BOD

BOLETÍN OFICIAL DEL MINISTERIO DE DEFENSA

AÑO XXXIX • MARTES, 18 DE ABRIL DE 2023 • NÚMERO 75

SUMARIO

III. — PERSONAL

CVE: BOD-2023-s-075-258
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

ARMADA

EJÉRCITO DEL AIRE Y DEL ESPACIO

CVE: BOD-2023-s-075-259
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

IV. — ENSEÑANZA MILITAR

V. — OTRAS DISPOSICIONES

VI. — ADMINISTRACIÓN DE JUSTICIA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Diseño y Maquetación:
Imprenta del Ministerio de Defensa

CVE: BOD-2023-s-075-260
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Cód. Informático: 2023008656.

Resolución 400/06254/23, de 9 de marzo, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de Desarrollo de Software en el Ministerio de Defensa.

La Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC) del Ministerio de Defensa (MDEF), aprobada mediante la Orden DEF/2639/2015, de 3 de diciembre, establece una visión global y única de los sistemas y tecnologías de la información y las comunicaciones (CIS/TIC) para facilitar su ordenación, coherencia y racionalización, y avanzar hacia una única Infraestructura Integral de Información para la Defensa (I3D). Propugna también la utilización de sistemas normalizados, homogéneos e interoperables, con empleo preferente de productos ya desarrollados en el ámbito nacional o aliado; y la racionalización de los recursos financieros y materiales en materia CIS/TIC para lograr la mejor provisión de servicios al menor coste posible.

Para la normalización técnica de los recursos CIS/TIC del MDEF, la Política CIS/TIC definió un modelo jerarquizado de arquitecturas similar al empleado por la OTAN, donde la Arquitectura Global CIS/TIC, aprobada en la Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, describió a alto nivel las capacidades CIS/TIC necesarias para cumplir la finalidad y los ejes estratégicos marcados por la Política CIS/TIC.

El proceso para la implantación de la I3D se regula en la Instrucción 33/2018, de 6 de junio, del Secretario de Estado de Defensa, por la que se aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS).

El Eje Estratégico 1 del PECIS se centra en el diseño, desarrollo y despliegue de la I3D, considerada como una infraestructura tecnológica que conforma una red privada destinada a los servicios de la defensa y seguridad nacional, dotada de los más altos estándares de calidad, disponibilidad, redundancia, seguridad y resiliencia.

La I3D debe ser una infraestructura en evolución permanente, para integrar nuevas tecnologías que permitan hacer de ella una infraestructura más flexible, escalable, inteligente y resiliente. Este aspecto se recoge como un requisito operativo en la Arquitectura Global CIS/TIC.

En este proceso de adaptación destacan los nuevos enfoques para el desarrollo de software y la aparición de metodologías y tecnologías habilitadoras que permitan un uso más eficiente de los recursos CIS/TIC del MDEF.

Para aprovechar la potencialidad de estas evoluciones tecnológicas y ordenar su aplicación en el Ministerio, es preciso definir una estrategia sobre el desarrollo de software en el marco de las Políticas vigentes (Política CIS/TIC, Política de Seguridad de la Información y del proceso de Transformación Digital), así como del resto del marco normativo de aplicación. En este sentido, destaca la necesidad de contemplar en los desarrollos software las normas relativas a la protección de datos personales, como la normativa relativa a la protección de datos personales, recogidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

En la actualidad, existen prácticas de vanguardia en la industria que permiten reducir el tiempo de entrega de desarrollos software para aportar valor a las organizaciones. Uno de estos enfoques es el conocido como DevSecOps (*Development – Security – Operations)* cuya práctica está siendo impulsada en el marco de las Organizaciones Internacionales de Seguridad y Defensa, en particular la OTAN.

DevSecOps agiliza el proceso de desarrollo de software, simplifica su despliegue e integra los cambios en el código tan pronto como sea posible y con la frecuencia necesaria, y de una forma segura. Su implantación implica también retos, encabezados por un cambio cultural de la organización, reflejado fundamental, pero no exclusivamente, en:

- Necesidad de procesos departamentales maduros, incluidos los operativos.
- Mayor nivel de cualificación del personal técnico.
- Mayores exigencias para la gestión y control de los componentes tecnológicos.
- Unificación de herramientas en todo el Departamento.
- Modificaciones orgánicas que permitan la generación de equipos de trabajo multifuncionales y transversales a las estructuras jerárquicas.

CVE: BOD-2023-075-10396
Verificable en https://sede.defensa.gob.es/acceda/bod

En el contexto actual, en el que los riesgos y amenazas evolucionan a un ritmo cada vez mayor, el despliegue seguro y en plazo de proyectos intensivos de software constituye un gran desafío. Para afrontarlo, se ha generalizado el enfoque DevSecOps para la obtención de software de Defensa. Este hecho también se está produciendo en el área de Defensa, como es el caso de la propia Agencia de Comunicaciones y Sistemas de Información de la OTAN (NCIA), al que se añade el de Estados Unidos y Reino Unido, que han considerado en su estrategia el uso de estos paradigmas de desarrollo software como elemento estratégico.

