Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Metodología para la Gestión de Servicios en un Centro de Explotación CIS de la Armada

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Manuel Rendón Fernández

DIRECTORES: Miguel Angel Ares Tarrío

Jose María Núñez Ortuño

CURSO ACADÉMICO: 2021-2022

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Metodología para la Gestión de Servicios en un Centro de Explotación CIS de la Armada

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de Telecomunicación

Universidad de Vigo

RESUMEN

El presente TFM propone una metodología genérica, flexible y eficiente que puede seguir cualquier Centro de Explotación CIS de la Armada para proveer los servicios CIS/TIC de su responsabilidad y competencia a las unidades de su ámbito geográfico, planteada a partir de estándares y metodologías ampliamente conocidos y probados, como son ITIL e ISO.

Se expondrá, apoyado en documentación que desarrolla la Gestión de Servicios en Defensa, el contexto del tema propuesto y la necesidad de emprender este TFM, detallando los objetivos extraídos del estudio previo de la situación actual, de manera clara y realista, y que en definitiva buscará su aplicación en un Centro de Explotación CIS (CECIS) como último escalón en la Gestión de Servicios CIS/TIC en la Armada, mostrando desde el inicio la situación a día de hoy con las diferentes instrucciones permanentes y no permanentes establecidas en este campo.

En su desarrollo se dará a conocer la estructura de la Armada y la actual gestión del Conocimiento y la Información en Defensa, algunas de las tecnologías, normativas e iniciativas relevantes en la gestión de servicios, procedimientos y modelos actualmente en práctica en entidades nacionales e internacionales, así como aplicaciones informáticas específicamente diseñadas para la gestión de los servicios con el fin de aportar valor al cliente con unos resultados de calidad. Se comentarán y analizarán trabajos previos realizados en el ámbito de la Gestión de Servicios, importantes para el desarrollo del TFM, para finalizar con una propuesta alcanzable de metodología a aplicar siguiendo una estructura de Service Level Agreement (SLA) apoyada en una consistente y completa herramienta de atención y gestión de incidencias.

PALABRAS CLAVE

Metodología, Gestión, Servicio, Explotación, ITIL

AGRADECIMIENTOS

Quisiera aprovechar la oportunidad que ofrece este apartado para agradecer su colaboración a las diferentes personas que me han ayudado en el desarrollo de este TFM de una u otra manera.

A mi tutor, Miguel Angel, por su total disponibilidad desde el comienzo, orientándome en la estructura a seguir en el estudio y no malgastar esfuerzo en direcciones fuera del alcance del trabajo, así como facilitándome material e ideas a emplear en la investigación.

A mis compañeros de máster, y de unidades como el CESTIC, la JECIS y de CECISDIZ, por haberme aportado grandes cantidades de documentación, ejemplos y sugerencias para afrontar esta complicada tarea.

Y finalmente a mi familia, esposa e hijas, por su infinita paciencia y comprensión; pidiéndoles disculpas por las incontables horas en las que no estuve disponible para ellas por estar inmerso en este proyecto.

Contenido

ÍNDICE DE FIGURAS

Índice de Tablas

1 INTRODUCCIÓN Y OBJETIVOS

Para comprender la necesidad de elaborar este trabajo es fundamental exponer previamente una serie de conceptos y normas preestablecidas que nos permitirán conocer el marco regulador en el que se encuentran los Centros de Explotación CIS (CECIS) de la Armada y cómo ejercen actualmente las funciones de su competencia, y así poder proponer una metodología acorde a referencias y estándares de buenas prácticas (ITIL e ISO).

Del estudio previo de la normativa reguladora, y del conocimiento del estado del arte y dinámica de trabajo actual de nuestros CECIS en el Armada, realizaremos a continuación un esfuerzo por definir una Metodología real y creíble basada en una mejora de lo que ya existe, y orientada hacia tres claros objetivos o pilares: proponer una estructura organizativa interna en los Centros que aporte mayor valor a los clientes, en definitiva los usuarios finales de redes y sistemas, basada en la creación de una Célula de Mantenimiento preventivo que siga las pautas que ITIL e ISO marcan a nivel internacional, empleando una herramienta de trabajo y gestión de servicios consistente y bien extendida en todas nuestras unidades, y por último documentando toda relación y nivel de servicios a proveer a las Unidades de la Armada en Acuerdos (*Service Level Agreement* – SLA).

