



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Hacia una gobernanza CIS/TIC efectiva en el Ministerio de
Defensa: Aplicación del marco COBIT y herramientas ITSM para la
gestión de servicios*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Antonio Rafael Murillo Martínez

DIRECTORES: Miguel Ángel Ares Tarrío

Milagros Fernández Gavilanes

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Hacia una gobernanza CIS/TIC efectiva en el Ministerio de
Defensa: Aplicación del marco COBIT y herramientas ITSM para la
gestión de servicios*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

Actualmente el Ministerio de Defensa está apostado activamente por la implantación de un modelo de alto nivel de gestión única de servicios CIS/TIC en el CESTIC, tomando como marco de referencia la metodología COBIT y utilizando la herramienta ITSM, ProactivaNet, para la implantación de la gestión por procesos.

En este marco, el presente TFM se propone varios objetivos fundamentales: En primer lugar, realizar un análisis de la implantación del modelo de gestión única de servicios CIS/TIC en el Ministerio, evaluando su eficacia y eficiencia. Este análisis incluirá una medición del rendimiento de los procesos utilizando el marco proporcionado por COBIT. Además, se formularán propuestas de mejora para fortalecer el gobierno de las TIC dentro del Ministerio.

Así mismo, el TFM se centrará en evaluar el despliegue de la herramienta ProactivaNet de gestión por procesos, analizando su efectividad y su contribución a la optimización de los mismos.

Por último, se llevará a cabo una comparativa detallada entre varias herramientas ITSM de software libre, con el objetivo de proporcionar una evaluación comparativa del rendimiento de ProactivaNet en relación con otras soluciones disponibles en el mercado.

Este enfoque integral permitirá una comprensión más profunda de la implementación y el impacto de las TIC en el Ministerio de Defensa, así como proporcionar recomendaciones concretas para mejorar la gestión y desempeño de gobierno TIC y la gestión de servicios en este ámbito.

PALABRAS CLAVE

Gestión de Servicios TI, ITSM, COBIT, ITIL, Monitorización de Servicios TI, Acuerdos de Nivel de Servicio (SLA), Operación de Servicios, Cuadros de Mando.

AGRADECIMIENTOS

A mi madre, por su apoyo incondicional a lo largo de mi vida.

A D. Miguel Ángel Ares Tarrío, por su orientación y consejo en la redacción de este trabajo.

A mis compañeros del Master, por su compañerismo y los buenos momentos vividos en Marín.

Al Comandante Richarte, por cambiar el Ejército con su magia.

Al Tcol. Blesa y al CF Iglesias, por ser los hermanos mayores que no he tenido.

Al Coronel García, por permitirme estar escribiendo estas líneas y enseñarme a ser un soldado.

A Su Majestad el Rey Don Felipe VI, por su confianza en el Cuerpo de Ingenieros Industriales del Estado y en nuestra aportación a la defensa de España.

A las Fuerzas Armadas, por todo lo que me han ofrecido, y que me muestren lo que esperan de mi a partir de ahora.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos	5
2 Estado del arte	7
2.1 La transformación digital en las administraciones públicas	7
2.2 La transformación digital en el Ministerio de Defensa	8
2.2.1 Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) ..	11
2.2.2 Infraestructura Integral de Información para la Defensa (I3D)	13
2.2.3 La Transformación Digital del MDEF en época reciente.....	13
2.2.4 Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC (AR GES CIS/TIC) ...	14
2.2.5 Catálogo de Servicios:	17
2.2.6 Centro de Gestión de Servicios CIS/TIC	17
2.2.7 Centro de Atención al Usuario CAU	18
2.2.8 Herramientas de monitorización de infraestructura TI	19
2.2.9 Cuadro de Mando (Dashboard)	20
2.2.10 Acuerdos de Nivel de Servicio (SLA)	21
2.2.11 Herramientas de observabilidad de datos	21
2.2.12 Capacidades del MDEF en materia CIS/TIC.....	22
2.3 Estándares y Marcos de Referencia para la gestión de servicios TI	27
2.3.1 Biblioteca de Infraestructura de Tecnologías de Información (ITIL).....	27
2.3.2 Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT) ..	29
2.3.3 Gestión de Servicios de Tecnologías de la Información (ITSM)	36
2.3.4 Relación entre los marcos ITIL, COBIT, DevOps e ITSM	40
3 Desarrollo del TFM	41
3.1 Alcance del desarrollo.....	41
3.2 Implantación de un Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF	42
3.2.1 Marco normativo de gestión:	46
3.2.2 TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D	46
3.2.3 Instrucción Técnica 04/24 del CESTIC Puesta en Operación de Nuevos Servicios en el Ámbito del CESTIC	48

3.2.4 Acuerdo de Provisión de Servicio 01/24 del CESTIC sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC.....	51
3.3 Monitorización de la infraestructura de I&T.	54
3.3.1 Recomendaciones para el Centro de Atención al Usuario (CAU) del CESTIC respecto la definición de métricas para evaluar su rendimiento:.....	59
3.3.2 Cuadro de Mando Integral de Monitorización.....	59
3.4 Herramienta única ITSM (ProactivaNet).....	68
3.5 Comparativa entre herramientas ITSM.....	78
3.5.1 Comparativa de la herramienta ProactivaNet:.....	80
3.5.2 Recopilación de información para el estudio comparativo:	80
3.5.3 Comparativa entre herramientas:.....	85
4 Resultados	88
5 Conclusiones y líneas futuras	90
5.1 Conclusiones	90
5.2 Líneas futuras	90
6 Bibliografía.....	94
Anexo I: CUESTIONARIO PARA ENTREVISTA CON RESPONSABLE DEL CENTRO DE ATENCIÓN AL USUARIO CAU SOBRE LA IMPLEMENTACIÓN DE LA HERRAMIENTA PROACTIVANET	96

ÍNDICE DE FIGURAS

Figura 2-1 Esquema del modelo de infraestructuras CIS/TIC de la I3D en el MDEF (Fuente: Presentaciones corporativas del CESTIC, MDEF).....	13
Figura 2-2 Integración entre el CEGES I3D y resto de capacidades mediante el Catálogo de Servicios (Fuente: Presentaciones corporativas del CESTIC, MDEF).....	18
Figura 2-3 Ejemplo de panel de visualización construido con la herramienta Grafana (13)	22
Figura 2-4 Contexto Operativo de las Capacidades del Ministerio de Defensa (7)	23
Figura 2-5 Relación entre las Capacidades de Gestión y resto de capacidades en el Ministerio de Defensa (7).....	24
Figura 2-6 Taxonomía de Capacidades CIS/TIC del Ministerio de Defensa (7)	25
Figura 2-7 Taxonomía de Capacidades de Gestión CIS/TIC (7)	26
Figura 2-8 Capacidades de Gestión y objeto que se desarrollan en la AR (7)	26
Figura 2-9 Representación de metas aplicables y métricas modelo (15)	31
Figura 2-10 Procesos de Gobierno del modelo Core de COBIT (15).....	31
Figura 2-11 Procesos de Gestión del modelo Core de COBIT (15).....	32
Figura 2-12 Presentación del Componente de Procesos del modelo Core de COBIT (15)	33
Figura 2-13 Niveles de Capacidad para los Procesos (15).....	34
Figura 2-14 Componente: flujos y elementos de información (15)	35
Figura 2-15 Ciclo de vida de Gestión de Servicios propuesto por ITSM	37
Figura 3-1 Ciclo de vida de Gestión de Servicios propuesto por ITSM (Fuente: Elaboración propia)	42
Figura 3-2 Representación idealizada de un Cuadro de Mando en formato velocímetro con información sobre áreas clave de mantenimiento para un Centro de Procesamiento de Datos (CPD) (Fuente elaboración propia)	62
Figura 3-3 Esquema de arquitecturas de monitorización automática existentes en el CESTIC, generadoras de eventos a registrar en un único repositorio, así como el área de supervisión a la que pertenecen: Infraestructura, Servicios o Seguridad. (Fuente elaboración propia)	66
Figura 3-4 Esquema de roles propuesto para la administración de ProactivaNet (Fuente: Elaboración propia)	74
Figura 3-5 Ejemplo de Panel informativo generado por ProactivaNet con diversa información sobre servidores y PCs. Nótese que alguna información ha sido eliminada por motivos de seguridad. (Fuente ProactivaNet)	87
Figura 5-1 Ejemplo de información presentada por la interfaz de ProactivaNet a los responsables de la resolución de incidencias del CAU (Fuente: ProactivaNet y elaboración propia).....	92

ÍNDICE DE TABLAS

Tabla 2-1 Identificación de la situación actual y objetivo a través del modelo de gestión única de servicios. (7).....	16
Tabla 3-1 Identificación de la situación actual y objetivo del CESTIC en relación al modelo para el gobierno y la gestión única de servicios. Fuente (7) y elaboración propia.	43
Tabla 3-2 Fases, procesos estandarizados de gestión y efectos a alcanzar por el MDEF. (7)	45
Tabla 3-3 Lista de actividades asociadas a la Práctica de gestión: APO05.04 Mantener los portafolios. (16).....	48
Tabla 3-4 Lista de actividades asociadas a la Práctica de gestión: APO09.03 Definir y preparar acuerdos de servicio. (16)	52
Tabla 3-5 Lista de actividades asociadas a la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T. (16).....	56
Tabla 3-6 Identificación de la situación actual y objetivo para las actividades previstas en la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T. (Fuente: Elaboración Propia)	58
Tabla 3-7 Componente C: Flujos y elementos de información para la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T (16).....	58
Tabla 3-8 Herramientas de monitorización disponibles para cada centro de datos del CESTIC (Fuente: Elaboración Propia)	63
Tabla 3-9 Situación actual y objetivo con la implementación de ProactivaNet en el CESTIC (Fuente: Elaboración propia).....	70
Tabla 3-10 Recopilatorio de las dimensionas valoradas favorablemente de ProactivaNet en el foro TI de Gartner. (Fuente: (18) y elaboración propia).....	81
Tabla 3-11 Recopilatorio de las dimensionas valoradas desfavorablemente de ProactivaNet en el foro TI de Gartner. (Fuente: (18) y elaboración propia).....	81
Tabla 3-12 Recopilatorio de las dimensionas valoradas favorablemente de ProactivaNet en el foro TI de Capterra. (Fuente: (19) y elaboración propia)	82
Tabla 3-13 Recopilatorio de las dimensionas valoradas desfavorablemente de ProactivaNet en el foro TI de Gapterra. (Fuente: (19) y elaboración propia)	83
Tabla 3-14 Tabla de coincidencias de opiniones favorables entre usuarios gestores de la herramienta ProactivaNet externos al CESTIC y la opinión de usuarios gestores de la herramienta pertenecientes al CAU del CESTC (Fuente: elaboración propia)	84
Tabla 3-15 Tabla de coincidencias de opiniones desfavorables entre usuarios gestores de la herramienta ProactivaNet externos al CESTIC y la opinión de usuarios gestores de la herramienta pertenecientes al CAU del CESTC (Fuente: elaboración propia).....	84
Tabla 3-16 Tabla comparativa entre herramientas ITSM (Fuente: (18), (19), (14)y elaboración propia).....	86

1 INTRODUCCIÓN Y OBJETIVOS

En un contexto de creciente digitalización y modernización de las administraciones públicas, el Ministerio de Defensa (MDEF) enfrenta el desafío de implementar una gobernanza eficiente y una gestión integral de los sistemas y tecnologías de la información y las comunicaciones (CIS/TIC). Este Trabajo de Fin de Máster (TFM) se enmarca dentro de este escenario de transformación digital, y tiene como principal propósito analizar la aplicación del marco COBIT y las herramientas ITSM como pilares para una gobernanza TIC eficaz en el MDEF. Con esta premisa, se busca contribuir al fortalecimiento de los procesos de gestión, alineándolos con los objetivos estratégicos del Ministerio.

Este Trabajo Fin de Máster (TFM) se ha desarrollado en un contexto de intensa actividad en el Ministerio de Defensa marcado por el impulso de la transformación digital y la modernización en la gestión de servicios TI. Este proceso incluye la definición de un nuevo marco normativo y la adopción de herramientas avanzadas de gestión de servicios.

La oportunidad y relevancia de este contexto han sido las principales motivaciones para orientar el TFM hacia estas áreas, integrando la aplicación del marco COBIT y herramientas ITSM para garantizar un enfoque técnico, estructurado y alineado con las mejores prácticas internacionales.

Este trabajo busca aportar un enfoque práctico y útil que permita fortalecer la gobernanza y el despliegue efectivo de los servicios. En un momento crucial para el MDEF como el actual, las contribuciones derivadas de un trabajo de estas características tienen un alto potencial de ser consideradas e implementadas, facilitando un despliegue efectivo y eficiente del marco y servicios referidos, representando una gran contribución a los objetivos del MDEF.

En el desarrollo del trabajo se plantean 4 objetivos fundamentales:

- En primer lugar, evaluar la implantación del modelo de gestión única de servicios CIS/TIC en el MDEF bajo el marco COBIT, a través del estudio del marco normativo aprobado a tal efecto.
- En segundo lugar, se presenta una propuesta para la monitorización de la infraestructura TI, como base para la medición y mejora de la calidad de los servicios TI prestados.
- En tercer lugar, se analiza el impacto del despliegue de la herramienta ITSM ProactivaNet como instrumento clave para la gestión por procesos, considerando su capacidad para mejorar la operatividad y el rendimiento de los servicios TIC; y se formulan propuestas para lograr una implementación efectiva de la herramienta en el MDEF.
- Finalmente, se realiza una comparativa entre diversas herramientas ITSM, con el objetivo de posicionar ProactivaNet frente a otras alternativas del mercado. Estas metas permiten un enfoque integral que no solo examina el estado actual, sino que también sienta las bases para futuras mejoras en la gobernanza y gestión TIC.

Organización de la memoria:

La memoria de este TFM presenta la siguiente estructura:

- Un primer capítulo introductorio, en el que se encuentra el lector.
- El segundo capítulo dedicado al Estado del Arte, tiene por objeto introducir los conceptos cuyo conocimiento será necesario para comprender, con posterioridad, del desarrollo del trabajo. Presenta tres subapartados:
 - El primero dedicado a la Transformación Digital en las Administraciones Públicas.
 - Un segundo subapartado que pone el foco en la Transformación Digital del Ministerio de Defensa, introduciendo los desarrollos normativos pasados, que han llevado al punto de partida de inicio de este Trabajo de Fin de Master.

- o Por último, un subapartado dedicado a los Estándares y Marcos de Referencia más importantes en la gestión de servicios TI, centrándose en la exposición en los más relevantes para el desarrollo de este trabajo (ITIL, COBIT e ITSM) y finalizando el apartado con una aclaración sobre las relaciones que se establecen entre los mismos.

- El tercer capítulo se focaliza en el desarrollo del TFM, e incluye las aportaciones personales del trabajo en las áreas objeto de estudio: El desarrollo del Modelo de Gestión de Servicios único para proporcionar Capacidades de Infraestructura de Información al Ministerio de Defensa, el establecimiento de una infraestructura de monitorización de TI para la supervisión de la gestión y evaluación de la eficiencia en la gestión de servicios, el estudio de la incorporación de la herramienta ITSM ProactivaNet al modelo para la gestión única de servicios del CESTIC, y para finalizar una evaluación entre herramientas ITSM con el propósito de determinar si la elección de ProactivaNet ha sido acertada para los propósitos del Ministerio de Defensa en este ámbito.

- En el cuarto capítulo se muestran los resultados logrados por el autor con este TFM en particular, y el Ministerio de Defensa con la implantación de un modelo único de gestión de servicios, en general.

- El quinto capítulo se dedica a las conclusiones del trabajo y a una serie de propuestas sobre cómo podría completarse este trabajo con una serie de líneas de actuación futuras en las distintas áreas desarrolladas en el contenido.

- El sexto capítulo está dedicado a la bibliografía.

- En último lugar, se incluye un anexo con el cuestionario seguido para la realización de la entrevista sobre la implementación de la herramienta ITSM ProactivaNet a los técnicos y responsables del Centro de Atención al Usuario (CAU) del CESTIC.

2 ESTADO DEL ARTE

2.1 La transformación digital en las administraciones públicas

Las llamadas Tecnologías de la Información y la Comunicación (en adelante TIC) son el conjunto de recursos y herramientas que se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos, como: ordenadores, teléfonos, televisores, etc.

En las últimas décadas, las TIC han transformado la sociedad. Los ciudadanos han adquirido nuevos hábitos y expectativas en la utilización de los servicios digitales, en su vida profesional y personal, actividades de ocio y en su relación con las Administraciones Públicas.

El verdadero impulso a la Administración electrónica en España lo dio la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos. Esta ley supuso la obligación para la Administración de introducir los medios electrónicos en las distintas fases de los procedimientos administrativos que implicaran una interacción con el ciudadano.

Pero mientras las Administraciones Públicas iban recorriendo ese complejo camino, el mundo TIC alumbraba otro concepto que ahora está en pleno apogeo: La Transformación Digital.

La Unión Internacional de Telecomunicaciones (UIT)¹ define la transformación digital como "el proceso de aprovechar las tecnologías digitales para reformar modelos de negocio, procesos, actividades y competencias, de manera que las organizaciones se adapten y respondan de manera más efectiva a las necesidades cambiantes del mercado, mejoren su rendimiento y optimicen sus recursos." Este proceso no solo incluye la adopción de nuevas tecnologías, sino también un cambio cultural dentro de la organización para fomentar la innovación, la agilidad y la orientación al cliente.

La transformación digital de la sociedad y la economía representan un reto que requiere de la implicación de todos: administraciones, empresas y ciudadanía. Este proceso esencial del siglo XXI supone la adopción y aplicación de tecnologías digitales en todos los ámbitos de la sociedad, incluyendo la economía, la educación, la Administración pública y la vida cotidiana, tal como describe el *Libro Blanco de la Digitalización* (1)

El Libro Blanco España Digital 2026 (2) contempla el proceso de transformación digital como una de las palancas principales de innovación tecnológica, desarrollo empresarial, modernización económica y progreso social.

En este nuevo contexto, la Administración Pública debe ser capaz de adaptarse de un modo ágil a estas nuevas demandas, proporcionando información y servicios digitales en cualquier momento, en cualquier lugar y por diferentes canales.

Para llevar a término esta transformación digital en la AGE, se aprobó el Plan de Transformación Digital de la AGE y sus organismos Públicos (PTD-AGE) 2015-2020 conocida como Estrategia TIC, y se promulgaron dos importantes normas la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas, que derogó la ley 11/2007; y la Ley 40/2015 de Régimen Jurídico del Sector Público, que pretenden convertir la Administración Pública en una «Administración Electrónica» a través de la generalización del uso de los medios electrónicos en el quehacer diario de la Administración.

¹ Organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Como resultado de estas medidas, se ha producido una importante inversión en la digitalización de las administraciones públicas que ha situado a España en el 2º puesto en la UE en materia de servicios públicos digitales, de acuerdo con el Índice DESI² del año 2020.

La situación excepcional generada por la pandemia de la Covid-19 ha puesto de manifiesto la urgencia y necesidad de desarrollar una Administración digital que pueda responder a las necesidades de los ciudadanos de una forma más ágil y efectiva.

En este contexto, en 2021 el Consejo de Ministros ha aprobado el Plan de Digitalización de las AAPP (2021-2025), segunda Estrategia TIC, enmarcado dentro de la Estrategia España Digital 2025.

Entre los objetivos del Plan destacan mejorar la accesibilidad de los servicios públicos a los ciudadanos y empresas, superar las brechas digitales sociales y territoriales e impulsar la eficiencia de las administraciones públicas mediante la digitalización de importantes ámbitos tractores como la Sanidad, la Justicia, o las políticas de Empleo...

Para responder a este desafío sin precedentes, el Gobierno de España lanzó en julio de 2020 la agenda España Digital, concebida como la hoja de ruta para impulsar el proceso de transformación digital del país. Esta agenda comprende diez ejes estratégicos. El número 5 está dedicado a la transformación Digital del Sector Público.

2.2 La transformación digital en el Ministerio de Defensa

El Ministerio de Defensa (en adelante MDEF), al igual que toda la Administración General del Estado (en adelante AGE) han de ofrecer el mejor servicio posible a la sociedad española.

Para ello el MDEF y las Fuerzas Armadas (en adelante FAS) tienen que avanzar en su digitalización, tanto en el ámbito operativo como en el funcional o administrativo; procurando que todos sus procesos y actividades, tanto internos de un órgano, como externos a él, que relacionen varios órganos o a estos con entes externos a la administración, como ciudadanos o empresas, estén digitalizados y soportados por software.

La transformación digital a acometer por el MDEF implica un cambio cultural y en el funcionamiento de las organizaciones basado en la gestión por procesos y en la orientación al dato, añadiendo como tercer elemento un importante soporte de servicios TI.

Actualmente el MDEF está apostado activamente por la implantación de un modelo de alto nivel de gestión única de servicios CIS/TIC³ tomando como marco de referencia la metodología COBIT⁴ y utilizando la herramienta ITSM⁵, ProactivaNet, para la implantación de la gestión por procesos; que serán objeto de estudio del presente TFM.

Estos retos presentes son el resultado de una evolución por parte del MDEF en su proceso de transformación digital, que tuvo su germen con la entrada en vigor del **Plan Director de Sistemas de Información y Telecomunicaciones** del año 2002, aunque en aquel momento el concepto "transformación digital" no aparecía explícitamente contemplado en la normativa.

² El Índice de Economía y Sociedad Digital (DESI o Digital Economy and Society Index) es un índice compuesto que resume cinco indicadores del rendimiento digital de Europa y que permite un seguimiento de la evolución de los Estados miembros de la Unión Europea en la competitividad digital.

³ El MDEF utiliza la nomenclatura "servicios CIS/TIC" para referirse a la totalidad de servicios relacionados con los Sistemas de Información y Comunicaciones (CIS, por sus siglas en inglés: Communication and Information Systems) y las Tecnologías de la Información y la Comunicación (TIC)

⁴ COBIT es un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de la información (TI) en una organización, y que se analizará con mayor detalle a continuación.

⁵ ITSM es un marco de gestión de servicios de TI que proporciona servicios para varias funciones de TI, y que se analizará con más detalle a continuación.

Este plan representó un primer esfuerzo formal y estructurado para modernizar las capacidades tecnológicas del Ministerio, sentando las bases para los avances posteriores en digitalización y gestión TIC.

El Plan Director representó la primera estrategia integral de TIC en el ámbito de la defensa, planteando la necesidad de centralizar, racionalizar y modernizar la infraestructura TIC. Así mismo, el Plan introdujo una visión más organizada de los sistemas de información y comunicaciones, fomentando una gestión más estratégica de las tecnologías e introduciendo las bases para la transformación digital, al sentar las bases de la interoperabilidad y la unificación tecnológica, que son pilares clave de la transformación digital actual.

Con este plan se lograron notables avances en el empleo de las TIC en el MDEF. Sin embargo, no se alcanzaron todas las Capacidades CIS/TIC⁶ esenciales ni se logró unificar la Red Global de Telecomunicaciones (RGT). Por otro lado, en lo referente a Arquitecturas CIS/TIC los sistemas en servicio no siguieron un modelo homogéneo de desarrollo.

Tradicionalmente, las redes del MDEF presentaban una gran heterogeneidad de redes de telecomunicación (WAN y LAN), plataformas de información (CPDs y equipos de sistemas de información) y equipamiento de usuario que participan los procesos TIC de Defensa. A esto se sumaba la variedad de grados de madurez y obsolescencia tecnológica de los distintos componentes de la Red y los Sistemas de Información, lo que dificulta la operación de los sistemas y limitaba la prestación efectiva de los servicios finales. Esta casuística aparece descrita de esta manera en el Trabajo del Master DIRETIC dedicado a la Infraestructura Integral de Información para la Defensa. (3)

Además, en este escenario existen medios CIS/TIC propios del Ministerio de Defensa y otros medios y servicios CIS/TIC contratados de forma separada por otros componentes del Ministerio, como la Secretaría de Estado de Defensa (SEDEF), el Estado Mayor de la Defensa (EMAD), los Ejércitos y la Armada.

El inicio de la transformación digital propiamente dicha del Ministerio de Defensa español en términos de normativa y planificación se puede situar en torno a la aprobación 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; con el que se pretendía el desarrollo y la ejecución de un modelo común de gobernanza de las Tecnologías de la Información y las Comunicaciones (TIC) en la Administración General del Estado y sus Organismos Públicos.

Este decreto supuso:

- Impulsar la creación de una estrategia TIC común para toda la AGE, lo que incluye a todos los ministerios, y que garantice el uso adecuado de los recursos informáticos de acuerdo a las necesidades derivadas de la estrategia general del Gobierno, con el fin de mejorar la prestación de los servicios públicos al ciudadano. Se concretaría en el Plan de Transformación Digital de la AGE y sus organismos Públicos (PTD-AGE) 2015-2020.
- Establece la obligación de desarrollar planes de acción específicos por cada ministerio, que representen la materialización de la estrategia, sentando las bases para el diseño del Plan de Acción para la Transformación Digital del Ministerio de Defensa.
- Establece la obligación de que cada ministerio creará una Comisión Ministerial de Administración Digital (CMAD) como órgano colegiado responsable del impulso y coordinación en materia de Administración Digital en sus respectivos departamentos, de elaborar estos planes de acción

⁶ Las capacidades en materia CIS/TIC se refieren a las capacidades requeridas por el MDEF en esta materia, para llevar a cabo con éxito las Misiones y Operaciones. Se hará referencia más detallada posteriormente.

sectoriales de transformación digital y del seguimiento de las actuaciones de la Estrategia TIC de la AGE.

- Introduce principios de interoperabilidad, eficiencia y seguridad como objetivos prioritarios en el uso de las TIC.

El **Plan de Transformación Digital de la AGE y sus organismos Públicos (PTD-AGE) 2015-2020** conocido como Estrategia TIC del año 2015, constituye el marco estratégico global para avanzar en la Transformación Digital de la Administración, estableciendo cinco objetivos estratégicos para el desarrollo gradual de la Administración Digital:

- 1) Incremento de la productividad y la eficacia.
- 2) El canal digital ha de ser el medio preferido por ciudadanos y empresas para relacionarse con la Administración.
- 3) Mayor eficiencia en la prestación de los servicios TIC en el seno de la Administración.
- 4) Gestión corporativa inteligente del conocimiento, la información y los datos.
- 5) Estrategia corporativa de seguridad y usabilidad.

La Estrategia TIC de 2015 y el Real Decreto 806/2014 sirvieron de marco para el desarrollo de un proceso de gran actividad legislativa en el MDEF que se concretaría en las siguientes disposiciones:

- La Orden DEF/2071/2015, de 5 de octubre, por la que se regula la **Comisión Ministerial de Administración Digital del Ministerio de Defensa**, establece el Plan de Acción del Ministerio de Defensa para la Transformación Digital, dividido en dos planes complementarios que comprenderán las actuaciones en materia de Administración Digital, Tecnologías de la Información y Comunicaciones a desarrollar en el conjunto del Departamento y sus organismos públicos adscritos.
- La 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 (Política CIS/TIC)**. (4) La Política CIS/TIC presenta una visión global e integral de los recursos del MDEF en materia CIS/TIC; y su desarrollo será competencia del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (en adelante CESTIC), que se estudiará a continuación.

Así mismo, la política CIS/TIC (4) propone avanzar hacia una **Infraestructura Integral de Información para la Defensa** (en adelante I3D), que comprenda tanto los Sistemas de Información y Comunicaciones (CIS) tanto permanentes como desplegables, y cuya gestión también recaerá en el CESTIC, y que será objeto de análisis a continuación.

Por último citar que la orden DEF/2639/2015, de 3 de diciembre, recoge en su anexo II que el Plan de Acción para la Transformación Digital será uno de los planes de acción de desarrollo del Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS).

- La 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 (AG CIS/TIC)** (5), también establece el marco técnico de referencia que guiará el proceso de Transformación Digital del Ministerio de Defensa, para lograr un mejor aprovechamiento de los servicios TIC y facilitar la revisión de procedimientos, procesos y estructuras que conlleva el proceso de digitalización.

En dicha AG CIS/TIC (5) se establece que los procesos principales identificados deberán ser revisados y desarrollados en cada uno de los ámbitos funcionales correspondientes, con el apoyo del CESTIC, en el marco del Proceso de Transformación Digital dirigido por la Comisión Ministerial de Administración Digital (CMAD). Así mismo, establece los tres pilares para la Transformación Digital del Ministerio de Defensa:

- 1) procesos funcionales y operativos;
- 2) productos de información; y
- 3) servicios CIS/TIC.

La AG CIS/TIC (5) recoge en su apartado 5, que la Estrategia de la Información deberá servir como punto de partida para abordar un Plan de Acción para la Transformación Digital, que racionalice los sistemas de información y facilite el mejor empleo de las TIC en una renovada organización basada en la gestión por procesos, propósito de la siguiente disposición.

Así mismo, la AG CIS/TIC (5) describe a alto nivel las Capacidades CIS/TIC necesarias para cumplir la finalidad y los ejes estratégicos de la política CIS/TIC (4), y que será objeto de estudio en un apartado posterior.

- La Instrucción 25/2018 del Secretario de Estado de Defensa por la que se aprueba la **primera parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital PATD (6)** que se encuentra alineado con la estrategia TIC de la AGE y con la propia política y estrategia CIS/TIC del Ministerio.

De acuerdo con el PATD (6) las actuaciones del MDEF para la Transformación Digital se articulan en cuatro grupos:

- 1) Planeamiento/Programación, que incluye las actuaciones relacionadas con planes, programas, documentación, normativa, convenios o procesos;
- 2) Infraestructuras, que incluye las actuaciones relacionadas con componentes de infraestructura tecnológica y de TIC;
- 3) Servicios AGE, que incluye las actuaciones cuya implementación ayuda a mejorar o extender al MDEF los servicios ofrecidos por la AGE; y
- 4) Servicios MDEF, que incluye las actuaciones que deben mejorar la transformación interna del Departamento.

- 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)**, que tiene por objeto asegurar un adecuado desarrollo de la Política CIS/TIC (4) y la AG CIS/TIC. (5)

El PECIS establece los ejes y los objetivos estratégicos, así como las acciones necesarias para desarrollar las capacidades CIS/TIC en la Defensa que permitirán a la I3D constituirse en la infraestructura vertebral imprescindible del MDEF que soportará todas estas capacidades.

2.2.1 Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

La 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 (Política CIS/TIC) dispone que el desarrollo de la política CIS/TIC (4) será competencia del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

Conforme al Real Decreto 63/2023, de 8 de febrero, por el que se modifica El Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, se establece que el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), con rango de dirección general, depende directamente de la Secretaría de Estado de Defensa.

Conforme a dicho Real Decreto, corresponden al CESTIC, en el ámbito de sus competencias, entre otras, las siguientes funciones:

- Definir y planificar las políticas y estrategias de los CIS/TIC, su desarrollo y actualización, coordinar su ejecución y velar por su cumplimiento en el ámbito del Departamento.
- Impulsar, desplegar y mantener actualizada la I3D como infraestructura tecnológica de carácter estratégico sobre la que se desplegarán los servicios CIS/TIC
- Dirigir el diseño, la obtención y la configuración de los CIS/TIC para garantizar la normalización, homologación y estandarización de dichos sistemas y su plena interoperabilidad
- Supervisar, gestionar y controlar la operación y el mantenimiento de los CIS/TIC para la provisión directa y segura de los servicios de la I3D, a través del Centro de Gestión de Servicios de la I3D. De este cometido se extrae la relevancia que tiene el CESTIC para el cumplimiento de los propósitos del presente TFM.
- Impulsar la publicación y gestión de un catálogo de servicios CIS/TIC en colaboración con las Fuerzas Armadas y el resto de ámbitos del Ministerio, otro cometido también relacionado con la temática del TFM.
- Definir y planificar la política de seguridad de la información, su desarrollo y actualización, coordinar su ejecución y velar por su cumplimiento en el ámbito del Departamento.
- Ejercer las actividades necesarias en materia de ciberseguridad para proteger la I3D y los activos de información que en ella se procesan.
- Impulsar la transformación digital del MDEF
- Desarrollar e impulsar programas, proyectos y actuaciones para el despliegue de servicios digitales, capacidades e infraestructuras que contribuyan a acelerar el proceso de transformación digital del Ministerio de Defensa.

El Director del CESTIC asume las funciones de Oficial Jefe de la Información (CIO) del Ministerio de Defensa.

En lo que respecta a su estructura, es un órgano directivo del CESTIC la Subdirección General de Planes y Servicios de Información y Telecomunicaciones, dentro de la cual es pertinente citar la existencia de la División de Operaciones de Red (En adelante DIVOPER)

La División de Operaciones de Red (DIVOPER) está centrada principalmente en la provisión de Servicios CIS/TIC, forma parte de la Estructura de Gestión CIS/TIC y, en el ámbito de competencias del CESTIC, tendrá las siguientes funciones:

- La provisión de servicios CIS/TIC de la I3D en producción y de su continuidad y resiliencia.
- La monitorización necesaria para la correcta operación de los servicios, gestionando de forma centralizada todas las incidencias, peticiones y la gestión de accesos a los mismos.
- El aseguramiento de los niveles de disponibilidad requeridos (según los correspondientes Acuerdos de Nivel de Servicio) de todos los servicios en producción y la elaboración de informes sobre la disponibilidad, capacidad y rendimiento de los mismos.
- El apoyo específico CIS/TIC al Órgano Central del departamento.
- El apoyo CIS/TIC a las diferentes Organizaciones Operativas desplegadas en Zona de Operaciones.
- La provisión y operación de los servicios CIS/TIC del Sistema de Mando y Control Nacional (SC2N), así como de su continuidad y resiliencia.

De lo anterior es comprensible que a lo largo del desarrollo del presente TFM, aparecerá de manera reiterada alusiones a esta división, ya que es la unidad responsable dentro del CESTIC, de las materias que son objeto del TFM.

2.2.2 Infraestructura Integral de Información para la Defensa (I3D)

La Política CIS/TIC (4) propone avanzar hacia una única Infraestructura Integral de Información para la Defensa (I3D), que se constituye como infraestructura de carácter estratégico del Ministerio de Defensa (MDEF) que se encargará de proporcionar servicios para los Sistemas y Tecnologías de Información y Comunicación (CIS/TIC) del Departamento.

La I3D se define como una red tecnológica bajo una autoridad operativa única, cuyo objetivo es optimizar el uso de sistemas de información y telecomunicaciones; permitiendo un acceso eficaz y seguro a los recursos de información de la Defensa, desde cualquier ubicación, geográfica o dinámica en las que operen las RAF; Todo ello en un contexto global en el que son críticos: la hiperconectividad, asegurar la libertad de acción en el ciberespacio, la superioridad de la información o las operaciones en el multidominio⁷ enmarcado en lo que se describe como una “esfera digital” (5)

El objetivo es evolucionar hacia una infraestructura CIS/TIC única, que facilitará la gestión centralizada de todos recursos CIS/TIC y la unificación de los Servicios CIS/TIC. Además, de una mejora aplicación de medidas de seguridad CIS/TIC y de seguridad de la información. La Figura 2-1 muestra la arquitectura propuesta con una infraestructura única CIS/TIC para el MDEF.