Otro reciente paradigma de desarrollo de software es el conjunto de metodologías ágiles (conocidas como *Agile*), en las que los requisitos y las soluciones evolucionan gracias al esfuerzo de equipos autónomos y multifuncionales de desarrollo para desplegar un primer «producto mínimo viable» que va mejorándose conforme a las impresiones de los usuarios, con los que establecen relaciones iterativas.

La aplicación de metodologías ágiles en el MDEF requiere de una sólida formación del personal, y un alto nivel de compromiso por parte de los usuarios, a pesar de la movilidad en los destinos que la carrera militar suele imponer; en definitiva, requiere un cambio cultural y tiene un impacto organizativo.

Por otra parte, la utilización de tecnologías como la de nube y de contenedores («contenerización»), permite el impulso y la optimización de recursos para el desarrollo de software en las organizaciones. A pesar de sus ventajas, la aplicación de la tecnología de contenedores supone un reto sobre la infraestructura tecnológica de la organización.

La capacidad de desarrollo software en el Ministerio de Defensa se encuentra distribuida en equipos pertenecientes a los distintos Ámbitos del Departamento, lo que requiere esfuerzos de coordinación y presenta un reto para asegurar la interoperabilidad de las aplicaciones. La diversidad y fragmentación dificultan el mantenimiento y la transferencia de conocimiento, ya que estos equipos utilizan tecnologías dispares y en ocasiones, infraestructuras propias.

A pesar de la existencia de algunas iniciativas globales en el MDEF, como el Marco Estructurado de Desarrollo Unificado de Servicios y Aplicaciones (MEDUSA), que proporciona un entorno unificado para el desarrollo de diferentes aplicaciones y su correcta integración en la infraestructura corporativa del MDEF, la coordinación y metodología de desarrollo de software en el Ministerio no es homogénea y se basa todavía en muchas tareas manuales.

El despliegue de la I3D como plataforma única de nuevos desarrollos impone la necesidad de homogeneizar tecnología, procedimientos y herramientas, con el fin de aumentar la eficiencia y mantener la seguridad durante el ciclo de vida de los servicios.

La Estrategia de desarrollo de software establece la visión general, los principios, objetivos generales y líneas de actuación estratégicas, así como las principales características del modelo de desarrollo de software en el MDEF.

En el ejercicio de la facultad que me confiere el artículo 4 del Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, y la disposición final primera de la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política CIS/TIC, dispongo:

Artículo único. *Aprobación de la Estrategia de Desarrollo de Software en el Ministerio de Defensa.*

Se aprueba la Estrategia de Desarrollo de Software en el Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición transitoria única. *Adaptación de los desarrollos en curso a la Estrategia.*

Para los procesos de desarrollo que se encuentren en curso a la entrada en vigor de esta Estrategia, se analizará caso a caso, y de acuerdo con su prioridad y la urgencia de su satisfacción, la necesidad de reorientarlos para adecuarse a lo regulado en esta Estrategia.

Disposición final primera. *Facultades dispositivas.*

Se faculta al Director del CESTIC para dictar, en el ámbito de sus competencias, las disposiciones oportunas para la aplicación de esta Resolución.

CVE: BOD-2023-075-10397
Verificable en https://sede.defensa.gob.es/acceda/bod

Disposición final segunda. *Entrada en vigor.*

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

Madrid, 9 de marzo de 2023.—La Secretaria de Estado de Defensa, María Amparo Valcarce García.

CVE: BOD-2023-075-10398
Verificable en https://sede.defensa.gob.es/acceda/bod

ESTRATEGIA DE DESARROLLO DE SOFTWARE EN EL MINISTERIO DE DEFENSA

CAPÍTULO I

Disposiciones Generales

Primero. *Finalidad.*

Esta Estrategia tiene por finalidad:

a) Proporcionar la visión general del desarrollo de software en el MDEF, su situación actual en el Departamento y el modelo de futuro que se quiere alcanzar.

b) Determinar los objetivos generales que se persiguen con la implantación de un nuevo modelo de desarrollo de software en el MDEF.

c) Establecer los principios que deben regir y guiar la consecución de los objetivos en relación con el desarrollo de software.

d) Definir las líneas de actuación estratégicas que deben guiar la consecución de los objetivos establecidos.

e) Establecer las principales características del gobierno de la presente Estrategia.

Figura 1. Ideograma de la Estrategia de Desarrollo de Software del MDEF.

Segundo. *Ámbito de Aplicación.*

La presente Estrategia será de aplicación en todos los desarrollos de software para los servicios que formen parte o que se integren en la I3D, que se realicen en el MDEF y sus Organismos Públicos adscritos. Se excluye del ámbito de aplicación, el desarrollo de software que forme parte inherente de sistemas y plataformas de armas.