Como conclusión de esta investigación se valorará si los citados objetivos han sido alcanzados, o al menos son alcanzables con los medios a disposición a día de hoy, y se trazarán unas posibles líneas futuras que podrían mejorar al resultado con el tiempo.

1.1 Política CIS/TIC y Estrategia de la Información y Coordinación GIC (Gestión de la Información y del Conocimiento) del Ministerio de Defensa (MDEF)

En este primer apartado se analizan tres documentos que, de manera escalonada, definen la Estrategia del Ministerio de Defensa en Politica CIS/TIC, su Estrategia en materia de Información y por último la coordinación de la GIC, con el objetivo final de explotar el valor estratégico de la información.

1.1.1 Política CIS/TIC

La Política de los Sistemas y Tecnologías de la Información y Comunicaciones (CIS/TIC) de Ministerio de Defensa[1], así como su estructura de gobierno para su coordinación, control y seguimiento tiene por objeto final que la información sea, por su valor estratégico, un activo

[1] 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 Minsiterio de Defensa.

debidamente protegido, fiable y accesible para los usuarios en base a su autorización y necesidad de conocer y se desarrolla a través de un Plan Estratégico CIS/TIC (PECIS).

Para su consecución se estructura, entre otras, en las siguientes iniciativas:

- Obtención de una Infraestructura Integral de Información para la Defensa (I3D), gestionada por el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), que deberá contar al menos con un Centro de Procesos de datos (CPD) de respaldo que asegure la continuidad de los servicios.
- Disponer de un modelo de gobierno integral de los CIS/TIC que proporcione la máxima eficacia y eficiencia en su gestión y dirección, garantizando la explotación de los servicios del Sistema de Mando y Control Militar (SMCM).
- Maximizar la gestión del recurso humano relacionado con CIS/TIC, promoviendo y conservando el conocimiento CIS/TIC en el propio personal, cuya formación se contemplará en el PECIS.

Al objeto de facilitar a todos los miembros de la organización unos servicios adecuados para desarrollar sus funciones, cometidos y misiones es fundamental trabajar en la integración de servicios con una gestión centralizada para su entendimiento con las herramientas de la Administración General del Estado (AGE), así como con los sistemas de los organismos internacionales a los que pertenecemos, la OTAN y la UE, siguiendo políticas y estrategias similares.

El documento de referencia define los siguientes conceptos:

- La gestión del servicio como el conjunto de capacidades y procesos para dirigir y controlar las actividades de la provisión de servicios y los recursos para su diseño, transición y mejora.
- Gobernar los CIS/TIC supone evaluar y dirigir su empleo para dar soporte a la organización y su monitorización para lograr los planes y objetivos marcados.
- Los medios CIS permanentes que conforman la infraestructura del MDEF para la gestión y transmisión de la información al Departamento y FAS se establecen en instalaciones fijas, por periodos de operación prolongados y atendiendo áreas geográficas amplias.
- Orientación a servicios es un modelo basado en procesos que permite controlar de extremo a extremo un servicio y lo centra en el cliente, dejando en segundo plano las capas tecnológicas que intervienen en el servicio y valorando la utilidad para el usuario y adecuación a sus requisitos.

Entre otros, los principios de la Política CIS/TIC del Ministerio son:

- Orientación a servicios de la infraestructura, identificando la información como un recurso estratégico para la obtención y gestión de los recursos CIS.
- Centralización que permita disponer de una visión global y única de los CIS/TIC.
- Seguridad, alcanzando el adecuado equilibrio entre protección de la información, necesidad de conocer y responsabilidad de compartir.
- Disponibilidad de los CIS/TIC y eficiencia en su obtención y empleo.
- Interoperabilidad a través de la alineación con la AGE, OTAN y UE.