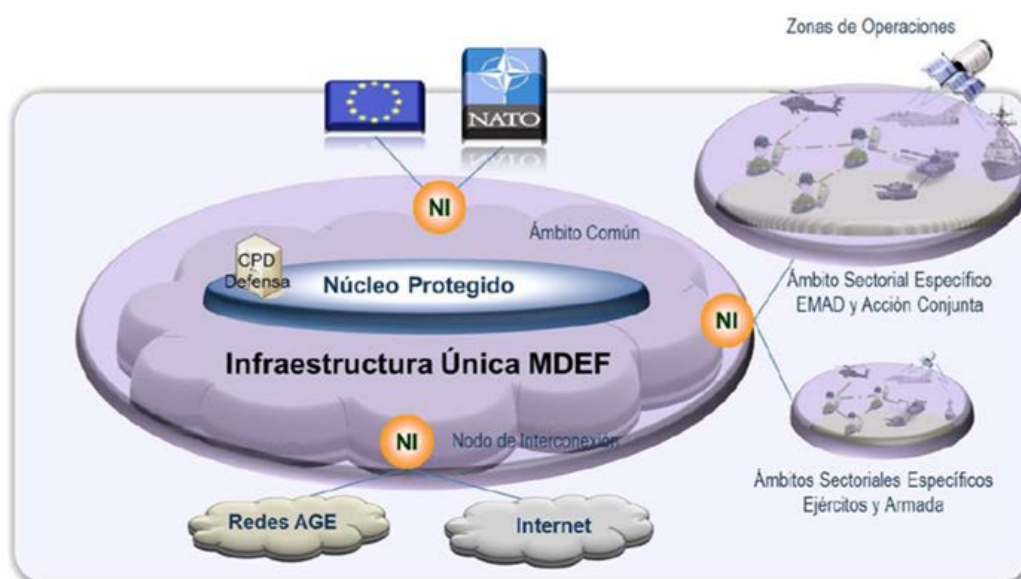


Figura 2-1 Esquema del modelo de infraestructuras CIS/TIC de la I3D en el MDEF (Fuente: Presentaciones corporativas del CESTIC, MDEF)

2.2.3 La Transformación Digital del MDEF en época reciente.

Con posterioridad a la aprobación de las disposiciones referidas anteriormente, fue aprobada la segunda parte del Plan de Acción del MDEF para la transformación Digital (PATD-2) (6), a través de la Instrucción 14/2020, de 15 de abril, del Secretario de Estado de Defensa, por la que se aprueba la

⁷ Según la NC “Operaciones Multi-Dominio” del Centro Conjunto de Desarrollo de Conceptos del CESEDEN del MDEF, se utilizarán el término “multi-dominio” en el entorno conjunto de las FAS para entender: “Aquellas operaciones realizadas por la Fuerza Conjunta que por su agilidad y complejidad, necesitan de una adecuada interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la integración de todas sus capacidades y así poder producir efectos en y desde cualquiera de los ámbitos de operación.”

segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital. PATD-2 (6)

Esta segunda parte del plan supone una ampliación del alcance hacia una transformación más integral, abarcando aspectos organizativos, operativos, datos e información, seguridad y la racionalización de los sistemas TIC. El plan Introduce objetivos como la interoperabilidad total de sistemas, la creación de plataformas de análisis masivo de datos y la incorporación de tecnologías emergentes.

Esta segunda parte del PATD (6) va dirigido a los medios y servicios que afectan a la defensa, consulta política, situaciones de crisis y seguridad del Estado o que manejan información clasificada de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

En línea con la primera parte, incluye las actuaciones a desarrollar en el conjunto del Departamento, con la finalidad principal de proceder a una revisión integral de las tareas, actividades y procesos funcionales y operativos y a la integración de los Servicios CIS/TIC en dichas actividades y procesos. Se posibilitará así cerrar la brecha existente entre las Capacidades Operativas y los Servicios CIS/TIC, aprovechando las posibilidades que estos últimos ofrecen, mejorando la calidad y facilidad de uso de dichos procesos, y en definitiva la eficiencia del Departamento.

Las actuaciones del MDEF para la segunda parte del PATD (6) se articulan en cinco dimensiones:

I. Organización y Personas: se incluyen las actuaciones concretas que potencian las estructuras existentes y necesarias para capacitar al MDEF en el modelado de las actividades y procesos necesarios para el desarrollo eficiente de sus funciones.

II. Procesos Funcionales y Operativos: Centrado en la gestión, modelado y creación de aplicaciones basadas en procesos, que permita el desarrollo de servicios que puedan ser utilizados por los usuarios.

III. Datos, Información y Conocimiento: Una de las áreas clave del PATD-2 (6) es la gestión de datos masivos (Big Data), mediante la creación de plataformas que permitan la exploración y el análisis en tiempo real de los datos provenientes de diversas fuentes

IV. Seguridad: En un entorno digital cada vez más complejo y vulnerable, el PATD-2 (6) dedica recursos significativos a reforzar las capacidades de ciberseguridad.

V. Racionalización de los Sistemas: El PATD-2 (6) promueve la interoperabilidad entre los sistemas TIC del MDEF y con aliados internacionales, lo cual es crucial en el contexto de operaciones conjuntas y coaliciones.

2.2.4 Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC (AR GES CIS/TIC)

El desarrollo de una metodología de gobierno, dirección y gestión CIS/TIC es una herramienta fundamental para abordar con éxito el proceso de transformación digital en el MDEF.

Puede afirmarse que el MDEF es pionero en este proceso, no existiendo en la actualidad otro modelo comparable para el Gobierno y Gestión Única de Servicios en otra Administración Pública española. El MDEF lidera por tanto en este camino de la transformación digital del sector público.

El proceso de transformación digital se apoya en tres pilares fundamentales: los procesos de negocio, los productos de información y los servicios CIS/TIC, que junto a la organización y las personas y a la seguridad de la información conforman las cinco dimensiones contempladas en la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital (PATD-2). (6)

En diciembre de 2023 el CESTIC aprobó la última versión de la **Arquitectura de Referencia (AR) única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7)**, que junto con la Arquitectura Global (AG) CIS/TIC (5) y el resto de las AR y las

Arquitecturas Objetivo (AO), conforman un modelo de normalización y un instrumento de coherencia e integridad técnica en la aplicación de la Política CIS/TIC (4) del Ministerio de Defensa (MDEF)

La Arquitectura de Referencia establece en su ámbito de aplicación, que esta será de aplicación para todos los productos y Servicios CIS/TIC proporcionados por la I3D del MDEF, así como a los procesos de gestión que soportan dichos servicios.

La Arquitectura de Referencia (7) define la visión del CESTIC para la realización de una gestión de servicios de la I3D exitosa, para lo cual, define los siguientes objetivos globales (OBG) para la Gestión de Servicios CIS/TIC de la I3D:

- OBG-1. Proporcionar un Modelo de Gestión de Servicios CIS/TIC centralizado, único, documentado, definible, repetible y escalable con las mejores prácticas recomendadas.
- OBG-2. Identificar claramente las funciones y responsabilidades de la Gestión de Servicios CIS/TIC de la I3D del MDEF
- OBG-3. Alinear los Servicios CIS/TIC con las necesidades actuales y futuras de los organismos del MDEF, a través de un Catálogo de Servicios.
- OBG-4. Entregar Servicios CIS/TIC de acuerdo a los Acuerdos de Nivel de Servicio (SLA)⁸ definidos.
- OBG-5. Garantizar el cumplimiento normativo y la posterior auditoría de los Servicios CIS/TIC mediante procesos repetibles.
- OBG-6. Aumentar la calidad de los Servicios CIS/TIC entregados y la madurez de los procesos operativos del CESTIC a través de la mejora continua
- OBG-7. Optimizar los costes en la provisión de Servicios CIS/TIC.

En resumen, el CESTIC debe proporcionar un modelo de gestión única de servicios, basada en procesos únicos para todo el MDEF, y amparado sobre un marco de trabajo integral para el gobierno y la gestión CIS/TIC. Debe alinear los servicios CIS/TIC con los objetivos del Ministerio de Defensa, y la gobernanza CIS/TIC. Su finalidad es proporcionar servicios seguros y de calidad, manteniendo un equilibrio entre la satisfacción del usuario, la optimización del riesgo y el uso de los recursos.

Para la materialización del primer objetivo (OBG-1) de implantación de un modelo para el Gobierno y Gestión Única de Servicios, el CESTIC publicó en junio de 2021, la **Visión 01/21 del CESTIC: Modelo de Alto Nivel de Gestión única de Servicios para su Aplicación al Centro de Gestión de Servicios CIS/TIC de la I3D**.

El objeto de este documento es presentar un modelo de alto nivel para la Gestión Única de Servicios CIS/TIC y su aplicación como visión de Centro de Gestión de Servicios (CEGES I3D), desde el cual se lleve a cabo la supervisión, monitorización y conducción integral y centralizada de la gestión, operación y seguridad de los servicios CIS/TIC de la I3D. El concepto de Centro de Gestión de Servicios (CEGES) de la I3D ya se encontraba previsto en el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS).

La Visión 01/21 ha orientado el desarrollo de la AR de Gestión CIS/TIC en esta materia. Ambos documentos se han basado en las buenas prácticas de gobierno y gestión de los servicios de Tecnologías de la Información (TI), COBIT 2019.

⁸ Un acuerdo de nivel de servicio (siglas ANS), también conocidas por las siglas SLA (del inglés Service Level Agreement), es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Fuente: Wikipedia.

La Visión 01/21 establece que este modelo de gobierno y gestión corporativa de los Servicios CIS/TIC se materializará a través de una herramienta ITSM⁹ como único canal de comunicación y repositorio de información.

Las herramientas ITSM son fundamentales para la gestión de los servicios, cubriendo su ciclo de vida completo: medida, monitorización y optimización. Esta herramienta actuará como la plataforma que facilita la estandarización de procesos y la creación de un catálogo de servicios para todos los departamentos involucrados.

La Visión 01/21 destaca dos puntos fundamentales en relación con la gestión de servicios a través de herramientas ITSM:

- **ITSM único:** El MDEF destaca la importancia de una herramienta ITSM unificada para gestionar de forma centralizada los servicios CIS/TIC. La herramienta debe ser simple, homogénea y alineada con los requisitos de la OTAN¹⁰.
- **Integración:** Además de la ITSM principal, otras herramientas específicas para la gestión de infraestructuras de telecomunicaciones e información deben integrarse con la plataforma ITSM central

Los pilares del modelo de gestión única de servicios son: Catálogo de Servicios, Procesos, Herramientas y Organización. A través del proceso de implantación de este modelo único de gestión de servicios se pretende avanzar de la situación actual (AS-IS) hasta la situación objetivo deseada (TO-BE).

Con la implantación de estos procesos se pretende modelar la transición reflejada en la **Tabla 2-1** desde la situación actual (AS-IS) hasta la situación objetivo (TO BE).¹¹

Pilares del Modelo	Situación actual de Gestión (AS-IS)	Situación objetivo de Gestión (TO-BE)
Catálogo de Servicios	No se dispone de un Catálogo de Servicios único ni valorado económicamente	Catálogo único con todos los servicios identificados y valorados
Procesos	Se identifican procesos diferentes según el servicio, no existiendo procesos estandarizados.	Procesos estandarizados, únicos y basados en buenas prácticas COBIT e ITIL
Herramientas	Duplicidad de herramientas que no dan soporte a todos los procesos de la gestión.	Herramienta única ITSM (sencillez y simplicidad). Racionalización de otras herramientas existentes.
Organización	Falta de coordinación y solapamiento de cometidos	Organización del personal según roles y mejora de la coordinación para su trabajo

Tabla 2-1 Identificación de la situación actual y objetivo a través del modelo de gestión única de servicios. (7)

⁹ Las herramientas ITSM (IT Service Management) son aplicaciones o plataformas que ayudan a las organizaciones tecnológicas a gestionar, optimizar y mejorar la calidad de los servicios TI que ofrecen a sus clientes. Fuente: <https://www.computing.es>

¹⁰ OTAN Organización del Tratado del Atlántico Norte (en inglés, North Atlantic Treaty Organization, NATO)

¹¹ La situación que se presenta como actual se refiere a la situación del MDEF a fecha de enero de 2024.

2.2.5 Catálogo de Servicios:

El Catálogo de Servicios se constituye como el elemento fundamental para el buen funcionamiento de la Arquitectura de Referencia de Gestión (AR GES CIS/TIC) (7), al ser el motor que gobierna el Modelo de Gestión Única y provee una imagen consistente, normalizada y precisa de los servicios CIS/TIC ofrecidos por el MDEF y orientados al usuario.

Su objetivo es actuar de nexo de unión entre el modelo de gestión deseado y la realidad actual, para transitar con el tiempo hacia un marco más eficiente y optimizado en la gestión de servicios, garantizando una visión global y única de los procesos implicados. Además, constituye la fuente de información única de los servicios CIS/TIC que se prestan en el marco del MDEF.

Partiendo de la realidad actual, el Catálogo integrará la estructura organizativa actual de los ámbitos sin modificación orgánica ni transferencia de recursos al CESTIC, e incorporará nuevos roles a medida que los servicios vayan integrándose en la I3D. El Catálogo tendrá una estructura matricial, mostrando los actores actuales que vinculan los roles del Modelo para cada servicio. Cada ámbito, bajo su responsabilidad, será libre de elegir los actores para los diferentes roles considerados en la AR GES.

Es importante destacar la necesidad de que los ámbitos¹² contribuyan incorporando sus estructuras de gestión específicas de forma que sea posible, a partir de la realidad actual, y con la existencia de un Catálogo consensuado, optimizar su Gestión. Para ello se contará además con una herramienta de ITSM común.

Para la gestión de Catálogo de Servicios, el CESTIC aprobado una serie de Instrucciones Técnicas¹³ (IT), con el objeto de establecer un marco normativo que permita alcanzar los requisitos de gobierno CIS/TIC a través de la gestión del marco de gestión CIS/TIC. Son los siguientes:

- Instrucción Técnica 10/24 del CESTIC: Gestión de Peticiones y de Incidencias en la I3D.
- Instrucción Técnica xx/24 del CESTIC: Gestión de la Configuración en la I3D.
- TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D
- Instrucción Técnica xx/24 del CESTIC Gestión de Problemas en la I3D
- Instrucción Técnica xx/24 del CESTIC Gestión de Cambios en la I3D

2.2.6 Centro de Gestión de Servicios CIS/TIC

El documento “Visión 01/22 del CESTIC: Concepto del Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D)” (8) abarca la estructura funcional y los procesos identificados, que han de incorporarse al modelo para el Gobierno y Gestión Única de Servicios CIS/TIC, para la consecución de sus objetivos.

Con anterioridad, la Política CIS/TIC (4) y el PECIS ya establecían como objetivo estratégico el diseño y despliegue de las capacidades de gestión de los servicios CIS/TIC de la I3D, mediante el Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D), que permitirá realizar una gestión centralizada de todos ellos y proporcionar a su vez, servicios de gestión.

Disponer de un Centro de Gestión de Servicios de la I3D (CEGES I3D) permitirá al CESTIC, como proveedor de los servicios CIS/TIC del MDEF, la gestión de servicios de forma proactiva, optimizada,

¹² En la “jerga” del Ministerio de Defensa, el concepto “ámbitos” hace referencia a los diferentes ejércitos, así como otras unidades de gran entidad, por ejemplo, la Unidad Militar de Emergencias (UME)

¹³ Una Instrucción Técnica en el ámbito de la gestión de servicios TI es un documento normativo o guía que detalla de manera específica, operativa y formal los procedimientos, estándares y responsabilidades a seguir en la prestación de un servicio o en la ejecución de una actividad relacionada con las Tecnologías de la Información (TI) Generalmente están alineadas con marcos de referencia como ITIL, COBIT o ISO/IEC 20000

eficiente, medible y con alta capacidad de respuesta y de calidad para satisfacer las necesidades funcionales y operativas requeridas. El Centro de Gestión de Servicios deberá ser dirigido y explotado por personal cualificado y adiestrado. Tendrá distribución física redundante (Con dos salas de Conducción de Operaciones en 2 ubicaciones) Debe ser capaz de funcionar de forma permanente (24x7x365) y garantizar la continuidad y la prestación de los servicios en todo momento.

El CEGES I3D, como área de Gestión del Servicio, estará compuesto por el Centro de Atención al Usuario (CAU), como punto único de contacto (Nivel 1 de la AR GES CIS/TIC) para todas las incidencias, peticiones y consultas de los usuarios, y por el Soporte CIS/TIC (Nivel 2 de la AR GES CIS/TIC). La herramienta ITSM ofrecerá un único canal a los usuarios y niveles de servicio para la resolución de peticiones e incidencias, como se refleja en la Figura 2-2:

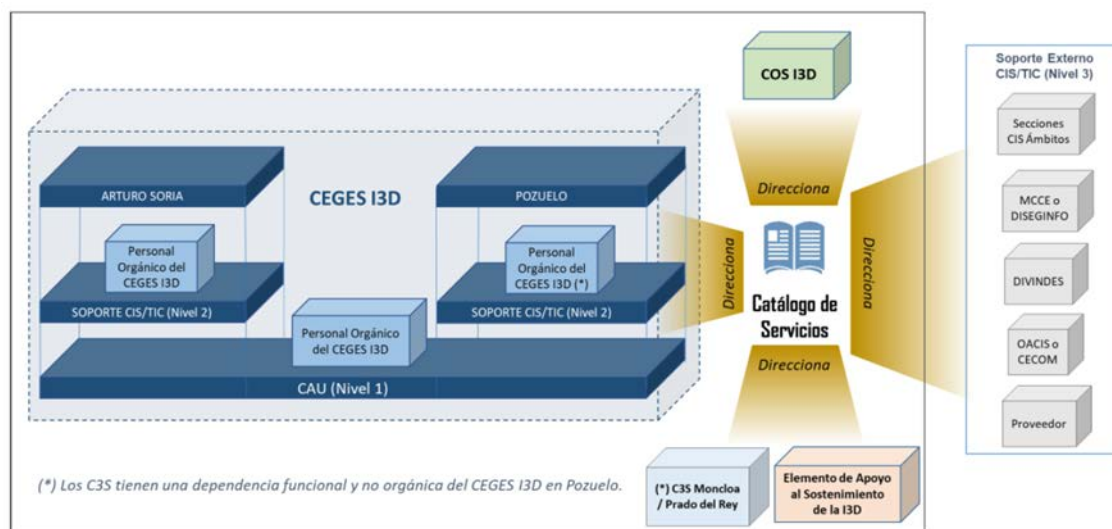


Figura 2-2 Integración entre el CEGES I3D y resto de capacidades mediante el Catálogo de Servicios (Fuente: Presentaciones corporativas del CESTIC, MDEF)

2.2.7 Centro de Atención al Usuario CAU

Un Centro de Atención al Usuario (CAU) se define como un conjunto de recursos tecnológicos y humanos, que tiene por objeto prestar servicios, con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las tecnologías de la información y la comunicación (TIC).

El Centro de Servicio al Usuario tiene una importancia vital en el Departamento de TI de una organización y debería ser el Punto Único de Contacto (SPOC) diario para los usuarios de TI; y tratará todas las incidencias y peticiones de servicio, utilizando habitualmente herramientas de software especializado para registrar y gestionar todos esos eventos. Esta definición se proporciona en los Apuntes Asignatura COM3 (9)

1. Durante el flujo de gestión de una incidencia, el CAU deberá realizar las siguientes actividades:
2. Identificación de la incidencia
3. Registro de la incidencia
4. Categorización de la incidencia, que permita realizar un análisis a posteriori de las mismas
5. Priorización de la incidencia: Teniendo en cuenta tanto su urgencia como su impacto
6. Diagnóstico inicial de la incidencia
7. Escalado de la incidencia, si procede por su complejidad
8. Investigación y diagnóstico
9. Resolución y recuperación
10. Cierre de la incidencia

2.2.8 Herramientas de monitorización de infraestructura TI

Dotcom-Monitor (10) define la supervisión o monitorización de la infraestructura TI como el proceso de seguimiento y gestión del estado y el rendimiento de todos los componentes de TI de una organización o centro de datos, tales como servidores, redes, bases de datos y aplicaciones.

La supervisión de la infraestructura garantiza que los sistemas críticos permanezcan operativos, que los problemas de rendimiento se resuelvan rápidamente y que se minimicen las interrupciones. Sin supervisión, las empresas corren el riesgo de sufrir tiempo de inactividad, degradación del rendimiento y vulnerabilidades de seguridad que pueden provocar pérdidas financieras y daños a su reputación.

Así mismo, de acuerdo con Dotcom-Monitor (10), otros beneficios aportados por la monitorización son la detección proactiva de problemas, el aumento del tiempo de actividad de los servicios, la reducción de costes, una mejor utilización de los recursos, e incluso, contribuir a una mejora de la seguridad al permitir detectar actividades inusuales.

En este punto, conviene destacar la diferencia existente entre monitorización y gestión de eventos, aunque son dos áreas íntimamente relacionadas.

La Gestión de Eventos se centra en la generación y detección de notificaciones significativas sobre el estado de los servicios e Infraestructura de TI. Aunque es cierto que la monitorización es necesaria para detectar y hacer el seguimiento de estas notificaciones monitorizar es un término más amplio que gestión de eventos. Por ejemplo, las herramientas de monitorización comprobarán el estado de un dispositivo para garantizar que esté operando dentro de los límites aceptables, incluso si ese dispositivo no estuviera generando eventos.

Es decir, el objetivo último es determinar que desviaciones en los parámetros de monitorización deben considerarse lo suficientemente relevantes como para desencadenar la generación de un evento, que deba ser monitorizado.

Una gestión eficiente de eventos requerirá la integración de una capa de lógica de negocio en nuestra herramienta de monitorización que permita discriminar que desviaciones en los parámetros o acumulaciones de los mismos, se consideren lo suficientemente significativas para generar una alarma o evento, que deba ponerse en conocimiento de los responsables de cada área o el responsable de la división.

Si se opta por seguir este esquema, la frontera entre monitorización y gestión de eventos, se volverá todavía más difusa, pero es posible que el borrado de esta frontera sea lo más útil para los objetivos de la organización en este caso.

Para poder realizar una monitorización de las infraestructuras es preciso contar con herramientas de monitorización. Las herramientas de monitorización son un sistema informático que se utiliza para seguir y supervisar en tiempo real el rendimiento y la funcionalidad de las redes, infraestructuras, sistemas y aplicaciones de una empresa. Son plataformas que se conectan con los diferentes sistemas de la organización para recopilar datos y métricas; y que permiten, de manera inmediata, obtener una visión completa del estado de los sistemas de una organización.

Dotcom-Monitor (10) destaca las siguientes soluciones de mercado, que permiten la monitorización de los servicios TI:

Nagios:

Nagios es una conocida herramienta de código abierto que ayuda a supervisar la disponibilidad y el rendimiento de la infraestructura de TI, cubriendo desde servidores hasta dispositivos de red y aplicaciones. Nagios utiliza un enfoque basado en complementos, recopila datos sobre los recursos del sistema, los servicios de red e incluso las condiciones ambientales.

Los beneficios clave que aporta Nagios son: Monitorización y alertas en tiempo real, arquitectura basada en plugins altamente personalizable, y sistema de notificaciones y alertas flexible.

Zabbix:

Zabbix es una herramienta de monitorización de código abierto para rastrear el rendimiento y la disponibilidad de la infraestructura de TI. Supervisa servidores, redes, aplicaciones y servicios, recopilando datos de parámetros de CPU, memoria, red y aplicaciones. Con umbrales y alertas personalizables, ayuda a identificar y abordar los problemas con prontitud, minimizando el tiempo de inactividad y asegurando operaciones sin problemas.

Zabbix también ofrece funciones de visualización como paneles, gráficos y mapas para un análisis de datos intuitivo. Al ser de código abierto, se beneficia de una comunidad dedicada que garantiza la mejora continua y se mantiene al día con los estándares de la industria y las tecnologías emergentes.

Los beneficios clave que aporta Zabbix son: Código abierto, paneles visuales para facilitar el análisis de datos y capacidad de supervisión de una amplia gama de infraestructuras de TI.

Splunk:

Splunk es una herramienta de análisis y monitoreo de datos que permite a las organizaciones recopilar, indexar y analizar grandes cantidades de datos generados por máquinas. Admite la ingesta de datos de diversas fuentes, como servidores, aplicaciones, sensores y dispositivos, lo que permite a las organizaciones centralizar y correlacionar sus datos para un análisis exhaustivo.

Las funcionalidades de búsqueda e informes de Splunk permiten a los usuarios extraer rápidamente información significativa de sus datos, identificar tendencias, detectar anomalías y monitorear el rendimiento del sistema en tiempo real. También ofrece potentes opciones de visualización, incluidos paneles y gráficos, para presentar datos de manera integral.

Además, Splunk admite la creación de aplicaciones e integraciones personalizadas a través de su API robusta, fomentando la extensibilidad y permitiendo a las organizaciones adaptar la plataforma a sus necesidades.

Los beneficios clave que aporta Splunk son: Centralizar datos de diversas fuentes para su análisis, supervisión en tiempo real del rendimiento del sistema, paneles y visualizaciones personalizados para obtener información sobre los datos, y admite aplicaciones personalizadas e integraciones a través de API.

2.2.9 Cuadro de Mando (Dashboard)

Un Cuadro de mando (o Dashboard en inglés) es un concepto amplio que representa una herramienta informática que proporciona visualizaciones rápidas de datos, diseñadas para mostrar, de manera concisa y personalizada, los indicadores clave de rendimiento (KPIs) y métricas importantes para una organización, o para una función específica. Los cuadros de mando son usados en diferentes áreas empresariales (finanzas, ventas, operaciones, TI, etc.) y están orientados a la toma de decisiones estratégicas o tácticas.

En el ámbito específico de las tecnologías de la información y comunicación y los servicios TI, un cuadro de mando es una herramienta visual que permite a los profesionales monitorizar, analizar y gestionar el rendimiento y la eficiencia de los sistemas, infraestructuras y servicios tecnológicos de una organización. Este tipo de dashboard recopila, integra y presenta datos clave en tiempo real o en intervalos específicos, relacionados con aspectos como la seguridad de la red, el rendimiento de servidores, el tráfico de datos, el estado de las aplicaciones, el uso de recursos en la nube, entre otros.

Los cuadros de mando TI proporcionan una vista consolidada y accesible de información crítica, facilitando la toma de decisiones rápidas y basadas en datos. Son fundamentales para identificar problemas potenciales, optimizar procesos y garantizar el correcto funcionamiento de los sistemas

tecnológicos de la empresa. Además, permiten a los equipos técnicos realizar un seguimiento de indicadores clave de desempeño (KPI), ayudando a mejorar la calidad del servicio y la eficiencia operativa en el entorno digital.

2.2.10 Acuerdos de Nivel de Servicio (SLA)

Los Acuerdos de Nivel de Servicio (SLA, por las siglas en inglés de Service Level Agreement), o también conocidos como Acuerdos de Provisión de Servicios (APS) de acuerdo con el libro: Preparación para la certificación ITIL Foundation V3. (11), se definen como los acuerdos resultado de una negociación entre el cliente y el proveedor del servicio o servicios informáticos. Se describen en un documento contractual denominado contrato de servicios. Este documento va a definir el servicio o servicios propuestos y los niveles de servicio esperados. Un SLA cubre uno o varios servicios, y se aplica a uno o varios clientes. Se debe validar y firmar por ambas partes (cliente y proveedor) Se trata de un compromiso sobre los objetivos a alcanzar para estos servicios, incluyendo los derechos y obligaciones de las partes, así como la responsabilidad de cada uno.

2.2.11 Herramientas de observabilidad de datos

Las herramientas de observabilidad de datos son plataformas que permiten monitorizar, analizar y obtener información procesable sobre el comportamiento, rendimiento y estado de los sistemas de TI, aplicaciones y servicios. Estas herramientas recopilan y correlacionan datos de tres pilares principales de observabilidad: logs (registros), métricas¹⁴ y trazas¹⁵. Su objetivo es ayudar a los equipos técnicos a identificar y resolver problemas más rápidamente, así como a optimizar la infraestructura y las aplicaciones.

Las herramientas de observabilidad de datos son útiles para la implantación de un modelo único de gestión de servicios, ya que permiten obtener de forma rápida, información completa y unificada, útil para la gestión de la totalidad de los servicios TI de los que sea responsable una organización.

Existen diversas plataformas para la observabilidad de datos, tales como: Datadog, Splunk Observability Cloud, New Relic, Prometheus o Grafana, entre otras. Si bien se centrará a continuación la exposición en Grafana, ya que es la más relevante para el desarrollo de este TFM.

Grafana:

Red Hat, Inc (12) define Grafana como una plataforma interactiva y open source de visualización de datos desarrollada por Grafana Labs. Dicha plataforma permite a los usuarios ver sus datos a través de tablas y gráficos que se unifican en un panel de control (o en varios) para facilitar la interpretación y la comprensión. También permite realizar consultas y configurar avisos sobre la información y los indicadores desde el lugar en el que se almacena dicha información, ya sea en entornos de servidores tradicionales, clústeres de Kubernetes y varios servicios de nube, entre otros. Grafana se diseñó según los principios del open source y con la creencia de que los datos deberían ser accesibles para toda la empresa.

De acuerdo con el Portal *openwebinars.net*. (13), se pueden destacar las siguientes características diferenciales de la plataforma Grafana:

- Posibilidad de conexión con la práctica totalidad de las fuentes de datos existentes, comúnmente conocidas como bases de datos como Graphite, Prometheus, Influx DB, Elasticsearch, MySQL, PostgreSQL, y otros

¹⁴ Las **métricas** aportan datos cuantitativos sobre el rendimiento del sistema y cómo se están utilizando los recursos disponibles. (19)

¹⁵ Las **trazas** aportan información sobre el recorrido de las solicitudes que realiza un sistema. (19)

- Solución de código abierto, que permite desarrollar complementos desde cero para su integración con varias fuentes de datos diferentes.
- Permite estudiar, analizar y monitorear datos durante un período de tiempo, técnicamente llamado análisis de series de tiempo.
- Puede ser implementado localmente por organizaciones que no desean que sus datos se transmitan a un proveedor de nube por razones de seguridad y otras.
- Existencia de una gran variedad de paneles con una amplia gama de opciones de visualización, como mapas geográficos, mapas de calor, histogramas...
- Posibilidad de configuración de alertas.

La Figura 2-3 muestra un ejemplo de panel de visualización construido con la herramienta Grafana.



Figura 2-3 Ejemplo de panel de visualización construido con la herramienta Grafana (13)

2.2.12 Capacidades del MDEF en materia CIS/TIC

La Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (CIS/TIC) AR GES CIS/TIC (7) representa la conexión entre los objetivos del MDEF en materia CIS/TIC, y las buenas practicas propuestas por el marco COBIT para la consecución de los objetivos de la organización; ya que la AR establece un marco integral para la gestión de los servicios CIS/TIC, basado en los principios y estructuras de COBIT.

La AR GES CIS/TIC (7) identifica y describe las Capacidades requeridas por el MDEF para llevar a cabo con éxito las Misiones y Operaciones. En este punto conviene destacar que en el documento se hace referencia a:

- Por un lado, a las capacidades operativas del Ministerio de Defensa, derivadas del proceso de Planeamiento de la Defensa, están relacionadas directamente con las misiones y operaciones que el Ministerio debe cumplir y no corresponden directamente con los dominios de COBIT (APO, BAI, DSS, MEA).¹⁶

¹⁶ Los objetivos de gobierno y gestión de COBIT se agrupan en cinco dominios. Se analizan en el subapartado: 2.3.2.1 Terminología y conceptos clave del marco de referencia COBIT

- Por otro lado, a las capacidades de gestión alineadas con COBIT para la gestión de sistemas y tecnologías de la información (CIS/TIC) Al establecer estas capacidades, la AR asegura que los servicios TIC del Ministerio se gestionen de manera segura, eficiente y en alineación con los objetivos estratégicos de defensa.

Capacidades Operativas en el Contexto del MDEF

Las capacidades operativas descritas en el documento están orientadas a soportar las misiones y tareas del Ministerio de Defensa, y se organizan bajo un marco de misión y operación propio, el cual responde a los requerimientos específicos del entorno de defensa.

Estas capacidades están estructuradas para permitir al Ministerio cumplir con sus objetivos estratégicos y operativos, como muestra la figura 2-4



Figura 2-4 Contexto Operativo de las Capacidades del Ministerio de Defensa (7)

En el contexto operativo de las capacidades se diferencian dos capas:

- Capa de misiones y operaciones:

La capa de Misiones y Operaciones representa el nivel de ambición política y militar del Departamento como consecuencia de las políticas, normas y estrategias que sean aprobadas en cada momento, así como a los posibles tipos de misiones y cometidos.

- Capa de capacidades operativas:

Se obtienen principalmente a partir del proceso de Planeamiento de la Defensa y del análisis de los procesos funcionales y operativos del Departamento. Algunos elementos clave de estas capacidades están directamente relacionados con los recursos CIS/TIC como son:

- o Capacidades de Usuario: Enfocadas en la provisión de servicios y herramientas que permiten a los usuarios finales (personal del Ministerio de Defensa y fuerzas operativas) llevar a cabo sus tareas operativas.
- o Capacidades de Infraestructura de Información: Diseñadas para proporcionar y mantener los sistemas de información que soportan las operaciones y el manejo de datos críticos en escenarios de defensa. Están directamente relacionadas con el propósito del presente TFM a través del análisis de la implantación del Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC.
- o Capacidades de Infraestructura de Telecomunicaciones: Estas capacidades garantizan las comunicaciones necesarias para las operaciones en tiempo real, tanto en entornos locales como desplegables.

- o Capacidades de Seguridad de la Información: Aseguran la protección de la información crítica y las comunicaciones.
- o Capacidades de Gestión de la Información y el Conocimiento: Apoyan la gestión y el análisis de grandes volúmenes de información y datos para facilitar la toma de decisiones estratégicas y operativas.

