de copias de trabajo de documentos clasificados SECRETO, ni aplicar este tratamiento de documentos especiales a los mensajes clasificados de grado SECRETO, siendo por tanto de aplicación lo aquí dispuesto a todos los documentos especiales clasificados como CONFIDENCIAL o RESERVADO y recomendable para los documentos clasificados como DIFUSIÓN LIMITADA.

3. Es potestativo del Jefe de Seguridad de la Información de cada ámbito permitir el tratamiento diferenciado de estos documentos especiales o por el contrario, mantener las medidas de protección correspondientes al grado de clasificación del documento clasificado. En el caso de que decida el manejo como documentos especiales deberá preservar lo dispuesto a continuación.

CAPÍTULO II

Copias de trabajo

Artículo 47. *Elaboración y marcado de documentos copia de trabajo de documentos clasificados.*

1. Cuando sea necesario, los Órganos de Control podrán elaborar copias de documentos con objeto de poder ser utilizadas como documentos de trabajo por personal autorizado, siguiendo el procedimiento general para las copias, traducciones y extractos del resto de documentos aplicando las mismas medidas de protección que se apliquen al Documento original, identificándolas adicionalmente con una marca especial en la que figure, al menos: copia de trabajo, fecha límite de destrucción y el nombre de su custodio destinatario (persona u organización).

2. Sólo podrán realizarse copias de trabajo de documentos clasificados de hasta grado RESERVADO.

3. Estas copias de trabajo tendrán una vida útil inferior a 15 días. Antes de que finalice este periodo, el custodio tiene la obligación de destruir este documento

Artículo 48. *Custodia y uso de copias de trabajo.*

Para la custodia y uso de copias de trabajo es de aplicación las mismas medidas de seguridad que para el resto de documentos clasificados.

Artículo 49. *Almacenamiento de copias de trabajo.*

Para el almacenamiento de copias de trabajo es de aplicación las mismas medidas de seguridad que para el resto de documentos clasificados.

Artículo 50. *Copia, traducción y extracto de copias de trabajo.*

No se permite la copia, traducción y extracto de una copia de trabajo. Deberá realizarse directamente del original del que proviene la copia de trabajo.

Artículo 51. *Transporte de copias de trabajo.*

Para el transporte de copias de trabajo es de aplicación las mismas medidas de seguridad que para el resto de documentos clasificados.

Artículo 52. Destrucción de copias de trabajo.

1. Las copias de trabajo deben ser destruidas bien, una vez finalizada la necesidad por la que se elaboraron y previo a la finalización de su vida útil, o una vez ha transcurrido el periodo de 15 días de validez de la misma.

2. La destrucción puede llevarla a cabo el propio custodio de la copia de trabajo o, puede llevarla a su correspondiente Órgano de Control para que procedan a su destrucción.

3. En caso, de que exista la necesidad de seguir manejando la copia de trabajo, transcurridos los 15 días desde su generación, se deberá solicitar al Órgano de Control correspondiente que genere una copia del documento. En ningún caso se podrá volver a solicitar una copia de trabajo de un documento con el fin de prorrogar el periodo de 15 días, del que se haya ya elaborado previamente una copia de trabajo.

4. Los Jefes de Seguridad de la Información de cada ámbito, deberán disponer de los mecanismos necesarios que garanticen que todas las copias de trabajo se destruyen debidamente y se controle dicha destrucción, empleándose, por ejemplo libros de registros para copias de trabajo.

Artículo 53. Registro e inventario de las copias de trabajo.

Las copias de trabajo de documentos clasificados, en el momento en el que se elaboran, deberán ser registradas en el Órgano de Control correspondiente, especificando que son «copias de trabajo» y que su vida útil es inferior a 15 días.

CAPÍTULO III

Mensajes clasificados

Artículo 54. Elaboración y transporte de mensajes clasificados.

1. Por defecto, los mensajes clasificados tendrán un tratamiento equivalente al del resto de documentos clasificados. Sin embargo, si debido a la naturaleza especial de los mensajes, la urgencia de la entrega, así como la posible indisposición del Órgano de Control correspondiente, se permite que el Centro de Comunicación (CECOM) que recibe el documento lo entregue directamente a la autoridad receptora, aplicando las medidas de seguridad que se detallan a continuación.

Artículo 55. Custodia y uso de mensajes clasificados.

Para la custodia y uso de mensajes clasificados es de aplicación las mismas medidas de seguridad que para el resto de documentos clasificados.

Artículo 56. Almacenamiento de mensajes clasificados.

Para el almacenamiento de mensajes clasificados es de aplicación las mismas medidas de seguridad que para el resto de documentos clasificados.

Artículo 57. Copia, traducción y extracto de mensajes clasificados.

1. En el caso de que sea necesario realizar una copia, traducción o extracto de un mensaje clasificado, esta copia deberá ser hecha por el Órgano de Control correspondiente y tendrá la misma vida útil que el mensaje original.

2. Deberán marcarse las copias, traducciones o extractos de mensajes clasificados siguiendo las indicaciones de marcado del resto de documentos clasificados.

Artículo 58. Destrucción, registro e inventario de los mensajes clasificados.

