

I. DISPOSICIONES GENERALES

MINISTERIO DE DEFENSA

14417 Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa.

La Agenda Digital para España, aprobada por Acuerdo de Consejo de Ministros de 15 de febrero de 2013, los objetivos identificados por la Comisión para la Reforma de las Administraciones Públicas (CORA), creada por Acuerdo del Consejo de Ministros del 26 de octubre de 2012, los objetivos, principios y acciones previstos en el artículo 9 del Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, y la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, modificada por la Ley 18/2015, de 9 de julio, marcan la senda del esfuerzo que está desarrollando el conjunto de la Administración para su Transformación Digital.

En este marco, el citado real decreto señala que la Administración debe adoptar una nueva cultura de la información y estar preparada para recoger, generar y tratar grandes volúmenes de información digital sobre sus operaciones, procesos y resultados. Igualmente, subraya que el desarrollo de las capacidades de análisis trasversal de la información permitirá optimizar la gestión, mejorar la toma de decisiones y ofrecer servicios interdepartamentales de manera independiente a la estructura administrativa.

En esta misma línea, el Plan de Transformación Digital de la Administración General del Estado y sus Organismos Públicos (Estrategia TIC), de 2 de octubre de 2015, como marco estratégico global de dicha transformación, ha determinado los mencionados objetivos, principios y acciones, como base de partida para la elaboración por los distintos Ministerios de sus respectivos Planes de Acción para la Transformación Digital.

En el citado plan se pretende conseguir una «Gestión corporativa inteligente del conocimiento, la información y los datos» (objetivo IV), mediante la obtención de una plataforma compartida interdepartamental para el uso proporcional, justificado y seguro de la información agregada, así como de sistemas de análisis de datos para la toma de decisiones, al mismo tiempo que una «Estrategia corporativa de seguridad y usabilidad» (objetivo V).

Con estas obligadas referencias, el Ministerio de Defensa debe completar su esfuerzo en el proceso de Transformación Digital mediante la puesta en marcha de una Estrategia de la Información que permita afrontar, dentro de su especificidad y con la debida prioridad sobre las misiones de las Fuerzas Armadas, el tratamiento eficaz, eficiente y seguro de la información como un recurso estratégico, sustentado por las TIC y sobre el cual se debe lograr la superioridad.

Para ello, también se tendrá en cuenta las estrategias y políticas de gestión de datos, información y conocimiento de carácter nacional, de la OTAN y de la UE, que faciliten la mejor interoperabilidad y la seguridad de los sistemas de información y telecomunicaciones (CIS) y de la información que transmiten y procesan.

Con esta visión integradora y global, la Estrategia de la Información del Ministerio de Defensa viene a regular sus características en el ámbito de la Defensa Nacional y a completar la base normativa sobre la que se sustenta su propio proceso de Transformación Digital, formada también por la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC) del Ministerio de Defensa aprobada por Orden DEF/2639/2015, de 3 de diciembre, que cubre el ámbito de los soportes tecnológicos y de los sistemas que facilitan las capacidades CIS/TIC del Departamento; por la Política de Gestión de Documentos electrónicos del Ministerio de Defensa, aprobada a través de la Orden ministerial 5/2017, de 9 de febrero, en la vertiente de la gestión del fomento y

soporte electrónico; y por la Política de Seguridad de la Información del Ministerio de Defensa, aprobada por la Orden ministerial 76/2006, de 19 de mayo, para alcanzar su protección adecuada, proporcionada y razonable.

Durante su tramitación, el proyecto de esta Orden ministerial fue informado por la Comisión Permanente de la Comisión Ministerial de Administración Digital, en cumplimiento del artículo 9.2.d) de la Orden DEF/2071/2015, de 5 de octubre, por la que se regula la Comisión Ministerial de Administración Digital del Ministerio de Defensa, y fue valorado favorablemente por la Secretaría General de Administración Digital, con arreglo a lo establecido en el artículo 7.4 del Real Decreto 806/2014, de 19 de septiembre.

En su virtud, dispongo:

Artículo 1. *Objeto.*

Es objeto de esta Orden ministerial establecer la Estrategia de la Información del Ministerio de Defensa, y las bases para definir la estructura de gestión de la información a nivel ministerial que permita su desarrollo.