Igualmente, entiende que la prestación de servicios vendrá regulada por Acuerdos de Nivel de Servicio (en el ámbito OTAN *Service Level Agreement*, SLA) entre el CESTIC como proveedor y los

clientes, donde se incluirán los servicios facilitados y los niveles de calidad, disponibilidad, de asistencia y mantenimiento a proporcionar.

Los servicios se organizarán, siguiendo el modelo OTAN, en servicios de Red y Telecomunicaciones, de Plataforma Informática, Básicos de Usuario y de Función Específica; y estarán controlados por servicios de Gestión, Operación y Mantenimiento y de Seguridad de la Información.

Durante el ciclo de vida completo de los servicios se llevará a cabo la Gestión de Riesgos, así como en todo plan y proyecto que desarrolle la Política CIS/TIC se velará por la toma de decisiones más adecuada. Como parte de este seguimiento continuo se programarán auditorías de calidad y cumplimiento, y se adoptarán modelos y metodologías de referencia estandarizadas de buenas prácticas en la gestión de los servicios y en la obtención, operación y mantenimiento de los sistemas. A este respecto se darán a conocer en el apartado 2 los referentes ITIL e ISO.

El Gobierno de los CIS/TIC es llevado a cabo en el MDEF a través de tres diferentes órganos:

El Consejo de Gobierno CIS/TIC, responsable de la coordinación seguimiento y control de la Política CIS/TIC, del cual forma parte el Segundo Jefe del Estado Mayor de la Armada (Segundo AJEMA), y que aprueba el catálogo de servicios y sus actualizaciones. Entre las directrices generales de la Política CIS/TIC, se ordena desarrollar un catálogo de servicios que contemple aquellos que pertenecen a nuestro ámbito sectorial y los compartidos con la AGE, promoviendo el empleo de estándares abiertos en la medida de lo posible al objeto de favorecer la flexibilidad y la reducción de costes y plazos de entrega.

Comisión Ejecutiva CIS/TIC, de la que es vocal permanente el Jefe de la Jefatura de Servicios Generales, Asistencia Técnica y Sistemas de la Información y Telecomunicaciones del Armada (AJECIS), partícipe en las funciones de supervisión y control de los resultados de los indicadores de rendimiento (Key Performance Indicators –KPI) y sus métricas relativas a la explotación y prestación de los servicios del catálogo, así como de coordinación del desarrollo de procesos de gestión de cambio y de divulgación y concienciación relacionados con la implantación del PECIS.

Comités CIS/TIC, donde destaca para el fin de este trabajo el comité de Gestión y Operación de los CIS/TIC del Ministerio, y del que forma parte un representante de la Jefatura CIS de la Armada.

Finalmente se nombra al Director del CESTIC, que es Secretario del Consejo de Gobierno CIS/TIC, responsable de impulsar el desarrollo de la política CIS/TIC así como de coordinar la Gestión de la Información y del Conocimeinto (GIC) asumiendo las funciones de CIO (*Chief Information Officer*), impulsando la implantación de una estructura de GIC que aproveche al máximo los servicios TIC.

1.1.2 Estrategia de la Información y Conocimiento

La Estrategia de la Información del Ministerio[2] establece las bases para estructurar su gestión, con el objetivo de preparar a la Administración para manejar grandes volúmenes de información digital y ser capaz de analizarla para optimizar su aprovechamineto y la toma de decisiones, así como ofrecer nuevos servicios interdepartamentales. Esta estrategia es desarrollada a su vez por una Instrucción para la GIC.

Pretende lograr una Gestión corporativa inteligente del conocimiento, entendido como información analizada y valorada que proporciona un valor añadido al usuario, y de los datos, para darles un tratamiento eficaz, eficiente y seguro como recurso estratégico que son. La calidad de la información

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

se mide por su exactitud y precisión, oportunidad, fiabilidad y usabilidad, y completitud. Gestión es el proceso centralizado, lógico y eficiente, desde la obtención del dato hasta convertirlo en conocimiento útil y reutilizable.