Los vínculos establecidos entre los diferentes tipos de capacidades se reflejan en la Figura 2-5:

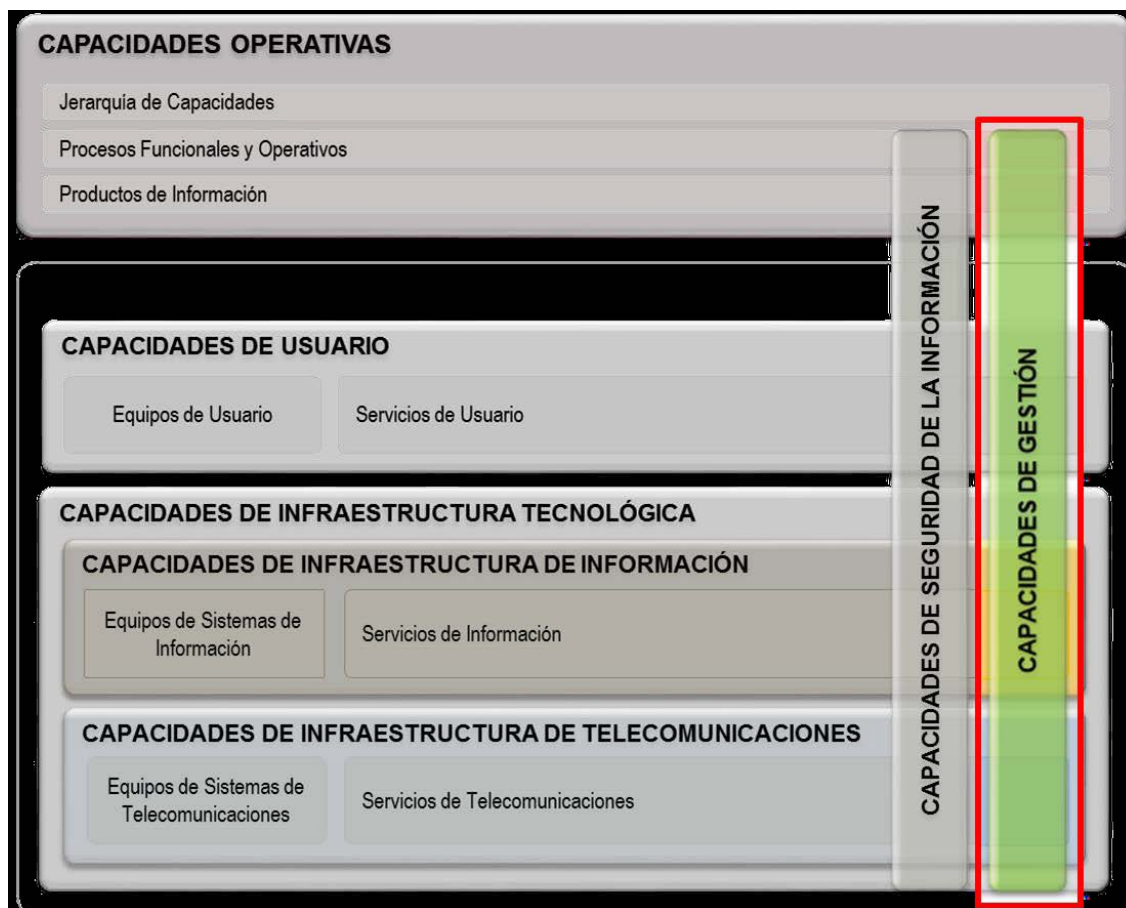


Figura 2-5 Relación entre las Capacidades de Gestión y resto de capacidades en el Ministerio de Defensa (7)

Capacidades CIS/TIC en el Contexto del MDEF

La definición y descripción de las Capacidades CIS/TIC deben dar soporte a las Capacidades Operativa. Las capacidades CIS/TIC son un conjunto de habilidades y recursos relacionados con los Sistemas de Información y Tecnologías de la Información y las Comunicaciones, y son fundamentales para la gestión efectiva de la información y las comunicaciones; y necesarias para cumplir la finalidad y los ejes estratégicos marcados por la Política CIS/TIC (4)

Las Arquitecturas de Referencia (AR) (7) desarrollan las Capacidades CIS/TIC y ofrecer las guías y especificaciones para el desarrollo de las Arquitecturas Objetivo del nivel inferior

La Arquitectura Global AG CIS/TIC (5) establece 4 objetivos principales para las capacidades CIS/TIC del MDEF:

- 1) Proporcionar una infraestructura integral de información unificada, tecnológicamente avanzada y optimizada, que facilite la plena autonomía y la libertad de acción.
- 2) Permitir lograr y mantener la superioridad de la información en las operaciones.

3) Posibilitar el acceso seguro a la información requerida en cualquier momento y en cualquier lugar.

4) Asegurar las características de adaptación, interoperabilidad, plena autonomía, adecuación, alta calidad, eficiencia, agilidad, carácter proyectable, movilidad estratégica, sostenibilidad y resiliencia de las Capacidades CIS/TIC del Ministerio de Defensa.

Las capacidades CIS/TIC se organizan en cuatro áreas de capacidades: de usuario, de infraestructura tecnológica, de seguridad de la información y de gestión, tal como muestra la Figura 2-6

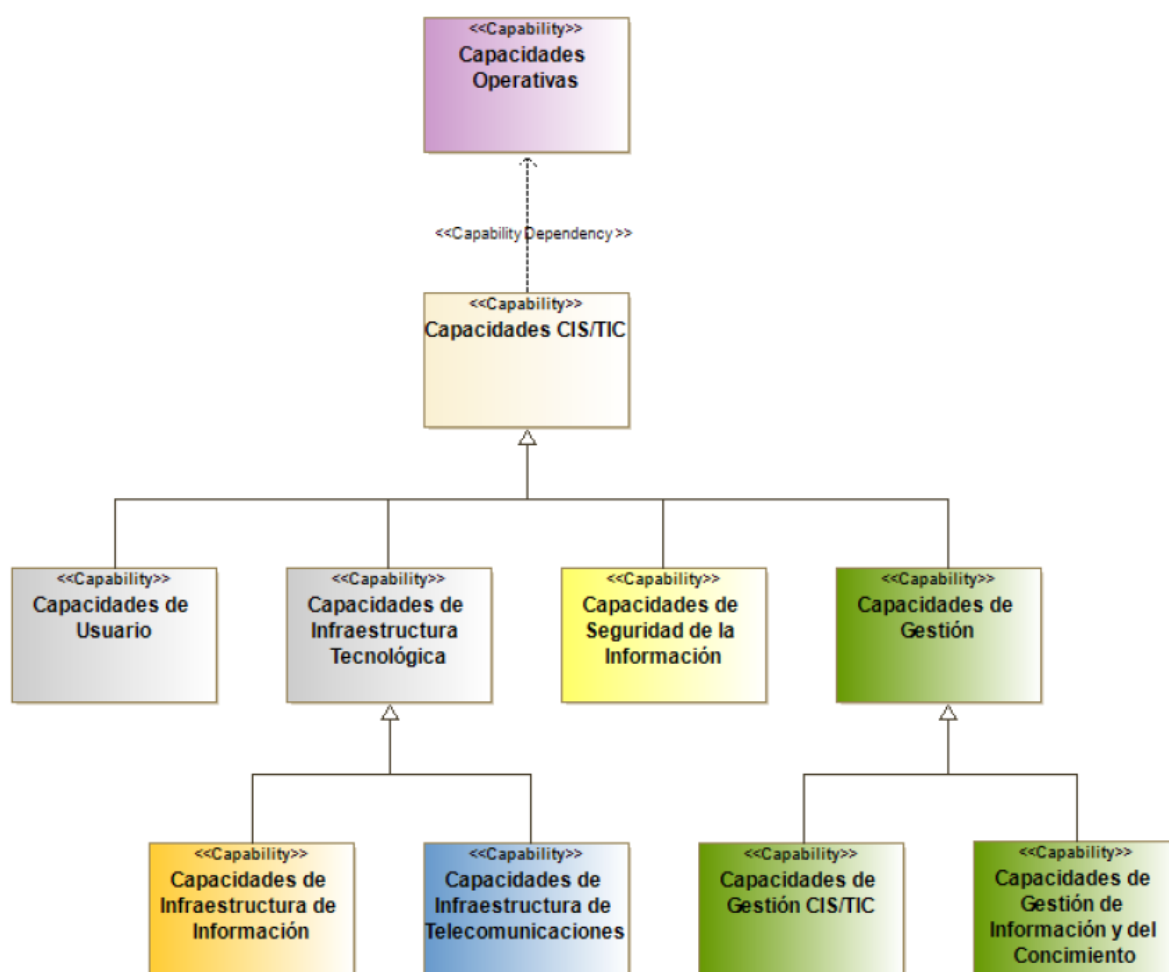


Figura 2-6 Taxonomía de Capacidades CIS/TIC del Ministerio de Defensa (7)

Capacidades de gestión:

Las capacidades de Gestión definidas en la AG CIS/TIC abarcan “el conjunto de Equipos y Servicios CIS/TIC de gestión de todas las Capacidades CIS/TIC del MDEF (usuario, infraestructura y seguridad de la información) que permitirán asegurar que los recursos y servicios disponibles se puedan asignar, priorizar y configurar de forma dinámica, proporcionando apoyo a la operación, administración y mantenimiento de dichas capacidades, así como a su seguridad y las operaciones de red”.

Estas capacidades abarcan tanto las necesarias para la prestación de Servicios CIS/TIC seguros conforme a los requisitos del Contexto Operativo del MDEF (Capacidades de Gestión CIS/TIC), como las necesarias para la Gestión de la Información y del Conocimiento (GIC) que se procesa, transmite y almacena mediante estos medios CIS/TIC (Capacidades GIC).

La Arquitectura Global AG CIS/TIC (5) identifica 4 subcapacidades de gestión de segundo nivel, reflejadas en la Figura 2-7 y Figura 2-8; y coincidentes con los 4 dominios de gestión en los que se agrupan los objetivos de gestión en el marco COBIT 2019¹⁷

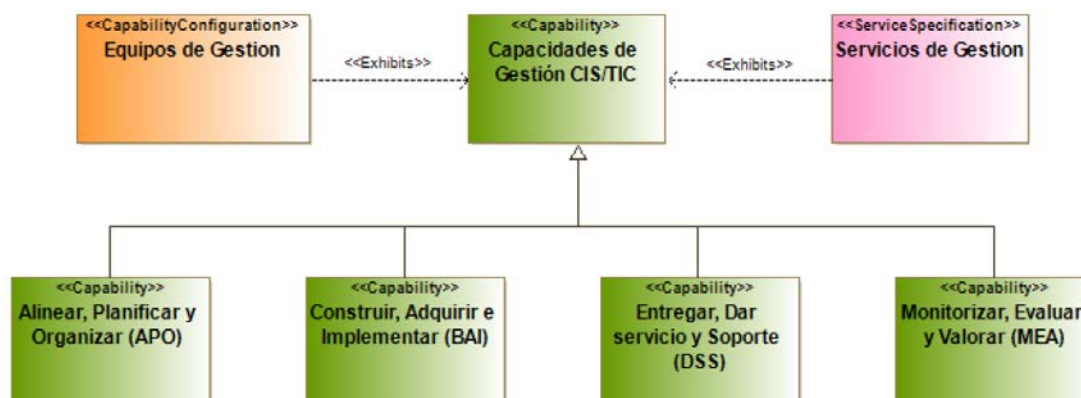


Figura 2-7 Taxonomía de Capacidades de Gestión CIS/TIC (7)

Capacidades de Gestión	Objeto
Capacidad de Alinear, Planificar y Organizar (APO)	Aborda la organización, estrategia y actividades de apoyo para los Servicios CIS/TIC.
Capacidad de Construir, Adquirir e Implementar (BAI)	Abarca la definición, adquisición e implementación de Servicios CIS/TIC y su integración con los procesos operativos del Ministerio.
Capacidad de Entregar, Dar servicio y Soporte (DSS)	Aborda la ejecución operativa y el soporte de los Servicios CIS/TIC.
Capacidad de Monitorizar, Evaluar y Valorar (MEA)	Aborda la monitorización y la conformidad de los medios CIS/TIC con los objetivos de rendimiento, objetivos de control y con todos los requerimientos.

Figura 2-8 Capacidades de Gestión y objeto que se desarrollan en la AR (7)

Para alcanzar los objetivos globales del MDEF anteriormente mencionados se debe llevar a cabo el desarrollo de las cuatro capacidades principales de gestión CIS/TIC.

Cada objetivo de gestión incluye varias prácticas de proceso de gestión, que se definen como un conjunto de acciones específicas diseñadas para alcanzar los objetivos de gobernanza y gestión de TI

El Ministerio de Defensa (MDEF) adopta el marco COBIT 2019 como estándar de mejores prácticas para la gestión de los sistemas de información y comunicaciones (CIS/TIC). Esto permite una dirección única con una gestión centralizada pero adaptada a las particularidades de cada área. El marco ofrece un sistema descentralizado en ejecución, pero con procesos estandarizados que facilitan la gobernanza y la coherencia operativa. El MDEF ha respetado la misma nomenclatura para sus procesos, que la sugerida en el modelo de referencia de procesos de COBIT.

El presente TFM tiene como uno de sus objetivos realizar un análisis de la implantación del modelo de gestión única de servicios CIS/TIC en el Ministerio, para lo cual sería relevante realizar un análisis detallado de como el modelo propuesto desarrolla cada una de las Capacidades de Gestión referidas, así como de sus objetivos y prácticas de gestión asociadas. Pero como en la práctica, este análisis de todos

¹⁷ Ver subapartado 2.3.2.1 Terminología y conceptos clave del marco de referencia COBIT

estos procesos excede el contenido razonable para un Trabajo de Fin de Máster, la exposición se centrará los procesos asociados a los objetivos de gobierno y gestión relevantes para la gobernanza TIC del MDEF.

2.3 Estándares y Marcos de Referencia para la gestión de servicios TI

Los marcos de trabajo de gestión de servicios de TI son estrategias estructuradas que guían la gestión de los servicios de TI dentro de la organización. Estas pautas proporcionan un conjunto de procesos, procedimientos y prácticas estandarizados diseñados para ayudar a ofrecer servicios de TI manera eficiente, segura y alineada con los objetivos del negocio. En una situación ideal, adherirse a un marco de trabajo de ITSM garantiza la alineación con los objetivos empresariales, la utilización óptima de los recursos y la mejora continua, aunque algunos marcos de trabajo se adaptan mejor a unas organizaciones que a otras. (14)

Los marcos de trabajo de ITSM más destacados y más utilizados en varios sectores TI son los siguientes: (14)

- ITIL: Ofrece un conjunto de prácticas recomendadas para la gestión de servicios de TI y se centra en alinear los servicios de TI con las necesidades empresariales.
- CMMI: La Integración del modelo de madurez de competencias (Capability Maturity Model Integration o CMMI) guía a las organizaciones en la mejora de los procesos proporcionando prácticas recomendadas para el desarrollo y el mantenimiento de los productos.
- Six Sigma: Es una estrategia basada en datos y diseñada para mejorar los procesos y alcanzar la excelencia operativa, eliminando por completo los errores mediante la identificación rápida de las causas raíz subyacentes a los defectos.
- COBIT: Es un marco de trabajo integral para gestionar y gobernar la TI empresarial. Se centra en alinear los objetivos de TI con los objetivos empresariales estratégicos, garantizar el cumplimiento normativo y optimizar las inversiones en TI.
- eTOM: El Mapa mejorado de operaciones de telecomunicaciones (Enhanced Telecom Operations Map o eTOM) ofrece un enfoque exhaustivo y orientado a la empresa que proporciona un lenguaje común y procesos estandarizados para garantizar la calidad y la eficiencia en la provisión de servicios de telecomunicaciones.
- ISO/IEC 20000: Es una norma internacional para ITSM. Describe los requisitos para que los proveedores de servicios puedan planificar, establecer, implantar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de servicio. El marco de trabajo ISO/IEC 20000 es compatible con muchos otros marcos de trabajo y estrategias, lo que garantiza el cumplimiento de los estándares de calidad al tiempo que optimiza la coherencia y la fiabilidad en la prestación de servicios.
- TOGAF: El Marco de trabajo de arquitectura de Open Group (Open Group Architecture Framework o TOGAF) es un marco de trabajo de arquitectura que se utiliza para desarrollar estrategias de TI eficientes a través de la mejora del diseño, la planificación, la implementación y el gobierno dentro de la arquitectura de TI de una organización.

En los siguientes subapartados, se analizan de forma más detallada los marcos de referencia para la gestión de servicios TI, más relevantes para el objeto del presente TFM:

2.3.1 Biblioteca de Infraestructura de Tecnologías de Información (ITIL)

La Biblioteca de Infraestructura de Tecnologías de Información (o ITIL, por sus siglas en inglés de Information Technology Infrastructure Library) es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas

de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidades y eficiencias en sus operaciones de TI. Esta definición aparece recogida en el libro: Preparación para la certificación ITIL Foundation V3 (11)

ITIL proporciona un marco de referencia para gestionar los servicios de TI a lo largo de su ciclo de vida, desde la planificación y el diseño hasta la entrega y la mejora continua.

Las prácticas de ITIL están generadas por la OGC (Office of Government Commerce, del Ministerio de Comercio Británico), quien tiene la propiedad intelectual. El enfoque ITIL se basa en la experiencia, es abierto, no propietario y público.

El MDEF en diversas disposiciones, cita a ITIL como ejemplo de marco de trabajo para tener en cuenta en la definición de procesos en los ciclos de vida de los servicios. Así mismo, en el desarrollo de este TFM se realizarán varias referencias a este estándar.

Los conceptos básicos de ITIL se basan en cuatro fundamentos: Las buenas prácticas, la gestión de los servicios, los procesos y las funciones, y el ciclo de vida de los servicios.

Para la introducción del marco ITIL y la gestión de servicios, existen una serie de conceptos que es conveniente aclarar, también para el entendimiento del presente TFM. Son los siguientes: (9)

- **Servicio:** Un servicio es un medio de entrega de valor a los clientes facilitando los resultados que los clientes desean lograr sin la responsabilidad sobre los costes y riesgos específicos. Los resultados se obtienen a través del desempeño de tareas y se ven limitados por la presencia de ciertas restricciones. En líneas generales, los servicios proporcionan resultados mediante la mejora del rendimiento y la reducción de las limitaciones de las restricciones.

- **Servicio de TI:** un servicio proporcionado por un proveedor de servicios TI. Un servicio de TI se compone de una combinación de tecnología de la información, personas y procesos.

- **Buenas practicas:** Son el marco o las líneas directrices para adoptar ITIL, que surgen como el resultado de la experiencia de las empresas.

- **Proceso:** Conjunto estructurado de actividades interrelacionadas, que permite alcanzar un objetivo.

- **Función:** Una función es un equipo o grupo de personas y de herramientas u otros recursos que se usan para ejecutar uno o más procesos o actividades. En muchas organizaciones, una función puede ser ejecutada a través de varios departamentos, equipos o grupos o puede ser ejecutada por un único grupo organizacional (ejemplo. Service Desk o Centro de Atención al Usuario)

La Operación del servicio ITIL describe las siguientes funciones en detalle: Service Desk (Mesa de servicio), Technical management (Gestión técnica), IT Operation management (Gestión de operaciones de TI) y Application management (Gestión de aplicaciones).

- **Rol:** Un rol es un conjunto de responsabilidades, actividades y autoridad asignada a una persona o equipo. Un rol es definido en un proceso o función.

Proveedor de servicios informáticos: Entidad que proporciona servicios a uno o varios clientes internos y externos.

- **Propietario del Servicio / Service Owner:** Rol responsable de la entrega de un determinado Servicio de TI. Es responsable de la mejora continua del servicio.

- **Gestor del Servicio (Service Manager):** Gestor que es responsable de gestionar el Ciclo de Vida de uno o más Servicios de TI de principio a fin.

- **Service Portfolio:** El Service Portfolio es el conjunto completo de servicios que se son gestionados por un proveedor de servicios

- Ciclo de vida del servicio: La arquitectura del Núcleo de ITIL se basa en el Ciclo de Vida del Servicio. Cada volumen del núcleo aparece representado en el Ciclo de Vida del Servicio.

Son fases del ciclo de vida del servicio: La Estrategia, el Diseño del Servicio, la Transición del Servicio, la Operación del Servicio y la mejora continua.

- Cadena de valor del servicio: que funciona como el ciclo de vida, describiendo seis actividades clave: planificar, interactuar, diseño y transición, obtener/crear, entregar y proporcionar soporte, y mejorar.

2.3.2 Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT)

Creada por la asociación norteamericana sin ánimo de lucro Information Systems Audit and Control Association (ISACA), COBIT® es el acrónimo en inglés de Objetivos de Control para la Información y la Tecnología relacionada.

COBIT es un marco de referencia para el gobierno y la gestión de la información y la tecnología, dirigido a toda la empresa. La I&T empresarial significa toda la tecnología y procesamiento de la información que la empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa, no limitándose por lo tanto al departamento de TI de una organización.

El marco de referencia propuesto por COBIT2019, y que se tomará como referencia para el desarrollo del presente TFM, aparece reflejado en los siguientes documentos:

- Marco de referencia COBIT® 2019: Introducción y metodología. (15)
- Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión. (16)

Ampliamente reconocido internacionalmente, ISACA define a COBIT como un “marco paraguas” que permite la alineación, mapeo e integración con múltiples estándares, marcos de referencia y regulaciones relevantes relacionados con los medios y servicios CIS/TIC. Esta consideración como “marco paraguas” es lo que ha facilitado su adopción por el MDEF como marco de referencia para asegurar la gestión efectiva de los sistemas y tecnologías de la información y comunicaciones (CIS/TIC). (15)

El MDEF ha adoptado COBIT 2019 para la consecución de los siguientes objetivos:

1. Estandarizar los procesos de gestión CIS/TIC a través de un enfoque normativo.
2. Garantizar la coherencia y la integridad técnica en todos los niveles del Ministerio.
3. Mejorar la gobernanza y la gestión de los servicios CIS/TIC, facilitando la centralización de la dirección estratégica y la descentralización operativa.
4. Optimizar la provisión de servicios CIS/TIC, asegurando su alineación con los objetivos operativos y estratégicos del Ministerio.
5. Monitorear y evaluar el cumplimiento de los servicios CIS/TIC con los niveles de rendimiento y control requeridos, facilitando la mejora continua de los procesos

A lo largo del desarrollo del TFM se volverá a hacer referencia a las interacciones entre COBIT y la gobernanza TIC en el MDEF. A continuación, la exposición se centrará Terminología y conceptos clave del marco de referencia COBIT, para introducir al lector en esta metodología.

2.3.2.1 Terminología y conceptos clave del marco de referencia COBIT

Gobierno y Gestión

El marco de referencia COBIT 2019 (15) hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.

El Gobierno asegura que:

- Las necesidades, condiciones y opciones de las partes interesadas se evalúan para determinar objetivos empresariales equilibrados y acordados.
- La dirección se establece a través de la priorización y la toma de decisiones.
- El rendimiento y el cumplimiento se monitorean en relación con la dirección y los objetivos acordados.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de dirección bajo el liderazgo del presidente.

Por su parte, la Gestión planifica, construye, ejecuta y monitorea actividades en alineación con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del director general ejecutivo (CEO).

COBIT define los componentes para crear y sostener un sistema de gobierno: procesos, estructuras organizativas, políticas y procedimientos, flujos de información, cultura y comportamientos, habilidades e infraestructura. Así mismo, define los factores de diseño que la empresa debería considerar para crear un sistema de gobierno más adecuado.

Si bien, se deben destacar una serie de conceptos erróneos acerca de COBIT que están relativamente generalizados:

- COBIT no es una descripción completa de todo el entorno de TI de una empresa.
- COBIT no es un marco de referencia para organizar procesos de negocio.
- COBIT no es un marco de referencia técnico (de TI) para gestionar toda la tecnología.
- COBIT no toma ni prescribe ninguna decisión relacionada con las TI. COBIT define todos los componentes que describen qué decisiones deberían tomarse, cómo deberían tomarse y quién debería tomarlas.

Objetivos de gobierno y gestión

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. La creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo.

El modelo core de COBIT abarca 40 objetivos de gobierno y gestión. COBIT define cada uno de ellos junto con su declaración de propósito, que es una elaboración más detallada de cada objetivo de gobierno y gestión.

Por otro lado, en relación a los objetivos de gestión, las necesidades de las partes interesadas deben transformarse en una estrategia factible para la empresa. COBIT 2019 (15) diferencia entre:

- Metas empresariales: Sobre las que tienen efecto las necesidades de las partes interesadas. COBIT 2019 identifica 13 metas empresariales a las que designa con la nomenclatura EGXX, junto con una serie de métricas asociadas a cada una de ellas.
- Metas de alineamiento: Sobre las que tienen efecto las metas empresariales. COBIT 2019 identifica 13 metas de alineamiento a las que designa con la nomenclatura AGXX, junto con una serie de métricas asociadas a cada una de ellas.

Las tablas del modelo COBIT también se proporcionan métricas de ejemplo para metas empresariales y metas de alineamiento. (Ver Figura 2-9)

Figura 3.3—Presentación de metas aplicables y métricas modelo	
El objetivo de gobierno/gestión respalda el logro de una serie de metas empresariales y de alineamiento primordiales:	
Metas empresariales	Metas de alineamiento
<EG REF> <DESCRIPCIÓN DE METAS>	<AG REF> <DESCRIPCIÓN DE METAS>
Métricas modelo para metas empresariales	Métricas modelo para metas de alineamiento
<EG REF> • <MÉTRICA>	<AG REF> • <MÉTRICA>
<EG REF> • <MÉTRICA>	<AG REF> • <MÉTRICA>

Figura 2-9 Representación de metas aplicables y métricas modelo (15)

Procesos de gobierno y gestión

Un objetivo de gobierno o gestión siempre está relacionado con un proceso (con un nombre idéntico o similar) y una serie de componentes relacionados de otros tipos para contribuir a lograr el objetivo.

Los objetivos de Gobierno están relacionados con Procesos de Gobierno. Los objetivos de gobierno se presentan en la Figura 2-10.

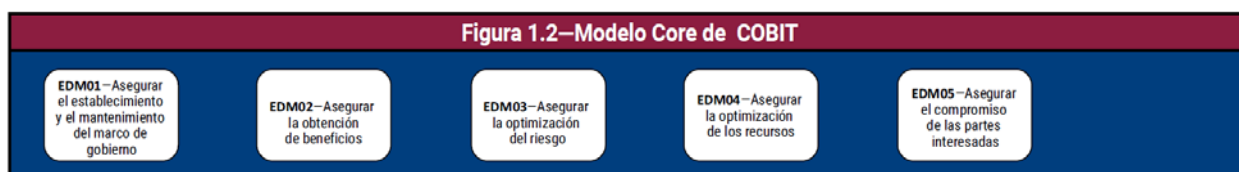


Figura 2-10 Procesos de Gobierno del modelo Core de COBIT (15)

Los objetivos de Gestión están relacionados con Procesos de Gestión.

Los objetivos de gestión representan las metas específicas que las áreas de TI deben alcanzar para apoyar los objetivos estratégicos de la organización. Estos se muestran en la Figura 2-11

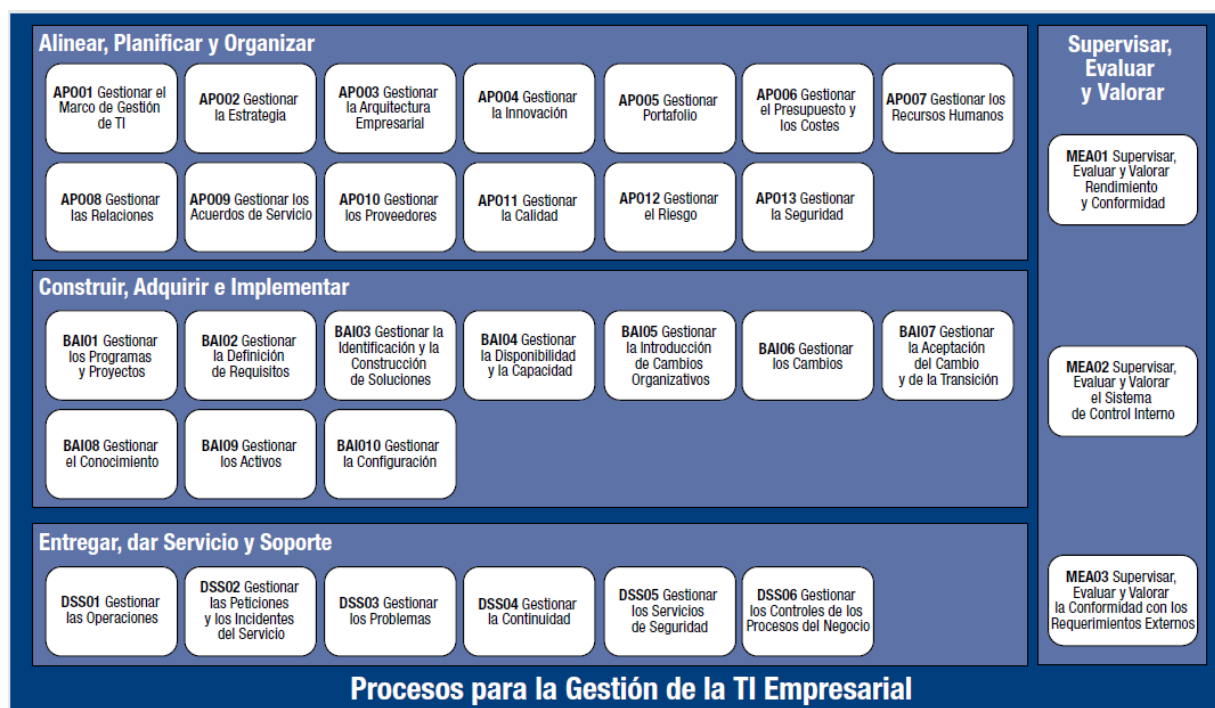


Figura 2-11 Procesos de Gestión del modelo Core de COBIT (15)

Los objetivos de gobierno y gestión de COBIT 2019 (15) se agrupan en cinco dominios. Los dominios se nombran mediante verbos que expresan el propósito clave y las áreas de actividad de los objetivos que los contienen.

Por un lado, los objetivos de gobierno se agrupan en el dominio **Evaluar, Dirigir y Monitorizar (EDM)**. En este dominio, el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia.

Por otro lado, objetivos de gestión se agrupan en cuatro dominios: (15)

- **Alinear, Planificar y Organizar (APO)** aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (I&T).
- **Construir, Adquirir e Implementar (BAI)** se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.
- **Entregar, Dar Servicio y Soporte (DSS)** aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad.
- **Monitorizar, Evaluar y Valorar (MEA)** aborda la monitorización del rendimiento y la conformidad de I&T con los objetivos de rendimiento internos, los objetivos de control interno y los requisitos externos.

Componentes del sistema de gobierno en COBIT 2019 (15)

Para satisfacer los objetivos de gobierno y gestión, cada empresa necesita establecer, personalizar y sostener un sistema de gobierno creado a partir de una serie de componentes, que interactúan entre sí, y que, de forma individual y colectiva, contribuyen al buen funcionamiento del sistema.

Los componentes pueden ser de diversos tipos. Los más comunes son los procesos. Sin embargo, los componentes de un sistema de gobierno incluyen también estructuras organizativas; políticas y procedimientos; elementos de información; cultura y comportamiento; habilidades y competencias; y servicios, infraestructura y aplicaciones.

Los Procesos describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de salidas que contribuyan a la consecución de la totalidad de los objetivos relacionados con las TI.

Se identifican 3 componentes del sistema de gobierno:

1) Componente A del sistema de gobierno: Procesos

Cada objetivo de gobierno y gestión incluye varias prácticas de proceso, que pueden ser de gobierno o gestión, según la Figura 2-12

Las **prácticas de proceso** se definen Como un conjunto de acciones específicas diseñadas para alcanzar los objetivos de gobernanza y gestión de TI. Estas prácticas están organizadas en procesos y proporcionan una guía estructurada para implementar y operar actividades clave que aseguren el cumplimiento de las metas empresariales relacionadas con las TIC. Cada proceso incluye una o más actividades. Cada práctica de proceso viene acompañada por un número limitado de métricas modelo para medir el logro de la práctica y su contribución al alcance del objetivo en su conjunto. (15)

Las **prácticas de gestión** son actividades específicas que se deben realizar para alcanzar los objetivos de gestión. Actúan como guías prácticas para implementar y ejecutar los procesos de gobernanza y gestión de TI.

Figura 3.4—Presentación del componente de procesos		
A. Componente: Proceso		
Práctica de gobierno/gestión	Métricas modelo	
<REF> <NOMBRE> <DESCRIPCIÓN>	<MÉTRICA>	
Actividades		Nivel de capacidad
1. <TEXTO>		<NR>
2. <TEXTO>		<NR>
n. <TEXTO>		<NR>
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
<NOMBRE DEL ESTÁNDAR>	<TEXTO>	
<NOMBRE DEL ESTÁNDAR>	<TEXTO>	

Figura 2-12 Presentación del Componente de Procesos del modelo Core de COBIT (15)

Se asigna un nivel de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos con distintos niveles de capacidad. Un proceso alcanza un cierto nivel de capacidad siempre que todas las actividades de ese nivel se realicen de forma satisfactoria. (15)

COBIT 2019, al igual que ITIL, respalda la Integración del Modelo de Madurez de la Capacidad (CMMI o Capability Maturity Model Integration), basado en un esquema de capacidad de los procesos que va de 0 a 5. El nivel de capacidad es una medida de lo bien que un proceso se ha implementado y funciona. (15)

La siguiente Figura 2-13 muestra el modelo, con los niveles de capacidad incrementales y las características generales de cada uno.

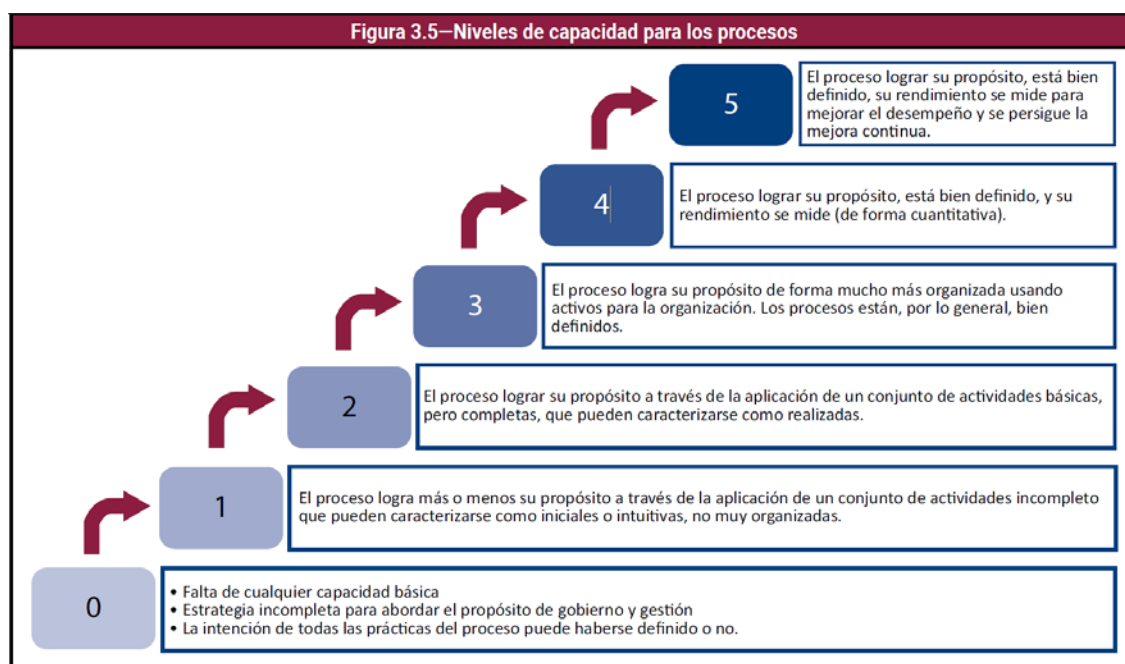


Figura 2-13 Niveles de Capacidad para los Procesos (15)

El modelo core de COBIT 2019 (15) asigna niveles de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos y las actividades requeridas para alcanzar los distintos niveles de capacidad.