Artículo 2. *Definiciones.*

Administración de la Información: Manejo de la información a lo largo de su ciclo de vida.

Ámbitos: Los ámbitos del Ministerio de Defensa a los efectos de esta Estrategia y en línea con la estructura de gobierno de la seguridad de la información del Departamento son:

- a) Estado Mayor de la Defensa.
- b) Secretaría de Estado de Defensa.
- c) Subsecretaría de Defensa.
- d) Ejército de Tierra.
- e) Armada.
- f) Ejército del Aire.
- g) Secretaría General de Política de Defensa.

Ciclo de vida de la información: El ciclo de vida de la información abarca las etapas de recopilación, creación o generación de información, organización (clasificación, calificación y descripción), recuperación, uso, accesibilidad y transferencia; y baja. Además, existirán unas tareas de planificación, almacenamiento y protección, que tendrán siempre en cuenta los requisitos de los procesos de gestión y operativos, abarcando todas las etapas del ciclo de vida.

Conocimiento: En el contexto de la jerarquía cognitiva, se trata de información analizada y valorada que proporciona un valor añadido para el usuario.

Custodio de la información: Persona u organismo responsable de conservar adecuadamente y proteger la información.

Datos: Es el nivel más bajo de la información en la jerarquía cognitiva y no suelen ser útiles hasta que no son procesados para darles significado. Consisten en señales sin procesar que se transmiten entre nodos en los sistemas de información.

Entendimiento: Aplicación de la percepción y del conocimiento para producir los resultados deseados, dando lugar a una comprensión objetiva de la realidad, dentro de un contexto más amplio y mediante la intervención intelectual y la experiencia humana. Marca el nivel superior de la pirámide cognitiva.

Estándar de información: Norma, patrón o referencia sobre un aspecto de la gestión de la información.

Explotación de la información: Uso de la información para lograr obtener la posición de ventaja que caracteriza la mejor gestión y la superioridad de la información.

Factores de calidad de la información: Criterios que determinan la calidad de la información, siendo estos exactitud, oportunidad, usabilidad, completitud, precisión y fiabilidad.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Información: Conjunto organizado de datos procesados que constituye un recurso estratégico del Departamento sobre el que se debe buscar la superioridad para facilitar el cumplimiento y alcanzar el éxito de los cometidos encomendados al Ministerio de Defensa y de las misiones de las Fuerzas Armadas.

Información relevante: Información de interés para la Defensa que ha de ser objetiva, oportuna, útil, completa, precisa y fiable. Cada ámbito del Departamento debe definir los requisitos de información, para apoyar eficazmente el ejercicio de las misiones y tareas asignadas.

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

Metadatos: Se definen como «datos sobre los datos». En la gestión de los documentos electrónicos, los metadatos son datos que describen el contexto, contenido y estructura de los documentos y su gestión a lo largo del tiempo.

Propietario de la información: La organización que crea y mantiene el contenido, define reglas de acceso, negocia y acepta liberar restricciones, establece instrucciones de disposición, y es la autoridad para el ciclo de vida de la información. En este caso es el Ministerio de Defensa.

Requisitos de información: Descripción de las necesidades de un usuario de información en relación a la información que precisa para el cumplimiento de las misiones y tareas asignadas.

Responsabilidad de compartir: La obligación individual y colectiva de hacer la información disponible y accesible para aquellas entidades que requieran la información para realizar las tareas individuales o colaborativas asignadas del Departamento.

Superioridad en la información: Ventaja relativa que se genera mediante el empleo de información relevante, principios y capacidades disponibles, de forma continua y dirigida adaptándose a cada situación. Este concepto debe entenderse más como la capacidad de adaptación al entorno cambiante en el que se actúe, que con el control de la información en sí misma. La superioridad ya no solo depende de la tecnología ni de la rapidez con la que la información se explote, sino con su oportunidad y capacidad de adaptación al contexto en el que se opere.

Usuario de la información: Persona o grupo de personas que generan o utilizan la información del Departamento para el desempeño de sus misiones y tareas a través de las actividades de explotación de la misma.

Artículo 3. *Ámbito de aplicación.*

La Estrategia de la Información será de aplicación en todo el Ministerio de Defensa y sus Organismos Públicos.