En este proceso se busca caracterizar y tipificar la información, a través de la integración de usuarios, procesos, productos obtenidos, equipos y Servicios CIS/TIC, y de una estructura de gestión de la información acorde, que maximice su fiabilidad y accesibilidad en todo momento y lugar, siempre con la adecuada protección.

Como objetivo estratégico, mejorar su explotación por medio de herramientas colaborativas que permitan el intercambio, actualización y reutilización de productos generados por los usuarios a través de los servicios CIS/TIC.

Para ello es necesario estandarizar los datos, la información, y los registros y archivos aplicando la política de Gestión de Documentos Electrónicos, implantando estándares de intercambio de información que potencien el empleo de los servicios web y estableciendo una estructura de gestión de la información y del conocimiento a través de los Servicios CIS/TIC, que además impulsarán la definición y activación del Catálogo de Servicios CIS/TIC.

1.1.3 Coordinación de la GIC en el Ministerio de Defensa

La GIC queda intrínsicamente vinculada a los medios CIS/TIC por las enormes posibilidades que estos aportan en su gestión eficiente, siendo los principales habilitadores de su valor estratégico. Por ello, se dan instrucciones[3] para la coordinación de la GIC en el Ministerio, facultando al Director del CESTIC a coordinar y desarrollar las disposiciones necesarias para su aplicación. El resultado será el Plan de Acción GIC, trianual, que entre otros tiene por objetivo alinear los productos de información, los procesos funcionales y operativos a los que pertenecen y los servicios CIS/TIC, como pilares de la Transformación Digital del MDEF.

El Plan de Acción GIC se apoyará en las Arquitecturas de Referencia (AR) de los medios CIS de carácter permanente (AR CIS) y la AR única para la Gestión CIS/TIC. En su organización se distinguen el nivel corporativo del Departamento y varios niveles específicos, siendo uno de ellos la Armada. La Autoridad para la GIC es el SEDEF y el responsable en la Armada es el Almirante Secretario General del Estado Mayor de la Armada (ASEGEMAR).

La evaluación de la Gestión GIC se medirá en base a parámetros y métricas específicos, *Key Goal Indicators* – KGI, cuantitativos y que indican si se están alcanzando los resultados objetivo, en los plazos y empleando los recursos previstos, y los *Key Performance Indicators* – KPI, cualitativos y que muestran si el intercambio de información y conocimiento es óptimo. Ambos aportan eficiencia en la toma de decisiones ágiles, eficientes y la superioridad en la información.

1.2 Gestión del Sistema de Mando y Control Militar (SMCM). Gestión de Calidad del Servicio en la IP C2

En estos dos documentos se puede entender el entorno en el que se encuentran los Sistemas de Mando y Control (C2) comunes y específicos empleados por la Armada, así como el proceso para la gestión de la calidad en redes IP.

[3] Instrucción 37/2019, de 9 de julio, del Secretario de Estado de defensa, para la coordinación de la GIC en el MDEF.

1.2.1 Gestión del SMCM

El Sistema de Mando y Control Militar (SMCM)[4] es el instrumento a disposición de los Mandos Militares, apoyados por sus Órganos Auxiliares, para definir, dirigir, organizar y en definitiva emplear las FAS, así como hacer seguimiento permanente de este empleo; integrando funciones y herramientas que aportan eficientemente el conocimiento necesario para decidir, ordenar y controlar la ejecución.

Estas funciones y herramientas son los sistemas conjuntos y los específicos de los Ejércitos fundamentales para ejercer el Mando y Control (C2). El componente CIS del SMCM engloba el Sistema de Telecomunicaciones Militares (STM) y el Sistema de Información Militar (SIM).

Los servicios proporcionados al usuario por el STM son voz, fax y videoconferencia (VTC), tanto segura como no segura. Por su parte, el SIM aporta los servicios de presentación, procesamiento y almacenamiento de información a través de red, mensajería, y herramientas de interoperabilidad, colaboración y gestión.

