



Comunicación

200

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DEFENSA

Néstor Ganuza Artiles

Comandante Ejército de Tierra
Área de Seguridad
Inspección General CIS
Secretaría de Estado de Defensa
Ministerio de Defensa

Palabras clave

*Política de Seguridad
Normativa de Aplicación de la Política de Seguridad
Consejo de Dirección de Seguridad de la Información
Niveles de Confidencialidad*

Resumen de su Comunicación

La Política de Seguridad del Ministerio de Defensa es el conjunto de normas y procedimientos que proporcionan dirección y soporte para la gestión de la seguridad de la información dentro del Ministerio de Defensa.

El Ministerio se ha encargado de la elaboración de la Política de Seguridad de la Información, de su tramitación de regulación orgánica y del establecimiento de ésta como la norma de más alto nivel a partir de la cual deben emanar el resto de medidas Normativas Organizativas y Tecnológicas necesarias para alcanzar una protección adecuada, proporcionada y razonable de la información.

Se deben proporcionar directrices y reglas de actuación a todos los miembros del Ministerio para alcanzar, como mínimo, el nivel de seguridad de la información que fije su máximo responsable, como objetivo a alcanzar y mantener:

Entre los beneficios perseguidos con la definición de esta política de seguridad cabe destacar:

- Disponer de una normativa de seguridad de la información única y actualizada para todo el Departamento.*
- Disponer de una estructura de seguridad acorde con los países de nuestro entorno.*
- Centralizar la dirección y la gestión de la seguridad del Ministerio.*

La elaboración y aprobación de la Política de Seguridad de la Información del Departamento es el proyecto más significativo del Área de Seguridad de la Inspección General de Sistemas de Información y Comunicaciones del Ministerio de Defensa (en adelante IGECIS), porque su entrada en vigor condiciona el resto de acciones asignadas a dicho Área. Esta norma, fundamental para la construcción de la Seguridad de la Información, tiene como objeto alcanzar la protección adecuada, proporcionada y razonable de la Información del Ministerio de Defensa mediante la preservación de su confidencialidad, integridad y disponibilidad, así como la integridad y disponibilidad de los recursos que la soportan. Para alcanzar dicho objetivo se recogen unas directrices comunes para todo el Ministerio, en las que se ha tenido en cuenta el cumplimiento de la normativa aplicable, tanto nacional como internacional (OTAN, UE, etc.), y un esquema Funcional para su dirección, ejecución y control.

El Plan de Seguridad, acción asignada al Área de Seguridad de la IGECIS, permitirá, una vez aprobada la Política de Seguridad de la Información, planificar las acciones y recursos necesarios para alcanzar los objetivos establecidos en la Política.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DEFENSA

1. Introducción

Esta ponencia presenta el proceso completo que se está siguiendo en el Ministerio de Defensa a la hora de definir una Política de Seguridad de la Información unificada que permita ofrecer una protección sobre la información adecuada, proporcionada y razonable, y que cumpla todas las normativas nacionales e internacionales vigentes en materia de seguridad.

Dada la importancia crítica de todos los recursos de información que maneja la Administración Pública, el presente documento puede servir como un punto de referencia para que otras entidades de la Administración General del Estado acometan iniciativas similares.

2. Antecedentes

El Real Decreto 1551/2004, por el que se establece la Estructura Básica del Ministerio de Defensa, asigna al Secretario de Estado de Defensa la tarea de coordinar la Política de Seguridad del Ministerio. Posteriormente mediante el escrito 300/1361 de 12 de abril de 2005, se encomienda a la IGECIS, como organismo dependiente de la Secretaría de Estado de Defensa encargado de la gestión de aspectos relacionados con las Tecnologías de la Información, la tramitación del Proyecto de Orden Ministerial por el que se insta a impulsar la promulgación de la normativa básica de la seguridad de la información en el Departamento.