CAPÍTULO II

Principios, objetivos y líneas de acción

Tercero. *Principios de la Estrategia de desarrollo de software.*

Los principios que regirán el desarrollo de software del Ministerio de Defensa son los siguientes:

a) Alineamiento

El desarrollo de software se alineará con la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (CIS/TIC), la Política de Seguridad de la Información, y la Estrategia de Gestión de la Información y del Conocimiento del MDEF, marco de la Transformación Digital del Departamento.

CVE: BOD-2023-075-10399
Verificable en https://sede.defensa.gob.es/acceda/bod

b) Automatización, estandarización, reutilización

El desarrollo de software estará presidido por la automatización de tareas, la estandarización de soluciones y la reutilización de componentes e información.

c) Eficiencia

El desarrollo de software perseguirá reducir los tiempos de entrega y los costes asociados, manteniendo los estándares de seguridad y calidad requeridos, independientemente de la metodología de desarrollo elegida (tradicional, ágil o híbrida).

d) Seguridad desde el diseño

La Seguridad estará presente en todo el ciclo de vida del desarrollo de software, mediante el cumplimiento del Esquema Nacional de Seguridad, y de cualquier otra normativa que sea de aplicación.

Cuarto. *Objetivos generales.*

Los objetivos generales que se establecen con la Estrategia de desarrollo de software del Ministerio de Defensa son:

a) Aplicar el enfoque DevSecOps, como modelo obligatorio para el ciclo de vida del software en el MDEF. Este paradigma implica la automatización y estandarización de los trabajos, tales como:

- Despliegue continuo (CD).
- Integración continua (CI).
- Controles de calidad y seguridad.
- Instrumentos de gobierno.
- Administración de la infraestructura como código (IaC).

Se impulsará la independización o desacople de las actividades de despliegue respecto de la tecnología de la plataforma donde se realizan.

La aplicación del enfoque de desarrollo DevSecOps en el MDEF debe implicar la estandarización del conjunto de herramientas que controlan todo el ciclo de vida del software (pipeline) con las que implante este paradigma.

b) Implantar la utilización de tecnología de contenerización y de nube, como elementos habilitadores e impulsores de los nuevos enfoques de desarrollo de software.

En el caso de los contenedores, éstos se establecen como obligación para nuevos desarrollos, sólo sujeto a excepciones por razones técnicas o de relación coste-beneficio.

En el caso de la nube, deberá evaluarse qué desarrollos son aptos para su empleo en función de los criterios que se determinen (sensibilidad de los datos, tiempo de respuesta, acreditación, etc.).

c) Introducir las metodologías ágiles en el MDEF. Debido al alto impacto que supone la introducción de metodologías ágiles en el MDEF, inicialmente sólo se aplicará en aquellos proyectos que se consideren más adecuados, hasta que el Departamento haya asumido el cambio cultural necesario para su generalización. Derivado de esta aplicación progresiva, inicialmente predominará la elección de metodologías tradicionales e híbridas para los proyectos de desarrollo de software.

d) Diseñar servicios CIS/TIC o aplicaciones de forma que sean fácilmente modificables, valorando desde la fase inicial del desarrollo el número de componentes en los que se debe dividir. Cada uno de estos componentes debe contener interfaces confiables y estables que eviten fallos involuntarios al desarrollar nuevas funcionalidades y que faciliten la búsqueda y corrección de errores.

e) Centralizar la dirección técnica de los desarrollos y facilitar la descentralización de su ejecución, para optimizar la capacidad disponible y garantizar la coherencia técnica y la seguridad.

La dirección técnica centralizada en el CESTIC se orientará a dos aspectos:

- Mantener la estandarización de procedimientos, herramientas y tecnologías empleadas por el nivel de ejecución descentralizada y materializado por los equipos de desarrollo del MDEF.
- Realizar la validación documental, técnica y de seguridad de los despliegues de servicios en la I3D.

CVE: BOD-2023-075-10400
Verificable en https://sede.defensa.gob.es/acceda/bod

f) Racionalizar los recursos, para proveer los servicios CIS/TIC de una manera más eficiente. Se debe mejorar la capacidad de desarrollo software disponible en el MDEF, optimizando los recursos humanos, económicos, de infraestructura y de tiempo, a través de una estructura funcional y colaborativa y de un conjunto de herramientas comunes.

Quinto. *Líneas de acción estratégicas.*

Las líneas de acción para alcanzar los objetivos expuestos en esta Estrategia son:

a) Evaluar el ciclo de vida actual del desarrollo de software en el MDEF. Se deberá realizar un análisis exhaustivo de la situación actual del desarrollo de software en el Departamento, identificando los equipos de desarrollo, sus procesos y prácticas actuales, así como la recopilación de las herramientas utilizadas. Esta evaluación tendrá como resultado un informe que identifique las debilidades y fortalezas del escenario actual, y proponga las recomendaciones necesarias en el ámbito organizativo, procedimental y tecnológico con el fin de implementar los nuevos paradigmas de desarrollo de software en el MDEF. La elaboración de este informe será responsabilidad de la estructura de gobierno que rige el desarrollo de la presente Estrategia. Entre estas recomendaciones debe indicarse, para los sistemas y servicios legados, la estrategia de evolución tecnológica más adecuada para cada caso.