Artículo 4. *Alcance de la Estrategia de la Información.*

Caracterizar y tipificar la información para facilitar su mejor aprovechamiento como recurso estratégico para el Ministerio de Defensa y así alcanzar la mejor gestión y la superioridad de la información, a través de la integración de usuarios, procesos, productos de información, equipos y Servicios CIS/TIC, y de una adecuada estructura de gestión de la información.

Artículo 5. *Principios de la Estrategia de la Información.*

Los principios que regirán esta Estrategia de la Información del Ministerio de Defensa son los siguientes:

a) La información es un recurso estratégico para la Defensa sobre el que se debe buscar la superioridad para facilitar el cumplimiento de las misiones y los cometidos

encomendados al Departamento, apoyando sus procesos funcionales y operativos, y los requisitos correspondientes, mediante la organización y el control de la misma a lo largo de su ciclo de vida, independientemente del medio y del formato en el que se encuentre.

b) La superioridad de la información se debe lograr a través de la administración, gestión, explotación y seguridad de la información, con una visión integral de la misma, considerando su relevancia y calidad, los procesos, las personas, la formación y la tecnología.

c) La información debe tener sus propios responsables en diversos niveles, de forma que exista un elaborador, un propietario y un custodio a lo largo de todo el ciclo de vida.

d) La gestión de la información precisa una estructura específica, que permita su mejor empleo y control y sienta las bases de la gestión del conocimiento.

e) La información será compartida para incrementar su valor como recurso estratégico de la Defensa, gestionando el compromiso entre «la responsabilidad de compartir» y la «necesidad de conocer», facilitando el acceso, el intercambio, la actualización, la más amplia reutilización y la eliminación de redundancias.

f) La información se debe normalizar y estandarizar a través de los productos de información, para permitir la plena interoperabilidad, la máxima cooperación y la mayor eficiencia y eficacia de los procesos.

g) La información se debe proteger aplicando las medidas necesarias para garantizar su disponibilidad, integridad y confidencialidad a lo largo de todo su ciclo de vida.

Artículo 6. *Finalidad y objetivos estratégicos.*

1. La finalidad de la Estrategia de la Información es proporcionar al Ministerio de Defensa un conjunto de directrices comunes globales y únicas que, basadas en los principios de la propia Estrategia, permitan que la información por su carácter estratégico para la Defensa, sea fiable y accesible con la debida protección, en todo momento y lugar, para cualquier usuario que la precise, conforme a su perfil autorizado, y a los requisitos de dicha información.

2. Para lograr la superioridad de la información en todo el Departamento se establecen tres objetivos estratégicos:

a) Alinear la Estrategia de la Información con las Políticas CIS/TIC y Seginfo, en el marco de la transformación digital del Departamento dentro de la Estrategia TIC del Estado.

En primer lugar, se deben desarrollar las capas de la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC) correspondientes a los procesos funcionales y operativos y a los productos de información, mediante la normalización y estandarización de los procesos y de la información, así como la identificación del valor de la información en cada caso. Las citadas capas de la AG CIS/TIC constituyen el nexo de unión entre los usuarios de la información en su contexto operativo y los CIS del Departamento.

En segundo lugar, se debe contemplar la seguridad de la información en los procesos de gestión de la misma para garantizar su confidencialidad, integridad y disponibilidad a lo largo de todo su ciclo de vida.

Finalmente, se deben orientar las actuaciones para lograr la transformación digital del Departamento mediante la revisión integral de las tareas y las actividades que constituyen los flujos de trabajo de los procesos del Departamento, con el fin de lograr la integración y el mejor empleo de los recursos y capacidades de las tecnologías de la información y las comunicaciones en dichos procesos.

b) Mejorar la explotación de la información. A través del uso de los productos de información facilitados por los Servicios CIS/TIC de una forma directa por parte de los usuarios, a través de herramientas colaborativas que permitan el intercambio, la actualización y la reutilización de la información, y de permanentes planes de formación para actualizar las capacidades y habilidades de los mismos usuarios.

c) Facilitar la accesibilidad sin perjuicio de la debida protección de la información. Se asegurará la información a lo largo del ciclo de vida con la flexibilidad necesaria para que sea accesible por los usuarios autorizados en el momento y lugar oportunos de forma segura y fiable, estableciendo un entorno que proteja los activos de información del Departamento de manera que la protección de la información no afecte a su transmisión o su tratamiento.