Calificar las actividades del proceso:

Un nivel de capacidad puede alcanzarse en distinto grado, lo cual puede expresarse mediante una serie de calificaciones.

Algunos métodos formales que conducen a una certificación independiente usan una serie de calificaciones binarias de aprobado/falla.

Métodos menos formales (usados con frecuencia en contextos de mejora del desempeño) funcionan mejor con una serie de calificaciones más amplia, como el conjunto siguiente:

- Completamente—El nivel de capacidad se alcanza para más del 85 por ciento
- Largamente—El nivel de capacidad se alcanza para entre el 50 por ciento y el 85 por ciento.
- Parcialmente—El nivel de capacidad se alcanza para entre el 15 por ciento y el 50 por ciento
- No—El nivel de capacidad se alcanza para menos del 15 por ciento.

Cuando procede, también se han incorporado referencias a otros estándares y guías en esta sección. La Documentación relacionada menciona todos los estándares, marcos de referencia y requisitos de cumplimiento y otras guías relevantes para el proceso en cuestión. En las referencias específicas se mencionan capítulos o secciones específicas dentro de la Documentación relacionada.

Si no aparece una documentación relacionada para un componente determinado, significa que no se conocen referencias aplicables de las fuentes cruzada. Se promueve que la comunidad de profesionales sugiera las guías correspondientes.

2) Componente C del sistema de gobierno: Estructuras organizativas

El componente de gobierno de las estructuras organizativas sugiere niveles de responsabilidad y rendición de cuentas para las prácticas de los procesos.

Se han definido, entre otros, diversos roles y estructuras organizativas dentro del contexto de COBIT 2019: Consejo de Administración, Comité Ejecutivo, Director general ejecutivo (CEO), Director de operaciones (COO), Director de riesgos (CRO), Director de TI (CIO), Director de tecnología (CTO), Director de tecnologías digitales (CDO).

3) Componente B del sistema de gobierno: Flujos y elementos de información

El tercer componente de gobierno proporciona una guía sobre los flujos y elementos de información vinculados con las prácticas de los procesos. Cada práctica incluye entradas y salidas, con indicaciones de origen y destino.

En general, cada salida se envía a un único destino o una serie limitada de destinos, por lo general, otra práctica de proceso de COBIT 2019 (15). Esa salida se convierte entonces en entrada para su destino. Esto queda reflejado en la Figura 2-14

C. Componente: Flujos y elementos de información				
Práctica de gobierno/gestión	Entradas		Salidas	
<REF> <NOMBRE>	De	Descripción	Descripción	A
	<REF>	<TEXTO>	<TEXTO>	<REF>

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
<NOMBRE DEL ESTÁNDAR>	<TEXTO>
<NOMBRE DEL ESTÁNDAR>	<TEXTO>

Figura 2-14 Componente: flujos y elementos de información (15)

Se definen a continuación los conceptos de las columnas de la figura:

- Entradas:

Se refiere a la información o elementos que son necesarios para iniciar o ejecutar una práctica o proceso de gobierno o gestión. Son los insumos que se requieren para que un proceso comience o se desarrolle de manera efectiva.

- Origen (Columna “De”):

Indica el origen de la entrada. Es decir, quién o qué proceso provee la entrada (insumo) necesario para que la práctica de gestión comience o continúe. Puede ser un área específica, otro proceso o un actor dentro de la organización.

- Descripción:

Aquí se describe detalladamente qué tipo de información o elemento es la entrada o salida. La descripción es crucial para entender qué es lo que se va a utilizar o lo que se generará al completar una tarea o proceso. Se refiere al contenido específico que está vinculado con esa entrada o salida.

- Salidas:

Son los resultados o productos generados al finalizar la ejecución de la práctica o proceso. Se trata de la información que se produce y que puede servir como insumo para otros procesos o ser utilizada por otros actores.

- Destino (columna “A”):

Este campo se refiere a quién recibe o qué proceso recibe la salida generada. En otras palabras, indica el destino de la salida, que puede ser otro proceso de negocio o un actor dentro del sistema de

gestión. Sin embargo, algunas salidas tienen muchos destinos (p. ej. todos los procesos de COBIT o todos los procesos dentro de un dominio).

2.3.3 Gestión de Servicios de Tecnologías de la Información (ITSM)

La gestión de servicios de tecnologías de la información (en inglés IT Service Management, ITSM) es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final. ITSM propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios de punta a cabo usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la Information Technology Infrastructure Library (ITIL) o el eSCM (enabled Service Capability Model).

El principio fundamental de ITSM es que las funciones de TI deben funcionar como un servicio, centrándose en las necesidades de los usuarios y alineando los sistemas tecnológicos con los objetivos empresariales establecidos. Por este motivo, ITSM va mucho más allá de las funciones básicas de soporte de TI. De hecho, la estrategia de ITSM debe abarcar todos los aspectos de la tecnología de la información dentro de la empresa, desde la configuración de equipos básicos hasta la identificación de interrupciones no planificadas del servicio u otros eventos disruptivos y la respuesta a ellos. ITIL es la más reconocida y confiable fuente de orientación sobre mejores prácticas en el área de ITSM. (14)

ITSM establece un puente esencial que conecta a los profesionales de TI de la organización con los usuarios finales, lo que aporta unos claros beneficios para las empresas, que tal como se recoge en el Marco COBIT 2019 (14), son los siguientes:

- Mayor agilidad: ITSM ayuda a las empresas a responder rápidamente a los cambios en el mercado y las oportunidades emergentes.
- Aumento de la satisfacción de los usuarios o empleados: Al prestar la TI como un servicio y mantener las necesidades de los usuarios en primer plano.
- Mejora de la capacidad de adaptación de los procesos: ITSM mejora la eficiencia de los procesos, lo que permite a las organizaciones gestionar procesos y desarrollos de TI más importantes sin comprometer la calidad.
- Detección de incidentes y respuesta más rápidas: La mayor visibilidad de la TI que aporta ITSM permite identificar los problemas potenciales y tomar acción antes de que estos se vuelvan más graves.

La gestión del servicio de TI (ITSM) se define un conjunto de capacidades organizativas especializadas que proporcionan valor a los clientes en forma de servicios. Las capacidades adoptan la forma de funciones y procesos para gestionar servicios durante un ciclo de vida, con especializaciones en estrategia, diseño, transición, operación y mejora continua. El acto de transformación de recursos en servicios de valor se encuentra en el centro de la gestión del servicio. Sin estas capacidades, una organización del servicio es simplemente un conjunto de recursos que, por sí mismos, tienen un valor intrínseco relativamente bajo para los clientes. (9)

Para finalizar este apartado, es relevante hacer referencia al concepto del ciclo de vida de la Gestión de Servicios de TI planteado por ITSM, que aparece como una evolución de más conocido ciclo de Vida de los Servicios ITIL, a su vez basado, en el ciclo de Deming, PDCA o Mejora Continua.



Figura 2-15 Ciclo de vida de Gestión de Servicios propuesto por ITSM¹⁸

El ciclo de Gestión de Servicios de ITSM, a diferencia del marco tradicional de ITIL, que organiza el ciclo en cinco fases (Estrategia, Diseño, Transición, Operación, y Mejora Continua del Servicio), agrupa los elementos en áreas funcionales que son más operativas y específicas, tal como se puede observar en la Figura 2-15

2.3.3.1 Herramientas de Gestión ITSM

Una herramienta de gestión de servicios de TI (ITSM por sus siglas en inglés, IT Service Management) es una plataforma de software diseñada para ayudar a las organizaciones a planificar, gestionar, entregar y soportar sus servicios de tecnología de la información (TI) de manera estructurada y alineada con los objetivos de negocio.

Una herramienta ITSM posibilita la gestión de las siguientes actividades:

- **Gestión de Incidentes:** Permite registrar, clasificar, priorizar, asignar y resolver incidencias reportadas por los usuarios, ayudando a restaurar el servicio normal lo antes posible y minimizar el impacto en las operaciones del negocio.
- **Gestión de Problemas:** Facilita la identificación y el análisis de las causas raíz de los incidentes recurrentes, evitando que estos se repitan y mejorando la estabilidad y la fiabilidad de los servicios.
- **Gestión de Cambios:** Proporciona un proceso estructurado para solicitar, aprobar y documentar cambios en la infraestructura de TI, reduciendo los riesgos asociados a los cambios en sistemas críticos.
- **Gestión de Activos y Configuración:** A través de una Base de datos de Gestión de la Configuración (CMDB por sus siglas en inglés Configuration Management Database) que permite la administración y el seguimiento de todos los activos de TI (hardware, software, redes, etc.) y de sus configuraciones. Esto ayuda a visualizar cómo interactúan los diferentes componentes y a planificar el soporte y el mantenimiento.
- **Catálogo de Servicios y Portal de Autoservicio:** Un catálogo de servicios documenta todos los servicios de TI que están disponibles para los usuarios. A través del portal de autoservicio, los usuarios pueden acceder a este catálogo, realizar solicitudes, consultar información y recibir soporte sin intervención directa del personal de TI.

¹⁸ ITSM - Alcor Solutions, Inc.

- **Gestión de Solicitudes de Servicio:** Facilita la gestión de peticiones de usuarios para acceder a servicios, realizar configuraciones o recibir soporte adicional, con un flujo de trabajo que asegura que cada solicitud sea atendida adecuadamente.
- **Acuerdos de Nivel de Servicio (SLA):** Las herramientas ITSM suelen incluir la funcionalidad de gestión de SLA, permitiendo definir, monitorear y asegurar el cumplimiento de los niveles de servicio acordados con los clientes y usuarios.
- **Informes y Métricas:** Las herramientas ITSM ofrecen capacidades de análisis y generación de reportes, lo cual permite a los equipos de TI medir el rendimiento, identificar tendencias, y detectar áreas de mejora.

Situación actual y soluciones de mercado

Las herramientas de gestión ITSM han evolucionado significativamente en la última década, pasando de simples sistemas de tickets a plataformas integrales que aprovechan la inteligencia artificial, automatización y análisis avanzado. De acuerdo con BMC Software (17) las herramientas ITSM modernas están incorporando nuevas capacidades como:

- **Inteligencia Artificial y Machine Learning** para la automatización inteligente de clasificación de tickets o la incorporación de Chatbots y asistentes virtuales para soporte de primer nivel.
- **Herramientas de análisis avanzado** para la gestión predictiva de servicios, de tendencias o capacidades de reporting avanzado.
- **Integración con herramientas ágiles de DevOps**¹⁹ como Jira, proporcionando capacidades de gestión de código y despliegue, automatización de pruebas y validación, y monitorización continua y feedback loops.

Entre las soluciones actuales de ITSM existentes en el mercado, de acuerdo con BMC Software (17) y ServiceNow, Inc, (14) se pueden destacar las siguientes:

BMC Remedy ITSM:

BMC Remedy, establecida en 1990, se ha mantenido como una de las soluciones ITSM más robustas y completas del mercado. La plataforma ha evolucionado significativamente desde sus inicios como un sistema cliente-servidor hasta convertirse en BMC Helix, su versión moderna basada en la nube. La plataforma muestra conformidad comprobada con ITIL, una amplia base de conocimientos y comunidad de usuarios y una gran capacidad de personalización.

Son características distintivas de BMC Remedy las siguientes:

- Gestión completa del ciclo de vida de incidentes y problemas.
- CMDB integrada con capacidades de descubrimiento automático
- Integración con herramientas de monitorización y gestión de eventos

ServiceNow:

ServiceNow se ha posicionado en la actualidad como uno de los líderes indiscutible en el mercado ITSM, destacando por su plataforma cloud-native y su capacidad de integración empresarial. Sus principales características incluyen:

- Arquitectura basada en una única plataforma que permite la gestión unificada de servicios

¹⁹ DevOps (acrónimo inglés de development -desarrollo- y operations -operaciones-) es un conjunto de prácticas que agrupan el desarrollo de software (Dev) y las operaciones de TI (Ops). Su objetivo es hacer más rápido el ciclo de vida del desarrollo de software y proporcionar una entrega continua de alta calidad. Fuente: Wikipedia.

- Capacidades avanzadas de automatización mediante flujos de trabajo
- Integración nativa con IA y Machine Learning para la categorización automática de incidentes
- Amplia biblioteca de integraciones y APIs
- Personalización extensiva mediante desarrollo low-code

Atlassian Jira Service Management:

Destacada por su integración natural con otras herramientas de desarrollo y colaboración, ofrece:

- Fuerte integración con herramientas de desarrollo y DevOps
- Automatización flexible y personalizable
- Amplio marketplace de plugins y extensiones

En la actualidad un gran número de grandes empresas a nivel mundial han implementado herramientas de Gestión de Servicios de TI (ITSM) para optimizar sus operaciones y mejorar la eficiencia en la prestación de servicios, como son: SAP® SuccessFactors HCM, Group Health (Kaiser Permanente Washington), Royal Bank of Scotland, entre otras²⁰.

En el ámbito de la Administración Pública española, diversas administraciones en todos los niveles han implantado soluciones de ITSM para gestionar sus servicios de TI, como son la Dirección General de Tráfico (a través del uso del software Jira)²¹, el Ministerio de Hacienda y Administraciones Públicas (que ha utilizado la herramienta BMC Remedy ITSM)²², el Ayuntamiento de Madrid o la Sociedad Municipal de Autobuses Urbanos de Valladolid, S. A. (AUVASA)²³

Herramienta de Gestión ITSM en el MDEF

Para el MDEF, la herramienta ITSM se constituye como el instrumento para materializar el modelo de alto nivel para el gobierno y la gestión única de servicios CIS/TIC, ya que Catálogo de Servicios y todos los procesos deben ser soportados por herramientas para la gestión de servicios, que actúen como catalizadores de la transformación digital, y ejecutados a través del concepto CEGES I3D. (8)

La herramienta a través de la cual el MDEF desarrollará todo este proceso de Gestión de Servicios es ProactivaNET ITSM Software.

ProactivaNet ITSM Software es una herramienta integral en la gestión de servicios de TI, cuyo fabricante es Espiral Microsistemas S.L. y su sede central está en España (Espacio Tecnológico Molinón, Gijón, Asturias) y tiene oficinas propias en México, Perú, Colombia y Chile.

La implementación de la nueva herramienta ProactivaNet para toda la I3D, se considera un factor crítico de éxito para alcanzar una gestión eficiente y única para todos los servicios CIS/TIC del Departamento. La utilización de la misma herramienta para todos los dominios de seguridad es esencial para la gestión única e integral de los servicios CIS/TIC, optimizando el recurso material y de personal, y permitiendo no sólo mantener las capacidades operativas actuales, sino aumentarlas debido a su potencialidad. Por todo ello, ProactivaNet se considera como una herramienta vital para el control, seguimiento y mejora de la prestación de los servicios que proporciona el CESTIC. La herramienta dispone del potencial necesario para desplegar todos los servicios de la I3D con todos sus procesos de gestión asociados.

²⁰ Fuente: <https://www.servicenow.com/es/lpebk/leave-legacy-itsm.html>

²¹ Fuente: Plataforma de contratación del sector público

²² Fuente: Plataforma de contratación del sector público

²³ Fuente: file:///C:/Users/AMURMAR/Downloads/Pliego%20de%20Condiciones%2020240120%20CM%20(1).pdf

El estudio de la incorporación de la herramienta ITSM al modelo para la gestión única de servicios del CESTIC se constituye como uno de los objetivos del presente TFM. Este análisis busca identificar y proponer soluciones para su implementación en diversas áreas clave. Sin embargo, dada la amplitud y complejidad que conlleva la implementación de una herramienta ITSM de estas características, resulta inviable abarcar todas sus dimensiones dentro del alcance de este TFM. Por ello, el trabajo se centrará en analizar y desarrollar las funcionalidades más relevantes y alineadas con el propósito definido para este estudio.

2.3.4 Relación entre los marcos ITIL, COBIT, DevOps e ITSM

Un marco de trabajo de TI adecuado puede suponer una diferencia muy positiva en la eficiencia y la utilización de los servicios de TI, y las empresas disponen de varios marcos de trabajo entre los que elegir. Entre los más populares se encuentran los asociados con ITSM/ITIL y DevOps.

Tal como se explicó anteriormente, ITSM hace referencia a un enfoque estratégico para diseñar, suministrar, gestionar y mejorar la forma en que se utiliza la tecnología de la información dentro de una organización. Garantiza que los servicios de TI estén en línea con las necesidades empresariales, para lo que incorpora diversas prácticas y procesos de prestación de servicios de un extremo a otro. De acuerdo con Service Now, (14) ITSM se ocupa del ciclo de vida continuo de los servicios de TI, no solo de su diseño o implementación.

Por su parte, el marco de trabajo ITIL suele considerarse un subconjunto de ITSM; ya que es un conjunto de pautas de prácticas recomendadas para la gestión de servicios de TI. ITIL proporciona las herramientas y técnicas necesarias para alinear los servicios de TI con las necesidades de la empresa.

Mientras que ITIL y ITSM se centran en la gestión de servicios de TI, COBIT se enfoca en la gobernanza general de TI y cómo se alinean las actividades de TI con los objetivos estratégicos de negocio. COBIT proporciona, por lo tanto, un marco de gobierno superior, que permite alinear diferentes metodologías con objetivos empresariales.

Por su parte DevOps se centra en la automatización y la integración entre equipos de desarrollo y operaciones, tendiendo por objetivo principal reducir el tiempo de entrega de software manteniendo alta calidad y confiabilidad.

ITSM, ITIL, DevOps y COBIT no son mutuamente excluyentes, y cada uno tiene sus propios objetivos y funciones, pudiendo utilizarse conjuntamente para ofrecer una estrategia más completa de gestión de TI. De hecho, muchos equipos modernos utilizan Desarrollo y operaciones junto con ITSM e ITIL.

3 DESARROLLO DEL TFM

3.1 Alcance del desarrollo.

El desarrollo de este trabajo se centrará en la implantación de un Modelo Único de Gestión de Servicios CIS/TIC para el Ministerio de Defensa Español, y en otras actividades conexas a ese propósito; cuya responsabilidad de desarrollo recae en la D.G. Centro de Sistemas y Tecnologías de la Información y Comunicaciones del Ministerio de Defensa (CESTIC)

El Alcance del desarrollo se estructurará en tres subapartados:

Un primer subapartado dedicado a la Implantación de un Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF, que comienza por incluir una imagen de la situación actual y describir el plan de implementación que el MDEF ha estimado conveniente seguir para alcanzar esta meta. A partir de aquí, el TFM se centra en la revisión de los 3 documentos normativos más importantes, que el MDEF ha aprobado para servir de marco para la instauración de este modelo de gestión. El TFM se centra en analizar el contenido de esta normativa para comprobar su alineamiento con el marco de referencia de gestión de servicios COBIT 2019 (15) y formula recomendaciones de mejora allí donde sea necesario, tomando como referencia los objetivos y prácticas de gestión aconsejados por COBIT que muestren una mayor vinculación con el propósito de cada norma.

Un segundo subapartado se dedica a la Monitorización de la infraestructura de I&T, que aparece incluido como uno de los objetivos dentro de la implantación del Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF, pero que cuenta con suficiente entidad como para dedicarle un apartado propio. Este subapartado se inicia con una descripción de la situación actual y los objetivos a perseguir con la monitorización. También se formulan unas recomendaciones de métricas de seguimiento específicas para el Centro de Servicio al Usuario (CAU)

A partir de este punto, el subapartado formula una propuesta para la visualización sintética de las variables relevantes a monitorizar relativas a la infraestructura y los servicios, con el objetivo de facilitar a los responsables una gestión eficiente de los mismos. Esta propuesta se concreta a través de la recomendación de la herramienta Grafana, para la construcción de paneles de observabilidad, y de un diseño de arquitectura de software que integre las distintas fuentes de datos mediante la herramienta ElasticSearch, como una única plataforma de almacenamiento de datos, de la que se alimente la Grafana para la generación de los paneles de visualización.

Un tercer subapartado se centra en la incorporación de la herramienta ITSM ProactivaNet al modelo para la gestión única de servicios del CESTIC. El subapartado comienza con el estudio de la sintonía existente entre la utilización de una herramienta ITSM y los principios del marco COBIT, siguiendo con una definición de la fotografía actual y una descripción de las metas a lograr con el despliegue de ProactivaNet. A continuación, se presenta una propuesta de esquema de implementación de la herramienta en el CESTIC, así como una definición de una estructura de roles y responsabilidades asociados a cada servicio, aspectos indispensables para garantizar un despliegue exitoso de la herramienta.

El desarrollo del TFM finaliza con un cuarto subapartado dedicado a una comparativa entre distintas herramientas de ITSM, para lo cual se formula una propuesta de metodología de estudio comparativo entre ProactivaNet, la herramienta utilizada SCANS utilizada hasta la actualidad en el MDEF, y otras soluciones del mercado. Esta comparativa se basa en información recopilada de fuentes internas y externas al CESTIC, concluyendo que ProactivaNet es una opción adecuada para los objetivos del MDEF en este ámbito.

La Figura 3-1 expuesta a continuación muestra las actuaciones específicas que en el desarrollo del TFM se han contemplado para cada una de las áreas funcionales planteadas por el ciclo de Vida de los Servicios ITIL



Figura 3-1 Ciclo de vida de Gestión de Servicios propuesto por ITSM (Fuente: Elaboración propia)

3.2 Implantación de un Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF

La Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7) establece como el primero de sus objetivos globales para el MDEF:

- OBG-1. Proporcionar un Modelo de Gestión de Servicios CIS/TIC centralizado, único, documentado, definible, repetible y escalable con las mejores prácticas recomendadas.

De acuerdo con este objetivo, el CESTIC debe proporcionar un modelo de gestión única de servicios, basada en procesos únicos para todo el MDEF, y amparado sobre un marco de trabajo integral para el gobierno y la gestión CIS/TIC. Debe alinear los servicios CIS/TIC con los objetivos del Ministerio de Defensa, y la gobernanza CIS/TIC. Su finalidad es proporcionar servicios seguros y de calidad, manteniendo un equilibrio entre la satisfacción del usuario, la optimización del riesgo y el uso de los recursos. (7)

Con la implantación de modelo de gobernanza, se pretende modelar la transición desde la situación actual (AS-IS) hasta la situación objetivo (TO BE) reflejada en la Tabla 3-1. La situación que se presenta como actual se refiere a la situación del Departamento a fecha de enero de 2024.

Situación actual de Gestión (AS-IS)	Situación objetivo de Gestión (TO-BE)
No se dispone de un Catálogo de Servicios único ni valorado económicamente	Catálogo único con todos los servicios identificados y valorados
Se identifican procesos diferentes según el servicio, no existiendo procesos estandarizados.	Procesos estandarizados, únicos y basados en buenas prácticas COBIT e ITIL
Duplicidad de herramientas que no dan soporte a todos los procesos de la gestión.	Herramienta única ITSM (sencillez y simplicidad). Racionalización de otras herramientas existentes.
Falta de coordinación y solapamiento de cometidos	Organización del personal según roles y mejora de la coordinación para su trabajo
No se han definido métricas que permitan evaluar los niveles de calidad del Servicio.	Definir métricas para evaluar la calidad de la prestación de los servicios, y realizar un seguimiento de las mismas.

Tabla 3-1 Identificación de la situación actual y objetivo del CESTIC en relación al modelo para el gobierno y la gestión única de servicios. Fuente (7) y elaboración propia.

Para la implantación de este Modelo de Gobierno y Gestión Única de Servicios, la Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7) plantea el desarrollo de un plan estructurado en una serie de fases secuenciales. Cada una de estas fases estará asociada a una serie de procesos de gestión correspondientes a los 4 dominios contemplados en los objetivos de gestión del marco COBIT 2019 (15). La culminación de estos procesos permitirá el logro de las capacidades de gestión CIS/TIC requeridas por el Departamento.

A continuación, se expone cada una de las fases con los efectos que se pretenden conseguir:

Fases	Procesos estandarizados	Efectos
Fase 1 – Soporte del Servicio	DSS01 – Gestionar las operaciones	• Prestación de servicios conforme a los requisitos operativos del MDEF. • Continuidad y disponibilidad del servicio. • Optimización de la funcionalidad de los procesos internos del MDEF. • Habilidades, motivación y productividad del personal.
	DSS02 – Gestionar las peticiones y las incidencias del servicio	
	DSS03 – Gestionar los problemas	
	DSS04 – Gestionar la continuidad	

	DSS06 – Gestionar los controles de procesos funcionales y operativos	
Fase 2 – Gestión del marco y de la estrategia de gestión de servicios	APO01 – Gestionar el marco de gestión CIS/TIC	• Enfoque de gestión consistente para los requisitos de gobierno CIS/TIC. • Enfoque holístico en el ámbito CIS/TIC con una estrategia global. • Arquitectura CIS/TIC en capas de procesos, datos, información, aplicaciones y tecnología. • Cambio eficiente en la organización. • Maximización de la probabilidad de éxito de un cambio organizativo. • Compromiso de las partes interesadas y reducción del riesgo al fracaso ante cambios organizativos. • Apoyo a la estrategia de transformación digital del MDEF
	APO02 – Gestionar la estrategia CIS/TIC	
	APO03 – Gestionar las arquitecturas CIS/TIC	
Fase 3 – Gestión del Catálogo de Servicios	APO05 – Gestionar el portafolio	• Portafolio y catálogo de servicios competitivo. • Cultura del servicio orientado al usuario. • Mejora en la prestación de servicios. • Continuidad del servicio. • Optimización de los procesos.
	APO09 – Gestionar los acuerdos de servicio	
	BAI05 – Gestionar el cambio organizativo	
Fase 4 – Despliegue del Servicio	BAI04 – Gestionar la disponibilidad y la capacidad	• Mejora de la continuidad y disponibilidad del servicio. • Disminución de incidencias críticas para el Departamento. • Agilidad para convertir los requisitos del Departamento en soluciones operativas. • Mejora en la idoneidad de soluciones CIS/TIC para el Departamento. • Mejora en la gestión de programas y proyectos de transformación digital.
	BAI06 – Gestionar los cambios CIS/TIC	
	BAI07 – Gestionar la aceptación y la transición de los cambios CIS/TIC	
	BAI09 – Gestionar los activos	
	BAI10 – Gestionar la configuración	
Fase 5 – Gestión de riesgos	APO12 – Gestionar el riesgo	• Mejora en la gestión del riesgo.
Fase 6 – Calidad y Mejora Continua	APO11 – Gestionar la calidad	• Ejecución de programas dentro del

	BAI02 – Gestionar la definición de requisitos	• plazo sin exceder el presupuesto y que cumplan con los requisitos y estándares de calidad. • Optimización de costes de los procesos. • Mejora en la gestión de programas y proyectos de transformación digital. • Mejora en la calidad de la información. • Optimización de los procesos. • Prestación de servicios con mayor calidad. • Mejora y optimización en los procesos a través de la explotación del conocimiento en el Departamento. • Mejora en la agilidad para convertir los requisitos del Departamento en soluciones operativas. • Supervisión del rendimiento y productividad. • Mejora en la toma de decisiones.
	BAI08 – Gestionar el conocimiento	
	MEA01 – Gestionar la supervisión del rendimiento y la conformidad	
Fase 7 – Relación con actores externos	APO10 – Gestionar los proveedores	• Prestación de servicios de forma competitiva. • Aseguramiento de la continuidad del servicio. • Aseguramiento del cumplimiento con normas y regulaciones externas. • Mejora en la productividad del personal. • Personal competente y motivado con un entendimiento de la tecnología. • Conocimiento y experiencia e iniciativas para la innovación en el MDEF. • Agilidad para convertir los requisitos del MDEF en soluciones operativas • Ejecución de programas dentro del plazo sin exceder el presupuesto y que cumplan con los requisitos y estándares.
	APO08 – Gestionar las relaciones	
	BAI03 – Gestionar la identificación y construcción de soluciones	

Tabla 3-2 Fases, procesos estandarizados de gestión y efectos a alcanzar por el MDEF. (7)

A lo largo del año 2024, el CESTIC ha logrado importantes avances en la materialización de un Modelo de Gestión de Servicios CIS/TIC centralizado.

En septiembre de 2024 el CESTIC consiguió definir y lanzar un Catálogo Único de Servicios, con el propósito de integrarlo en la herramienta ProactivaNet, lo que implica la consecución del primer punto de la Tabla 3-1 Identificación de la situación actual y objetivo del CESTIC en relación al modelo para el gobierno y la gestión única de servicios. Fuente (7) y elaboración propia.

Hay que tener en cuenta, por tanto, que la situación a inicio de redacción de este TFM, a otoño de 2024, no es la misma que la situación inicial planteada en la Tabla 3-1 Identificación de la situación actual y objetivo del CESTIC en relación al modelo para el gobierno y la gestión única de servicios. Fuente (7) y elaboración propia., que muestra la fotografía a comienzos de 2024.

Una vez definido el catálogo de servicios, el siguiente paso para el logro de las capacidades de gestión CIS/TIC requeridas por el Departamento, consiste en el despliegue de una herramienta única ITSM (ProactivaNet). El cumplimiento de este fin está muy alineado con el objetivo de gestión APO01 – Gestionar el marco de gestión CIS/TIC, contemplado en la Fase 2 – Gestión del marco y de la estrategia de gestión de servicios, del plan de implantación del Modelo de Gobierno y Gestión Única de Servicios propuesto en la Tabla 3-2 Fases, procesos estandarizados de gestión y efectos a alcanzar por el MDEF. (7)

El despliegue de una herramienta ITSM en el CESTIC constituye en sí mismo un proyecto de gran envergadura, y es por ello por lo que se le dedicará un subapartado propio dentro de este TFM (3.3)

3.2.1 Marco normativo de gestión:

Diseñar un Modelo de Gestión de servicios TI para una organización comprende el también establecimiento de un marco normativo de gestión, con procedimientos y prácticas claras, para la normalización independiente del dominio Alinear, Planificar y Organizar; este proceso implica la implantación del uso de Instrucciones Técnicas (IT) e Instrucciones Operacionales (IOP) en base a plantillas. Esta información es básica para la implantación del sistema. Así mismo, es preciso la creación de una estructura formal que permita la gestión de los procesos y servicios de TI de forma eficiente, transparente y conforme a las políticas y objetivos organizacionales.

Como se ha mencionado con anterioridad, para la gestión de Catálogo de Servicios, el CESTIC aprobado Instrucciones Técnicas y otros documentos, con el objeto de establecer un marco normativo de gestión. Para el propósito de este TFM, los documentos más relevantes a analizar son los siguientes:

- TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D
- Instrucción Técnica 04/24 del CESTIC Puesta en Operación de Nuevos Servicios en el Ámbito del CESTIC
- Acuerdo de Provisión de Servicio 01/24 del CESTIC Sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC

3.2.2 TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D

Para el análisis del marco normativo propuesto para el Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF, se considera relevante el estudio de la TD176 - Instrucción Técnica del CESTIC GESTIÓN DEL CATÁLOGO DE SERVICIOS CIS/TIC EN LA I3D, tomando como referencia el Objetivo de Gestión APO05 - Gestionar el portafolio, proporcionado por el marco COBIT 2019. (16)

Objetivo de Gestión APO05 - Gestionar el portafolio.

Este objetivo de gestión pertenece al Dominio: Alinear, Planificar y Organizar. El análisis del mismo se realiza en la correspondiente tabla de Proceso: Objetivo de gestión: APO05 - Gestionar el portafolio, del documento denominado “Objetivos de gobierno y gestión, COBIT 2019 Marco de Referencia” (16), la cual establece las siguientes previsiones para este objetivo:

Descripción: Ejecutar la dirección estratégica establecida para las inversiones, en línea con la visión de la arquitectura empresarial y la hoja de ruta de I&T. Considerar las diferentes categorías de inversiones y las limitaciones de recursos y financiación. Evaluar, priorizar y equilibrar los programas y servicios, gestionando la demanda dentro de las limitaciones de recursos y financiamiento, basándose en su alineación con los objetivos estratégicos, el valor y el riesgo de la empresa. Mover los programas seleccionados al portafolio de productos o servicios activa para su ejecución. Supervisar el rendimiento del portafolio general de productos y servicios, y programas, proponiendo ajustes según sea necesario en respuesta al rendimiento del programa, producto o servicio, o cambiando las prioridades de la empresa.

Propósito: Optimizar el rendimiento del portafolio general de programas en respuesta al rendimiento individual de programas, productos y servicios y a las cambiantes prioridades y demandas de la empresa. El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:

Son metas empresariales vinculadas con este objetivo:

- EG01 Portafolio de productos y servicios competitivos
- EG08 Optimización de la funcionalidad de procesos del negocio internos
- EG12 Gestión de programas de transformación digital

Son metas de alineamiento vinculadas con este objetivo:

- AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T
- AG05 Prestación de servicios de I&T conforme a los requisitos del negocio

Para el Objetivo de gestión: APO05 - Gestionar el portafolio, el marco COBIT 2019 (16) prevé diversas prácticas de gestión:

- Práctica de gestión - APO05.01 Determinar la disponibilidad y las fuentes de fondos.
- Práctica de gestión - APO05.02 Evaluar y seleccionar programas para financiar.
- Práctica de gestión - APO05.03 Monitorizar, optimizar e informar sobre el rendimiento del portafolio de inversión.
- Práctica de gestión - APO05.04 Mantener los portafolios.
- Práctica de gestión - APO05.05 Gestionar el logro de beneficios.

Para el caso particular del análisis de mejora de las operaciones en el CESTIC, es muy relevante el estudio de la práctica de Práctica de gestión prevista en el Marco COBIT 2019 (16): APO05.04 Mantener los portafolios.

APO05.04 Mantener los portafolios:

Mantener los portafolios de los programas y proyectos de inversión, productos y servicios de I&T y los activos de I&T. Para esta práctica de gestión, el marco COBIT propone las siguientes metas y actividades:

Métricas modelo

- a. Números de programas y proyectos finalizados

b. Tiempo transcurrido desde la última actualización del portafolio de servicios

Actividades vinculadas a la Práctica de gestión APO05.04 Mantener los portafolios. (Tabla 3-3)

Actividades	Nivel de capacidad
1. Crear y mantener portafolios de programas de inversión habilitados por I&T, servicios prestados por I&T y activos de I&T, que forman la base para el presupuesto de I&T actual y respaldan los planes tácticos y estratégicos de I&T.	3
2. Trabajar con gestores de servicios para conservar el portafolio de servicios. Trabajar con gestores de operaciones, gestores de producto y arquitectos para conservar los portafolios de activos. Priorizar los portafolios para respaldar las decisiones de inversión..	
3. Retirar un programa del portafolio de inversiones activas cuando los beneficios empresariales deseados se han alcanzado o cuando está claro que los beneficios no se alcanzarán dentro de los criterios de valor establecidos para el programa.	