Contribuye a los Objetivos Estratégicos: a), b) y c).

b) Establecer las guías de referencia tecnológicas y procedimentales para el desarrollo de software en el MDEF, elaborando toda la normativa necesaria. Debe establecerse un marco de referencia común que asegure, entre otros, la calidad de los desarrollos, los estándares de seguridad, su coherencia técnica, la estandarización de procedimientos (roles, actividades, hitos, orquestación de equipos de desarrollo, operación y seguridad, etc.) y que incorpore los criterios de decisión para la aplicación del tipo de metodología más adecuada (tradicional, ágil o híbrida). El CESTIC elaborará la normativa asociada, apoyándose en la Estructura de Gobierno de la presente Estrategia para su validación.

Contribuye a los Objetivos Estratégicos: a), c), d) y e).

c) Implantar una infraestructura para el empleo de los nuevos paradigmas (DevSecOps, nube y contenerización). El CESTIC proveerá la infraestructura disponible para todo el MDEF, como parte de los servicios de la I3D, que permita el despliegue de nuevos servicios basados en las tecnologías de nube y contenerización. Esta infraestructura permitirá la provisión de entornos de desarrollo en modo servicio ("as a Service") para los equipos de desarrollo del MDEF. Además, el CESTIC proporcionará una plataforma unificada, basada en DevSecOps, con el conjunto de herramientas (pipeline) estandarizadas para el desarrollo seguro de software. De este modo, se facilitará la homogeneización y automatización de las actividades necesarias en el Despliegue Continuo y la Integración Continua (CI/CD).

Contribuye a los Objetivos Estratégicos: a), b) e) y f).

d) Impulsar la compartición de componentes de software. Debe incentivarse el intercambio y la reutilización de componentes y patrones de diseño de software, con el fin de evitar silos y servicios gestionados de manera independiente. El uso de estos componentes compartidos permite obtener arquitecturas y configuraciones homogéneas, mejora la escalabilidad, interoperabilidad, seguridad y tiempos de puesta en producción de los desarrollos software. Uno de los aspectos principales para impulsar la reutilización, lo representa el uso de servicios transversales del Departamento (gestión de identidades, interfaces, datos gobernados, etc.).

Contribuye a los Objetivos Estratégicos: d) y f).

e) Potenciar la gestión por procesos y el gobierno del dato en el MDEF. Ambos paradigmas deben guiar la identificación de necesidades de desarrollo de aplicaciones y de reutilización de información de calidad en el MDEF, permitiendo detectar las necesidades transversales del Departamento. Por este motivo, se impulsará el empleo de la plataforma de Transformación Digital del MDEF (ARGO, plataforma de Armonización para la Gestión de la Organización) y su modelo de gobierno.

Contribuye a los Objetivos Estratégicos: e) y f).

f) Crear una Red de Centros de Desarrollo de Software del MDEF. Se definirá un ecosistema de capacidades de desarrollo de software del Departamento sobre la base de unidades, centros, estructuras u órganos existentes con responsabilidad en el desarrollo de software en todos los Ámbitos del Ministerio. El establecimiento de esta red pretende facilitar la sinergia entre los centros, el apoyo mutuo, la optimización de recursos y el alineamiento de iniciativas.

Contribuye a los Objetivos Estratégicos: e) y f).

CVE: BOD-2023-075-10401
Verificable en https://sede.defensa.gob.es/acceda/bod

g) Adaptar la adquisición. Se revisará y se ajustará el proceso de adquisición del MDEF, para proyectos de desarrollo de software, a los elementos que se deriven del desarrollo de la presente Estrategia.

Contribuye a los Objetivos Estratégicos: c) y f).

h) Implementar planes de formación de metodologías DevSecOps, Agile, de la tecnología de contenerización y de nube. La formación del personal interno del MDEF será un elemento clave para que éstos logren una mejor compresión del nuevo modelo de desarrollo de software, así como para que el conocimiento resida dentro del Departamento y no dependa exclusivamente de proveedores externos. Se debe potenciar la gestión del talento, mediante especialización técnica de personal y su desarrollo profesional dentro Ministerio.

Contribuye a los Objetivos Estratégicos: a), b) y c).

CAPÍTULO III

Elementos del modelo de desarrollo de software

Sexto. *Modelo de servicio para el desarrollo software.*

Para diseñar los modelos de servicio de desarrollo de software del MDEF, se establecen varios niveles: de dirección, de ejecución y de gestión.

La dirección funcional será ejercida por los Ámbitos y la dirección técnica por el CESTIC. El nivel de ejecución estará materializado por la Red de Centros de Desarrollo de Software, y el nivel de gestión por la estructura de Gobierno de la presente Estrategia (detallado en su artículo decimosegundo), el cual se integra como impulsor y coordinador de todas las actuaciones.