Artículo 7. *Directrices generales.*

1. Identificar y desarrollar los procesos funcionales y operativos y los productos de información, en cada ámbito a través de las siguientes medidas:

a) Revisar y simplificar los procesos funcionales y operativos para aprovechar las posibilidades que ofrecen las Capacidades CIS/TIC y contribuir a la mejora del funcionamiento interno del Ministerio de Defensa, incorporando de forma flexible nuevas funcionalidades y eliminando redundancias y duplicidades.

b) Identificar los indicadores necesarios para medir la eficacia y eficiencia de los procesos.

c) Identificar y desarrollar detalladamente los productos de información normalizados previstos en la AG CIS/TIC.

d) Alinear los Servicios CIS/TIC con los procesos funcionales y operativos del Departamento, para lograr una visión global y única de dichos Servicios CIS/TIC.

e) Implantar las medidas de carácter operativo y tecnológico que faciliten la gestión de la información del Departamento.

2. Identificar el valor de los datos y de la información, en cada ámbito a través de las siguientes medidas:

a) Establecer las tipologías de datos aplicables a cada contexto y situación, permitiendo la necesaria flexibilidad en su definición.

b) Establecer los criterios para fijar la relevancia, pertinencia y oportunidad de la información.

c) Determinar los factores de calidad que determinan la superioridad de la información en cada contexto funcional u operativo y situación.

3. Estandarizar los datos, la información, los registros y los archivos, a través de las siguientes medidas:

a) Establecer e implantar modelos de datos que permitan compartir y explotar la información y desarrollar la capacidad de análisis de grandes volúmenes de datos.

b) Aplicar la Política de Gestión de Documentos Electrónicos.

c) Identificar la información potencialmente reutilizable desde la concepción de los sistemas de información.

d) Actualizar la normativa que regula el Registro Electrónico Central y el resto de registros del Departamento.

e) Desarrollar soluciones tecnológicas o reutilizar otras para digitalizar la actividad de las diversas áreas funcionales del Departamento.

f) Implantar estándares de intercambio de información en todos los sistemas, y preferentemente, al compás de la entrada en servicio de herramientas colaborativas normalizadas, potenciando el uso de servicios web.

g) Fomentar y facilitar el análisis sistematizado, predictivo y evaluativo, sobre múltiples fuentes de datos.

4. Implementar planes de formación y mejorar en el empleo de aplicaciones de usuario y herramientas colaborativas, a través de las siguientes medidas:

a) Establecer e implantar planes de formación para el uso de herramientas colaborativas normalizadas y la mejor gestión de la información.

b) Fomentar el empleo de entornos de trabajo colaborativos entre los distintos ámbitos, integrando así a los usuarios, la información, los datos y los procesos.

c) Fomentar el uso de formatos reutilizables en la gestión de los datos y de la información.

5. Establecer una estructura de gestión de la información orientada a facilitar el desarrollo de los cometidos del Departamento y el trabajo de su personal a través de las siguientes medidas:

a) Definir e implantar una estructura para la gestión de la información en la propia estructura del Departamento.

b) Avanzar hacia la creación de una estructura de gestión del conocimiento.

c) Alinear a nivel departamental la estructura funcional de Gestión de la Información con la estructura funcional de la SEGINFO.

6. Facilitar el acceso directo a la información a través de los Servicios CIS/TIC, independientemente de los medios que utilicen y de su ubicación, a través de las siguientes medidas:

a) Simplificar las aplicaciones de usuario sin perjuicio de su nivel de clasificación.

b) Avanzar en el diseño de los nuevos servicios orientados a las plataformas móviles, permitiendo todo tipo de documentos electrónicos: imagen, audio o video, etc.

c) Definir y actualizar la cartera de Servicios CIS/TIC del Ministerio de Defensa y activar el Catálogo de Servicios CIS/TIC, simplificando las aplicaciones de usuario en formato sencillo e intuitivo.

7. Proteger y gestionar el riesgo de los datos, la información y el conocimiento, de manera que la debida protección de la información no afecte a su tratamiento o transmisión, a través de las siguientes medidas:

a) Revisar los niveles de clasificación de la información.

b) Fomentar la confianza en el uso de los servicios digitales.

c) Permanente análisis y conocimiento del riesgo en todos los Servicios que gestionen información.