Tabla 3-3 Lista de actividades asociadas a la Práctica de gestión: APO05.04 Mantener los portafolios. (16)

En este punto se considera apropiado estudiar si el documento TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D, muestra concordancia con las actividades asociadas Práctica de gestión APO05.04 Mantener los portafolios, teniendo en cuenta la situación actual del desarrollo de estas actividades en el CESTIC.

De este análisis, se concluye que el documento TD176 - Instrucción Técnica del CESTIC: Gestión del Catálogo de Servicios CIS/TIC en la I3D; muestra alineación con las prácticas de gestión del portafolio establecidas en COBIT. Sin embargo, es importante resaltar que este documento se enfoca principalmente en la gestión del catálogo de servicios operativos y en mantener la información precisa y actualizada en la herramienta ITSM, no en el portafolio completo que incluye servicios en todas las fases de su ciclo de vida.

El documento cumple con varios elementos relevantes para APO05.04, tales como:

- Mantenimiento de información precisa sobre el catálogo: Define un proceso detallado para la actualización, auditoría y gestión de calidad de los datos de los servicios, alineado con el objetivo de APO05.04 de garantizar que el portafolio esté completo y refleje la realidad operativa.
- Roles y responsabilidades: Asigna roles específicos (como el Gestor del Catálogo y los responsables de vistas) para asegurar que el catálogo esté actualizado y que cada vista relevante reciba la información adecuada, lo cual es consistente con el enfoque de COBIT en la asignación clara de roles para mantener la integridad del portafolio
- Vistas estructuradas del catálogo: Ofrece distintas vistas (usuario, técnica, y de seguridad) que responden a las necesidades de los interesados, apoyando la transparencia y alineación del catálogo con los objetivos del negocio, lo cual también está alineado con APO05.04

3.2.3 Instrucción Técnica 04/24 del CESTIC Puesta en Operación de Nuevos Servicios en el Ámbito del CESTIC

Con el objeto de evaluar el marco normativo propuesto para el Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC en el MDEF, se estima pertinente el análisis de la Instrucción Técnica 04/24 del CESTIC Puesta en Operación de Nuevos Servicios en el Ámbito del CESTIC, tomando como

referencia el marco proporcionado por COBIT 2019 (16). El propósito de este documento se encuentra muy alineado con el Objetivo de Gestión BAI07 Gestionar la aceptación y transición de los cambios de TI

BAI07 Gestionar la aceptación y transición de los cambios de TI

Este objetivo de COBIT se enfoca en asegurar que los nuevos servicios y sistemas estén preparados para la puesta en operación de manera estructurada. Incluye una serie de prácticas para garantizar que el servicio cumpla con los estándares de calidad y esté alineado con las necesidades del negocio antes de su implementación completa.

Este objetivo de gestión pertenece al Dominio: Construir, adquirir e implementar. El análisis del mismo se realiza en la correspondiente tabla de Proceso: BAI07 Gestionar la aceptación y transición de los cambios de TI, del documento denominado “Objetivos de gobierno y gestión, COBIT 2019 Marco de Referencia” (16), la cual establece las siguientes previsiones para este objetivo:

Descripción: Aceptar formalmente y hacer operativas las nuevas soluciones. Incluir la planificación de la implementación, conversión de sistemas y datos, pruebas de aceptación, comunicación, preparación de la puesta en producción, paso a producción de nuevos o modificados procesos de negocio y servicios de I&T, soporte temprano de la producción y revisión posterior a la implementación. (16)

Propósito: Implementar soluciones de forma segura y conforme a las expectativas y resultados acordados.

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Son metas empresariales vinculadas con este objetivo:

- EG01 Portafolio de productos y servicios competitivos

Son metas de alineamiento vinculadas con este objetivo:

- AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas

Como se ha mencionado anteriormente, cada objetivo de gobierno y gestión incluye varias prácticas de proceso, y cada proceso incluye una o más actividades.

Para el Objetivo de gestión: BAI07 — Gestionar la aceptación y transición de los cambios de TI, se prevén diversas prácticas de gestión:

- Práctica de gestión - BAI07.01 Establecer un plan de implementación.
- Práctica de gestión - BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.
- Práctica de gestión - BAI07.03: Plan de pruebas de aceptación.
- Práctica de gestión - BAI07.04: Establecer un entorno de pruebas.
- Práctica de gestión - BAI07.05 Realizar pruebas de aceptación.
- Práctica de gestión - BAI07.06 Promover a producción y gestionar las liberaciones (releases).
- Práctica de gestión - BAI07.07 Proporcionar soporte oportuno en producción.

La Instrucción Técnica 04/24 del CESTIC Puesta en Operación de Nuevos Servicios en el Ámbito del CESTIC establece las consideraciones a tener en cuenta para la planificación, transición y operación de nuevos servicios SIC/TIC en el marco de la nueva I3D, cuya responsabilidad de provisión recaiga en el CESTIC.

Como aspectos del documento alineados con COBIT2019 se pueden destacar los siguientes:

- **Capacidad de Alinear, Planificar y Organizar (APO):** El documento aplica el subproceso APO09 (Gestionar los Acuerdos de Servicio), con un enfoque claro en la definición de roles, responsabilidades y gestión del cambio. Esto ayuda a mantener la calidad de los servicios y asegurar una transición bien organizada.

- **Capacidad de Construir, Adquirir e Implementar:** En la fase de despliegue y aceptación, se incluyen elementos esenciales como la Acta de Aceptación del Servicio (AAS), el Plan de Gestión del Cambio (PGC) y un conjunto completo de pruebas de validación. Este enfoque es coherente con BAI07 (Gestionar la aceptación y transición de los cambios)

- **Roles y Responsabilidades Claramente Definidos:** La Matriz RACI ayuda a definir los roles en el proceso de puesta en operación, alineándose con los principios de COBIT sobre asignación de responsabilidades

- **Documentación Técnica y Pruebas:** La instrucción incluye documentación detallada como Manual de Usuario, Manual de Operación/Administración, y pruebas funcionales y de rendimiento. Esto respalda los principios de COBIT de asegurar la disponibilidad y continuidad de los servicios.

- **Capacidad de Monitorizar, Evaluar y Valorar:** El documento establece mecanismos de control, con informes periódicos de cumplimiento del SLA, alineándose con MEA01 (Monitorear, evaluar y medir el desempeño y la conformidad).

Aunque el documento está bien alineado con el marco COBIT 2019 (16) en varias áreas esenciales, existen ciertos elementos que podrían mejorarse o añadirse para reforzar su conformidad con dicho marco:

- **Alineación Estratégica y Valor para el Negocio:** Aunque el documento describe roles y responsabilidades, no se establece claramente una alineación con objetivos estratégicos del MDEF o de cómo el nuevo servicio aportará valor a nivel organizacional. COBIT sugiere que cualquier nuevo servicio debería demostrar su contribución al valor de negocio y sus objetivos.

- **Gestión de Riesgos (EDM03):** No se incluye un análisis detallado de riesgos asociados con la puesta en operación de los nuevos servicios, ni se establecen controles específicos.

- **Plan de Continuidad (DSS04):** No se prevé la definición de un plan de continuidad específico para asegurar que el servicio se mantenga operativo en caso de incidentes.

- **Enfoque en la Mejora Continua:** Aunque se menciona la recopilación de lecciones aprendidas, falta un ciclo claro de retroalimentación para realizar mejoras en el proceso de puesta en operación basado en la experiencia adquirida.

- **Participación y Comunicación con Stakeholders (APO08):** La instrucción podría beneficiarse de un proceso de consulta y comunicación con las partes interesadas clave durante la transición de servicios. COBIT sugiere un enfoque proactivo para la gestión de stakeholders, asegurando que los usuarios y áreas implicadas estén informados y participen activamente en la transición.

- **Evaluación del Desempeño y Alineación con el SLA:** Aunque se describen métricas de seguimiento, el documento podría incluir indicadores clave de rendimiento (KPIs) adicionales que midan el éxito de la transición, la satisfacción del usuario y la efectividad del soporte temprano en producción, promoviendo una alineación completa con el Acuerdo de Nivel de Servicio (SLA).

- **Se podría prever la realización de un Análisis Temprano de Riesgos** en las primeras fases del proceso, documentando riesgos y medidas de mitigación para cada etapa de la puesta en operación.

3.2.4 Acuerdo de Provisión de Servicio 01/24 del CESTIC sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC

La Arquitectura de Referencia (AR) única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC), establece como el cuarto de sus objetivos globales (OBG) para la Gestión de Servicios CIS/TIC de la I3D, el siguiente:

- OBG-4. Entregar Servicios CIS/TIC de acuerdo a los Acuerdos de Nivel de Servicio (SLA) definidos.

El Acuerdo de Provisión de Servicio 01/24 del CESTIC Sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC, aprobado en abril de 2024, se constituye como el primer Acuerdo de Provisión de Servicio (APS) aprobado en el contexto de la nueva Gestión de Servicios CIS/TIC de la I3D. Por lo tanto, este APS se erige como la referencia a partir del cual, definir y aprobar los diferentes acuerdos de nivel de servicio provisionados por el CESTIC a sus respectivos clientes.

El propósito de este documento se encuentra muy alineado con el Objetivo de Gestión APO09 Gestionar los acuerdos de servicio

Objetivo de Gestión APO09 Gestionar los acuerdos de servicio

Este objetivo de gestión pertenece al Dominio: Alinear, planificar y organizar. El análisis del mismo se realiza en la correspondiente tabla de Proceso: Objetivo de gestión: APO09 Gestionar los acuerdos de servicio, del documento denominado “Objetivos de gobierno y gestión, COBIT 2019 Marco de Referencia” (16), la cual establece las siguientes previsiones para este objetivo:

Descripción: Alinear los productos y servicios habilitados por I&T y los niveles de servicio con las necesidades y expectativas de la empresa, incluidos la identificación, especificación, diseño, publicación, acuerdo y monitorización de los productos y servicios de I&T, niveles de servicio e indicadores de rendimiento.

Propósito: Asegurarse que los productos, servicios y niveles de servicio de I&T satisfagan las necesidades actuales y futuras de la empresa.

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Son metas empresariales vinculadas con este objetivo:

- EG01 Portafolio de productos y servicios competitivos
- EG08 Optimización de la funcionalidad de procesos del negocio internos

Son metas de alineamiento vinculadas con este objetivo:

- AG05 Prestación de servicios de I&T conforme a los requisitos del negocio

Para el Objetivo de gestión: APO09 — Gestionar los acuerdos de servicio, se prevén diversas prácticas de gestión:

- Práctica de gestión - APO09.01 Identificar los servicios de I&T.
- Práctica de gestión - APO09.02 Catalogar los servicios habilitados por I&T.
- Práctica de gestión - APO09.03 Definir y preparar acuerdos de servicio.
- Práctica de gestión - APO09.04 Monitorizar y reportar los niveles de servicio.
- Práctica de gestión - APO09.05 Revisar los acuerdos y los contratos de servicio.

Para el caso particular del análisis de mejora de la provisión de servicios en el CESTIC, es relevante el estudio de la práctica de Práctica de gestión: APO09.03 Definir y preparar acuerdos de servicio, a la que se dedica el siguiente apartado:

Definir y preparar acuerdos de servicio basados en las opciones de los catálogos de servicio. Incluir acuerdos operativos internos.

Métricas modelo:

- a. Número de procesos de negocio con acuerdos de servicio no definidos
- b. Porcentaje de servicios de TI activos cubiertos por acuerdos de servicio

Actividades vinculadas a la Práctica de gestión APO09.03 Definir y preparar acuerdos de servicio (ver Tabla 3-4)

Actividades	Nivel de capacidad
1. Analizar los requisitos para acuerdos de servicio nuevos o modificados recibidos de la gestión de relaciones con el negocio a fin de asegurar que puedan satisfacerse. Considerar aspectos como los tiempos de servicio, disponibilidad, rendimiento, capacidad, seguridad, privacidad, continuidad, problemas de cumplimiento y regulatorios, usabilidad, limitaciones de la demanda y calidad de los datos.	2
2. Redactar borradores de acuerdos de servicio al cliente basados en los servicios, paquetes de servicios y opciones de nivel de servicio en los catálogos de servicios relevantes.	
3. Finalizar los acuerdos de servicio al cliente con la gestión de relaciones con el negocio.	
4. Determinar, acordar y documentar acuerdos operativos internos que sustenten los acuerdos de servicio al cliente, si corresponde.	3
5. Relacionarse con la gestión de proveedores externos para garantizar que los adecuados contratos comerciales con proveedores de servicios externos sustenten los acuerdos de servicio al cliente, si corresponde.	

Tabla 3-4 Lista de actividades asociadas a la Práctica de gestión: APO09.03 Definir y preparar acuerdos de servicio. (16)

Alineamiento de los Acuerdos de Provisión de Servicios con el marco COBIT

Para garantizar que un Acuerdo de Provisión de Servicio (SLA) se encuentra alineado con el marco COBIT 2019 (16), se deben integrar prácticas de gobierno y gestión que aseguren la calidad del servicio, el cumplimiento de objetivos estratégicos de TI, y la gestión de riesgos.

El autor cita a continuación una serie de puntos que se consideran claves para definir un SLA conforme a los requisitos del marco COBIT 2019 (16):

1. Definir el Propósito del SLA y los Objetivos de Negocio

El SLA debe reflejar el valor que el servicio aporta al negocio, en términos de cómo el SLA ayuda a cumplir objetivos de negocio específicos, alineándolo con los Objetivos de Gobierno y Gestión de COBIT

2. Especificar Alcance y Responsabilidades:

Es muy importante asegurar que todos los aspectos clave del servicio estén meridianamente definidos. Se identifican los siguientes puntos clave:

- Identificar qué servicios están específicamente cubiertos por el SLA (por ejemplo, mantenimiento de redes, soporte de infraestructura, servicios de ciberseguridad)
- Aclaración de los niveles de servicio (Por ejemplo, tiempos de respuesta, disponibilidad, tiempos de resolución de incidentes, etc.)
- Definición de Indicadores clave de rendimiento (KPIs), determinando que indicadores se utilizan para medir el desempeño de los servicios (Por ejemplo, tiempo de disponibilidad, tiempo de resolución, etc.)
- Concreción de las obligaciones de las partes, para asegurar una claridad en la responsabilidad, un aspecto clave para el gobierno de TI
- Establecimiento de penalizaciones o recompensas
- Determinar los tiempos de revisión del SLA

3. Definir y Medir los Niveles de Servicio

Establecer métricas específicas y cuantificables (KPIs) para medir el desempeño. Estas métricas deben estar orientadas a evaluar la disponibilidad, tiempo de respuesta, capacidad de resolución y calidad de servicio. Algunos ejemplos de métricas:

- Disponibilidad del Servicio: Uptime en términos porcentuales.
 - Tiempos de Respuesta: Tiempos de respuesta específicos para solicitudes, incidentes y problemas.
 - Resolución de Incidentes: Porcentaje de incidentes resueltos en el tiempo acordado.
- Se deben realizar informes periódicos sobre el rendimiento de estos indicadores.

4. Alineación con el Marco de Objetivos de Gobierno y Gestión COBIT 2019 (16)

Utilizar el marco de objetivos de COBIT para alinear las métricas del SLA. Los más relevantes incluyen:

- Objetivo de gobierno EDM03: Asegurar la optimización del riesgo (como la gestión de incidentes).
- Objetivo de gestión APO09: Gestión de relaciones, para definir responsabilidades y expectativas mutuas.
- Objetivo de gestión DSS02: Gestión de solicitudes de servicio e incidentes, asegurando tiempos de respuesta adecuados.
- Objetivo de gestión DSS03: Gestión de problemas, para prevenir incidentes recurrentes.
- Objetivo de gestión MEA01: Gestionar la monitorización del desempeño y la conformidad del SLA

5. Establecer los Procesos de Monitoreo y Mejora Continua

COBIT 2019 (16) enfatiza la mejora continua y el monitoreo de desempeño. Define procesos de evaluación y revisiones periódicas para asegurarse de que el SLA sigue siendo relevante y eficaz. Esto se relaciona con los objetivos de gestión MEA01 y MEA02, que cubren monitoreo y evaluación del desempeño y el cumplimiento.

- MEA01: Gestionar la monitorización del desempeño y la conformidad
- MEA02: Gestionar el sistema de control interno

6. Gestión de Riesgos y Cumplimiento

Define mecanismos de control y planes de contingencia para mitigar riesgos asociados al cumplimiento del SLA, en línea con objetivo de gobierno EDM03: Asegurar la Optimización del riesgo.

Ajuste del Acuerdo de Provisión de Servicio aprobado por el CESTIC al marco proporcionado por COBIT

Se realiza a continuación un análisis del ajuste del documento “Acuerdo de Provisión de Servicio 01/24 del CESTIC Sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC” al marco proporcionado por COBIT:

Se puede afirmar que el documento se encuentra alineado con el marco COBIT 2019 en términos de prácticas, objetivos y elementos esenciales de gobernanza y gestión; así como con el software IT Service Management (ITSM) ProactivaNet.

El acuerdo está bien estructurado, siguiendo un esquema claro y detallado, incluyendo la estructura documental, procesos de gestión de la disponibilidad, Definición de Roles y Responsabilidades

No obstante, se pueden citar una serie de puntos faltantes o mejorables en la redacción de los siguientes APS necesarios para la provisión de los servicios responsabilidad del CESTIC, para que estos tengan una mejor alineación con el marco propuesto por COBIT 2019

- **Enfoque Estratégico:** Debería aparecer con mayor claridad una conexión explícita del acuerdo con los objetivos estratégicos del negocio o de la Misión del MDEF
- **Gestión de Riesgos:** Aunque menciona conceptos como "best effort" y manejo de incidentes críticos, no hay un análisis detallado de riesgos ni un plan formal de mitigación vinculado a los servicios acordados, como se recomienda en EDM03 (Asegurar la optimización del riesgo).
- **Planes de Contingencia:** No se describen detalladamente los planes para la continuidad del servicio en caso de fallos mayores, algo que es esencial en DSS04 (Gestionar la Continuidad) y debería integrarse para una mejor alineación.
- **Participación de los StakeHolders:** Si bien las responsabilidades están bien definidas, no se menciona la implicación de usuarios clave o stakeholders en la definición o revisión de los servicios, un aspecto recomendado por COBIT 2019 (16) en APO09.01 (Definir y preparar acuerdos de servicio).
- **Mejoras Continuas Basadas en Resultados:** El enfoque de mejora continua no menciona explícitamente cómo los resultados de las métricas (porcentaje de SLA cumplidos, incidencias fuera de plazo, etc.) se utilizarán para proponer cambios específicos.
- **Transparencia en Penalizaciones y Compensaciones:** No incluye un esquema claro de sanciones o compensaciones por incumplimiento de los SLA, lo que podría alinearse con la gobernanza de cumplimiento en EDM02 (Asegurar la entrega de beneficios).

3.3 Monitorización de la infraestructura de I&T.

La Arquitectura de Referencia (AR) única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7), define dentro de sus objetivos globales (OBG) para la gestión exitosa de los servicios CIS/TIC de la I3D:

- **OBG-4. Entregar Servicios CIS/TIC de acuerdo a los Acuerdos de Nivel de Servicio (SLA) definidos.**
- **OBG-6. Aumentar la calidad de los Servicios CIS/TIC entregados y la madurez de los procesos operativos del CESTIC a través de la mejora continua**
- **OBG-7. Optimizar los costes en la provisión de Servicios CIS/TIC.**

Así mismo, el plan estructurado para la implantación del Modelo de Gobierno y Gestión Única de Servicios, previsto en la Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7) dedica su fase 6 a la calidad y la mejora continua.

La consecución de estos objetivos dentro del Modelo de Gobierno y Gestión Única de Servicios, no sería posible sin la definición de una estrategia de monitorización de los servicios, que permita evaluar la calidad de los mismos conforme unos requisitos establecidos en unos Acuerdos de Nivel de Servicio previamente definidos.

La definición de una estrategia de monitorización está en línea con el Objetivo de Gestión DSS01 - Gestionar las operaciones, previsto en el marco COBIT 2019 (16).

Objetivo de Gestión DSS01 - Gestionar las operaciones.

Este objetivo de gestión pertenece al Dominio: Entregar, dar servicio y soporte. El análisis del mismo se realiza en la correspondiente tabla de Proceso: Objetivo de gestión: DSS01 - Gestionar las operaciones, del documento denominado “Objetivos de gobierno y gestión, COBIT 2019 Marco de Referencia” (16), la cual establece las siguientes previsiones para este objetivo:

Descripción: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados. Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas.

Propósito: Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado.

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Son metas empresariales vinculadas con este objetivo:

- EG01 Portafolio de productos y servicios competitivos
- EG08 Optimización de la funcionalidad de procesos del negocio internos

Son metas de alineamiento vinculadas con este objetivo:

- AG05 Prestación de servicios de I&T conforme a los requisitos del negocio

Para el Objetivo de gestión: DSS01 - Gestionar las operaciones, se prevén diversas prácticas de gestión: (16)

- Práctica de gestión - DSS01.01 Ejecutar procedimientos operativos
- Práctica de gestión - DSS01.02 Gestionar servicios terciarizados de I&T.
- Práctica de gestión - DSS01.03 Monitorizar la infraestructura de I&T.
- Práctica de gestión - DSS01.04 Gestionar el medioambiente.

Para el caso particular del análisis de mejora de las operaciones en el CESTIC, es muy relevante el estudio de la práctica de Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T; ya que, como se cita en la Tabla 3-1 Identificación de la situación actual y objetivo del CESTIC en relación al modelo para el gobierno y la gestión única de servicios. Fuente (7) y elaboración propia.; actualmente el CESTIC no cuenta con métricas definidas que permitan evaluar los niveles de calidad del Servicio.

Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T.

Monitorizar la infraestructura de I&T y eventos relacionados. Almacenar suficiente información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones.

Métricas modelo:

- a. Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática
- b. Porcentaje de activos de infraestructura monitorizados conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos

Actividades vinculadas a la Práctica de gestión DSS01.03 Monitorizar la infraestructura de I&T. (Ver Tabla 3-5)

Actividades	Nivel de capacidad
1. Registrar los eventos. Identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento.	2
2. Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos	3
3. Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos. Encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria.	
4. Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones.	
5. Garantizar que se creen tickets de incidentes en el plazo debido a la hora de monitorizar desviaciones identificadas en los umbrales definidos.	
6. Establecer procedimientos para monitorizar los registros de eventos. Llevar a cabo revisiones regulares.	4

Tabla 3-5 Lista de actividades asociadas a la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T. (16)

A continuación, se analizan las actividades asociadas Práctica de gestión DSS01.03 Monitorizar la infraestructura de I&T, teniendo en cuenta la situación actual del desarrollo de estas actividades en el CESTIC.

Se pretende modelar la transición desde la situación actual (AS-IS) hasta la situación objetivo (TO BE). A continuación, la Tabla 3-6 expone la situación actual y objetivos de Monitorización de la infraestructura de I&T:

Actividades	Situación actual de Gestión (AS-IS)	Situación objetivo de Gestión (TO-BE)
1. Registrar los eventos. Identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento.	Se utiliza una pluralidad de herramientas cada una encargada de monitorizar un servicio o un tipo de activo, pero no existe una integración de información que permita obtener de manera sencilla una visión general de la situación	Conseguir una plataforma que permita integrar la información de los diferentes sistemas de monitorización
2. Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos	Los inventarios de activos críticos para cada servicio son confusos. No existe un inventario único general. No es fácilmente identificable cuantos activos son comunes a varios servicios.	Conseguir una lista de activos única, que efectivamente sean monitorizados y las relaciones existentes entre ellos.
3. Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos. Encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria.	Las reglas no están definidas. Se valora la criticidad de una situación en base a los indicadores mostrados por las herramientas de monitorización.	Definición de reglas claras que permitan determinar de forma objetiva la criticidad de eventos adversos.
4. Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones.	Multiplicidad de registros de eventos, cada uno asociado a su propio sistema.	Creación de un registro único de eventos. En línea con el “objetivo III.11.Crear una Plataforma de Análisis Masivo de Datos e Información para analizar y explotar la información de manera más eficaz”, contemplado en el PATD-2 (PLAN DE ACCIÓN DEL MINISTERIO DE DEFENSA PARA LA TRANSFORMACIÓN DIGITAL) (6)
5. Garantizar que se creen tickets de incidentes en el plazo debido a la hora de monitorizar desviaciones	Múltiples políticas de tickets, independientes para cada servicio o activo.	Una política unificada y un sistema integrado de generación de notificaciones.

identificadas en los umbrales definidos.		
6. Establecer procedimientos para monitorizar los registros de eventos. Llevar a cabo revisiones regulares.	Inexistencia de un plan único de monitorización. Alto grado de subjetividad en la planificación en las revisiones.	Procedimientos únicos y objetivos de monitorización.

Tabla 3-6 Identificación de la situación actual y objetivo para las actividades previstas en la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T. (Fuente: Elaboración Propia)

Centrándose en el tercer componente de gobierno: Flujos y elementos de información, perteneciente al Objetivo de gestión: DSS01 - Gestionar las operaciones, e individualizado para práctica de gestión DSS01.03 Monitorizar la infraestructura de I&T, el marco COBIT 2019 (16) prevé las siguientes entradas y salidas para dicha práctica de proceso (Ver Tabla 3-7):

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS01.03 Monitorizar la infraestructura de I&T.	BAI03.11	Definiciones de servicios	Reglas de monitorización de activos y estados de eventos	DSS02.01; DSS02.02
			Tickets de incidentes	DSS02.02
			Logs de eventos	Interna

Tabla 3-7 Componente C: Flujos y elementos de información para la Práctica de gestión: DSS01.03 Monitorizar la infraestructura de I&T (16)

Entradas: En este caso, la entrada proviene de la práctica BAI03.11, que pertenece al proceso de Construir, Adquirir e Implementar (BAI), y específicamente al desarrollo de la definición de servicios.

Salidas: Aquí se describe qué es lo que se genera como resultado de la práctica. Las salidas son varios elementos:

- Reglas de monitorización de activos y estados de eventos: Este resultado incluye la creación de reglas o criterios para monitorear los activos de I&T y el estado de los eventos que se producen en la infraestructura.
- Tickets de incidentes: Como resultado del monitoreo, se pueden generar tickets o reportes de incidentes cuando se detectan problemas o fallos en los sistemas.
- Logs de eventos: También se generan registros (logs) que detallan los eventos que han ocurrido durante el monitoreo de la infraestructura.

Destino de la Salida: Indica a quién o a qué proceso se dirige la salida generada. En este caso:

- Las reglas de monitorización de activos y estados de eventos se envían a las prácticas de gestión DSS02.01 y DSS02.02

DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.

DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.

- Los tickets de incidentes también se dirigen al proceso DSS02.02.
- Los logs de eventos tienen un destino interno, lo que indica que probablemente se utilicen de manera interna para realizar auditorías o revisiones posteriores dentro del mismo proceso.

Todos estos componentes (salidas) van a ser tenidas en cuenta para elaborar la estrategia de monitorización, tal y como se muestra a continuación:

3.3.1 Recomendaciones para el Centro de Atención al Usuario (CAU) del CESTIC respecto la definición de métricas para evaluar su rendimiento:

Actualmente el Centro de Atención al Usuario (CAU) del CESTIC no dispone de métricas definidas y aprobadas para evaluar su desempeño en su formidable contribución a la gestión de servicios TI en el MDEF.

TIL plantea una serie de métricas para evaluar la salud, madurez, eficiencia, eficacia y cualquier oportunidad de mejora de las operaciones del Centro de Servicio al Usuario. Ante la inexistencia de métricas actuales para evaluar el desempeño del Centro de Atención al Usuario (CAU) actualmente en funcionamiento, a través de la utilización de sus herramientas de gestión de peticiones e incidentes (concretamente SCANS), se propone seguir las recomendaciones de ITIL para la definición de métricas de funcionamiento de un centro de gestión de servicios. (9)

Son métricas recomendadas por ITIL para un Centro de Servicio al Usuario:

- Tasa de resolución en la primera línea: el porcentaje de llamadas resueltas en la primera línea, sin la necesidad de escalados a otros grupos de soporte.
- Tiempo medio de resolución de una incidencia (cuando se resuelva en la primera línea)
- Tiempo medio para escalar una incidencia (cuando no sea posible una resolución en la primera línea)
- El número de llamadas, desglosado por hora y día de la semana; combinado con la métrica del tiempo medio de llamada, es crítico para determinar el número de personal necesario.

Además de realizar el seguimiento de las medidas tangibles del rendimiento del Centro de Servicio al Usuario (a través de las métricas descritas más arriba), también es importante evaluar las mediciones más intangibles, como, por ejemplo, cómo perciben los clientes y usuarios que se ha respondido a sus llamadas, si sienten que el operador del Centro de Servicio al Usuario fue cortés y profesional, si inculcan o no confianza al usuario.

3.3.2 Cuadro de Mando Integral de Monitorización.

Disponer de una herramienta de monitorización integrada para todos los servicios e infraestructuras TI del CESTIC es la base para lograr una Gestión eficiente de Eventos.

Para la elaboración de un cuadro de mando (o dashboard) que permita monitorizar el estado de los servicios informáticos del CESTIC, es esencial seleccionar las variables clave que proporcionen una visión integral de la salud, rendimiento y disponibilidad de tus infraestructuras y servicios TIC

DIVOPER es la unidad del CESTIC sobre la que recae la competencia en la gestión de los servicios TI proporcionados por el MDEF, y, por lo tanto, será también la unidad responsable de elaborar y mantener el cuadro de mando integral para la monitorización de servicios.

Como se ha señalado previamente, un cuadro de mando (o Dashboard) es un concepto amplio que representa una herramienta de visualización de datos.

Si bien un cuadro de mando es un concepto muy genérico que puede englobar muchas utilidades, a medida que el autor ha ido elaborando el TFM, este ha sido más consciente de que la monitorización de la infraestructura de TI requiere de una herramienta más específica, orientada en la monitorización en tiempo real, más que en el análisis histórico de datos, y dirigido a ingenieros y operadores de TI, en lugar a individuos con un perfil más ejecutivo o gerencial.

De lo anterior, el autor deduce que lo más apropiado para la monitorización de la infraestructura TI es contar con una plataforma de visualización y monitorización de datos, que permita construir **paneles de observabilidad** en tiempo real. Este es un concepto más técnico y preciso, en lugar de referirse al mismo simplemente como “cuadro de mando” o “dashboard” de forma genérica, que, si bien es cierto, es una denominación muy extendida para esta funcionalidad.

Para la construcción de paneles de observabilidad existen diversas herramientas de BI (Business Intelligence) como Power BI, Tableau, Grafana o Kibana, que posibilitan la integración de múltiples fuentes de datos y su visualización en paneles interactivos y fáciles de interpretar.

Se tratan de herramientas de software especializadas en la visualización de datos en tiempo real, orientada principalmente a monitorear sistemas de TI, infraestructura, aplicaciones y métricas de rendimiento. Son ideales para observabilidad y monitoreo continuo en entornos de DevOps.

Estas herramientas pueden conectarse a los sistemas de monitorización, directamente o a través de bases de datos o registros intermedios, y extraer los datos relevantes (por ejemplo, desde Nagios, Zabbix, o herramientas de monitoring en la nube como AWS CloudWatch).

Las herramientas de visualización en tiempo real se especializan en integrar datos provenientes de herramientas de monitorización y observabilidad, tales como Prometheus, InfluxDB, Elasticsearch, y también puede conectarse a bases de datos SQL, MongoDB, y otros.

De la investigación realizada, se concluye que la herramienta a recomendar por el autor para la elaboración de paneles de observabilidad de datos en el MDEF sea Grafana, ya que por cuya característica de código abierto, muestra una gran capacidad de integración con la amplia variedad de softwares para la monitorización de activos con los que cuenta el MDEF (como se estudiará a continuación). Otros motivos para decantarse por esta herramienta son la versatilidad y capacidad de adaptación de sus paneles de visualización, a los requisitos específicos que se necesitan para esta herramienta en el MDEF. Así mismo, la posibilidad de implementar la herramienta de forma on-premise, sin depender de aplicaciones en la nube, se alinea con los estrictos requisitos de seguridad del MDEF, permitiendo mantener internamente la custodia de datos sensibles y reforzando el control sobre su infraestructura de TI.

El panel de observabilidad debe ser dinámico, visual y orientado a la acción, permitiendo a los responsables TIC tomar decisiones rápidas y basadas en datos confiables. Las métricas clave a monitorear incluyen disponibilidad, desempeño, seguridad, cumplimiento, incidentes, experiencia del usuario, y eficiencia operativa, todas basadas en marcos como ITIL, ISO 20000, y COBIT.

Por expreso deseo del responsable de DIVOPER, se procurará en la medida de lo posible que las variables a monitorizar sean mostradas en el cuadro de mando con indicadores tipo velocímetro (o speedometro) para permitir una visualización lo más amigable y directa posible.

Los velocímetros son especialmente útiles para representar porcentajes o valores que se mueven dentro de un rango claro y con umbrales de alerta, por lo que son perfectos para representar disponibilidad, uso de recursos, tiempo de respuesta, SLAs, ancho de banda y satisfacción del usuario. Estas métricas son ideales para ser visualizadas de manera rápida y efectiva, permitiendo a los equipos técnicos tomar decisiones inmediatas si alguna de ellas cae en el área de advertencia o crítica.

3.3.2.1 Variables críticas a monitorizar en el Cuadro de Mando

Se va a establecer una distinción entre las variables a monitorizar para la infraestructura de soporte a los servicios TI (Redes y Centros de Procesamiento de Datos) y las variables a monitorizar para los servicios TI

Variables críticas a monitorizar en la infraestructura TI

El objetivo es identificar las variables más relevantes, por cada sector de mantenimiento, que permitan determinar la salud de las infraestructuras de cada uno de los Centros de Datos (5 en total) cuya gestión es responsabilidad de la División de Operaciones de Red (DIVOPER) del CESTIC.

Con el objetivo de ofrecer una visión más clara y resumida de la situación, cada cuadro de mando o panel específico para cada centro de datos mostrará un indicador independiente o velocímetro para cada una de las siguientes dimensiones o sectores clave de mantenimiento:

- **Electricidad:** Recoger en un único indicador sintético la situación del conjunto de componentes de suministro eléctrico del centro de datos, comprendiendo estos, según el caso: Grupo Electrónico, Sistemas de Alimentación Ininterrumpida (SAI o UPS), Cuadros de Suministro Eléctrico.
- **Clima:** Recoger en un único indicador sintético la situación de los diversos sistemas de climatización existentes en cada centro de datos (Unidades condensadoras interiores y exteriores, enfriadoras, inrows...) así como los niveles de temperatura y humedad óptimos.
- **PCI:** Un único indicador sintético que muestre el estado de los diferentes sistemas de detección (rápida y convencional), de los sistemas de extinción, así como el cumplimiento de la normativa en materia de revisiones.
- **Seguridad:** Refleja en un único indicador sintético el estado de las medidas de seguridad física y lógica, abarcando la eficiencia de los sistemas de control de acceso, funcionamiento de cámaras de seguridad,
- **Telecomunicaciones:** Un indicador sintético que muestre el estado de las conexiones de red, ancho de banda disponible y latencia.