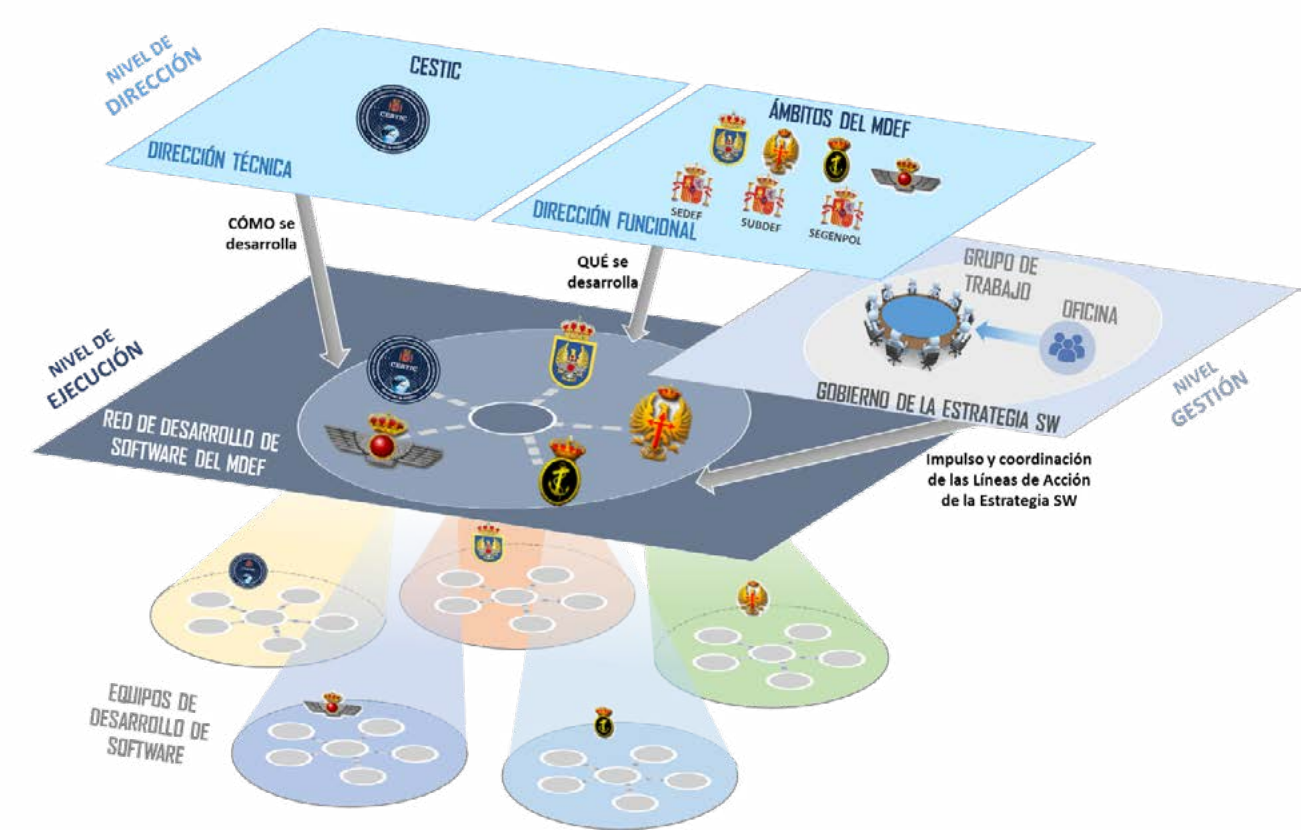

Figura 2. Ideograma de la estructura de desarrollo de software del MDEF.

CVE: BOD-2023-075-10402
Verificable en https://sede.defensa.gob.es/acceda/bod

Con esta premisa, en el MDEF se establecerán dos posibles modelos de servicio:

- Modelo de ejecución descentralizada.

En este modelo, el Ámbito dispone del personal necesario y con la habilitación de seguridad adecuada para llevar a cabo el desarrollo de un nuevo servicio CIS/TIC.

El CESTIC, como proveedor de servicios de la I3D, será el encargado de poner a su disposición los entornos de desarrollo y las herramientas necesarias.

El Ámbito será el encargado de llevar a cabo el desarrollo de su servicio específico. La implementación se realizará siguiendo la estandarización de procedimientos, herramientas y tecnologías que haya emitido el CESTIC.

Para aquellos servicios que se desplieguen en la I3D, el CESTIC será el responsable de validar los desarrollos implementados, según la normativa que se establezca, desde la perspectiva:

· Documental.
· Técnica, referente a la calidad de los activos desarrollados.
· De auditoría de conformidad con las políticas y normas aplicables en materia de seguridad.

- Modelo de ejecución centralizada.

En este modelo, el CESTIC es el encargado de desarrollar los elementos que componen el nuevo servicio. Las herramientas y entornos de desarrollo necesarios serán provistos por el CESTIC.

El CESTIC elaborará la normativa que regule estos modelos de servicios, apoyándose en la Estructura de Gobierno de la presente Estrategia.