1. El destinatario de un mensaje clasificado enviado a través de los CECOM deberá informar, con la mayor brevedad posible, de dicha recepción a su correspondiente Órgano de Control para que éste proceda a su registro e inventario. Este registro en el Órgano de Control, no tiene porqué corresponderse con el registro de documentos clasificados, pudiendo ser un registro específico.

2. Transcurridos, como máximo, 15 días desde su transmisión, o si este ha dejado de ser válido, deberá ser destruido convenientemente, bien por parte de la autoridad receptora o por el correspondiente Órgano de Control. En el caso de que se considere, que el mensaje sigue siendo válido y no puede ser destruido, dejará de ser considerado como un mensaje pasando a ser un documento clasificado. En este caso, deberá aplicar las medidas de seguridad correspondientes con el grado de clasificación del documento, incluyendo su debido registro.

TÍTULO III

Servicio de Protección de Materias Clasificadas del Ministerio de Defensa

CAPÍTULO I

Principios generales del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa

Artículo 59. Composición del Servicio de Protección de Materias Clasificadas del Ministerio de Defensa.

1. El SPMC del Ministerio de Defensa, está compuesto por el SCPMC, los SGPMC y los SLPMC, denominados todos genéricamente Órganos de Control.

2. Se deberá, en la medida de lo posible, aprovechar la estructura funcional e infraestructura existente de los Órganos de Control para la gestión de información clasificada ajena al Ministerio de Defensa (por ejemplo, Información OTAN, UE, etc.), de modo que éstos se constituyan como Órganos de Control para la información clasificada del Ministerio de Defensa, integrándose en el SPMC del Ministerio de Defensa.

3. El responsable del área de Seguridad de la Información en los Documentos establecerá las directrices, estructura y funcionamiento generales de dicho servicio, quién lo elevará al DSIDEF para su aprobación.

Artículo 60. Finalidad y responsabilidades de los Órganos del Control.

1. La finalidad de los Órganos de Control es asegurar la correcta gestión de los documentos clasificados en cualquier formato, ámbito o situación en que se encuentre, y en concreto, el registro, manejo, distribución, control y archivo de los documentos clasificados de acuerdo a la normativa en vigor.

2. Los Órganos de Control que componen el SPMC serán responsables de recibir, inventariar, custodiar, distribuir y destruir o transferir al sistema archivístico de la Defensa todos los documentos clasificados que manejen, según proceda.

3. Además deberá disponer de un inventario actualizado con la información de los documentos que están bajo su control y de todas las personas autorizadas a tener acceso a los documentos clasificados.

Artículo 61. Principios generales de los Órganos de Control.

1. Previo a su puesta en funcionamiento, todos los Órganos de Control deberán estar debidamente autorizados a manejar información clasificada del grado equivalente al de la información que van a disponer.

2. El personal que vaya a manejar la información del Órgano de Control deberá disponer de la HPS acorde al grado de clasificación que vaya a manejar.

3. El Órgano de Control no podrá manejar información hasta que la instalación donde se aloje esté autorizada y su personal disponga de la HPS necesaria.

4. Todos los Órganos de Control deberán tener nombrado un responsable del SPMC, que será el responsable de que se ejecuten todas las tareas operativas de su Órgano de Control.

CAPÍTULO II

Servicio Central de Protección de Materias Clasificadas

Artículo 62. *Servicio Central de Protección de Materias Clasificadas.*

1. El SCPMC se encuentra en el nivel corporativo, bajo la dependencia funcional del DSIDEF, quién deberá aprobar y autorizar su estructura y funcionamiento.

2. El SCPMC estará bajo la responsabilidad funcional del responsable del área de Seguridad de la Información en los documentos quién establecerá su estructura y funcionamiento.

3. El SCPMC será el Órgano de Control interlocutor con organismos ajenos al Ministerio de Defensa para el intercambio de documentos con grado RESERVADO, cuando sea necesario, y documentos con grado SECRETO, entre el Ministerio de Defensa y estos organismos.

4. El SCPMC será el Órgano de Control de referencia que actuará como punto de entrada genérico para la recepción de documentos clasificados con destino final el Ministerio de Defensa, cuando no se especifique expresamente a qué Órgano de Control va dirigido el documento clasificado.

CAPÍTULO III

Servicio General de Protección de Materias Clasificadas

Artículo 63. *Servicio General de Protección de Materias Clasificadas*

1. En cada uno de los ámbitos del Nivel Específico existirá un SGPMC con dependencia funcional del SCPMC del Ministerio de Defensa y bajo la responsabilidad del Jefe de Seguridad de la Información del ámbito quién deberá establecer las directrices, estructura y funcionamiento de dicho Servicio.

2. La Autoridad del ámbito correspondiente deberá autorizar la estructura y funcionamiento del SGPMC de su ámbito.

CAPÍTULO IV

Servicio Local de Protección de Materias Clasificadas

Artículo 64. *Servicio Local de Protección de Materias Clasificadas (SLPMC).*

1. En las UCO, cuando sea necesario el manejo de documentos clasificados, se establecerá un SLPMC, bajo la autoridad de la UCO y con dependencia funcional del Jefe de Seguridad de la Información del ámbito.