A continuación, se muestra en la siguiente figura, el resultado de cuadro de mando para la monitorización del estado de las infraestructuras en el CESTIC, diseñado para que muestre un indicador independiente para cada una de las siguientes dimensiones o sectores clave de mantenimiento por cada centro de datos, presentado además en formato de velocímetro.

En este punto es destacable citar que, en la literatura y normativa existente sobre gestión y mantenimiento de centros de datos, no existe ninguna referencia a la utilización de cuadros de mando en formato velocímetro para la representación de los parámetros clave de mantenimiento para centros de datos. Por lo que la inclusión de esta propuesta en el presente TFM se considera un aspecto genuinamente innovador en esta materia, tal como se muestra en la Figura 3-2.

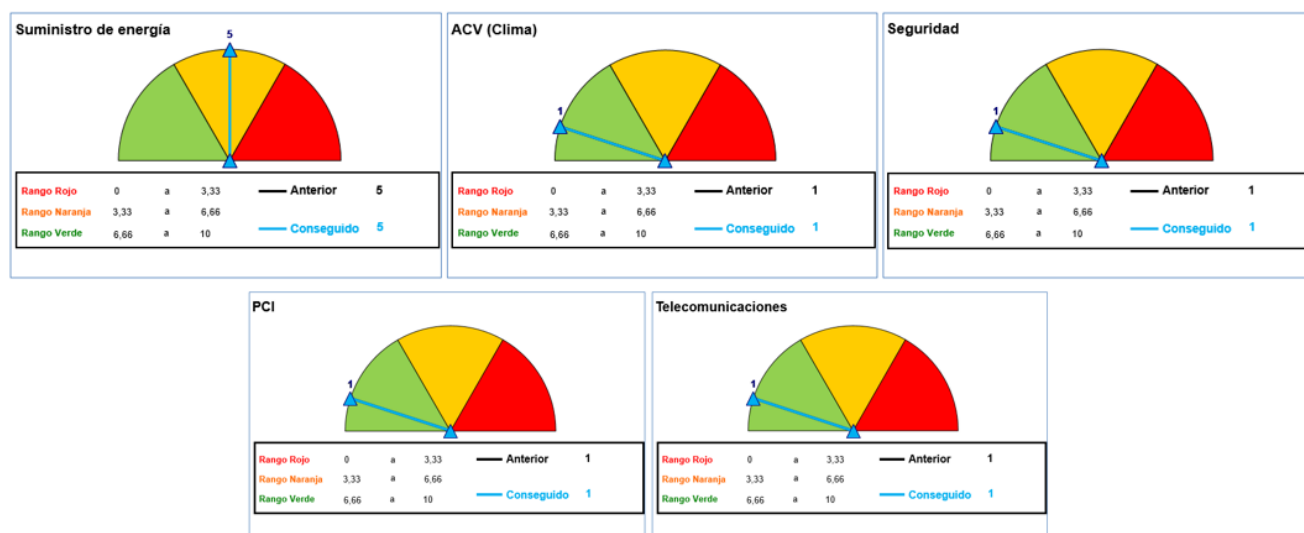


Figura 3-2 Representación idealizada de un Cuadro de Mando en formato velocímetro con información sobre áreas clave de mantenimiento para un Centro de Procesamiento de Datos (CPD) (Fuente elaboración propia)

En la representación figurada anterior, cada dial del velocímetro se divide en 3 sectores en función de la criticidad de la situación para cada sector de mantenimiento (Verde - Rango normal, Amarilla – Advertencia, Roja – Situación Crítica)

El valor numérico para cada situación sectorial se asignaría en función de una lógica de negocio previamente definida, en la que se valoraría la criticidad de cada uno de los elementos de la infraestructura y su impacto en el funcionamiento del centro de datos, si este quedara fuera de servicio. Por ejemplo, la situación del velocímetro que muestra el estado de suministro de energía, aparece con un valor 5 (Amarillo – Rango de advertencia) Este nivel podría ser indicativo de que el grupo electrógeno ha experimentado problemas de arranque en los últimos meses. Esta situación, por si sola, no interrumpe el servicio que presta el centro de datos, pero podría desencadenar una situación crítica, de apagado del centro, si se produjera un corte largo de suministro eléctrico y el grupo electrógeno no fuera capaz de arrancar, impidiendo el suministro de energía de respaldo.

La herramienta de visualización Grafana presenta una amplia gama de opciones de visualización en sus paneles, por lo que la programación de velocímetros con esta información sería una tarea sencilla. La construcción de estos paneles se propone como una línea de trabajo futura a este TFM.

Monitorización automática

Para la parametrización de las variables críticas a monitorizar en el CPD se siguen las recomendaciones sobre las métricas modelo planteadas por COBIT 2019 (16) en la Práctica de gestión DSS01.03 Monitorizar la infraestructura de I&T:

- Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática.
- Porcentaje de activos de infraestructura monitorizados conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos.

Centrándose en la métrica, Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática, las infraestructuras del CESTIC cuentan diversos sistemas de monitorización automáticos que supervisan un gran porcentaje de activos pertenecientes a las distintas áreas de mantenimiento. Estos sistemas son los siguientes:

- Nagios XI que es una herramienta de monitoreo de infraestructura de TI (El estado de servidores, aplicaciones, servicios, dispositivos de red e incluso los sistemas de alimentación ininterrumpida del CPD en nuestro caso)
- Data Center Expert (DCE) que es una herramienta de monitoreo y gestión para la supervisión del rendimiento de nuestros centros de datos. (Monitoreo de hardware, Seguimiento del uso de energía, Alertas y notificaciones e informes y análisis)
- IT Advisor: Herramienta de análisis de infraestructura y planificación de capacidades para los centros de datos.
- Software BMS (Building Management System) de Schneider Electric de monitorización en tiempo real de las infraestructuras del centro de datos y control de las mismas.
- Herramienta de desarrollo propio para la Monitorización de redes de transporte foráneas a la I3D.
- Herramienta EXTREME CLOUD IQ SITE ENGINE para la Monitorización de redes de transporte de la I3D.
- Herramienta EXTREME CLOUD MANAGEMENT CONTROL para la gestión de las comunicaciones dentro de los centros de Datos de la I3D

En la siguiente Tabla 3-8 se muestran que sectores para cada centro de datos, se encuentran cubiertos por cada una de las herramientas anteriores.

	CPD 1					CPD 2					CPD 3					CPD 4					CPD 5				
	Energía	Clima	Seguridad	PCI	Telecomunicaciones	Energía	Clima	Seguridad	PCI	Telecomunicaciones	Energía	Clima	Seguridad	PCI	Telecomunicaciones	Energía	Clima	Seguridad	PCI	Telecomunicaciones	Energía	Clima	Seguridad	PCI	Telecomunicaciones
Nagios XI						X	X	X	X			X	X	X							X	X	X	X	
DCE	X	X	X	X												X	X	X	X						
BMS	X	X																							
EXTREME					X					X					X					X					X

Tabla 3-8 Herramientas de monitorización disponibles para cada centro de datos del CESTIC (Fuente: Elaboración Propia)

Variables críticas a monitorizar en los servicios TI

Las normas y marcos de referencia más utilizados en la industria para evaluar el estado de los servicios TIC, tales como ITIL, COBIT, y ISO 20000, establecen una serie de recomendaciones sobre las variables críticas que se deben considerar en la elaboración de un cuadro de mando para la monitorización de servicios TI y de la infraestructura de soporte a los mismos.

Las magnitudes que se expresan a continuación, permiten una fácil adaptación a ser representadas con indicadores tipo velocímetro dentro del contexto de monitorización de los servicios TIC del CESTIC. Se indica a continuación como se adaptaría cada una de estas magnitudes a un indicador tipo rejón:

1. La disponibilidad o el tiempo de actividad de los servicios TIC es un buen candidato para un velocímetro, ya que tiene un rango claro (de 0% a 100%). El indicador podría mostrar:

- Rango normal (verde): 99% – 100% de disponibilidad.
- Advertencia (amarillo): 95% – 98% de disponibilidad.
- Crítico (rojo): Por debajo del 95%.

Propósito: Este velocímetro permite una rápida visualización del porcentaje de disponibilidad de un servicio o infraestructura, lo que es clave para la gestión de SLAs y para la identificación de problemas de disponibilidad.

2. Desempeño del Sistema (Uso de CPU, Memoria, Almacenamiento)

Indicadores de los recursos de los sistemas que están siendo utilizados. Es importante monitorear la capacidad de los servidores para prevenir cuellos de botella.

El uso de recursos como la CPU, memoria o almacenamiento se puede medir en porcentajes y tiene un rango que va desde 0% hasta un valor máximo determinado (100%). Un velocímetro puede mostrar:

- Rango normal (verde): 0% – 80% de utilización.
- Advertencia (amarillo): 80% – 90% de utilización.
- Crítico (rojo): Más del 90% de utilización.

Propósito: Estos indicadores permiten monitorear en tiempo real el estado de la infraestructura, ayudando a evitar cuellos de botella o el riesgo de caídas por falta de recursos.

3. Tiempo de Respuesta (Latency)

El tiempo de respuesta de las aplicaciones o de la red (latencia) es una métrica crítica para la experiencia del usuario. Puede ser representada de manera efectiva con un velocímetro en un rango de milisegundos (ms).

- Rango normal (verde): 0 ms – 200 ms (o un valor dependiendo de la aplicación).
- Advertencia (amarillo): 200 ms – 500 ms.
- Crítico (rojo): Más de 500 ms.

Propósito: Un velocímetro para latencia es útil para detectar problemas de desempeño que afectan la experiencia del usuario y la funcionalidad de los sistemas.

4. Cumplimiento de SLAs

Los SLAs (Acuerdos de Nivel de Servicio) son acuerdos clave para la monitorización de los servicios. El porcentaje de cumplimiento de estos acuerdos puede representarse con un velocímetro para mostrar el estado en tiempo real de la calidad del servicio.

- Rango normal (verde): 95% – 100% de cumplimiento de SLAs.
- Advertencia (amarillo): 90% – 95% de cumplimiento de SLAs.
- Crítico (rojo): Menos del 90% de cumplimiento.

Propósito: Esto ayuda a visualizar rápidamente si el nivel de servicio acordado se está cumpliendo.

5. Uso de la Red (Ancho de Banda)

El uso de la red es otra métrica que se puede medir en porcentaje y es muy útil para detectar problemas de congestionamiento de red. Un velocímetro podría representar el ancho de banda utilizado frente al total disponible.

- Rango normal (verde): 0% – 70% de uso de ancho de banda.
- Advertencia (amarillo): 70% – 90% de uso de ancho de banda.
- Crítico (rojo): Más del 90% de uso de ancho de banda.

Propósito: Permite monitorear la capacidad de la red y detectar posibles cuellos de botella antes de que afecten el rendimiento de los servicios.

6. Número de Incidentes Críticos Abiertos

El número de incidentes críticos abiertos es otra métrica que puede ser representada efectivamente con un velocímetro. Esto te da una visualización inmediata del volumen de problemas graves que podrían estar afectando los servicios.

- Rango normal (verde): 0 incidentes.
- Advertencia (amarillo): 1 – 3 incidentes.
- Crítico (rojo): Más de 3 incidentes.

Propósito: Permite visualizar la carga de trabajo crítica y la necesidad de intervención inmediata en los servicios.

7. Satisfacción del Usuario

La satisfacción del usuario es una métrica cualitativa importante que puede ser medida a través de encuestas o puntuaciones. Un velocímetro puede mostrar el nivel de satisfacción basado en una escala de 1 a 10.

- Rango normal (verde): 8 – 10 (satisfacción alta).
- Advertencia (amarillo): 5 – 7 (satisfacción moderada).
- Crítico (rojo): 1 – 4 (satisfacción baja).

Propósito: Permite monitorear la experiencia del usuario de manera visual y rápida, proporcionando alertas de posibles problemas en los servicios.

Para la monitorización de servicios TI, el CESTIC cuenta con la herramienta de monitorización Nagios, en la que también se integran algunas áreas de monitorización de la infraestructura. También se está desplegando progresivamente la herramienta Splunk. De estas herramientas se puede tomar la información o logs que alimenten el cuadro de mando.

Al margen de las anteriores, el CESTIC se encuentra desplegado la herramienta Instana de IBM, que es un APM o plataforma de monitoreo y gestión de aplicaciones, diseñada para proporcionar visibilidad completa en tiempo real sobre el rendimiento de las aplicaciones, los microservicios y la infraestructura en entornos de TI complejos. El propósito de Instana es realizar un levantamiento de servicios en tiempo real, identificando las trazas entre servidores o, dicho de otro modo, los flujos entre los diferentes elementos de configuración. Esto permitirá identificar servicios completos, algo fundamental para el modelado de la Base de datos de Gestión de la Configuración (CMDB por sus siglas en inglés Configuration Management Database) para administración y el seguimiento de todos los activos de TI y de sus configuraciones, lo que constituye una parte fundamental dentro de la implementación de la suite de ProactivaNet.

3.3.2.2 Diseño de Arquitectura de Software para la Integración de las distintas fuentes en una única plataforma de visualización de métricas en tiempo real:

Para la visualización en un único panel, de los aspectos críticos a monitorizar tanto por el lado de los servicios como por el de la infraestructura IT, es preciso encontrar un medio que sirva de repositorio común a la información recogida por las diversas fuentes heterogéneas disponibles.

La Figura 3-3 mostrada a continuación representa una integración de información proveniente de tres ámbitos de supervisión: El área de Infraestructura TI, el área de servicios TI y el área de seguridad.

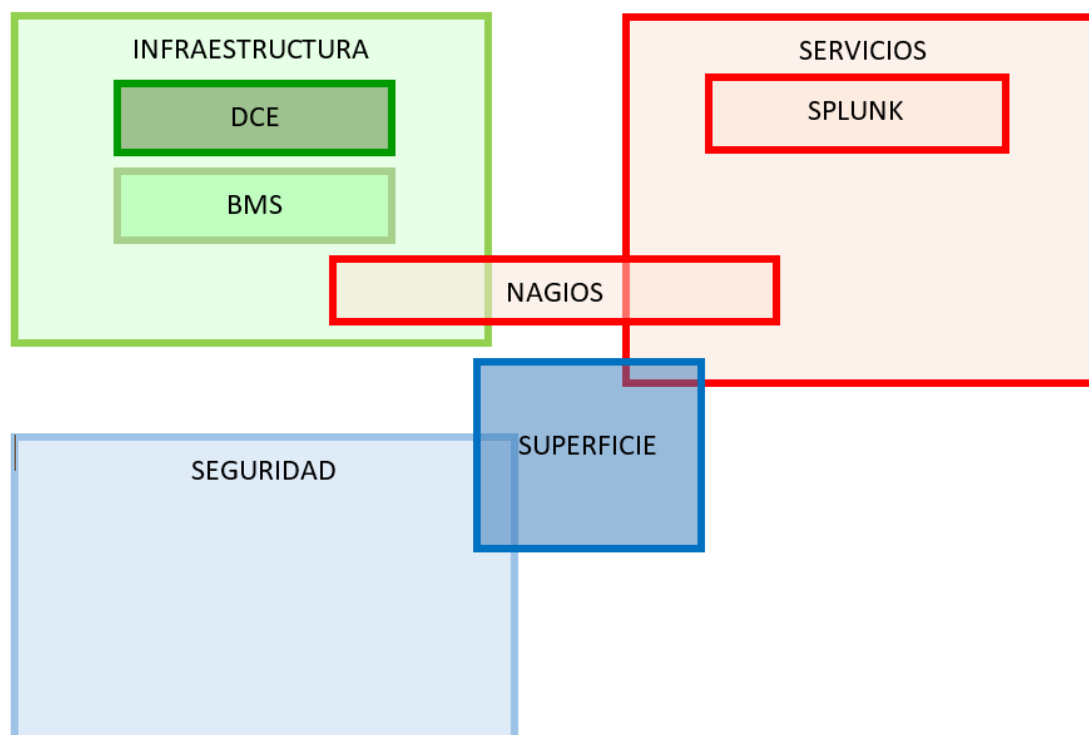


Figura 3-3 Esquema de arquitecturas de monitorización automática existentes en el CESTIC, generadoras de eventos a registrar en un único repositorio, así como el área de supervisión a la que pertenecen: Infraestructura, Servicios o Seguridad. (Fuente elaboración propia)

El autor considera que la herramienta más adecuada para la construcción de paneles de observabilidad, que permitan mostrar la información más relevante para que la División de Operaciones de Red (DIVOPER) del CESTIC pueda cumplir su misión de gestión de servicios TI para le MDEF, sería Grafana, ya que es una plataforma que muestra elevada versatilidad, capacidad de integración con múltiples fuentes de datos (Nagios, Splunk, etc.), existencia de APIs para su automatización, y por último, pero muy importante, DIVOPER dispone de personal que ya cuenta con experiencia en desarrollo con esta herramienta, habiéndose utilizado en el pasado para mostrar información relativa a ciertos servicios.

Plataforma de recogida de datos

Ya que toda la información proveniente de herramientas de monitorización y áreas de supervisión distintas se quiere mostrar en una única plataforma de visualización, parece lógico en este punto la búsqueda de un repositorio único de eventos operativos cubiertos por los sistemas de detección automática, los que diferentes sistemas viertan sus registros de logs con eventos de monitorización.

Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones; es una de las actividades contempladas en la práctica de gestión DSS01.03 Monitorizar la infraestructura de I&T. La creación de un registro de log de eventos figura explícitamente como una de las salidas internas de esta práctica de gestión.

En este apartado también es relevante volver a citar el segundo Plan de Acción del Ministerio de Defensa para la Transformación Digital (PATD-2) (6), aprobado por Instrucción 14/2020, de 15 de abril, del Secretario de Estado de Defensa, por la que se aprueba la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital. Este plan incluye las actuaciones en materia de Administración Digital, Tecnologías de la Información y Comunicaciones a desarrollar en el conjunto del Departamento y sus organismos públicos adscritos, sobre dichos medios y servicios. Tiene como

finalidad principal lograr un mejor aprovechamiento de los Servicios CIS/TIC mediante la revisión integral de las tareas, actividades y procesos para lograr una transformación digital, basada en la integración de las Capacidades CIS/TIC en dichas actividades y procesos.

El PATD-2 (6) propone 43 actuaciones para el logro de estos objetivos. Estas 43 actuaciones se agrupan en las 5 dimensiones del plan. Algunos de estos objetivos se encuentran muy alineados con el ámbito de estudio de este TFM:

Dentro de la dimensión III. Datos, Información y Conocimiento, son objetivos relevantes, los siguientes:

- III.11. Crear una Plataforma de Análisis Masivo de Datos e Información para analizar y explotar la información de manera más eficaz.
- III.12. Identificar los indicadores necesarios para la toma de decisiones.
- III.13. Crear Servicios CIS/TIC (cuadros de mando, informes, alertas, etc.) con los indicadores identificados para la toma de decisiones.

Por su parte, dentro de la dimensión IV: Seguridad, es pertinente el objetivo:

- IV.4. Monitorizar la disponibilidad y calidad de los nuevos servicios.

Centrándose la exposición en el objetivo III.11. Crear una Plataforma de Análisis Masivo de Datos e Información para analizar y explotar la información de manera más eficaz; resulta fundamental reconocer las ventajas de implementar una infraestructura tecnológica centralizada e interoperable. Disponer de una plataforma unificada para el registro de eventos y almacenamiento de información, accesible por todos los sistemas del MDEF, facilitaría de manera significativa el registro, búsqueda y análisis de datos relevantes.

Esta plataforma también proporcionaría un soporte integral para un cuadro de mando que permita visualizar, en tiempo real, el estado de los servicios y la infraestructura de TI, lo cual es esencial para la toma de decisiones informadas y ágiles.

Para cumplir este objetivo, el MDEF ha propuesto la creación de una plataforma basada en herramientas de análisis masivo de datos (Big Data) y tecnologías de Inteligencia Artificial, que permitan explorar y analizar tanto la información almacenada como los eventos registrados en tiempo real por el MDEF.

Esta propuesta abarca justamente todas las necesidades de monitorización de infraestructura de TI objeto de este análisis.

La solución adoptada por el MDEF para la creación de una plataforma de análisis de datos ha sido la ofrecida por la empresa IBM y denominada IBM Cognos Analytics.

IBM Cognos Analytics es una plataforma avanzada de inteligencia empresarial (BI) que permite a las organizaciones explorar, analizar, visualizar y compartir datos de manera eficiente. Proporciona herramientas para generar informes, cuadros de mando y análisis, permitiendo a los usuarios tomar decisiones basadas en datos en entornos empresariales.

Esta herramienta se encuentra actualmente en proceso de implantación en el MDEF. Cognos ofrece recursos para la creación de informes y exploración de datos históricos, óptimos para la creación de cuadros de mando; pero para la realización de análisis en tiempo real, lo que se pretende en este proyecto, se precisaría una integración con una base de datos vitalizada.

La virtualización de datos crea una capa que permite acceder y analizar datos de múltiples fuentes en tiempo real, sin tener que moverlos físicamente a una base de datos específica. Esto reduce el tiempo de procesamiento, al permitir el acceso en tiempo real a datos distribuidos; así como facilita la combinación de datos de diferentes fuentes en una vista unificada.

La solución de IBM para análisis de datos en tiempo real es IBM Cloud Pak for Data. IBM Cloud Pak for Data es una plataforma de datos e IA que incluye capacidades de virtualización de datos. Esta virtualización permite a herramientas como IBM Cognos Analytics realizar análisis en tiempo real,

Actualmente el MDEF está desarrollando el proyecto de implementación IBM Cloud Pak for Data, lo que incluye el recurso de bases de datos virtualizadas, para poder aprovechar al máximo las capacidades de Cognos, pero transcurrirá bastante tiempo hasta que esta pueda estar operativa, lo que obliga a buscar una alternativa si se quiere que el objetivo de monitorización de la infraestructura TI, pueda ser alcanzado en un plazo razonable.

Esta situación lleva a apostar por la utilización de ElasticSearch como plataforma intermedia de registro de eventos.

Una línea futura para la continuación de este TFM sería el estudio de desarrollo de la plataforma ElasticSearch y su integración con los sistemas de monitorización existentes en el CESTIC, permitiendo la creación de un único repositorio de logs, que posteriormente podrían ser analizados utilizando diversas herramientas de Business Intelligence.

Los diversos software de monitorización cuentan con APIs²⁴ ya desarrolladas que permiten realizar llamadas o consultas a las bases de datos internas de las aplicaciones, donde se registran sus logs. Las descargas de los logs en texto plano se realizarán en el repositorio deseado.

3.4 Herramienta única ITSM (ProactivaNet)

Una vez contando con procesos definidos y estandarizados, el siguiente paso para el logro de las capacidades de gestión CIS/TIC requeridas por el Departamento, consiste en el despliegue de una herramienta única ITSM (ProactivaNet)

La implementación de una herramienta ITSM se alinea con los siguientes objetivos de gestión de COBIT 2019: (16)

- APO01 - Gestionar el Marco de Gestión de TI: La herramienta ITSM proporciona una estructura formal para gestionar los procesos y servicios de TI de forma eficiente, transparente y conforme a las políticas y objetivos organizacionales. Una herramienta ITSM facilita el establecimiento de Procesos y Procedimientos Estandarizados, proporciona visibilidad y trazabilidad de los servicios y activos de TI disponibles, promueve la mejora continua en los procesos de TI, garantiza el cumplimiento de políticas y controles de TI internos, proporciona soporte a la gobernanza y facilita la integración de todos los procesos de TI dentro de un marco unificado de gestión. (16)

- APO05 - Gestionar el Portafolio: Una herramienta ITSM ayuda a mantener un catálogo de servicios actualizado y accesible, lo cual facilita la gestión del portafolio de servicios TIC, permitiendo el seguimiento y la evaluación del rendimiento de los servicios que están en producción y los que están en fases de diseño o retiro. (16)

- BAI06 - Gestionar Cambios: En este caso, la herramienta ITSM se utiliza para gestionar las solicitudes de cambio (RFC). Una herramienta ITSM proporciona un flujo de trabajo estructurado que facilita la autorización, seguimiento y control de los cambios. (16)

- DSS02 - Gestionar Solicitudes e Incidentes de Servicio: Este objetivo cubre la capacidad de respuesta a solicitudes e incidentes. La herramienta ITSM permite la captura, priorización, escalación y resolución de incidencias y solicitudes, mejorando así la satisfacción del usuario final y la continuidad del servicio. (16)

²⁴ Las APIs (Interfaces de programación de aplicaciones) son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos. (Fuente: Wikipedia)

- **DSS03 - Gestionar Problemas:** Permite abordar la identificación y la resolución de problemas subyacentes que causan incidentes recurrentes. Una herramienta ITSM suele incluir funcionalidades de gestión de problemas, permitiendo un análisis más detallado de las causas raíz y el seguimiento de las soluciones a largo plazo. (16)

- **MEA01 - Monitorear, Evaluar y Evaluar el Desempeño y la Conformidad del Sistema:** A través de una herramienta ITSM, es posible monitorear el rendimiento del servicio, evaluar la eficacia de las operaciones y asegurar la conformidad con los acuerdos de nivel de servicio (SLA), un aspecto clave en la evaluación y monitoreo continuo de TI según COBIT. (16)

De lo anterior, se concluye que la implantación de una plataforma de gestión de servicios ITSM (ProactivaNet), permitirá al CESTIC alinear sus procesos y servicios TI de manera inequívoca con el marco COBIT. La implementación de la nueva herramienta de gestión de servicios de TI única para toda la I3D, se considera un factor crítico de éxito para alcanzar una gestión eficiente y única para todos los servicios CIS/TIC del Departamento.

A través de la implantación de la herramienta de gestión de servicios ProactivaNet, se pretende modelar la transición reflejada en la Tabla 3-9, desde la situación actual (AS-IS) hasta la situación objetivo (TO BE) a través de las siguientes prácticas de gestión: (16)

Prácticas de gestión	Situación actual de Gestión (AS-IS)	Situación objetivo de Gestión (TO-BE)
APO01.10 Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión.	Falta de racionalización y optimización de los recursos. Mantenimiento actual de multitud de herramientas de gestión (ICIS, SCANS, GESTIONAL...).	Centralización en una única herramienta de gestión ITSM (ProactivaNet)
APO08.03 Gestionar la relación con el negocio.	No existe una fuente única de datos ni un canal único de comunicación para todos los actores de gestión, incluido el usuario final.	Utilizar un único canal de comunicación para todos los actores de gestión. Peticiones de servicio e incidentes clasificados y priorizados.
APO09.02 Catalogar los servicios habilitados por I&T.	No existe un único Catálogo de Servicios CIS/TIC identificado, implementado e interactivo en una herramienta de gestión.	ProactivaNet debe ser la plataforma tecnológica que aloje y gestione para que todos los procesos operen satisfactoriamente.
DSS01.01 Ejecutar procedimientos operativos.	No existe una única herramienta para la gestión integral de los servicios CIS/TIC, lo cual dificulta una ejecución eficiente y, por consiguiente, una carga de trabajo adicional del personal por redundancias de cometidos	Utilizar Proactiva como herramienta única de gestión integral de los servicios CIS/TIC

DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	Las herramientas actualmente desplegadas disponen de una capacidad de soporte a incidencias y peticiones, pero carecen de módulos de soporte a otros procesos de gestión críticos (catálogo, niveles de servicio, cambios, activos y configuración, proveedores...).	Una gestión integrada de incidencias y peticiones con una misma herramienta. Creación de un repositorio con todos los procedimientos críticos a disposición del Centro de Atención al Usuario, más allá de los que atañen a los sistemas y servicios de la I3D, gestionados a través de ProactivaNet. Es necesario definir una estructura que permita asignar la responsabilidad a cada servicio / activo.
MEA01.02 Establecer objetivos de rendimiento y conformidad. MEA01.03 Recopilar y procesar los datos de rendimiento y conformidad.	Las herramientas actualmente desplegadas no permiten la configuración de métricas ni informes, por lo que es muy difícil conocer el nivel de soporte que CESTIC proporciona a los servicios de la I3D, ni tampoco identificar disfunciones en la gestión de forma proactiva. No se ha definido ni evaluado ningún KPI relativo a niveles de provisión de servicio.	Definición de métricas e informes que permitan conocer los niveles de soporte ofrecidos por el CESTIC. Definir KPIs de servicio y realizar un seguimiento de los mismos.

**Tabla 3-9 Situación actual y objetivo con la implementación de ProactivaNet en el CESTIC
(Fuente: Elaboración propia)**

De la tabla anterior se concluye que, dentro del marco COBIT, existen una serie de objetivos de gestión y prácticas de gestión cuya observación resulta muy relevante para la consecución del objetivo de despliegue de una herramienta ITSM. Se analizan a continuación:

Objetivo de Gestión APO01 Gestionar el Marco de Gestión de TI

El objetivo de Gestión APO01 Gestionar el Marco de Gestión de TI, pertenece al Dominio COBIT: Alinear, Planificar y Organizar (APO). El desarrollo del mismo se especifica en la correspondiente tabla de Proceso: Objetivo de gestión: APO01 Gestionar el Marco de Gestión de TI, del documento “Objetivos de gobierno y gestión, COBIT 2019 Marco de Referencia” (16), la cual establece las siguientes previsiones para este objetivo:

Descripción: Diseñar el sistema de gestión para la I&T de la empresa basándose en las metas empresariales y otros factores de diseño. En base a este diseño, implementar todos los componentes necesarios del sistema de gestión.

Propósito: Implementar un enfoque de gestión consistente para permitir que se alcancen los requisitos de gobierno empresarial, con cobertura de componentes de gobierno, como los procesos de gestión, las estructuras organizativas, los roles y las responsabilidades, las actividades confiables y

repetibles, los elementos de información, las políticas y procedimientos, las habilidades y las competencias, la cultura y el comportamiento, y los servicios, infraestructura y aplicaciones.

Prácticas de gestión: Cada objetivo de gobierno y gestión incluye varias prácticas de proceso, y cada proceso incluye una o más actividades. El marco COBIT 2019 (16) prevé para el Objetivo de gestión: APO01 Gestionar el Marco de Gestión de TI, diversas prácticas de gestión:

- Práctica de gestión - APO01.01 Diseñar el sistema de gestión para la I&T de la empresa
- Práctica de gestión - APO01.02 Gestionar la comunicación de objetivos, dirección y decisiones tomadas.
- Práctica de gestión - APO01.03 Gestionar la implementación de procesos (para respaldar la consecución de objetivos de gobierno y gestión).
- Práctica de gestión - APO01.04 Definir e implementar las estructuras organizativas.
- Práctica de gestión - APO01.05 Establecer roles y responsabilidades.
- Práctica de gestión – APO01.06 Optimizar la ubicación de la función de TI.
- Práctica de gestión – APO01.07 Definir la propiedad de la información (datos) y del sistema de información.
- Práctica de gestión – APO01.08 Definir las habilidades y competencias objetivo.
- Práctica de gestión - APO01.09 Definir y comunicar políticas y procedimientos.
- Práctica de gestión - APO01.10 Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión.
- Práctica de gestión - APO01.11 Gestionar la mejora continua del sistema de gestión de I&T.

Para el caso despliegue de una herramienta única ITSM, es muy relevante el estudio de la práctica de Práctica de gestión: APO01.01 Diseñar el sistema de gestión para la I&T de la empresa para respaldar el sistema de gobierno y gestión, así como la práctica APO01.10 Definir e implementar la infraestructura, servicios y aplicaciones. Así mismo, otras prácticas de gestión también estarán relacionadas con este objetivo, como se verá posteriormente.

En virtud de lo expuesto anteriormente, el siguiente paso sería definir un esquema de implantación de la herramienta ProactivaNet.

Esquema de implantación de la herramienta ProactivaNet:

Se propone un esquema en varias fases para la implantación de la herramienta ProactivaNet, en línea con las recomendaciones del marco COBIT y adaptado a las necesidades surgidas ante la implantación real de la herramienta.

Fases de implementación de ProactivaNet:

1. Establecer una Oficina de Proyecto (OP) de ProactivaNet: Esta Oficina estará compuestas por un jefe de proyecto, que contará con un equipo de apoyo directo, además de un equipo de apoyo interno del CESTIC formado por una persona de cada unidad y de un equipo de apoyo externo formado por los servicios profesionales de la empresa adjudicataria. La asignación del roles y responsabilidades deberá adaptarse a la estructura interna del CESTIC.
2. Elaborar un Plan de Proyecto: Se requiere la elaboración de un planeamiento minucioso de implantación por fase, dado el carácter estratégico y transversal que supone el despliegue de la herramienta ITSM/ITAM ProactivaNet para proporcionar y garantizar la gestión única de esta

Dirección General como responsable principal de la provisión de los servicios CISTIC del Departamento.

3. Definición de un catálogo único de servicios de la I3D: Se considera que este trabajo debe estar terminado antes del inicio del proyecto de implantación de ProactivaNet, ya que es la columna vertebral sobre el que se despliegan, posteriormente, el resto de los módulos de la herramienta. Además, en esta fase, debe decidirse la información a incluir en ProactivaNet, así como el modelo de integración (y en qué grado) con otras herramientas empleadas para el descubrimiento de servicios.
4. Definición de una estructura de roles / responsabilidades para cada servicio / activo registrado en la herramienta ITSM. Se considera necesario la definición de una estructura que permita segmentar a los responsables por cada ámbito funcional en el plano CIS/TIC para cada uno de los ámbitos en los que se dividen las FFAA, así como realizar un escalado de las incidencias. Sin la definición de una estructura, cada perfil técnico tendrá asignado sus permisos de manera individual, lo que resultará en una tremenda dificultad a la hora de gestionar roles de grupos cuando un grandísimo número de usuarios hayan sido creados.
5. Despliegue de los módulos de la herramienta, correspondientes con procesos de gestión de la Arquitectura de Referencia GES CIS/TIC:

ITAM:

- Descubrimiento y G. Activos.
- G. Configuración (CMDB)
- G. Capacidad y Disponibilidad.
- G. Proveedores y Contratos.

ITSM:

- G. Portafolio y Catálogo de Servicios.
 - G. Incidencias y Peticiones.
 - G. Niveles de Servicio.
 - G. Conocimiento (KB).
 - G. Problemas.
 - G. Cambios.
 - G. Continuidad.
6. Determinación del Servicio o grupo de servicios CIS/TIC de la I3D (Usuario, Infraestructura de Información e Infraestructura de Telecomunicaciones) gestionados en la herramienta.
 7. Ámbitos donde se despliega la herramienta. El plan debe contemplar el despliegue progresivo e incremental de la herramienta para su uso en todos los ámbitos, de forma que pueda ser utilizada por los usuarios de los servicios de la I3D
 8. Elaboración de Instrucciones Técnicas (ITs) homogéneas por proceso de gestión CIS/TIC de la I3D e Instrucciones Operacionales (IOP) derivadas.