Séptimo. *Fases del ciclo de vida de desarrollo de software.*

La utilización de DevSecOps como paradigma obligatorio para el desarrollo de software necesita de una estrecha coordinación entre los equipos de desarrollo, seguridad y operaciones con el fin de alcanzar las prácticas de Integración Continua (CI), Despliegue Continuo (CD) y Seguridad de Código.

Siguiendo este paradigma, se puede descomponer el ciclo de vida del software en ocho fases: planificar, desarrollar, compilar, probar, liberar, desplegar, operar y monitorizar; la seguridad está presente en todas ellas.

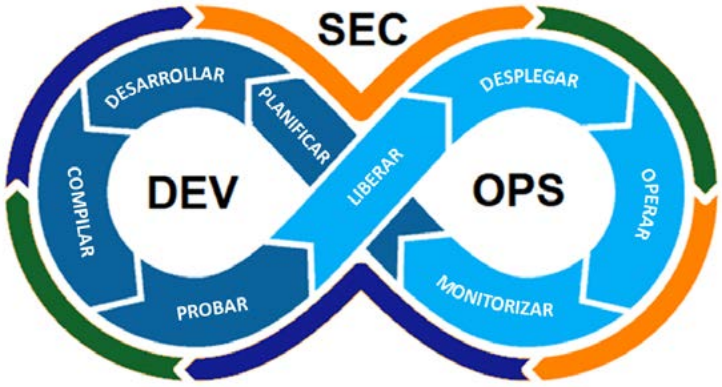

Figura 3. Fases del ciclo de vida de DevSecOps.

Las actividades que componen cada una de estas fases serán estandarizadas y soportadas por el mismo marco metodológico (roles, hitos, entregables, etc.) para todo el MDEF.

La elección de la metodología para el desarrollo de software (tradicional, ágil o híbrida), se establecerá después de una evaluación que incluya al menos los siguientes criterios:

- Disponibilidad del Solicitante del servicio.

CVE: BOD-2023-075-10403
Verificable en https://sede.defensa.gob.es/acceda/bod

- Tipo de alcance y requisitos: claros, maduros y estables o cambiantes.
- Velocidad requerida para la entrega de productos.
- Complejidad del proyecto a desarrollar.
- Disponibilidad de asignación de recursos técnicos.

En caso de que la evaluación técnica determine que puede aplicarse más de una metodología, se utilizará de manera preferente la metodología ágil.

Se establecerá el control de los desarrollos realizados mediante el establecimiento de métricas que supervisen factores de calidad operativos (corrección, fiabilidad, eficiencia, seguridad, facilidad de uso, etc.), de mantenimiento (flexibilidad, facilidad de prueba, de soporte, etc.) y evolutivos (portabilidad, reutilización, interoperabilidad, etc.).

Este proceso de desarrollo de software debe estar integrado con el resto de los elementos del Modelo de Gestión de Servicios CIS/TIC (Catálogo de Servicios, procesos de gestión de la demanda, gestión de cambios, de activos y configuración, etc.) que se establezcan para el MDEF.

El desarrollo normativo que contemple todos estos aspectos del ciclo de vida del desarrollo de software será elaborado por el CESTIC, apoyándose en la Estructura de Gobierno de la presente Estrategia.