3. Grupo de Trabajo Normativa Seguridad de la Información

El Grupo de Trabajo que se encargó de la promulgación de la Normativa de Seguridad de la Información, tenía la siguiente composición:



Grupo Trabajo Normativa Seguridad de la Información

▪ EMAD	▪ SUBDEF
▪ SEDEF	• Gabinete
• Gabinete	• Asesoría Jurídica General
• DGAM	• SEGENTE
• DIGENIN	• DIGENPER
• IGECIS	▪ SEGENPOL
▪ E. TIERRA	▪ CNI
▪ ARMADA	
▪ E. AIRE	

4. Proyecto Normativa IGECIS

La Normativa Básica de Seguridad de la Información se estructura en 3 niveles normativos

Proyecto Normativa IGECIS



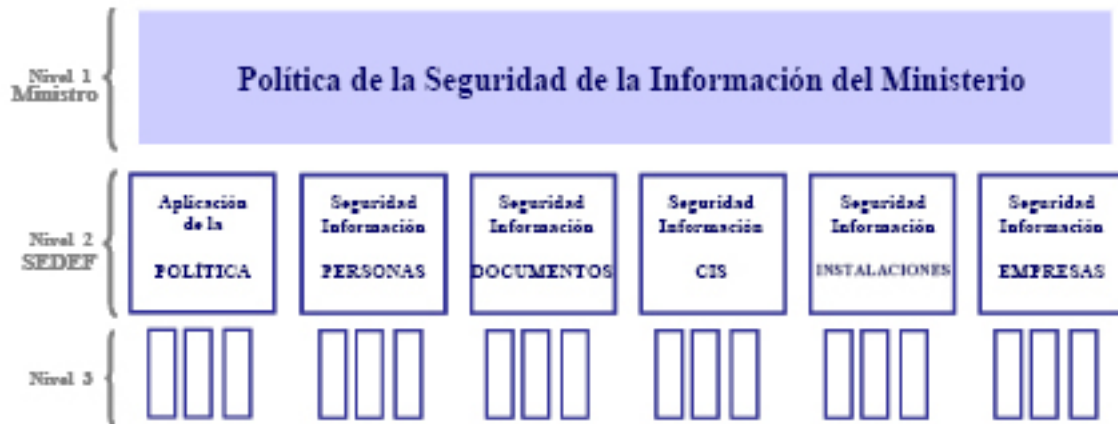
1. **Primer nivel normativo > Proyecto de Orden Ministerial**
 - **“Política de Seguridad de la Información”**
2. **Segundo nivel normativo > Proyectos de Instrucción de SEDEF**
 - **Normas de Aplicación de la Política**
 - **Normas sobre Seguridad de la Información en las PERSONAS**
 - **Normas sobre Seguridad de la Información en los DOCUMENTOS**
 - **Normas sobre Seguridad de la Información en los SISTEMAS**
 - **Normas sobre Seguridad de la Información en las INSTALACIONES**
 - **Normas sobre Seguridad de la Información en las EMPRESAS**
3. **Tercer nivel normativo > Diferentes proyectos de disposiciones reglamentarias**

Como puede apreciarse el primer paso consistió en promulgar una Orden Ministerial de definición de la Política de Seguridad de la Información.

Aparte de la definición de la Política de Seguridad de la Información es primordial la actualización de su cuerpo normativo para adecuarse a la continua evolución de las Tecnologías de la Información.

La nueva Política de Seguridad de la Información es necesaria para:

- Racionalizar la normativa actual.
- Actualizar conceptos según la evolución de las Tecnologías de la Información.
- Crear un único documento base de referencia.
- Facilitar la coordinación del desarrollo normativo.
- Establecer los mismos criterios para el ámbito global del Ministerio de Defensa.
- Alcanzar un conjunto normativo equilibrado y completo.