La Gestión de SMCM se sustenta en una Estructura de Gestión conjunta, con dirección centralizada desde el Centro de Gestión del SMCM (CGS), perteneciente al CESTIC, y ejecución descentralizada por Órganos de Apoyo CIS (AOCIS) de los Ejércitos y Armada responsables de cada nodo, Figura 1-1. Las incidencias son controladas y resueltas por los AOCIS, escalando aquellas que no sean de su responsabilidad o no posean medios para su resolución.

Esta estructura es el resultado de las funciones de gestión extraídas de modelos de gestión CIS como el *Information Technology Infraestructure Library* (ITIL) y otras que como consecuencia de la evolución del estado del arte se han considerado útiles en su aplicación a la gestión CIS.

En el nivel de operación, control y logística y con relación funcional con el CGS, están los Centros de Operaciones Específicos (COE), donde la Armada tiene el COE-AR, para canalizar las relaciones entre el CGS y el Cuartel General de la Armada. Los OACIS serán el nivel de apoyo al usuario, con dependencia funcional del CGS, y que en la Armada reciben el nombre de Centros de Explotación CIS (CECIS).

Estos OACIS tendrán en plantilla el personal necesario para desarrollar sus tareas de gestión de acuerdo al marco establecido en los Acuerdos de Nivel de Servicio, incluyendo por supuesto la disponibilidad de atención al usuario. Siguiendo la estructura por niveles, la Armada cuenta con el CECIS de primer nivel en el CGA, CECISMAD, y de segundo nivel en áreas localizadas y periféricas, como son Ferrol, Cartagena, Cádiz, Rota y Las Palmas.

En cada uno de ellos se debe nombrar un Administrador local del Sistema (AS-L), un Operador de Sistema de Telecomunicaciones (OST), un Responsable Logístico (RL) y un Punto de Contacto CIS de Mando y Control (C2 CIS-POC).

[4] Instrucción General 01/10, de 21 de enero, del JEMAD, del componente CIS del Sistema de Mando y Control Militar (SMCM).

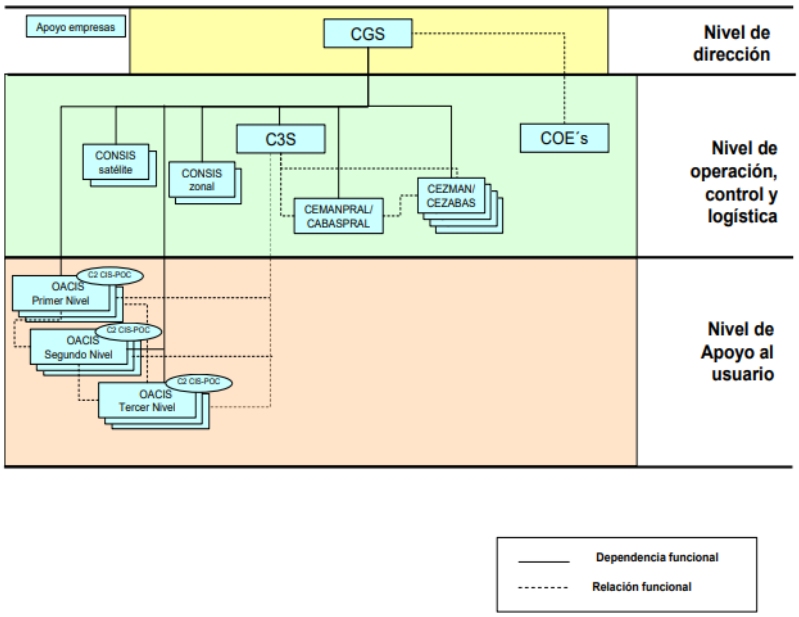

Figura 1-1. Estructura de Gestión del SMCM

1.2.2 Gestión de Calidad de servicio en la IP C2

La Red IP C2 (Mando y Control), o Subsistema de Conmutación de Paquetes, es un recurso más del STM visto en el subapartado anterior, con la finalidad de transportar servicios de datos, voz y video de los sistemas de información conjuntos y específicos de los Ejercitos.