2. El responsable de Seguridad de la información de la UCO deberá establecer las directrices, estructura y funcionamiento de dicho Servicio, siguiendo las indicaciones que le marque su Jefe de Seguridad de la Información.

3. Adicionalmente el Jefe de Seguridad de la Información del ámbito establecerá la relación funcional de los SLPMC con su SGPMC.

4. La Autoridad del ámbito correspondiente deberá autorizar la estructura y funcionamiento de los Servicios Locales de su ámbito.

TÍTULO III

Estructura Funcional de la Seguridad de la Información en los Documentos

CAPÍTULO I

Nivel Corporativo de la Seguridad de la Información en los Documentos

Artículo 65. *Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF).*

El DSIDEF dirigirá y velará por el cumplimiento de la seguridad de la información en los documentos en el Departamento, conforme a lo establecido en el artículo segundo de

la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa y en sus normas de aplicación.

Artículo 66. Responsable del área de Seguridad de la Información en los Documentos.

1. Al responsable de Seguridad de la Información en los Documentos le corresponde, en el ámbito del Departamento, coordinar, supervisar y evaluar la seguridad de la información en los documentos.

2. El responsable del área de Seguridad de la Información en los Documentos será el responsable de establecer y controlar la estructura funcional y funcionamiento del SCPMC, que canalizará al DSIDEF para su aprobación.

3. El responsable del área de Seguridad de la Información en los Documentos establecerá las directrices generales para la apertura, modificación y cierre de los Órganos de Control del SPMC que canalizará al DSIDEF para su aprobación.

4. El responsable del área de Seguridad de la Información en los Documentos elaborará los procedimientos del nivel corporativo derivados de esta norma.

Artículo 67. Responsable del Servicio Central de Protección de Materias Clasificadas.

Será responsable de llevar a cabo todas las tareas relacionadas con la operativa de funcionamiento de su Órgano de Control: registro, manejo, distribución, control y archivo, y cualquier otro cometido que en esta materia le sea encomendada. Sus cometidos incluyen los siguientes:

a) Coordinar la actividad de los Servicios Generales de Protección de Materias Clasificadas.

b) Canalizar, cuando corresponda, el intercambio de documentos clasificados con los SGPMC y los Órganos de Control ajenos al Ministerio.

CAPÍTULO II

Nivel Específico de la Seguridad de la Información en los Documentos

Artículo 68. Jefes de seguridad de la información.

El Jefe de seguridad de la información de cada ámbito, en relación con la seguridad de la información en los documentos en su ámbito, será responsable de:

a) Dirigir y controlar la implantación de las medidas de seguridad de la información en los documentos.

b) Dirigir y controlar los Órganos de Control existentes en su ámbito.

c) Establecer la estructura de los SPMC de su ámbito (SGPMC y SLPKC) para su posterior aprobación por parte de las autoridades correspondientes.

d) Coordinar las medidas de seguridad de la información en los documentos con los diferentes responsables de la ejecución de todas las tareas relacionadas con la operativa o ejecución de la seguridad de la información en los documentos.

e) Generar los procedimientos de protección de los documentos.

f) Promover la formación y concienciación en seguridad de la información en los documentos, que sea necesaria.

g) Recibir y valorar los informes de incidentes de seguridad de la información en los documentos, adoptar o proponer las medidas correctoras oportunas y, según lo establecido, informar al DSIDEF a través del jefe o autoridad del ámbito correspondiente.

h) Establecer el procedimiento y los mecanismos necesarios para obtener la información necesaria de los registros e inventarios de sus Órganos de Control.

i) Asignar al Jefe de Seguridad de la Información en los Documentos y a los responsables de los Órganos de Control de su ámbito aquellos cometidos que él considere oportuno en las áreas de su competencia.



Artículo 69. *Jefe de seguridad del área de la información en los documentos.*

Dependiendo funcionalmente del Jefe de Seguridad de la información de su nivel específico, será responsable de los cometidos que éste le asigne.

Artículo 70. *Responsable de seguridad de la información de la Unidad, Centro u Organismo (UCO).*

Cuando sea necesario, el Jefe de Seguridad de la Información propondrá, a la autoridad de su ámbito, la designación de un responsable de seguridad de la información de la UCO, que ejecutará las acciones que el Jefe de Seguridad de la Información le asigne en esta materia.

Artículo 71. *Responsable de los Servicios Generales y Locales de Protección de Materias Clasificadas.*

Dependiendo funcionalmente del Jefe de Seguridad de la Información de su ámbito de Nivel Específico, serán responsables de llevar a cabo todas las tareas relacionadas con la operativa de funcionamiento de su Órgano de Control: registro, manejo, distribución, control y archivo de los documentos clasificados, principalmente y cualquier otro cometido que su jefe de seguridad de la información del ámbito les asigne en esta materia.

Artículo 72. *Personal del Ministerio de Defensa.*

Todo el personal del Ministerio de Defensa que necesite manejar documentos con información del Ministerio de Defensa deberá seguir las indicaciones de su correspondiente jefe de seguridad de la información y la normativa existente en vigor.