Respecto al segundo nivel normativo de estructuración de la Seguridad de la Información del Ministerio de Defensa, se definen una serie de áreas según el ámbito al que afecte la información que se maneja:

- **SEGINFOPER:** Esta norma pretende recoger los requisitos de seguridad relacionados con las Personas.
- **SEGINFODOC:** Esta norma trata de recoger los requisitos de seguridad relacionados con los documentos, dando prioridad al Control y Registro de documentos certificados como confidenciales.
- **SEGINFOCIS:** Esta norma pretende recoger los requisitos de seguridad relacionados con los Sistemas de Información y Telecomunicaciones.
- **SEGINFOINS:** Esta norma pretende recoger los requisitos de seguridad relacionados con las instalaciones.
- **SEGINFOEMP:** Esta norma pretende recoger los requisitos de seguridad relacionados con las empresas.

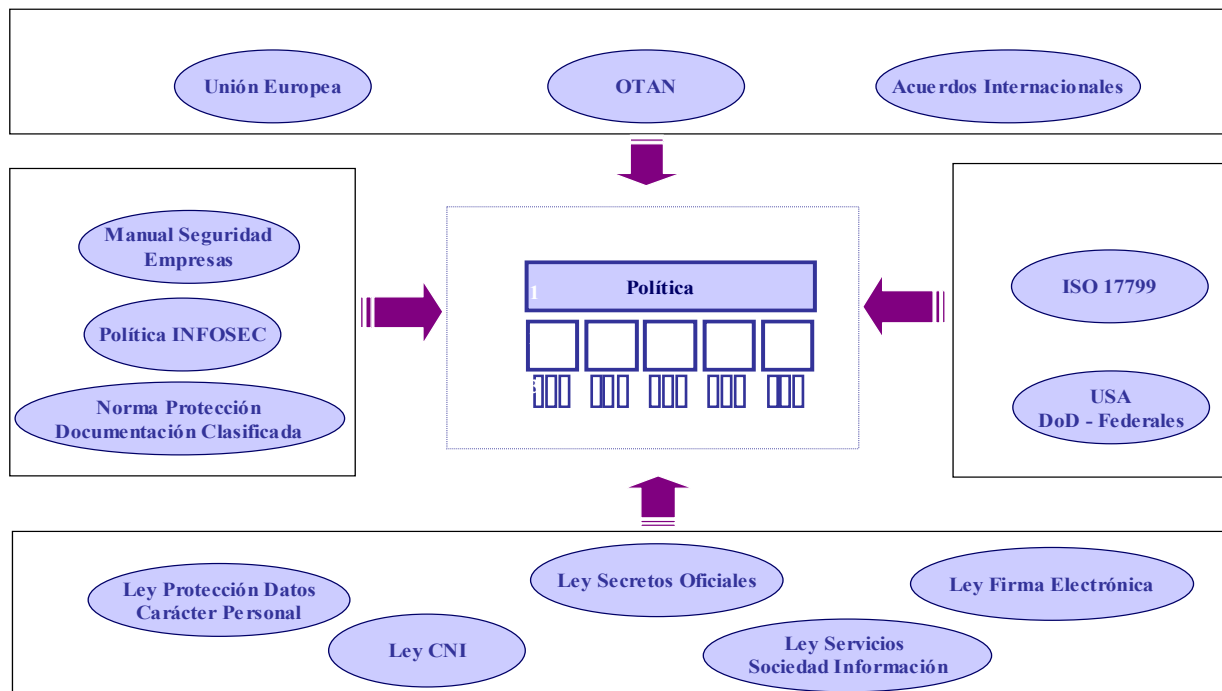
Áreas de la Seguridad de la Información



En el esquema anterior **HPS** hace referencia a la Habilitación Personal de Seguridad y **NdC** a Necesidad de Conocer.

Como se indicó en la introducción del presente documento, la Política de Seguridad de la Información debe recoger distintos términos recogidos en diferentes normativas, tanto nacionales como internacionales, que componen el **Cuerpo Normativo de Seguridad**.