Específicamente para este conjunto de servicios, el Centro de Gestión del SMCM promulgó las directrices[5] necesarias para alcanzar y respetar los grados de calidad adecuados, sujetas a la verificación y optimización del Organo de Explotación de Red del STM.

En primer lugar se agrupan los servicios en los siguientes 5 tipos:

- Control y Gestión de Red.
- Servicios en Tiempo Real.
- Difusión de contenidos Multimedia.
- Aplicaciones interactivas.
- Transferencia y otros servicios de datos.

Estos cinco tipos dan lugar a las 10 clases de servicio soportadas por la Red IP C2 y que pueden verse en la siguiente tabla 1-1:

Clase de Servicio	Descripción
Control de red	Funciones de enrutamiento y control de red y cifradores
OAM	Configuración y monitorización de red
Señalización	Señalización de los servicios de telefonía y videoconferencia
Telefonía	Transporte de información de los servicios VoIP

[5] Instrucción Técnica para la Gestión de la Calidad de Servicio en la Red IPC2 del STM (T-001 V.2), de 13 de julio de 2005, del Coronel Jefe STM de JESPREMAD.

Emulación	**Emulación de circuitos sobre IP**
Interactivo en Tiempo real	**Datos de sensores y Data Links**
Videoconferencia	**Servicios de videoconferencia**
Broadcast	**Difusión de audio y video**
Estándar	**Servicios de datos sin tratamiento diferenciado**
Estándar no garantizado	**Servicios no garantizados de datos sin tratamiento diferenciado**

Tabla 1-1. Clases y descripción de servicios en la Red IP C2.

Además, se identifican unos objetivos de calidad ya estipulados para cada Clase, la técnica de acondicionamiento, los valores DSCP[6] (Diffserv Code Point), tipos de colas y mecanismos de descartes, como se puede ver en la tabla 1-2.

Clase de Servicio	Descripción	DSCP			Objetivos de Calidad			Acondicionamiento en Acceso	Tipo Cola	Mecanismo descarte
		Nombre	Binario	Decimal	Retardo (one-way delay)	Jitter	Pérdida paquetes			
Control de red	Funciones de enrutamiento y control de red y cifradores	*CS6*	110000	48	400 ms	---	1%	Tasa más ráfaga limitadas	Ponderada	*AQM*
OAM	Configuración y monitorización de red	*CS2*	010000	16	---	---	1%	Tasa más ráfaga limitadas	Ponderada	*AQM*
Señalización	Funciones de señalización y control de los servicios de VoIP	*CS5*	101000	40	400 ms	---	0,1%	Tasa más ráfaga limitadas	Ponderada	Trasero
Telefonía	Transporte de información de los servicios VoIP	*EF*	101110	46	150 ms	50 ms	0,1%	Tasa más ráfaga limitadas	Prioritaria	Trasero
Emulación	Emulación de circuitos sobre IP		101100	44	150 ms	50 ms	0,1%	Tasa más ráfaga limitadas	Prioritaria	Trasero
Interactivo en Tiempo real	Datos de sensores y Data Links	*CS4*	100000	32	400 ms	---	0,1%	Tasa más ráfaga limitadas	Ponderada	Trasero
Videoconferencia	Servicios de videoconferencia	*AF41*	100010	34	400 ms	---	1%	Remarcado de tráfico excedente (fuera de *SLA*) a *AF42* (*>CIR*) o a *AF43* (*>PIR*)	Ponderada	*AQM por DSCP*
		AF42	100100	36	---	---	---			
		AF43	100110	38	---	---	---			
Broadcast	Difusión de audio y video	*CS3*	011000	24	---	---	0,1%	Tasa más ráfaga limitadas	Ponderada	Trasero
Estándar	Servicios de datos sin tratamiento diferenciado	*CS0*	000000	0	---	---	---	Remarcado de tráfico excedente (fuera de *SLA*) a *CS1*	Ponderada	*AQM*
Estándar no garantizado	Servicios no garantizados de datos sin tratamiento diferenciado	*CS1*	001000	8	---	---	---	---	---	---

Tabla 1-2. Objetivos de calidad en la Red IP C2.