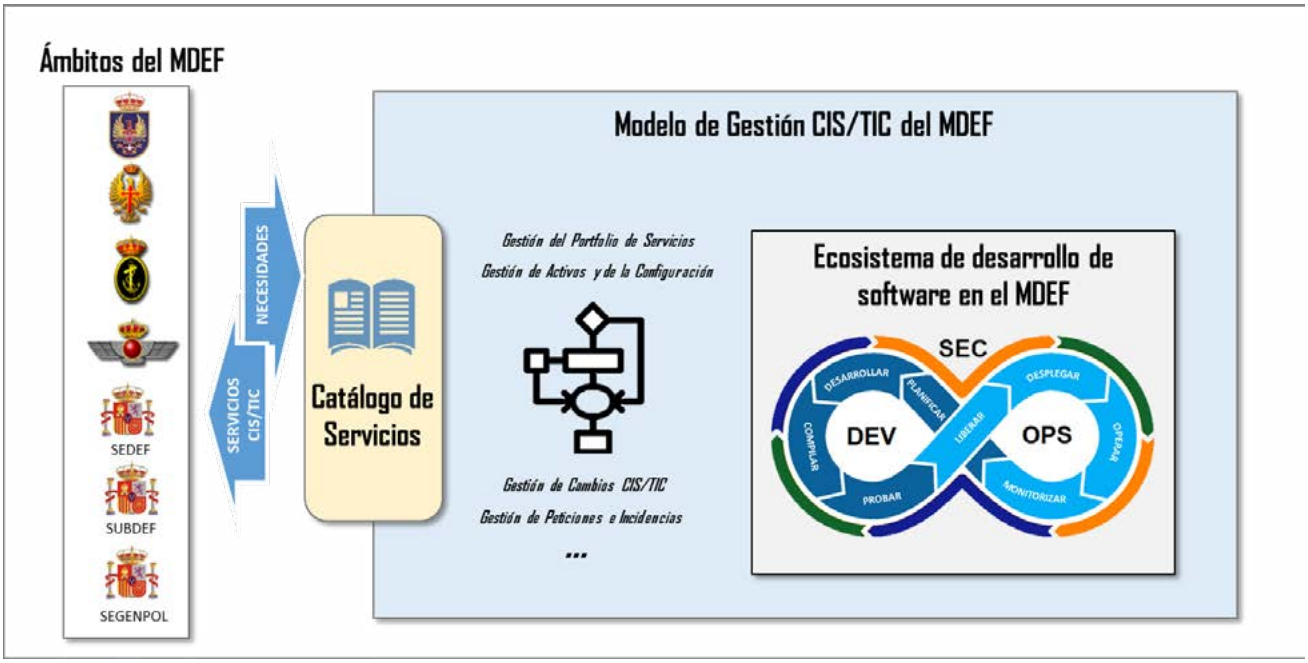

Figura 4. Ideograma de la integración del desarrollo de software y la gestión CIS/TIC en el MDEF.

En todo caso, lo establecido en este apartado, se aplicará teniendo en cuenta lo regulado en el objetivo general del apartado cuarto c.

Octavo. *Seguridad en el proceso de desarrollo de software.*

La Seguridad es un aspecto clave que debe estar alineado con el principio de «seguridad desde el diseño» y la normativa de aplicación existente en el MDEF. Para el desarrollo seguro de software en el MDEF, se establece lo siguiente:

- Integración del cumplimiento de la normativa de seguridad, (tanto interna como externa al Departamento) en el ciclo de vida del desarrollo de software, especialmente el Esquema Nacional de Seguridad (ENS).
- Desarrollo de componentes seguros que sean generales y reutilizables en otros proyectos, en lugar de crear soluciones individuales particularizadas a cada caso.

CVE: BOD-2023-075-10404
Verificable en https://sede.defensa.gob.es/acceda/bod

- Establecimiento de unos estándares mínimos de seguridad para las entregas, mediante la implementación de evaluaciones y auditorías automáticas que controlen el progreso dentro del proceso. Dichas auditorías y evaluaciones de seguridad, serán diseñadas por Órganos de Auditoría Técnica (OAT) certificados por el Centro Criptológico Nacional (CCN).

- Supervisión continua y automatizada, por parte de los equipos de operación de la seguridad del MDEF, para la detección y prevención de riesgos, incidentes y amenazas, acorde al Modelo de Gestión CIS/TIC del MDEF, establecido en la Arquitectura de Referencia de Gestión Única, y teniendo en cuenta, en aquellos aspectos de aplicación, la Arquitectura de Referencia para la Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT).

- Utilizar un ciclo de desarrollo seguro de software que incluya actividades que garanticen su seguridad, tales como las pruebas de penetración, la revisión de código y el análisis de arquitectura.

Adicionalmente, deberán establecerse las acciones para la implantación y acreditación de las herramientas necesarias para llevar a cabo el proceso de desarrollo de software, en concreto, aquellas que componen la plataforma unificada basada en DevSecOps. Dicha acreditación estará basada en las guías CCN-STIC correspondientes y deberá alinearse con el proceso que actualmente están impulsando las Organizaciones Internacionales de Seguridad y Defensa a las que España pertenece, en particular la OTAN.

Noveno. *Herramientas para el desarrollo de software.*

Las actividades del ciclo de vida de desarrollo de software deben estar apoyadas por un conjunto de herramientas CIS/TIC que permitan optimizar los beneficios de los nuevos paradigmas indicados en la presente Estrategia, y que faciliten el mayor grado de automatización del proceso de desarrollo.

El CESTIC, como proveedor de servicios de la I3D, será el responsable de proporcionar estas herramientas en una plataforma unificada de desarrollo. De esta forma, se conseguirá una optimización de los recursos del Departamento, así como una estandarización en el proceso de desarrollo. Se estima que el conjunto mínimo de herramientas necesarias de las que dispondrá la plataforma es:

- Entornos de desarrollo (IDE), para el diseño de aplicaciones de software.
- Repositorio de código, para gestionar y controlar el versionado del código fuente elaborado.
- Herramientas de IaC, para la administración de la infraestructura.
- Orquestador de Integración Continua y de Despliegue Continuo, para la orquestación automática de los flujos de trabajo.
- Repositorio de paquetes de software, para el almacenamiento de los archivos binarios creados después de la compilación del código y de otros activos asociados (archivos de configuración, scripts de implantación, etc.).
- Herramientas de análisis de la calidad del código, para evaluar la calidad del software desarrollado.
- Herramientas de análisis de la seguridad del código, para evaluar las vulnerabilidades y deficiencias de seguridad del software desarrollado.
- Herramienta de gestión de tareas, para facilitar la organización eficaz de las tareas de una persona o de un equipo de trabajo.