Por la importancia que tiene en la implementación de la herramienta ProactivaNet, el TFM se centra a continuación en la definición de la fase 4 del plan de implantación: Definición de una estructura de roles / responsabilidades para cada servicio / activo registrado en la herramienta ITSM

Fase 4: Definición de una estructura de roles / responsabilidades para cada servicio / activo registrado en la herramienta ITSM

A fecha de noviembre de 2024, una vez aprobado y transferido el catálogo de servicios a la División de Operaciones de red (DIVOPER) del CESTIC; DIVOPER debe centrarse en la definición de una estructura de roles / responsabilidades para cada servicio / activo registrado en la herramienta ITSM, que permita la gobernanza del referido Modelo para el Gobierno y Gestión Única de Servicios CIS/TIC a través de esta herramienta.

Para hacer esto posible es preciso integrar el esquema de gestión proporcionado por la herramienta ProactivaNet, en la estructura departamental y de responsabilidades existente previamente en la organización.

Este TFM se centra en el estudio de esta cuestión, con el objetivo de facilitar DIVOPER asesoramiento en los puntos clave para la definición de esta estructura y la implementación efectiva de la herramienta ProactivaNet.

La definición de esta estructura de roles y responsabilidades también está alineada con las siguientes prácticas de gestión planteadas por el marco COBIT e incluidas en el Objetivo de gestión: APO01 Gestionar el Marco de Gestión de TI:

- Práctica de gestión - APO01.04 Definir e implementar las estructuras organizativas.
- Práctica de gestión - APO01.05 Establecer roles y responsabilidades.

La herramienta ProactivaNet separa el acceso a los procesos de gestión con una doble opción: Por un lado, la gestión de activos, a través del módulo ITAM, y del que, por acuerdo de la Dirección, la competencia en su administración ha sido delegada en la Unidad de Estrategia, Demanda y Calidad (UEDEC) y que por lo tanto no corresponderá a DIVOPER; y por otro lado el Service Desk, a través de la herramienta ITSM, cuya competencia de administración recae en DIVOPER.

Desde el módulo de Gestión de Activos (ITAM) se accederá a los activos y su administración, así como a la Base de datos de Gestión de la Configuración (CMDB)

Por su parte, desde el **módulo Service Desk (ITSM)** se accederá a la mayoría de Prácticas de Gestión contempladas en ITIL. Estas Prácticas de Gestión son las siguientes:

- Gestión de incidencias y peticiones.
- Gestión de problemas.
- Gestión de cambios.
- Gestión del Catálogo de Servicios
- Gestión de proveedores.
- Gestión de la continuidad
- Gestión de los Acuerdos de Nivel de Servicio (SLA)

Esto implica, que desde el punto de vista de la Gestión de Servicios (ITSM) la mayoría de las prácticas de gestión de servicios entrarían dentro de Service Desk. En consecuencia, los administradores de Gestión de Activos en PROACTIVANET son los únicos que pueden relacionar los CIs (o elementos de configuración) con los servicios; y, por tanto, les corresponde en exclusiva la Gestión de la Configuración (CMDB) que es una práctica de gestión de servicios (ITSM).

Al margen de que se haya dispuesto que diferentes unidades realizarán la gestión de los módulos de ProactivaNet, es necesario la definición de un grupo o usuario que realice una gestión de la herramienta a nivel de administrador o superadministrador, por debajo del cual, se encontrarían los administradores de ITAM, ITSM, CMDB, Gestor del Cambio y Gestor del Catálogo de Servicios.

Se determina que lo más conveniente es que este rol de Administrador de ProactivaNet recaiga en la Unidad de Servicios de Información, perteneciente a la División de Operaciones de Red (DIVOPER), al ser la unidad que cuenta con los medios técnicos para asumir las funciones que implica la asunción de dicho rol de superadministrador. Estas funciones son las siguientes:

- Administración general de la herramienta a nivel de infraestructura.
- Mantenimiento de la infraestructura de máquinas virtuales y bases de datos de las Instancias de ProactivaNet, tanto en dominios de alta clasificación como en dominios de baja clasificación.
- Resolución de incidencias por corte o malfuncionamiento del servicio.
- Actualización de versiones de la herramienta.
- Creación de los diferentes tipos de roles dentro de la herramienta, así como la asignación de los permisos a cada rol y la modificación de los mismos según la necesidad.
- Asignación de roles a los administradores de cada proceso de gestión.
- Administración de todos los elementos transversales a los procesos de gestión de servicios, como localizaciones, unidades, bases, categorías, cambios en la matriz de prioridades...

Por debajo de este superadministrador, se encontrarían las 6 funciones separadas que se asignarán a los distintos responsables dentro del CESTIC, como muestra la Figura 3-4.

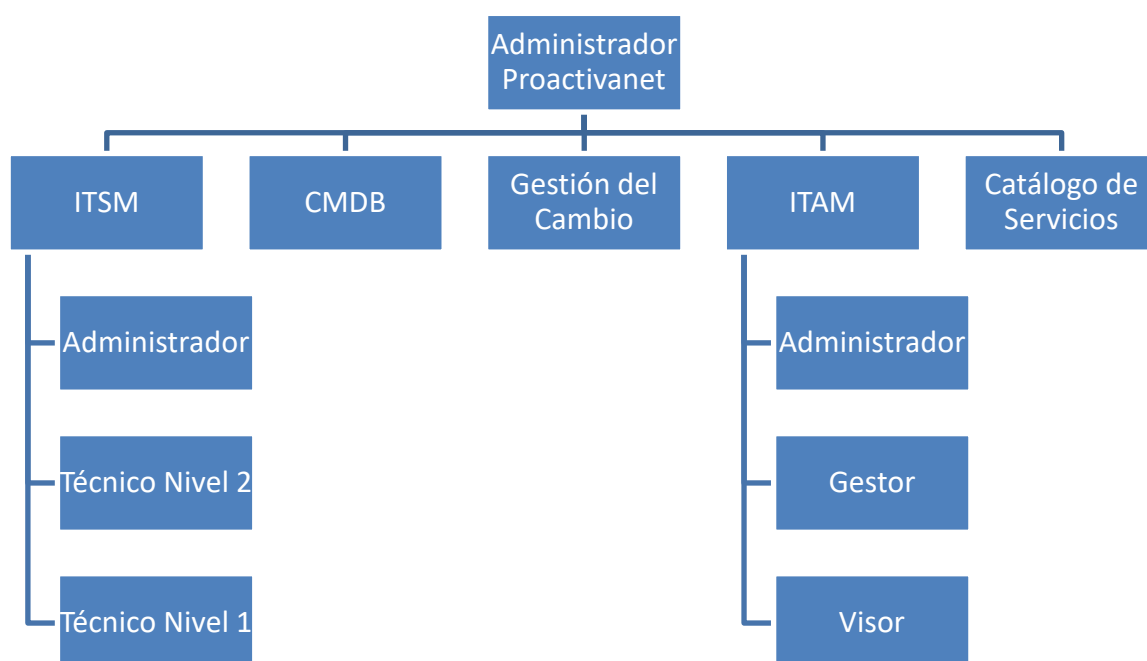


Figura 3-4 Esquema de roles propuesto para la administración de ProactivaNet (Fuente: Elaboración propia)

En resumen, el superadministrador creará los grupos de Administradores en ProactivaNet y estos comprenderán: los usuarios de Superadministrador, Administradores de ITAM, ITAM Gestor, ITAM

Visor, Administradores de ITSM, ITSM Técnico Nivel 2, ITSM Técnico Nivel 1 y Gestor Catálogo Servicios.

Definición de la estructura de funciones y roles dentro del módulo Service Desk ITSM

La función de gestión del módulo de Service Desk, a través de sus diferentes roles, debe ser asumida por la unidad CEGES dentro de DIVOPER. Como se ha mencionado con anterioridad en el presente TFM, el CEGES es el Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D), que se configura como el Centro de Servicio Único al Usuario para toda la red I3D del MDEF, según establece la Visión 01/22 del CESTIC: Concepto del Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D) (8)

La asunción de esta función por el CEGES permite alinear las necesidades de implementación de la herramienta ProactivaNet con la previsiones establecidas en el documento Visión 01/22 del CESTIC (8), así como en la Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC); sobre la necesidad de creación de un Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES), como base para la implantación de un modelo único de gestión de servicios.

Esta propuesta es coherente con todos los documentos de referencia para la Gestión de Servicios en el MDEF, y permite dar cumplimiento a los mismos.

Se presenta la siguiente propuesta de niveles dentro de la función Service Desk ITSM:

- El Administrador de Usuarios: Se encargará de asignación de usuarios y grupos, la asignación de accesos, roles y modificación de perfiles de acceso. El Administrador de Usuarios tendrá acceso al menú de Gestión de Accesos dentro de la Administración.
- Técnico Nivel 2: Técnicos más especializados, que se ocuparán de las incidencias escaladas desde primera línea, que no puedan ser resueltas por los técnicos de nivel 1. La Arquitectura de Referencia GES CIS/TIC lo denomina como Soporte CIS/TIC.
- Técnico Nivel 1: Es la primera línea de todo el soporte técnico, actuando como punto de contacto único al usuario. Se ocupa de la recepción de incidencias, atención inmediata y escalado a segunda línea. Este apoyo será ofrecido por la sección del Centro de Atención al Usuario (CAU), cuyo personal ofrecerá un soporte básico para la resolución de las incidencias y las peticiones.

Otros roles previstos por la herramienta ProactivaNet para el módulo Service Desk ITSM son los siguientes:

- Encuestas Gestor: Administra el módulo de Gestión de Encuestas de Satisfacción de los usuarios.
- Gestor de dashboards del Service Desk: Que administra métricas y dashboards del Service Desk.
- Supervisor de incidencias / peticiones: Tiene acceso a las incidencias / peticiones en base a las reglas de negocio de Supervisión.
- Rol de solo lectura de Dashboards: Podrá consultar todos los dashboards disponibles de forma que pueda supervisar las métricas del Service Desk. Este rol por sí sólo no consume licencia.

Para poder materializar estos 3 niveles principales de roles, se deben crear 3 grupos en el Active Directory de la organización, del tipo:

- _LMDEF-ITSM-ADMINISTRADOR
- _LMDEF-ITSM-TN2
- _LMDEF-ITSM-TN1

Una vez creados estos grupos, se agregarían los distintos usuarios a los mismos, según determine el responsable de ITSM.

Una vez asignados los roles en los tres niveles, habría que comunicar a los distintos Ámbitos que crearan los mismos grupos, que se vincularían a los grupos Padre y heredarían los permisos asignados. Los grupos de los Ámbitos serían (XXX hace referencia al nombre de cada una de las unidades existentes en AD):

- _LXXX-ITSM-ADMINISTRADOR
- _LXXX-ITSM-TN2
- _LXXX-ITSM-TN1

En este punto, conviene destacar que tanto la Arquitectura de Referencia (AR) Única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC) (7); como la Visión 01/22 del CESTIC: Concepto del Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D) (8), plantean un esquema de gestión de incidencias con 4 niveles de soporte en función de la dificultad para su resolución. Estos niveles son los siguientes:

- Soporte de Nivel 0: Tareas que puede llevar a cabo el usuario final sin interacción ni ayuda profesional CIS/TIC.
- Soporte de Nivel 1: Primera línea de todo el soporte técnico. Se ocupa de la recepción de incidencias, atención inmediata y escalado a segunda línea.
- Soporte de Nivel 2: Técnicos con habilidades especializadas más allá del Nivel 1
- Soporte de Nivel 3: Nivel más alto de habilidades especializadas proporcionadas por equipos externos al CEGES.

Sin embargo, en la propuesta planteada en este TFM, se reduce este esquema a niveles, más una serie de roles supervisores. Se plantea esta opción para semejarlo al modelo de escalado de incidencias, que, en el ámbito de la Ciberseguridad, ya está gestionando el Centro de Operaciones de Seguridad de la I3D (COS I3D) de la D.G. CESTIC.

Este modelo de escalado ha demostrado relativo éxito en la misma organización, por lo que se plantea semejar el modelo de gestión de incidencias ITSM al modelo de Gestión de Operaciones de Seguridad, en base a que la organización ya cuenta con experiencia de gestión con este modelo y ha mostrado buenos resultados.

Definición de la estructura de funciones y roles dentro del módulo de Gestión de Activos ITAM

Para este módulo se plantea un esquema en 3 niveles a semejanza de la estructura propuesta para el Service Desk ITSM

Para poder materializar estos 3 niveles principales de roles, se deben crear 3 grupos en el Active Directory de la organización, del tipo:

- _LMDEF-ITAM-ADMINISTRADOR: El Administrador de Inventario dispondrá de acceso total al módulo de ITAM y la posibilidad de parametrizar todos los procesos licenciados: Gestión de Activos, Gestión de la Configuración (CMDB), Gestión de la Capacidad y la Disponibilidad, y Gestión de Proveedores y Contratos.

- **_LMDEF-ITAM-GESTOR:** El gestor de inventario podrá consultar todos los datos del módulo de ITAM y los procesos licenciados, pero sólo podrá editar datos de la Gestión de Activos. Este rol por sí solo no da acceso al menú de Administración del módulo de ITAM.

- **_LMDEF-ITAM-VISOR:** O editor de acceso restringido. Podrá consultar y editar datos de la Gestión de Activos exclusivamente de las localizaciones y/o clasificaciones hardware a las que tenga acceso.

Otros roles previstos por la herramienta ProactivaNet para el módulo ITAM son los siguientes:

- **Gestor de dashboards de gestión de activos:** Que administra métricas y dashboards de gestión de activos. (Creación y edición de dashboard mediante control de cambios).

- **Gestor de monitorizaciones:** Podrá consultar todos los datos del módulo de ITAM y los procesos licenciados, pero sólo podrá editar datos del módulo de Monitorización. Accederá a la herramienta de monitorización con credenciales de administrador.

- **Técnico monitorizaciones:** Podrá consultar todos los datos del módulo de ITAM y los procesos licenciados, pero sólo podrá editar datos del módulo de Monitorización. Accederá a la herramienta de monitorización con credenciales de usuario.

Una vez creados estos grupos, se agregarían los distintos usuarios a los mismos, según determine el responsable de ITAM.

Una vez asignados los roles en los tres niveles, habría que comunicar a los distintos Ámbitos que crearan los mismos grupos, que se vincularían a los grupos Padre y heredarían los permisos asignados. Los grupos de los Ámbitos serían (XXX hace referencia al nombre de cada una de las unidades existentes en AD):

- **_LXXX-ITAM-ADMINISTRADOR**
- **_LXXX-ITAM-GESTOR**
- **_LXXX-ITAM-VISOR**

Otras funciones de la herramienta más allá de ITSM e ITAM

Gestión del Catálogo de Servicios: La gestión del catálogo de servicios la asumirá la Oficina Técnica de la División de Operaciones de Red (DIVOPER), al ser a unidad dentro de la división encargada de impulsar una correcta incorporación de los servicios al ámbito de DIVOPER. En este caso se contempla un único rol de Gestos de Catálogo de Servicios SCM, cuyo cometido es la administración del módulo de catálogo de servicios.

Gestor de la CMDB: Esta función la asumirá el mismo equipo de trabajo que la Administración de ProactivaNet, es decir, la Unidad de Servicios de Información, perteneciente a DIVOPER, si bien el responsable funcional encargado de dirigir este equipo será nombrado por la División de Diseño y Evaluación de Arquitecturas (DISEVAR) del CESTIC, ya que es la división con competencias en el diseño de arquitecturas. El Gestor de la CMDB podrá consultar todos los datos del Inventario, pero sólo podrá editar datos vinculados a la CMDB.

Gestión del Cambio: Esta función la asumirá el mismo equipo de trabajo que la Administración de ProactivaNet, es decir, la Unidad de Servicios de Información, perteneciente a la División de Operaciones de Red (DIVOPER). Aunque en este caso la responsabilidad funcional recae en el responsable designado por el CHIEF OPERATING OFFICER (COO), al ser responsable de la gestión del cambio en el CESTIC.

3.5 Comparativa entre herramientas ITSM

Para realizar una comparativa efectiva entre distintas herramientas de ITSM, que tenga en cuenta principalmente a ProactivaNet, y evaluar su rendimiento en relación con otras soluciones disponibles en el mercado, es importante seguir un proceso estructurado que considere tanto aspectos funcionales como operacionales.

En el presente TFM se presenta una propuesta de comparativa para herramientas ITSM. Para la redacción de una propuesta servirá de inspiración la información contenida en el libro: Preparación para la certificación ITIL Foundation V3 (11)

De acuerdo con esta iniciativa, una comparativa debería considerar los siguientes puntos:

1) Primero: Comenzar por la selección de la herramienta a comparar:

Como se ha visto a lo largo de este TFM, el MDEF está implantado la herramienta ITSM ProactivaNet, por lo que sería interesante establecer una comparación de esta herramienta con otras.

Hasta el momento el CAU del CESTIC ha utilizado una herramienta de seguimiento de tickets, de desarrollo propio del MDEF, denominada SCANS, por lo que resultaría muy relevante una comparativa entre estas herramientas para poder valorar cuantitativa y cualitativamente, las mejoras términos de rendimiento, eficiencia y productividad, logrados por el MDEF con el despliegue de ProactivaNet.

Si bien es cierto que, como en el momento de finalización de este TFM, el despliegue de ProactivaNet no se ha completado, no es posible en el momento actual realizar una comparativa completa entre la funcionalidad de ambas herramientas.

Un estudio comparativo entre herramientas ITSM podría tener en cuenta también otras soluciones populares de mercado, como ServiceNow, BMC Remedy, Jira Service Now, Cherwell, o Ivanti Service Manager... algunas de las mismas ya han sido referidas con anterioridad en este TFM.

2) Segundo: Definir Criterios de Evaluación.

Los criterios de evaluación deben abarcar los aspectos más relevantes para el negocio y la operación de la organización. Algunos de los más importantes incluyen:

a) Aspectos relativos a la funcionalidad, como son:

- Gestión de Incidentes: ¿Cómo maneja la herramienta la identificación, seguimiento y resolución de incidentes?

- Gestión de Problemas: ¿ProactivaNet y las demás herramientas permiten la identificación proactiva de problemas y su resolución?

- Gestión de Cambios: ¿La herramienta proporciona un proceso estructurado para la gestión de cambios, minimizando riesgos?

- Gestión de Solicitudes de Servicio: ¿Cómo maneja la herramienta las solicitudes de servicios estándar (como restablecer contraseñas, instalar software)?

- Base de Conocimiento: ¿Ofrece un repositorio accesible y eficaz para resolver incidencias sin intervención del equipo de soporte?

- Automatización: ¿La herramienta ofrece capacidades de automatización para reducir tareas manuales?

b) Elementos relacionados con la usabilidad y la experiencia de usuario:

- Interfaz de Usuario (UI): ¿Es intuitiva, fácil de usar, personalizable y accesible para usuarios no técnicos?

- **Accesibilidad Móvil:** ¿Las herramientas ofrecen aplicaciones móviles o interfaces web adaptadas para acceso remoto?

- **Capacitación y Soporte:** ¿Qué tan fácil es aprender y usar la herramienta? ¿El soporte al cliente y la documentación son adecuados?

c) **Capacidades de Integración y compatibilidad de la herramienta.**

- **Integraciones con otras herramientas:** ¿ProactivaNet y las herramientas comparadas permiten integraciones con otras plataformas y soluciones existentes, como sistemas ERP²⁵, herramientas de monitorización, etc.?

- **Compatibilidad con otras plataformas:** ¿La herramienta es compatible con distintos sistemas operativos, entornos en la nube, y dispositivos?

d) **Rendimiento y Escalabilidad**

- **Velocidad y Tiempo de Respuesta:** ¿Qué tan rápido responde la herramienta a solicitudes de los usuarios y gestiona grandes volúmenes de datos?

- **Escalabilidad:** ¿Es capaz de adaptarse al crecimiento de la organización y al aumento de la complejidad de los servicios de TI sin perder eficiencia?

e) **Coste Total de Propiedad (TCO²⁶)**

- **Licencias y Precios:** ¿Cómo se estructura el modelo de precios? ¿Es más económico o costoso que otras soluciones?

- **Costos adicionales:** ¿Existen costos adicionales asociados con personalizaciones, soporte, formación, mantenimiento?

f) **Seguridad y Cumplimiento**

- **Control de Acceso y Autenticación:** ¿La herramienta incluye un control de acceso robusto y funciones de autenticación para asegurar los datos?

- **Cumplimiento Normativo:** ¿Cumple la herramienta con normativas de privacidad y seguridad de datos relevantes como RGPD, ISO 27001, etc.?

g) **Capacidades de generación de Informes y Análisis:**

- **Capacidades de Informes:** ¿Qué tan robustas son las capacidades de generación de informes y análisis? ¿Se pueden crear informes personalizados y detallados?

- **Indicadores Clave de Rendimiento (KPI):** ¿La herramienta permite definir y hacer seguimiento de KPIs para evaluar el desempeño de los servicios?

3) Tercero: Recopilación de datos y pruebas

Para una evaluación comparativa precisa, se pueden realizar varias acciones, como:

- **Solicitar demos o pruebas gratuitas:** Contacta con los proveedores de las herramientas seleccionadas para solicitar demostraciones o acceso a versiones de prueba.

²⁵ ERP (Enterprise Resource Planner): Es un sistema de planificación de recursos empresariales que permite la gestión integrada de los principales procesos en una empresa.

²⁶ El término TCO significa costo total de propiedad. Es una evaluación de todos los costos en los que incurre su organización al adquirir, instalar, ejecutar y mantener su infraestructura de TI

- Consultar Opiniones de Usuarios: Revisa comparativas y opiniones en plataformas de terceros, como Gartner, Forrester, Capterra y TrustRadius, donde los usuarios comparten sus experiencias.
- Análisis de Casos de Uso: Compara cómo cada herramienta maneja situaciones específicas en tu entorno (por ejemplo, gestión de incidencias en un entorno de alta disponibilidad).
- Evaluación de Soporte: Analiza el soporte técnico que ofrece cada herramienta, tanto en términos de tiempo de respuesta como calidad del servicio.

4) Evaluación Cuantitativa y Cualitativa de las herramientas

- Evaluación Cuantitativa: Establecer un sistema de puntuación para cada uno de los criterios mencionados anteriormente. Por ejemplo, cada herramienta puede ser evaluada en una escala del 1 al 5 en aspectos como facilidad de uso, integración, rendimiento, etc. Esto te permitirá comparar directamente los resultados de cada herramienta en términos absolutos.
- Evaluación Cualitativa: Aparte de las puntuaciones numéricas, evalúa aspectos más subjetivos, como la satisfacción de los usuarios, la facilidad de implementación, y cómo se alinea la herramienta con la estrategia y necesidades a largo plazo del MDEF.

5) Finalmente, redactar un informe comparativo que incluya:

- Resumen ejecutivo: Resaltando las fortalezas y debilidades de cada herramienta.
- Análisis de cada criterio: Presenta la evaluación detallada de cada herramienta, acompañada de ejemplos específicos y métricas cuantitativas.
- Recomendaciones: Basadas en los resultados, sobre cuál herramienta se adapta mejor a las necesidades del MDEF.

3.5.1 Comparativa de la herramienta ProactivaNet:

Como se ha referido en el apartado, la implementación de ProactivaNet por el MDEF no se ha completado, lo que impide realizar una comparativa de rendimiento real de Proactiva en relación con su herramienta predecesora SCANS.

Se va a utilizar la propuesta de comparativa formulada en el apartado anterior para avanzar en la definición de un informe comparativo que tenga como principal objetivo la evaluación de la herramienta ProactivaNet, pudiendo ser la culminación de este informe comparativo, un propósito para un proyecto posterior, más allá del alcance de este TFM

3.5.2 Recopilación de información para el estudio comparativo:

El punto tercero del estudio propuesto hace referencia a la Recopilación de datos y pruebas.

Una fuente de información son las opiniones de los usuarios expuestas en plataformas especializadas. Se consultan los siguientes foros:

Valoraciones sobre ProactivaNet en FORO TI de Gartner:

El Foro TI de Gartner (18) es una de las plataformas en línea más populares, donde los usuarios de tecnología empresarial pueden compartir experiencias, hacer preguntas y ofrecer reseñas sobre productos y servicios tecnológicos.

De acuerdo con el FORO sobre TI de Gartner, se recogen las siguientes opiniones de usuarios sobre el software ITSM ProactivaNet:

De las 30 opiniones reportadas en el FORO de GARTNER sobre el software ITSM ProactivaNet, los usuarios destacan como puntos a favor y en contra de la herramienta ITSM las siguientes (Ver Tabla 3-10):

Dimensión valorada favorablemente	Número de opiniones favorables
Plataforma / Portal intuitiva	5
El soporte facilitado por la empresa	4
Elevado grado de configurabilidad	2
Seguimiento de las prácticas de ITIL	1
Buen gestor de KPI	1
Solidez del producto	1

Tabla 3-10 Recopilatorio de las dimensiones valoradas favorablemente de ProactivaNet en el foro TI de Gartner. (Fuente: (18) y elaboración propia)

La opinión favorable más repetida está relacionada con la amabilidad de la interfaz, que es una opinión destacada por 5 de los 30 usuarios que han reportado valoración.

Otro aspecto muy destacado por los usuarios es el acompañamiento brindado por la empresa durante el proceso de implementación y las opciones de configuración de la herramienta.

Opiniones desfavorables (Tabla 3-11):

Dimensión valorada desfavorablemente	Número de opiniones desfavorables
Sin evidencias de desventajas	1
Limitada compatibilidad de la herramienta con otros recursos (por ejemplo, BBDD de Oracle, herramientas BI)	3
Generación de tickets poco intuitiva para los usuarios	2
Implementación del software compleja	1
Configuración de la gestión de activos compleja	1
Inferior grado de madurez comparado con herramientas similares	1
Complejidad en la configuración de los agentes	1
Pobre Interfaz gráfica para la parte de usuario	2

Tabla 3-11 Recopilatorio de las dimensiones valoradas desfavorablemente de ProactivaNet en el foro TI de Gartner. (Fuente: (18) y elaboración propia)

Valoraciones sobre ProactivaNet en FORO TI de Capterra:

Capterra es una plataforma web que funciona como directorio y sistema de reseñas de software empresarial. Permite a usuarios comparar, evaluar y revisar diferentes soluciones de software.

De acuerdo con el FORO sobre TI Capterra en el que se registran opiniones de usuarios de la herramienta ProactivaNet, en él se destacan titulares como: “Eficacia en la gestión de servicios”, “ProactivaNet: Una solución integral para la gestión de activos y servicios de TI”, “Un gran soporte y respaldo para nuestra institución”, “Mejor herramienta integral ITSM”

De las 16 opiniones reportadas en Capterra sobre el software ITSM ProactivaNet, los usuarios destacan como puntos a favor y en contra de la herramienta ITSM las siguientes:

Opiniones favorables (Tabla 3-12):

Dimensión valorada favorablemente	Número de opiniones favorables
Acompañamiento en el proceso de implementación	4
Amigabilidad de la interfaz	6
Gestión automatizada del inventario de hardware	1
Seguimiento de las prácticas de ITIL	1
Capacidad de personalización	1
Facilidad de incorporación de procesos complejos	1

Tabla 3-12 Recopilatorio de las dimensiones valoradas favorablemente de ProactivaNet en el foro TI de Capterra. (Fuente: (19) y elaboración propia)

La opinión favorable más repetida está relacionada con la amabilidad de la interfaz, que es una opinión destacada por 6 de los 16 usuarios que han reportado valoración. Este era también el aspecto valorado más favorablemente en el Foro de Gartner sobre la herramienta.

Otro aspecto muy destacado por los usuarios es el acompañamiento brindado por la empresa durante el proceso de implementación.

Opiniones desfavorables (Tabla 3-13):

Dimensión valorada desfavorablemente	Número de opiniones desfavorables
Sin evidencias de desventajas	3
Dificultad de implementar modificaciones por su diseño modular	4
Requerimientos en Service Desk	1
Problemas con las actualizaciones	2
Lentitud en el logging en el inicio de sesión por los técnicos	1
Precio	1
Percepción visual	1
Manejo de multiproyectos en la mesa de servicios	1

Tabla 3-13 Recopilatorio de las dimensiones valoradas desfavorablemente de ProactivaNet en el foro TI de Gapterra. (Fuente: (19) y elaboración propia)

Por su parte, la opinión desfavorable más destacada atiende a la dificultad de implementar modificaciones, por su diseño modular, que es una dimensión destacada como mala en 4 de las 16 valoraciones.

Otro aspecto con valoración negativa por más de un usuario son los problemas con las actualizaciones. También es relevante que 3 usuarios no hayan encontrado ningún elemento negativo que resaltar.

Valoración de la herramienta ProactivaNet por los usuarios del CESTIC y comparativa con la herramienta SCANS anterior.

En este punto, además de tener en cuenta las opiniones de los usuarios de Proactiva de otras empresas, sería relevante conocer el juicio que los usuarios del MDEF tienen sobre la misma.

Una vez comenzada la implantación de la herramienta ProactivaNet en el CESTIC, y estando los futuros Administradores de la herramienta inmersos en el proceso de configuración inicial de la misma, se considera relevante estudiar las opiniones que las personas de la organización se van formando sobre la herramienta; a pesar de que en la fecha de redacción de estas líneas, a diciembre de 2024, la utilización de la herramienta no es masiva ni generalizada, a lo que debe sumarse el sesgo negativo que pueden ocasionar los problemas iniciales vinculados al proceso de implementación de cualquier software, que puede generar opiniones negativas de los usuarios sobre ciertos aspectos de la herramienta, pero estas opiniones podrían variar con el tiempo una vez la aplicación se encuentre “más rodada”.

Para el objeto de este apartado, se considera particularmente interesante la impresión que sobre la herramienta ProactivaNet comienza a formarse el equipo del Centro de Atención al Usuario (CAU), que es el punto único de contacto de Nivel 1, dentro del CEGES I3D, para todas las incidencias, peticiones y consultas de los usuarios.

Con anterioridad a la implantación de ProactivaNet, el Centro de Atención al Usuario (CAU) contaba con una herramienta de seguimiento de tickets, de desarrollo propio del MDEF, denominada SCANS, que contaba con un larguísimo historial de años de utilización en el MDEF y por lo tanto se puede considerar una plataforma consolidada. En consecuencia, la resistencia al cambio es un factor a tener en cuenta a la hora de analizar las opiniones de los usuarios de la nueva herramienta.

Para conocer la opinión que el personal del CAU encargado de la resolución de incidencias, se plantea la realización de una breve entrevista a la responsable del Centro de Atención al Usuario (CAU), que permita recopilar tanto las opiniones sobre distintos aspectos de la nueva herramienta, como una valoración del desempeño de la misma en relación con la herramienta SCANS utilizada hasta la fecha.

El Cuestionario Seguido para la realización de la entrevista se encuentra recogido en el Anexo I: CUESTIONARIO PARA ENTREVISTA CON RESPONSABLE DEL CENTRO DE ATENCIÓN AL USUARIO CAU SOBRE LA IMPLEMENTACIÓN DE LA HERRAMIENTA PROACTIVANET

En las tablas que se muestran a continuación (Tabla 3-14 y Tabla 3-15) se muestra el grado de coincidencia de opiniones entre los usuarios gestores de la herramienta ProactivaNet, que han reflejado sus pareceres en los foros de internet analizados, y las valoraciones que los usuarios gestores del CAU del CESTIC han podido formarse con la utilización de ProactivaNet hasta la fecha, y que han reflejado en sus respuestas en la entrevista. Como se puede observar, el grado de coincidencia de las opiniones para cada dimensión es muy alto entre usuarios internos y externos.

Dimensión valorada favorablemente por gestores de ProactivaNet externos al CESTIC	Opinión en encuesta a gestores del CAU del CESTIC
Plataforma / Portal intuitiva	Intuitiva para usuarios finales Compleja para usuarios gestores
El soporte facilitado por la empresa	En total acuerdo
Elevado grado de configurabilidad	En total acuerdo
Seguimiento de las prácticas de ITIL	En total acuerdo
Buen gestor de KPI	Todavía no implementados
Solidez del producto	Rendimiento más lento que aplicación legada

Tabla 3-14 Tabla de coincidencias de opiniones favorables entre usuarios gestores de la herramienta ProactivaNet externos al CESTIC y la opinión de usuarios gestores de la herramienta pertenecientes al CAU del CESTIC (Fuente: elaboración propia)

Dimensión valorada desfavorablemente por gestores de ProactivaNet externos al CESTIC	Opinión en encuesta a gestores del CAU del CESTIC
Generación de tickets poco intuitiva para los usuarios	Intuitiva para usuarios finales Compleja para usuarios gestores
Implementación del software compleja	En total acuerdo
Elevado número de requerimientos en Service Desk	En total acuerdo
Inferior grado de madurez comparado con herramientas similares	En acuerdo
Complejidad en la configuración de los agentes	En total acuerdo
Pobre Interfaz gráfica para la parte de usuario	En acuerdo

Tabla 3-15 Tabla de coincidencias de opiniones desfavorables entre usuarios gestores de la herramienta ProactivaNet externos al CESTIC y la opinión de usuarios gestores de la herramienta pertenecientes al CAU del CESTIC (Fuente: elaboración propia)

Del contenido de la entrevista, se desprende que, en general, la valoración que hacen los técnicos gestores del CAU del CESTIC, así como de sus responsables, es positiva, tanto en lo que respecta al desempeño hasta el momento de ProactivaNet, al que asignarían un valor de 8 en una escala del 1 al 10, como en lo que concierne a las expectativas futuras, cuando se produzca un despliegue completo de la herramienta para todos los usuarios del Ministerio. Con todo, los gestores hacen hincapié en la complejidad inicial que supone la familiarización con la herramienta, llegándola a definir como:

“Amplia, Completa, Espaciosa, pero con muchos recovecos y escondites.”²⁷

²⁷ Descripción proporcionada por el responsable del CAU ante la pregunta: ¿Cómo definirías ProactivaNet en una palabra o frase?

A continuación, se presentan diversos aspectos sobre ProactivaNet que han surgido durante la entrevista y que el autor considera que merecen ser destacados:

- El programa no permite generar un número de referencia del ticket hasta que no se han cumplimentado todos sus campos. La información que concierne a un ticket se encuentra repartida por diferentes pestañas en lugar de estar agrupada en una única ventana.
- La interfaz que ofrece la herramienta a los usuarios gestores es más “pobre” que para los usuarios finales que registran los tickets a través del Portal de ProactivaNet.
- Queda pendiente por definir cierto número de estructuras (más allá de las contempladas en el presente TFM), organizaciones, nombres de unidades y emplazamientos, definir localidades, contactos, tipologías, Base de Conocimiento...
- Las funcionalidades que ofrece ProactivaNet para asistir a los gestores del CAU en la resolución de incidencias, como son el acceso inmediato a la información sobre las características del equipo del usuario y a la documentación técnica vinculada con el servicio, o la pestaña investigación, que permite dejar trazabilidad sobre la gestión de la incidencia; tienen un alto potencial de ser muy útiles para servir a los gestores en la resolución de posibles incidencias.
- Los gestores consideran que serán precisos ajustes y personalizaciones futuras en la herramienta para que esta pueda presentar una buena escalabilidad de cara a absorber toda la demanda futura de peticiones del MDEF.