En el siguiente cuadro se pueden apreciar los Organismos de procedencia de las distintas normativas que componen el citado Cuerpo Normativo de Seguridad:



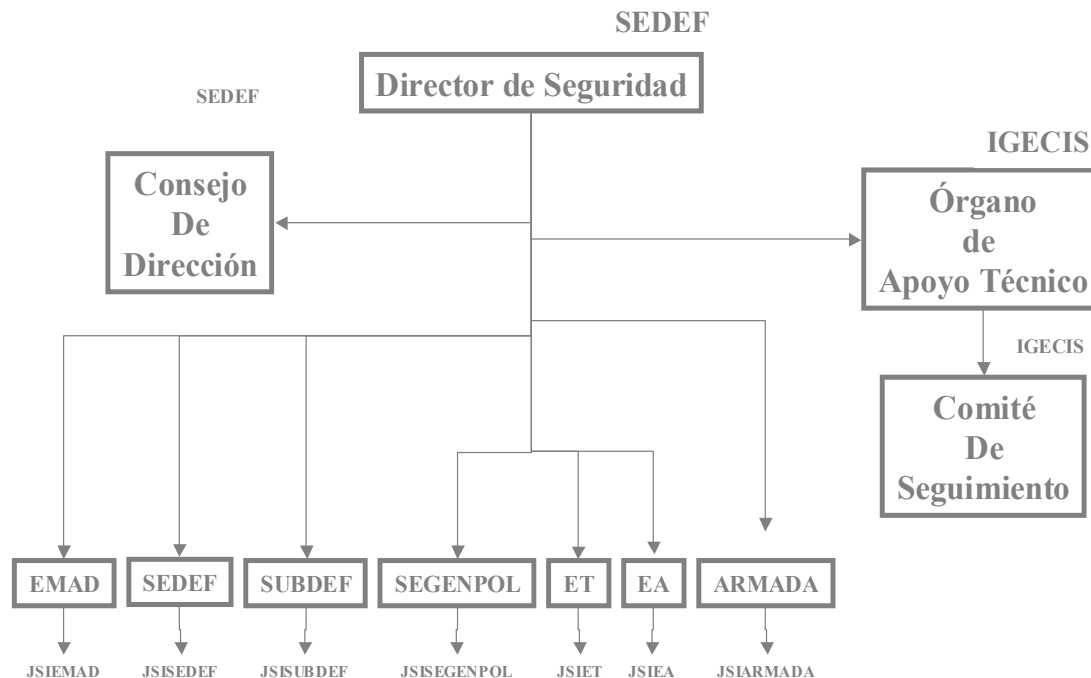
Conforme al Real Decreto 1551/2004, la Dirección de la Seguridad de la Información recae en el Secretario de Estado de Defensa, cuyas misiones en este ámbito se pueden resumir en los siguientes puntos:

1. Dirigir la Seguridad de la Información.
2. Velar por el cumplimiento de la Política establecida.
3. Definir la Estructura Funcional.

El Secretario de Estado contará para estas tareas con el asesoramiento de un Consejo de Dirección de Seguridad de la Información formado por vocales de distintos departamentos del Ministerio de Defensa y un secretario perteneciente a la IGECIS.

Los diferentes organismos implicados en materia del desarrollo normativo de la Política de Seguridad se distribuyen según el siguiente esquema:

Esquema Funcional



Como principal novedad en el esquema anterior, se puede citar la figura del Órgano de Apoyo Técnico, cuya responsabilidad recae también en la IGECIS.

La función a desarrollar por parte de la IGECIS, como órgano de Apoyo Técnico recoge las siguientes tareas:

- Prestar apoyo y asesoramiento Técnico al Director.
- Elaborar, mantener y proponer al Director Normas, Planes, Programas y Procedimientos.
- Dirigir el Servicio PDC¹ del Ministerio.
- Elaborar propuestas de clasificación.
- Elaborar la Guía de Clasificación.
- Enlace con CNI² y Organismos Externos.
- Evaluar la Seguridad, Informe Anual.
- Estudiar nuevas tendencias

Dentro de la distribución anterior es muy importante diferenciar qué organismos se ocupan de la Definición de la Política de Seguridad y cuáles se encargan de definir las Normas de Aplicación de dicha política. En lo que respecta al Ministerio de Defensa se dividen las responsabilidades de la siguiente manera:

PDC: Protección Documentación Clasificada.