Artículo 8. *Desarrollo de la Estrategia de la Información.*

Para el desarrollo de esta Estrategia se elaborará una instrucción para la gestión de la información y el conocimiento del Ministerio de Defensa, que establezca su estructura funcional en el Ministerio de Defensa y su relación con los procesos funcionales y operativos y con los Servicios CIS/TIC.

Artículo 9. *Estructura de la gestión de la información del Ministerio de Defensa.*

1. Se designa como Autoridad de gestión de la información del Ministerio de Defensa al Secretario de Estado de Defensa, que tendrá en todo el Departamento las funciones de dirigir y velar por el cumplimiento de los principios y objetivos de esta Estrategia.

2. La estructura funcional de gestión de la información del Ministerio se integrará en la organización de la Comisión Ministerial de Administración Digital (CMAD) a nivel corporativo. Bajo su autoridad, la Comisión Permanente de dicha Comisión Ministerial de Administración Digital (CPCMD) velará por el desarrollo de esta Estrategia y por la implantación y coordinación de una estructura de gestión de la información en todos los ámbitos del Ministerio de Defensa.

3. El CIO del Ministerio de Defensa deberá coordinar la estructura de gestión de la información a nivel corporativo, supervisando el cumplimiento de las políticas de referencia y el desarrollo de esta Estrategia, base del proceso de transformación digital del Departamento.

4. Cada ámbito específico deberá:
- Clasificar y calificar la información, los sistemas y los Servicios CIS/TIC en base a los conceptos establecidos en el anexo I-Ciclo de Vida de la Información.
 - Implementar las estructuras de organización, gobernanza y control de la gestión de la información en la propia estructura orgánica del ámbito, así como los programas de formación del personal.
 - Identificar los responsables y gestores de la información y del conocimiento.
 - Identificar los diversos perfiles de los responsables y usuarios de la información en su ámbito.
 - Evaluar la eficacia y eficiencia de la administración y de la gestión de la información y del conocimiento.

Artículo 10. *Roles y responsabilidades.*

Se establecen las siguientes responsabilidades para un correcto desarrollo de esta Estrategia y de la implantación de la Estructura de Gestión de la Información y del Conocimiento:

- Responsable del Dato: Responsable de garantizar la calidad, fiabilidad y no duplicidad de los datos. Debe garantizar la precisión, consistencia, credibilidad y actualidad de los datos, así como que estén completos.
- Responsable del Proceso: Responsable del conjunto estructurado de actividades de un determinado proceso que estén diseñadas para lograr un objetivo específico. Debe asegurar que el proceso se compone de actividades interconectadas para producir como resultado una salida definida fiable, a partir de una o varias entradas, empleando las herramientas de gestión y control necesarias.
- Responsable de los Productos de Información: Responsable del conjunto de información que se considera como la entrada y/o salida formal de un proceso funcional y operativo. Debe asegurar que los productos de información cumplan con los estándares de calidad.
- Usuarios de la Información: Los usuarios de la información del Departamento, con sus respectivos perfiles de acceso, utilizarán la información en cualquiera de las fases de su ciclo de vida a través de los procesos y servicios de información establecidos.

Disposición adicional única. *No incremento del gasto público.*

Las medidas incluidas en esta norma no podrán suponer incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición final primera. *Facultades de aplicación.*

Se faculta al Secretario de Estado de Defensa para dictar las instrucciones y órdenes de servicio, en el ámbito de sus competencias, para la aplicación y ejecución de esta Orden ministerial.

Disposición final segunda. *Entrada en vigor.*

La presente Orden ministerial entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

Madrid, 27 de noviembre de 2017.–La Ministra de Defensa, María Dolores de Cospedal García.

ANEXO I

Ciclo de vida de la información

En este anexo se proporciona un marco de referencia para asegurar que la información es manejada de forma eficiente y segura, incluyendo la gestión de todos los aspectos a lo largo de su ciclo de vida, el cual engloba la recopilación, creación o generación de información; organización (clasificación, calificación y descripción); recuperación, uso, accesibilidad y transferencia; y baja.