3.5.3 Comparativa entre herramientas:

En base a la información recopilada de diversas fuentes externas sobre diversas herramientas ITSM ampliamente conocidas por el público, junto con las opiniones y experiencia que el personal interno del CESTIC está experimentando con el uso de la herramienta (Por ejemplo, el responsable del CAU, que aporta su conocimiento y valoración sobre la herramienta ITSM de desarrollo corporativo utilizada hasta la fecha, o el propio autor del presente TFM que es conocedor de otras funcionalidades de la herramienta) que considera que se dispone de información suficiente como para poder elaborar la siguiente Tabla 3-16 comparativa entre herramientas ITSM:

La valoración de la dimensión se relajará mediante una gradación: Baja – Media – Alta – Muy Alta

Dimensión de la herramienta valorada	Proactiva	SCANS	Jira Service Manager	BMC Remedy ITSM	ServiceNow
Gestión de Incidentes y Problemas	Alta	Alta	Alta	Muy Alta	Muy Alta
Gestión de cambios	Alta	Baja	Media	Alta	Alta
Gestión de Solicitudes de Servicio	Media	Baja	Media	Alta	Alta
Opciones de automatización	Media	Baja	Media	Muy Alta	Muy Alta
Experiencia de Usuario	Alta	Alta	Alta	Media	Muy Alta
Integración y Compatibilidad	Muy Alta	Baja	Alta	Muy Alta	Muy Alta
Rendimiento y Escalabilidad	Alta	Baja	Media	Muy Alta	Muy Alta
Coste Total de Propiedad (TCO) ²⁸	Media	Sin datos	Media	Alta	Baja
Soporte de la empresa	Muy Alta	No aplica	Media	Alta	Muy Alta
Seguridad	Muy Alta	Alta	Alta	Muy Alta	Muy Alta
Informes y análisis	Muy Alta	Baja	Media	Muy Alta	Muy Alta

Tabla 3-16 Tabla comparativa entre herramientas ITSM (Fuente: (18), (19), (14)y elaboración propia)

Conclusión:

Aunque ProactivaNet puede no ser tan avanzada como otras soluciones de mercado en áreas como automatización (donde ServiceNow o BMC Remedy ITSM poseen grandes capacidades de IA), o rendimiento y escalabilidad (ya que para implementaciones extraordinariamente grandes, la escalabilidad de ProactivaNet podría ser limitada en comparación con herramientas como BMC Remedy ITSM o ServiceNow), el autor considera que para las funcionalidades requeridas para el MDEF, sí que podría afirmarse que ProactivaNet es una de las mejores soluciones del mercado para el propósito y funciones que se requieren.

Así mismo, ProactivaNet obtiene excelentes puntuaciones en áreas que el MDEF puede considerar como más prioritarias, como son:

- Soporte: ProactivaNet ofrece un soporte excelente, con un enfoque en la atención al cliente y adaptado a las necesidades locales.
- Coste Total de Propiedad: ProactivaNet suele ser más accesible en términos de costes iniciales y de mantenimiento en comparación con soluciones como ServiceNow.

²⁸ La valoración de Coste Total de la Propiedad asigna un valor Muy Alto a herramientas competitivas en precio, y un valor Bajo a herramientas con un coste mayor.

- Seguridad: La herramienta está diseñada con altos estándares de seguridad, especialmente para entornos sensibles como instituciones gubernamentales.
- Generación de informes y análisis: ProactivaNet incluye potentes capacidades de generación de informes y análisis.

Justificación de las valoraciones en la tabla comparativa para la herramienta ProactivaNet:

Para las dimensiones: Gestión de cambios, Gestión de Solicitudes de Servicio; se asignado una valoración conservadora, en base a las opiniones expresadas por el personal del CAU, así como otras valoraciones presentadas en los foros por los usuarios.

Para la dimensión: “Gestión de Incidentes y Problemas” se asigna una clasificación Alta, a pesar de las opiniones expresadas por el personal del CAU (cuya incorporación a uso de la herramienta es reciente) ya que ProactivaNet está certificada en ITIL 4, así como en las normas ISO 9001, ISO 20000, ISO 27001 e ISO 27017, lo que le garantiza una posición destacada en la gestión de incidentes y problemas.

Las dimensiones “Opciones de automatización” e “Integración y Compatibilidad” se valoran como Muy Altas. Esto es así porque el autor ha podido comprobar que la plataforma ProactivaNet ha aportado soluciones a necesidades no contempladas inicialmente para la herramienta. Por ejemplo, durante el periodo de redacción de este TFM, ProactivaNet ha aportado un desarrollo propio de un Script que ha permitido la distribución de software con ficheros .exe y .msi de forma automática, así como la copia de unas librerías. Estas funciones las ha realizado la herramienta de manera satisfactoria. Esta necesidad surgió con posterioridad a la adquisición de Proactiva, y se determinó que debía ser esta herramienta la que realizara la distribución; demostrando la herramienta una gran versatilidad y capacidades de automatización.

La dimensión “Informes y Análisis” también se puntúa con la nota más alta, ya que ProactivaNet ha demostrado una gran capacidad para generar informes en los que integra información procedente de diversas fuentes, y es capaz de generar indicadores sintéticos complejos, como, por ejemplo: Mostrar cuantos PCs o Servidores dispone el MDEF clasificados por modelo, familia de procesador o versión del sistema operativo, así como el estado de actualización de los equipos. Se muestran ejemplos a continuación en la Figura 3-5:

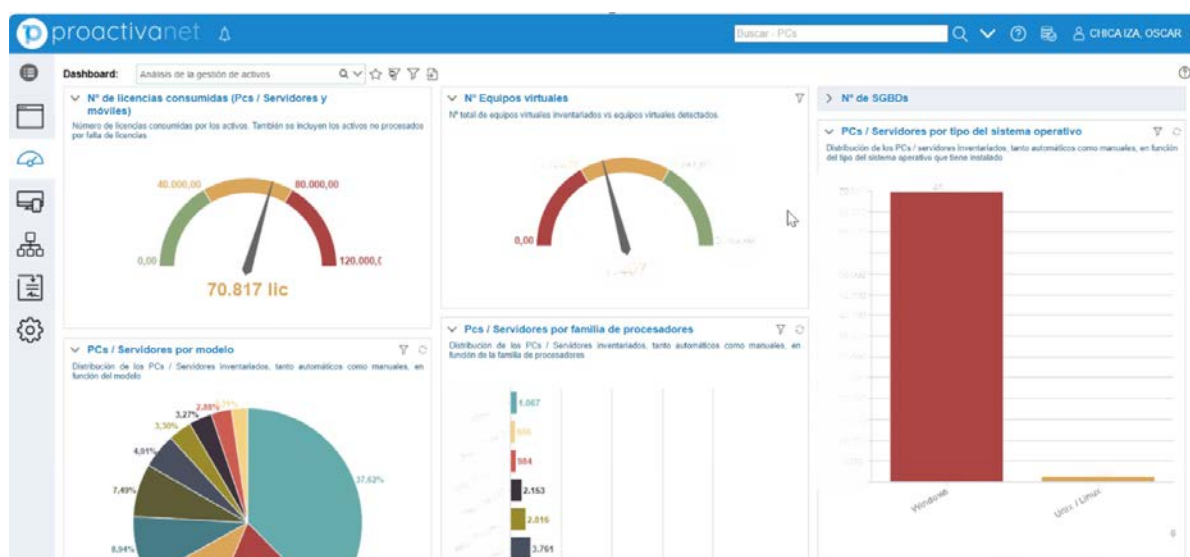


Figura 3-5 Ejemplo de Panel informativo generado por ProactivaNet con diversa información sobre servidores y PCs. Nótese que alguna información ha sido eliminada por motivos de seguridad. (Fuente ProactivaNet)

4 RESULTADOS

La apuesta del MDEF por el desarrollo de un modelo de gestión única de servicios CIS/TIC en el MDEF, sustentado en el marco COBIT y en el despliegue de la herramienta ITSM ProactivaNet, está comenzando a obtener resultados en diversas áreas clave, a pesar de lo reciente del inicio de su despliegue. En particular, se destaca la estandarización de procesos y la mejora de la gestión TIC, en áreas en las que anteriormente no existían desarrollos previos, como un catálogo unificado de servicios, procesos estandarizados inspirados por un marco ITSM, la implantación de una herramienta integral de gestión de servicios, la creación de una jerarquía para la gestión de servicios, o la definición de métricas para evaluar la calidad en la prestación de servicio

Uno de los principales logros es la consolidación de un catálogo de servicios unificado, que facilita la gestión centralizada y la alineación de los servicios con las necesidades estratégicas del Ministerio. Este catálogo de servicios se constituye como la clave de bóveda para el resto de actuaciones posteriores.

Se presentan los resultados que, a juicio del autor, se han logrado en las diferentes áreas abordadas en el desarrollo de este TFM:

Marco normativo de Gestión:

El MDEF es además pionero, dentro de la Administración Pública Española, en el desarrollo de un modelo para el gobierno y la gestión de servicios estas características, con inspiración profunda inspiración en el marco COBIT.

Si bien es cierto que otras Administraciones Públicas Españolas han dado pasos en su transformación digital para la mejora de sus servicios TI, por ejemplo con la adopción de herramientas ITSM para gestión de servicios TI, que como se ha mencionado anteriormente, están utilizando la Dirección General de Tráfico (con Jira) o el Ministerio de Hacienda y Administraciones Públicas (con BMC Remedy ITSM); ninguna otra Administración Pública ha aprobado hasta la fecha un marco normativo tan extenso relativo a la creación de un modelo de gestión de servicios, y ello a pesar de que el Plan de Transformación Digital de la Administración General del Estado (PTD-AGE) 2015-2020 establece la obligación de que los ministerios y organismos de la Administración General del Estado elaboren sus propios planes de transformación digital. Esto es algo que se puede comprobar fácilmente consultado las publicaciones normativas de otros ministerios en esta área.

Por ejemplo, el Ministerio de Industria ha emprendido acciones para el impulso de la transformación digital del tejido productivo español, como es la estrategia Industria Conectada 4.0 lanzada en el año 2015, y que comprende un Plan de Acción para acelerar la transformación digital de la industria española a través del lanzamiento de líneas de ayudas y del estímulo de las competencias digitales; y que incluye también un modelo de gobernanza para la industria conectada 4.0 dirigido a asegurar el éxito de esta iniciativa, pero que en ningún caso representa un modelo transversal para el gobierno de todas las unidades del Ministerio vinculadas al sector de las tecnologías TI o sus servicios, como sí lo supone el modelo propuesto para el Ministerio de Defensa. (20)

En conclusión, a lo anterior, el MDEF no ha podido contar con el respaldo de la experiencia o lecciones aprendidas de otras Administraciones para poder navegar con apoyos en esta travesía hacia la transformación digital, lo que pone de manifiesto el gran mérito de esta empresa llevada a cabo por el personal del MDEF, y más concretamente del CESTIC.

En cuanto a la adaptabilidad del modelo de gestión única de servicios al marco COBIT, un análisis de la normativa elaborada para este marco muestra un elevado grado de adaptación al mismo, aunque queda margen para optimizar ciertas prácticas de gestión, como la monitorización de activos y la gestión de cambios.

La normativa analizada en el desarrollo de este trabajo, ha reflejado una buena adaptación a las recomendaciones establecidas en el marco COBIT para los objetivos y prácticas de gestión que se han

tenido capacidad de abordar en este trabajo. Por ello, aunque puede haber áreas de mejora, si considera que el desarrollo de la normativa es satisfactorio y en línea con los principios sobre gestión de servicios TI más comúnmente aceptados.

Herramienta ProactivaNET

La implementación de la herramienta ITSM ProactivaNet ha demostrado ofrecer un gran número de posibilidades para la gestión eficiente de servicios, poniendo a disposición de los responsables de la gestión del sistema de incidencias un gran número de herramientas que sin duda contribuirán a la mejora de la eficiencia en la gestión de servicios TI por el CESTIC; a pesar de los problemas iniciales aparecidos, derivados de la curva de aprendizaje, ya que evidentemente la destreza del personal encargado de gestión de incidencias con el manejo de la nueva herramienta es inferior, en las primeras etapas, a la que ya tenía con el manejo de una herramienta ya afianzada y amplio historial de uso.

Por su parte, las recomendaciones presentadas en este trabajo relativas a la implantación de la herramienta ProactivaNet y la definición de una jerarquía que permita la gestión de servicios y el escalado de las incidencias, han sido tenidas en cuenta por el personal responsable de la implantación de este servicio en el CESTIC, por lo que el autor se puede considerar satisfecho de que el estudio llevado a cabo en este TFM ha tenido utilidad práctica real y está comenzando a generar resultados visibles para la organización. Si bien el autor es consciente que ha sido imposible abordar todos los aspectos vinculados a la implementación de la herramienta en un único TFM, dada la amplitud y complejidad de este proceso. Con todo, las áreas más decisivas para el inicio de la implementación sí han podido ser abordadas.

Comparativa entre herramientas ITSM

La realización de un análisis comparativo con otras herramientas ITSM del mercado, incluyendo SCANS, actualmente utilizada en el MDEF, y otras soluciones reconocidas, ha puesto de manifiesto que ProactivaNet ofrece una ventaja competitiva en términos de coste-beneficio, aunque se identificaron áreas de mejora en la integración de sistemas analíticos avanzados.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Como conclusión, se puede afirmar que la implementación de un modelo único de gestión de servicios CIS/TIC basado en el marco COBIT y apoyado en herramientas ITSM como ProactivaNet, se constituye como una estrategia efectiva para mejorar la gobernanza TIC en cualquier organización, y particularmente en el Ministerio de Defensa.

Aunque todavía es pronto para una evaluación completa de la eficiencia que se logrará con esta estrategia, ya que el alcance para los usuarios finales todavía es muy limitado en el momento de redacción de estas líneas; se puede afirmar a fecha de diciembre de 2024 que la creación de este marco ha aportado claridad procedimental y calidad en términos de información, a los servicios CIS/TIC ofrecidos por el MDEF. Los responsables funcionales de implementación de nuevas herramientas y servicios TI ya perciben una menor confusión a la hora de definir la documentación y las arquitecturas necesarias para el despliegue de nuevos servicios, ya que, gracias a la nueva normativa, estas directrices son uniformes para todos, sin sujeción a la interpretación ni dar lugar a la confusión debido a información no comunicada correctamente a los promotores de los servicios.

Herramientas como el Catálogo de Servicios ofrecen información que ahora se encuentra disponible para todo el personal del MDEF, y esta información se ofrece de forma democrática e ininterrumpida para todos los usuarios, sin excepciones ni nichos de información.

Particularizando las conclusiones en relación con los objetivos del TFM, el autor considera que estos han sido cumplidos, ya que se han realizado aportaciones que abarcan todo el proceso de implementación de un modelo para la transformación digital. Estas contribuciones han alcanzado desde los aspectos normativos, hasta áreas más eminentemente prácticas como la toma de decisiones clave para poder comenzar la implantación de una herramienta ITSM, como son la definición de una estructura de funciones y roles en la herramienta o un esquema de implantación.

A modo de cierre, mencionar que la comparativa entre herramientas ITSM ha arrojado un resultado positivo al comprobarse que ProactivaNet ha sido una buena solución de mercado para las necesidades del MDEF. Esto permite reforzar la confianza en el proceso de definición de un modelo de gestión única de servicios, y alienta a seguir trabajando por mejorar y completar este esquema en un futuro.

5.2 Líneas futuras

Se autor expone una serie de líneas actuación futuras que permitirían completar el estudio iniciado en cada una de las áreas abordadas en el desarrollo de este TFM:

Marco normativo de Gestión:

El presente TFM ha tenido como uno de sus objetivos realizar un análisis de la implantación del modelo de gestión única de servicios CIS/TIC en el Ministerio, a través del análisis de la normativa aprobada por el CESTIC, desde el punto de vista de las recomendaciones que establece el marco facilitado por COBIT para alguno de los objetivos y prácticas de gestión que mostraban una mayor vinculación con el objeto de la misma.

Por ejemplo, la “Instrucción Técnica del CESTIC relativa a la Gestión del Catálogo de Servicios CIS/TIC en la I3D”, se analiza desde las disposiciones establecidas por el marco COBIT para el Objetivo de Gestión APO05 - Gestionar el portafolio, así como sus prácticas de gestión asociadas.

El objetivo último sería realizar un análisis de como el modelo de gestión propuesto, desarrolla cada una de las capacidades de gestión del marco COBIT, así como de sus objetivos y prácticas de gestión asociadas. Pero como en la práctica, este análisis de todos estos procesos excede el contenido razonable para un Trabajo de Fin de Máster, la exposición se centró en los procesos asociados a los objetivos de

gobierno y gestión relevantes más para la gobernanza TIC del MDEF, pero podría en un futuro extenderse el análisis al resto de objetivos de gestión asociados al contenido de cada norma.

Acuerdos de provisión de Servicios:

Tomando como base el primer acuerdo definido para la provisión de los servicios suministrados por el CESTIC para la I3D, el “Acuerdo de Provisión de Servicios 01/24 del CESTIC Sistema de Mando y Control Nacional (SC2N) para la Conducción de Operaciones de Presencia, Vigilancia y Disuasión (OPVD) hasta Alcanzar la FOC”; deberá realizarse un extenso de trabajo de definición de los niveles calidad y entrega para cada uno de los servicios incluidos en el nuevo Catálogo de Servicios. Estos niveles de disponibilidad deberán ser definidos teniendo en consideración la opinión de todas las partes implicadas: El usuario del servicio (o ámbitos), el responsable funcional del servicio, el proveedor del Servicio (DIVOPER para los servicios proporcionados por el CESTIC) y el Centro de Atención al Usuario (CAU) del CESTIC.

Así mismo, estos Acuerdos de Nivel de Servicio se pueden mejorar siguiendo las recomendaciones formuladas para los mismos en el desarrollo del TFM, para lograr un mejor alineamiento de los mismos con el marco propuesto por COBIT 2019 (16).

Monitorización de la infraestructura IT:

El presente TFM establece el punto de partida para implantar una arquitectura que permita lograr una correcta monitorización de los servicios prestados por el CESTIC.

La investigación realizada ha permitido determinar que la base de datos vectorial proporcionada por el motor de búsqueda y analítica de RESTful, Elasticsearch, se constituye como el mejor repositorio unificado de logs (registros), métricas y trazas, al servicio del MDEF; antes de que pueda ser completado el registro único de datos oficial del MDEF que proporcionará la herramienta IBM Cognos Analytics. Por su parte, el trabajo de investigación también ha determinado que Grafana representa la mejor herramienta para la presentación de informes de observabilidad para la toma de decisiones para los responsables de la gestión de servicios, y que deberá ser alimentada con la información almacenada en la base de datos de Elasticsearch.

En base a lo anterior, para lograr el objetivo de establecimiento de esta infraestructura, los desarrolladores deberán seguir los siguientes pasos para su culminación:

- 1) Definir exactamente de qué forma se pueden traspasar los registros de logs propios de cada una de las herramientas contempladas en la monitorización (Nagios XI, Splunk, Data Center Expert, Schneider BMS...) al repositorio Elasticsearch. Determinar si es necesario el uso de Servidor syslog, o la necesidad de desarrollo de APIs específicas para un software, si son válidas las APIs proporcionadas por los fabricantes...

- 2) Una vez lograda la comunicación, deberían definirse reglas de lógica de negocio para estos registros, en función de la importancia que presente cada activo para el funcionamiento de los servicios. Un ejemplo vinculado la monitorización de la infraestructura: Si existen varias condensadoras que enfrían una determinada zona de un centro de datos, la avería en una de ellas podría tener una importancia baja, ya que otras condensadoras podrían asumir su carga de enfriamiento. Pero si la avería se produce en una zona en la que solamente se recibe aire frío de una condensadora, un error de la misma debería saltar una alarma crítica de funcionamiento.

- 3) Una vez definidos los dos anteriores, se podrían delimitar los tipos de registros que deberá reportar cada software, para que solo se reporten los logs que estén asociados con eventos críticos, de modo que no se saturen los registros con información que sea irrelevante reportar.

4) Construcción del panel de observabilidad en base a las recomendaciones establecidas en el subapartado 3.3.2.1 *Variables críticas a monitorizar en el Cuadro de Mando*; relativas a la construcción de indicadores (relojes o speedómetros) y los niveles de criticidad dentro de los mismos, en función de la variable a analizar.

5) Con el paso del tiempo deberá realizarse una revisión del desempeño de la herramienta y formular propuestas de mejora, en línea con el planteamiento presentado por el ciclo de Deming para la mejora continua de los procesos.

Implantación de la herramienta ProactivaNET

Todavía queda mucho por hacer en el proceso de implantación de la herramienta ProactivaNet.

En un primer paso, una vez implementadas las propuestas de este TFM, deberán redactarse Instrucciones Operativas (IOPs) para cada uno de los servicios incluidos en el Catálogo de Servicios. Una Instrucción Operativa (IOP) es un documento que detalla los pasos específicos a seguir para realizar una tarea o proceso dentro de un entorno operativo. Su objetivo principal es estandarizar y formalizar la ejecución de actividades, que sirvan de ayuda al personal del CAU para guiar la gestión de las incidencias que los usuarios vayan abriendo en ProactivaNet, lo que permitirá alcanzar altos niveles de calidad en la gestión de servicios, así como el cumplimiento de los Acuerdos de Nivel de Servicio definidos.

La herramienta ProactivaNet ofrece muchas opciones para asistir al personal del CAU en la resolución de incidencias. Por ejemplo, cuando un usuario abre un ticket, ProactivaNet asocia toda la información sobre el equipo del usuario al ticket, de modo que esta información ya es visible directamente al personal del CAU responsable de resolución de la incidencia, sin necesidad de consultarla al usuario del servicio. Así mismo toda la información relativa al usuario también está disponible para el personal del CAU. Esto ahorra tiempo en consultas innecesarias y permite incrementar la eficiencia en la provisión de servicios. Ejemplo de estas opciones se muestra en la Figura 5-1.

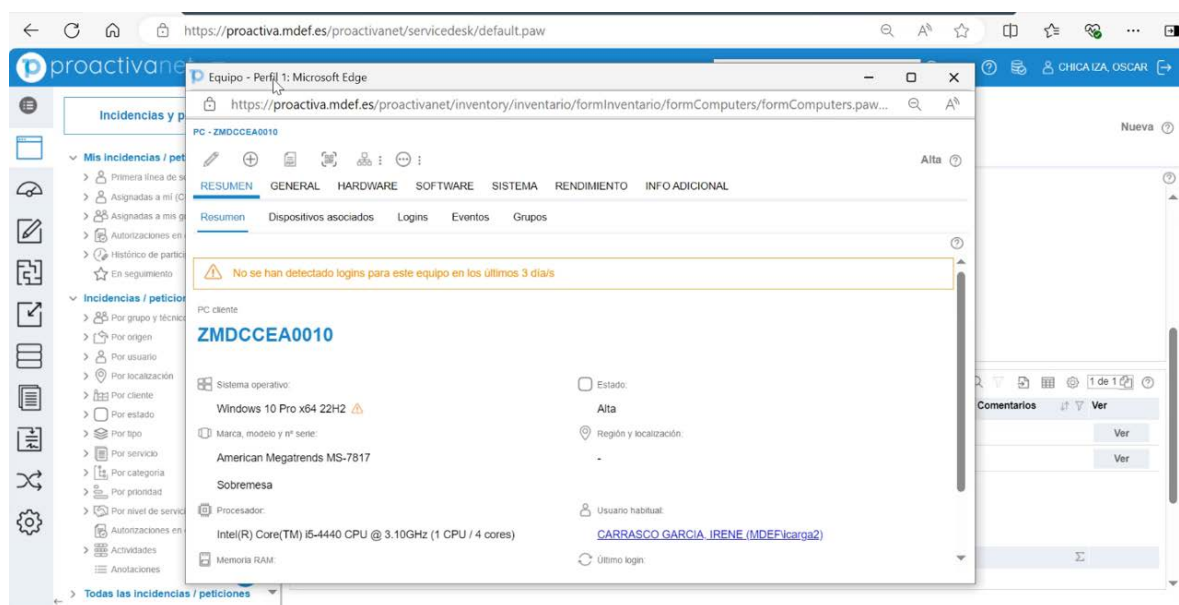


Figura 5-1 Ejemplo de información presentada por la interfaz de ProactivaNet a los responsables de la resolución de incidencias del CAU (Fuente: ProactivaNet y elaboración propia)

En conclusión, son líneas de trabajo futuro, la redacción de estas futuras IOPs y la formulación de recomendaciones para que también se encuentren alineadas con ITIL, COBIT u otros marcos de referencia. Así mismo, una posible área de estudio a futuro es determinar como todas estas capacidades

de la herramienta ITSM podrían utilizarse para lograr una gestión de servicios TI más eficiente en el MDEF.

Otra actuación a desarrollar de forma paralela a la anterior es el despliegue de agentes auditores de la herramienta en los activos TI del MDEF, que permitirán la definición de la Base de datos de Gestión de la Configuración (CMDB) utilizada para administración y el seguimiento de todos los activos de TI (hardware, software, redes, etc.) y de sus configuraciones; y que es una de las funciones esenciales de cualquier herramienta ITSM, para el logro de una gestión eficiente de activos.

Comparativa entre herramientas ITSM:

Esta comparativa se podría completar con las siguientes propuestas:

- Incluir un mayor número de soluciones en mercado en la comparativa, no solamente las más populares, para el estudio sea lo más transversal y completo posible.
- Incluir un estudio económico del coste de despliegue de las distintas alternativas, lo que permitiría incluir en el análisis una dimensión de costes, además de las funcionales tenidas en cuenta en este trabajo.
- Realizar una propuesta de implementación de otra herramienta ITSM de software libre y realizar un piloto de la misma, para poder comparar su operativa con ProactivaNet en condiciones de funcionamiento comparables. Esto permitiría confrontar su facilidad de utilización para el usuario, su rendimiento, escalabilidad...

6 BIBLIOGRAFÍA

1. **Making Science S.A.** *Libro Blanco de la Digitalización. Una actualización del documento Una Iniciativa para la Transición Digital*. [Internet]. 2024. [consultado 2024 octubre 11] : s.n.
2. **Ministerio de Asuntos Económicos y Transformación Digital.** *Libro Blanco España Digital 2026*. [Internet] 2024 [consultado 2024 octubre 11] : disponible en: https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf.
3. **Piñeiro Iglesias, David. Murillo Martínez, Antonio Rafael. Jiménez Ciudad, Francisco Javier.** *Trabajo COM8 Infraestructura Integral de Información para la Defensa 2023*. 2023. [consultado 2024 octubre 20].
4. **Ministerio de Defensa.** *Politica de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa*. Madrid : Subdirección General de Publicaciones y Patrimonio Cultural, 2015. [consultado 2024 noviembre 02].
5. **Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC).** *Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC)*. 2016. [consultado 2024 noviembre 02] : Subdirección General de Publicaciones y Patrimonio Cultural. Ministerio de Defensa. Secretaría General Técnica. Disponible en: <https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministeri>.
6. —. *Plan de acción del Ministerio de Defensa para la transformación digital*. 2020. [consultado 2024 octubre 20] : Subdirección General de Publicaciones y Patrimonio Cultural. Ministerio de Defensa. Secretaría General Técnica. Disponible en: <https://publicaciones.defensa.gob.es/plan-de-accion-del-ministerio-de-defensa-para-la-transformacion-digital-libro-pdf.html>.
7. —. *Arquitectura de Referencia (AR) única para la Gestión de Sistemas y Tecnologías de Información y Comunicaciones (AR GES CIS/TIC)*. 2023. [consultado 2024 octubre 15] : Subdirección General de Publicaciones y Patrimonio Cultural. Ministerio de Defensa. Secretaría General Técnica.
8. —. *Visión 01/22 del Cestic: Concepto del Centro de Gestión de Servicios CIS/TIC de la I3D (CEGES I3D)*”. Madrid. 2021 [consultado 2024 diciembre 02] : s.n.
9. **Tarrío, Miguel Ángel Ares.** *Apuntes Asignatura COM3 Master Universitario en Dirección TIC para la Defensa*. s.l. : Universidad de Vigo. [consultado 2024 diciembre 02], 2024.
10. **Dotcom-Monitor.** dotcom-monitor. [En línea] 2024. [Citado el: 20 de 12 de 2024.] <https://www.dotcom-monitor.com/blog/es/las-15-mejores-herramientas-de-monitoreo-de-infraestructura/>.
11. **Baud, Jean-Luc.** *Preparación para la certificación ITIL Foundation V3*. Barcelona : 2011. ENI Ediciones [consultado 2024 diciembre 02].
12. **Red Hat, Inc.** www.redhat.com. [En línea] 13 de 5 de 2024. [Citado el: 28 de 12 de 2024.] <https://www.redhat.com/es/topics/data-services/what-is-grafana>.
13. **Martínez, Jerson.** Que es Grafana y primeros pasos. *openwebinars.net*. [En línea] 2024. [Citado el: 28 de 12 de 2024.] <https://openwebinars.net/blog/que-es-grafana-y-primeros-pasos/>.
14. **ServiceNow, Inc.** servicenow . [En línea] 2024. [Citado el: 20 de 12 de 2024.] <https://www.servicenow.com/>.
15. **ISACA.** *Marco de referencia COBIT® 2019: Introducción y metodología*. ISACA. Schaumburg, IL. 2018 : [consultado 2024 septiembre 02].
16. —. *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*. Schaumburg, IL. 2018 : [consultado 2024 septiembre 02].

17. **bmcsoftware.** [En línea] BMC Software, Inc., 2024. [Citado el: 10 de 12 de 2024.] <https://www.bmcsoftware.es/it-solutions>.
18. **Gartner.** [En línea] Gartner, Inc., 2024. [Citado el: 18 de 11 de 2024.] https://www.gartner.com/reviews/market/it-service-management-platforms/vendor/proactivanet/product/proactivanet_.
19. **Capterra.** [En línea] Capterra, Inc., 2024. [Citado el: 6 de 12 de 2024.] <https://www.capterra.es/software/1010807/proactivanet>.
20. **Ministerio de Industria.** Iniciativa Industria Conectada 4.0. [En línea] 2015. [Citado el: 13 de 12 de 2024.] <https://www.industriaconectada40.gob.es/SiteCollectionDocuments/informe-industria-conectada40.pdf>.
21. **tobeit.es.** Los pilares de la observabilidad: logs, métricas y trazas. [En línea] 2024. [Citado el: 28 de 12 de 2024.] <https://tobeit.es/los-pilares-de-la-observabilidad-logs-metricas-y-trazas/>.

ANEXO I: CUESTIONARIO PARA ENTREVISTA CON RESPONSABLE DEL CENTRO DE ATENCIÓN AL USUARIO CAU SOBRE LA IMPLEMENTACIÓN DE LA HERRAMIENTA PROACTIVANET

El objeto de esta entrevista es recopilar opiniones sobre la herramienta ProactivaNet para identificar fortalezas y áreas de mejora en su implementación, así como para compararla con la herramienta SCANS utilizada anteriormente. Se pretenden evaluar diferentes aspectos clave de ProactivaNet relacionados con la usabilidad, funcionalidad, impacto en el trabajo diario y percepción general.

Se plantean a continuación una serie de cuestiones agrupadas en diferentes secciones:

EXPERIENCIA GENERAL

- 1) ¿Cómo describirías tu experiencia general utilizando ProactivaNet hasta la fecha? (Ej.: Intuitiva, compleja, eficiente, limitada)
- 2) ¿Hay funcionalidades de ProactivaNet que consideres complicadas? ¿Por el contrario hay otras funciones que te parezcan más asequibles?
- 3) ¿Cómo maneja la herramienta las solicitudes de servicios estándar (como restablecer contraseñas, instalar software)?
- 4) En una escala del 1 al 10, ¿cómo valorarías el desempeño de ProactivaNet hasta ahora?
- 5) Si tuvieras que definir ProactivaNet en una palabra o frase, ¿cuál sería?

FUNCIONALIDAD

- 6) En lo que respecta a la Interfaz de Usuario (UI) ¿Se puede afirmar que esta es intuitiva, fácil de usar, personalizable y accesible para usuarios no técnicos?
- 7) Gestión de Incidentes: ¿Cómo valoras el manejo de la herramienta en los que respecta a la identificación, seguimiento y resolución de incidentes?
- 8) ¿Cómo valoras la interfaz que ofrece la herramienta a los técnicos del CAU?
- 9) La herramienta ofrece información inmediata sobre las características del equipo del usuario, además de permitir un acceso inmediato a la documentación técnica vinculada con este servicio. ¿Es esto eficaz? ¿Representa una ayuda para los técnicos respecto al programa anterior?
- 10) La pestaña investigación permite dejar trazabilidad sobre la gestión de la incidencia. Si bien parece que la información debe ser cumplimentada por el propio técnico. ¿Es esto útil?

RENDIMIENTO

- 11) ¿Consideras que la herramienta responde rápido a solicitudes de los usuarios y gestiona bien grandes volúmenes de datos?
- 12) ¿Consideras que Proactiva será capaz de adaptarse al crecimiento de la organización y las futuras necesidades, en definitiva, que presenta una buena escalabilidad?

INFORMES Y ANÁLISIS

- 13) ¿Consideras que la herramienta tiene buena capacidad de generación de informes y análisis?
- 14) ¿La herramienta permite definir y hacer seguimiento de KPIs para evaluar el desempeño de los servicios? ¿Consideras aceptable el diseño de este módulo? ¿Es personalizable?

COMPARATIVA CON OPINIONES DE OTROS USUARIOS

15) Otros usuarios de ProactivaNet han valorado como puntos fuertes de la herramienta los siguientes ¿Estás de acuerdo?

- Portal intuitivo
- El soporte brindado por la herramienta.
- Elevado grado de configurabilidad / Capacidad de personalización

16) Otros usuarios de ProactivaNet han destacado los siguientes puntos débiles de la herramienta. ¿Estás de acuerdo con ello?

- Generación de tickets poco intuitiva para los usuarios
- Implementación del software compleja
- Elevado número de requerimientos en Service Desk
- Inferior grado de madurez comparado con herramientas similares
- pobre Interfaz gráfica para la parte de usuario

COMPARATIVA CON SCANS

17) En términos de rapidez para gestionar incidencias, ¿cómo calificarías a ProactivaNet frente a SCANS? (Ej.: Más rápida, igual, más lenta)

18) ¿Qué aspectos de la herramienta te parecen más útiles o efectivos en comparación con SCANS?

19) ¿Consideras que la transición de SCANS a ProactivaNet está siendo fácil o difícil? ¿Por qué?

20) ¿Consideras que ProactivaNet ha incorporado todas las funcionalidades esenciales que usabas en SCANS? Si no, ¿cuáles echas de menos?

21) ¿Piensas que, en un futuro, el cambio a ProactivaNet facilitará o dificultará tu trabajo diario? ¿Por qué?