Una vez desplegados los desarrollos de software en entornos productivos, se utilizarán los servicios transversales disponibles en el MDEF para la monitorización del correcto funcionamiento de los desarrollos y para la supervisión continua de seguridad.

Décimo. *Gestión del talento y formación.*

El personal del MDEF involucrado en el ciclo de vida del software recibirá formación en los aspectos tecnológicos y metodológicos requeridos para la presente Estrategia (DevSecOps, metodologías ágiles, tecnología de nube, tecnología de contenedores, etc.), con el fin de fomentar el conocimiento dentro del Departamento, tal y como indican los principios de esta Estrategia. Deberá tener reflejo en un plan de gestión del talento y de formación para este personal del MDEF.

CVE: BOD-2023-075-10405
Verificable en https://sede.defensa.gob.es/acceda/bod

CAPÍTULO IV

Desarrollo e Implantación de la Estrategia de Desarrollo de Software y Estructura de Gobierno

Decimoprimero. *Desarrollo e implantación de la Estrategia de Desarrollo de Software.*

Se elaborará un plan de implantación por el Grupo de Trabajo regulado en el apartado decimosegundo, en el que se definirá las actuaciones y proyectos necesarios para desarrollar las líneas de acción establecidas en esta Estrategia, de forma gradual y comenzando con cambios de alcance reducido:

a) Evaluar el ciclo de vida actual del desarrollo de software en el MDEF.
b) Establecer las guías de referencia tecnológicas y procedimentales para el desarrollo de software en el MDEF.
c) Implantar una infraestructura para el empleo de los nuevos paradigmas (DevSecOps, nube y contenerización).
d) Impulsar la compartición de componentes de software.
e) Potenciar la gestión por procesos y el gobierno del dato en el MDEF.
f) Crear una Red de Centros de Desarrollo de Software del MDEF.
g) Adaptar la adquisición.
h) Implementar planes de formación de metodologías DevSecOps, Agile, de la tecnología de contenerización y de nube.

En dicho Plan se identificarán para cada proyecto o actuación:

- Descripción del proyecto o actuación.
- Objetivos.
- Plazos previstos de inicio y consecución.
- Actores implicados y matriz de responsabilidades (RASCI).
- Interdependencia con proyectos de desarrollo del PECIS (o integración en ellos).
- Recursos implicados (humanos, materiales, financieros y formativos).

La ejecución de estos proyectos o actuaciones se adaptará a la evolución en el contexto tecnológico y normativo que afecte al desarrollo de software en el MDEF.

Decimosegundo. *Estructura de Gobierno de la Estrategia de Desarrollo de Software.*

Un Grupo de Trabajo llevará a cabo el desarrollo, seguimiento, coordinación y control de esta Estrategia. Estará compuesto por los siguientes miembros:

a) Presidente: Un Oficial de empleo Teniente Coronel, Capitán de Fragata o funcionario de nivel equivalente, destinado en el CESTIC, designado por el Director de este Centro.
b) Vocales permanentes: representantes de los órganos con responsabilidad en materia CIS/TIC del Estado Mayor de la Defensa, del Ejército de Tierra, la Armada, del Ejército del Aire y del Espacio, y el CESTIC.
c) Secretario: Un oficial o funcionario de nivel equivalente, designado por el Presidente.

Dependerá del Comité de Sistemas de Información del MDEF, en el seno de la estructura de Gobierno CIS/TIC, y en los casos que se considere oportuno, informará a otros órganos de la estructura de gobierno CIS/TIC, de la estructura de gobierno de la Seguridad de la Información y de la estructura de gobierno para la Transformación Digital (como la Comisión Permanente de la Comisión Ministerial para la Administración Digital -CPCMAD-).
El GT propondrá el plan de implantación al Comité de Sistemas de Información del MDEF.
En función de los asuntos concretos a tratar, se podrá convocar a representantes de los Ámbitos del MDEF para evaluar la aplicabilidad de los trabajos realizados en su actividad. En caso de ser necesaria la coordinación con actores externos al Ministerio, se podrá contar con la participación de personal de empresas, universidades centros de investigación, etc.

CVE: BOD-2023-075-10406
Verificable en https://sede.defensa.gob.es/acceda/bod

Como soporte técnico-operativo del Grupo de Trabajo, se establecerá una Oficina de apoyo, dotada con personal especialista del CESTIC. Este personal tendrá una dedicación de apoyo principal a la Oficina y dispondrá de conocimientos en diferentes disciplinas del desarrollo de software (metodologías, herramientas, calidad, arquitectura, etc.).

El Grupo de Trabajo se constituirá en un plazo no superior a tres meses desde la entrada en vigor de esta Estrategia y se reunirá con carácter periódico. La Oficina de apoyo, por sus requerimientos técnicos y competenciales, se constituirá en un plazo no superior a dos meses desde la fecha de constitución del Grupo de Trabajo.

CVE: BOD-2023-075-10407
Verificable en https://sede.defensa.gob.es/acceda/bod