Además de las etapas mencionadas anteriormente, existirán las tareas de planificación, almacenamiento y protección, que tendrán siempre en cuenta los requisitos de la misión y abarcarán todas las etapas del ciclo de vida.

El propósito de la planificación es producir y comunicar planes efectivos y viables requeridos para manejar la información de una manera eficiente y segura. La planificación abarcará todas las etapas del ciclo de vida y tendrá siempre en cuenta los requisitos de la misión.

El almacenamiento garantiza el mantenimiento de información activa e inactiva independientemente del medio y el formato, incluido el papel, en las infraestructuras de almacenamiento adecuadas. La protección tiene por objeto salvaguardar la confidencialidad de la información, mantener su integridad y garantizar su disponibilidad a lo largo de todo el ciclo de vida. Requiere la implementación de mecanismos de protección y la evaluación de su efectividad.

De esta forma se conseguirá una gestión de la información que permita la toma de decisiones mediante el intercambio de información dentro y fuera del Ministerio. A continuación, se detalla cada etapa:

1. Recopilación, creación o generación. El Ministerio de Defensa recopila, crea y genera información de cualquier fuente, formato o medio. La información puede ser recopilada, creada o generada por individuos u/y organismos, tanto civiles como militares. La información se recopilará, creará o generará de acuerdo con el marco y los planes de gestión de la información aplicables.

2. Organización. Para compartir, usar y reutilizar la información, esta debe organizarse de una forma estandarizada que permita que la información sea accesible y fácil de encontrar, protegiéndola del acceso no autorizado. La información debe ser fácil de consultar y recuperar, así como de ser difundida. La organización consta de los siguientes procesos:

a) Clasificación: Consiste en la identificación y estructuración sistemática en categorías, de acuerdo a lo indicado en el Anexo III, de toda la información de Ministerio de Defensa de acuerdo a las funciones y actividades que la originan.

b) Descripción: Implica representar la información y sus niveles de agrupación mediante información estructurada en metadatos que servirán para su localización y uso a lo largo de su ciclo de vida. (ej. Capítulo 3 y Anexo 3 de la Política de Gestión de documentos electrónicos del Ministerio de Defensa).

c) Calificación: Comprende la determinación de la información relevante y la valoración de la información para el establecimiento de los plazos de conservación, acciones de transferencia y eliminación, régimen de acceso y el dictamen de la autoridad calificadora.

3. Recuperación, uso, accesibilidad y transferencia. Esta etapa trata la localización y explotación de la información, para obtener la información correcta por el usuario adecuado, en el momento oportuno y en el formato que permita tomar una decisión informada o la ejecución de una misión asignada. Esta etapa incluye:

a) Optimizar el uso, difusión, intercambio y reutilización de la información garantizando su relevancia, exactitud y autenticidad.

b) Presentar la información en un formato adecuado y utilizable.

c) Asegurar la accesibilidad y la diseminación segura de acuerdo a las directrices y políticas de seguridad y sensibilidad.

4. Baja. La etapa de baja se ocupa de la aplicación de las decisiones tomadas en la tarea de planificación para transferir información de valor permanente a los archivos del Ministerio o destruir información que sólo tenía un valor temporal y ya no es necesaria.

ANEXO II

Jerarquía cognitiva

Para llevar a cabo una correcta gestión de la información y del conocimiento, y poder crear valor añadido a través de la información del Ministerio de Defensa, es necesario en primer lugar establecer un proceso de aprendizaje y asimilación que permita partir de los datos en bruto hasta la capacidad de explotarlos a través de la información contextualizada para obtener una ventaja competitiva.

La gestión de la información debe ir desde la obtención del dato, asegurando su calidad, fiabilidad y no duplicidad, hasta que éste es transformado en información y conocimiento y almacenado para su uso y reutilización cuando sea necesario.

Para evolucionar hacia una organización centrada en el conocimiento, conforme establece la Política CIS/TIC en su artículo 7.5, es necesario aplicar los principios de la presente Estrategia para alcanzar los objetivos señalados, dada la necesidad de llevar a cabo una gestión corporativa de los datos, la información y el propio conocimiento.

El proceso de aprendizaje debe hacerse por medio de la jerarquía cognitiva, que se podría definir como un conjunto de modelos para representar las relaciones aparentemente estructurales entre datos, información, conocimiento y entendimiento.