CNI: Centro Nacional de Inteligencia.

5. Información en el Ministerio de Defensa

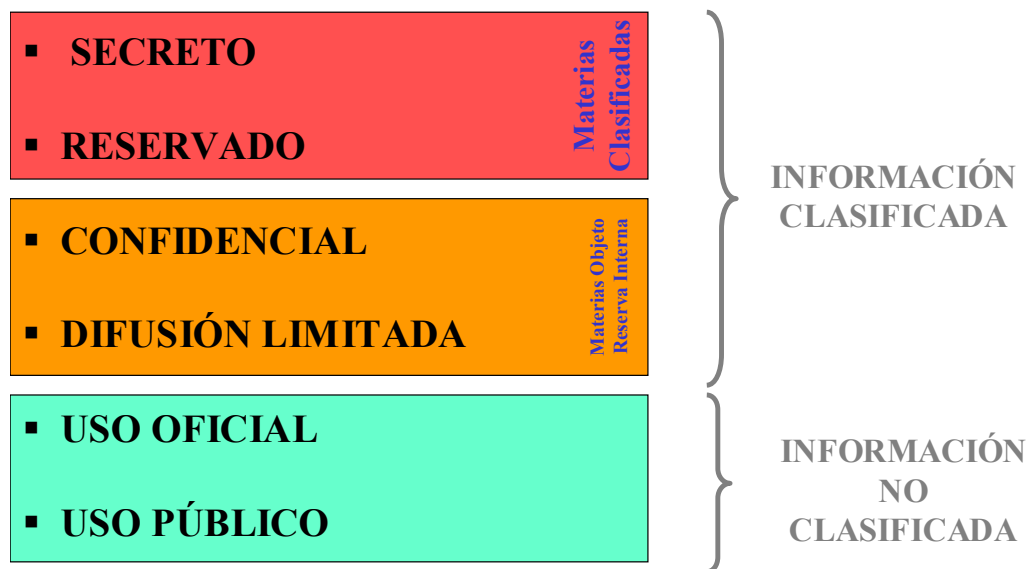
Es muy importante conocer las diferentes formas en que se presenta la información, así como el ciclo de vida que recorre ésta, para poder definir una Política de Seguridad que realmente proteja los recursos informáticos de manera eficaz.

Toda información referente al Ministerio de Defensa debe clasificarse de acuerdo con los siguientes parámetros de manera que se puedan aplicar una normativa dentro de la Política de Seguridad u otra:

1. Atributo: Esto es, si la información es clasificada o no.
2. Formato soporte de la información: papel, formato electrónico, etc.
3. Lugar de generación de la información: Interna o Externa al Ministerio.

Respecto a la Clasificación de la Información según sus requerimientos de Seguridad, se establecen los 6 niveles siguientes:

Clasificación de la Información



Una vez que se dispone de una Política de Seguridad y de una Normativa para su aplicación se debe ordenar todo la información de la que se dispone en función del gráfico anterior:

6. Conclusiones

En el Ministerio de Defensa dentro del ámbito de la seguridad de la información, se está produciendo un cambio muy significativo: la transición desde un modelo de gestión de la seguridad sin unas directrices comunes, a uno corporativo de dirección y gestión de la seguridad. Una de sus acciones más destacables, aunque no la única, es la elaboración de Política de Seguridad de la Información y la organización de la seguridad (por la que se asignarán responsabilidades en materia de seguridad a autoridades del Ministerio y a los Cuarteles Generales, logrando mayor eficacia y coordinación), además:

- La definición de la Política de Seguridad del Ministerio de Defensa es una actuación fundamental para el desarrollo de todos los demás proyectos tecnológicos del Departamento, ya que todos ellos deben cumplir los condicionantes de protección de la Información recogidos en la citada Política de Seguridad.

- La Política de Seguridad de la Información va a producir un cambio de hábito y cultura en los usuarios dentro del Ministerio de Defensa que debe llevar asociadas medidas de Gestión del Cambio.