Se debe identificar, estructurar y categorizar la información empleada en el Ministerio de Defensa para que pueda ser gestionada de una forma centralizada, lógica y eficiente. Esta gestión permitirá organizar la información para su integración de acuerdo a los requisitos de información identificados por los responsables funcionales de cada ámbito. La correcta organización y gestión de la información permitirá obtener productos de información de calidad y ponerlos a disposición de la organización de manera relevante, pertinente y oportuna para incorporarlos a la toma de decisiones.

ANEXO III

Organización de la información

Para llevar a cabo una correcta gestión de la información, es necesario organizar y estructurar la información que se maneja y almacena para poder explotarla de una forma ágil. Para ello, se establecen tres ámbitos de información, seis funciones y diecisiete ámbitos funcionales en el Departamento:

1. Información operativa.

- a) Operaciones: Operaciones militares.
- b) Seguridad: Seguridad militar.

2. Información corporativa.

a) Gestión:

Gestión de Personal.

Gestión Sanitaria.

Gestión Económico Financiera.

Gestión de Infraestructuras.

Justicia Militar.

Gestión Administrativa, Apoyo, Vida y Funcionamiento.

Gestión Logística y de Recursos Materiales.
Gestión TIC.
Gestión Documental y Mensajería.
Enseñanza, Formación y Adiestramiento.

b) Estrategia y relaciones internacionales:

Planeamiento, Control y Decisión Estratégica.
Apoyo a la Decisión Política y Relaciones Internacionales.

3. Información pública.

a) Cultura e imagen institucional:

Cultura y Publicaciones.
Comunicación e Imagen Institucional.

b) Gestión: Gestión Ambiental.

Este cuadro de clasificación podrá sufrir modificaciones.

ANEXO IV

Abreviaturas y acrónimos

AG CIS/TIC: Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa.

AGE: Administración General del Estado.

CESTIC: Centro de Sistemas y Tecnologías de Información y Comunicaciones.

CIO: Director de Sistemas y Tecnologías de Información y Comunicaciones (en inglés, Chief Information Officer).

CIS: Sistemas de Información y Telecomunicaciones (en inglés, Communications and Information Systems).

CMAD: Comisión Ministerial de Administración Digital (CMAD).

CORA: Comisión para la Reforma de las Administraciones Públicas.

CPCMAD: Comisión Permanente de la Comisión Ministerial de Administración Digital.

ENI: Esquema Nacional de Interoperabilidad.

ENS: Esquema Nacional de Seguridad.

FAS: Fuerzas Armadas.

MINISDEF: Ministerio de Defensa.

OTAN: Organización del Tratado del Atlántico Norte (en inglés, NATO).

SEGINFO: Seguridad de la Información.

TIC: Tecnologías de la Información y la Comunicación.

ANEXO V

Referencias normativas

Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, desarrollada mediante el Decreto 242/1969, de 20 de febrero, y modificada por la Ley 48/1978, de 7 de octubre, Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada. 2016

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

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

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Comisión para la Reforma de las Administraciones Públicas (CORA), creada por Acuerdo de Consejo de Ministros de 26 de octubre de 2012.

Agenda Digital para España, aprobada por Acuerdo de Consejo de Ministros de 15 de febrero de 2013.

Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos.

Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Estrategia TIC (Plan de Transformación Digital de la AGE y sus Organismos Públicos, aprobada en CM de 2 de octubre de 2015.

Orden DEF/2071/2015, de 5 de octubre, por la que se regula la Comisión Ministerial de Administración Digital (CMAD) del Ministerio de Defensa.

Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

Instrucción 64/2015, de 7 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas de seguridad de la información para la elaboración, clasificación, cesión, distribución y destrucción de información del Ministerio de Defensa.

Instrucción 53/2016, de 24 de agosto, 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.

Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa.

Orden ministerial 5/2017, de 9 de febrero, por la que se aprueba la Política de gestión de documentos electrónicos del Ministerio de Defensa.

Normativa de la Oficina Nacional de Seguridad para la protección de la información clasificada. 2016.

C-M (2007)0118, NATO Information Management Policy (NIMP) de 28 de enero de 2008.

C-M (2008)0113, The Primary Directive on Information Management (PDIM) de 18 de diciembre de 2008.