Será necesario por tanto que el tráfico llegue a la Red marcado en origen con los valores DSCP según el tipo de tráfico para poder realizar el acondicionamiento necesario.

La Gestión del Nivel de Servicio (*Service Level Management* –SLM) tiene por objeto asegurar que los objetivos de niveles de servicios están documentados en Acuerdos de Nivel de Servicio (Service Level Agreement-SLA), y velar porque los niveles alcanzados se correspondan con lo firmado. Es por tanto necesario definir un SLA entre el proveedor de servicio de transporte IP, el STM, y los sistemas de información integrados en la red. Los parámetros a incluir en el documento se extraerán de las características técnicas aportadas en la descripción oficial de cada sistema y serán pactadas por ambas partes. A modo de ejemplo, la figura 1-2 para un servicio dependiente de un nodo concreto.

Por lo general, se aplica una política de prestación basada en porcentajes sobre el ancho de banda del enlace disponible para todos los servicios. Y más minuciosamente en enlaces satélite, donde se recoge que debe establecerse un SLA para cada Autorización de Acceso Satélite (AAS) planificada y

[6] DSCP. Medio para clasificar y gestionar el tráfico en la red además de proveer calidad de servicio (QoS) en la capa IP de las redes modernas. Emplea un campo de 6 bits en el encabezamiento IP para la clasificación de paquetes. https://www.dialogic.com/glossary/differentiated-services-code-point-dscp

todos los servicios solicitados en ella entre el Estado Mayor Conjunto (EMACON) y el AOS del Sistema de Información.

Provisión: Router e Interface		RCT-XXX	
Hostname router + Interface		Solicitud Sistema	SLA Ofrecido
Clases	Datos	Nodo Tipo X	SLA-X
Control de Red	BW	10 kb/s	10 kb/s
OAM	BW	10 kb/s	10 kb/s
	Aplicaciones/Protocolos gestión/Monitorización		
Señalización	BW	16 kb/s	16 kb/s
Telefonía	BW	64 kb/s	64 kb/s
	Tipo Códec	G729a	G729a
	Número de llamadas simultaneas	2	2
Emulación	BW	0	0
Interactivo en Tiempo Real	BW	0	0
Videoconferencia	BW	372 kb/s	372 kb/s
	Tipo de Compresión	H323	H323
Broadcast	BW	0	0
Estándar	BW	256 kb/s	256 kb/s
	Tipo de Compresión		
Estándar No Garantizado	BW	N/A	N/A

Fecha	Firma AOS S.I.	Firma CGS

Figura 1-2. Ejemplo para SLA por Nodo (RCT) y Sistema de Información

1.3 Concepto de Operaciones (CONOPS) del CESTIC

Ya expuesta la organización al más alto nivel de nuestra estructura y dirección CIS/TIC en el MDEF a través de los documentos anteriores, en este apartado conoceremos en detalle la distribución por áreas del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) así como sus competencias, reguladas en su Concepto de Operaciones (CONOPS)[7].

Entre sus funciones destaca:

- La dirección del diseño, obtención y configuración de los CIS/TIC y Seguridad de la Información garantizando la normalización, homologación, estandarización e interoperabilidad, tanto nacional como internacional.
- Coordinar la GIC del Departamento con la Transformación Digital y la AGE.
- Gestión y supervisión de servicios, controlando su operación y mantenimiento como Autoridad Operacional de los sistemas.

La Política CIS/TIC, ya vista en el Subapartado 1.1 asume como una de sus principales iniciativas la priorización de las actuaciones orientadas a satisfacer las necesidades de servicios CIS/TIC de las FAS, y en este mismo sentido la Arquitectura Global CIS/TIC incluye entre sus acciones derivadas:

- Desarrollar un modelo de interoperabilidad de los CIS TIC del MDEF, basado en un catálogo unificado de estándares (CUE), un catálogo de servicios y un catálogo unificado de productos CIS/TIC (CUP).
- Desarrollar un modelo de gestión particular basado en la combinación de las mejores prácticas y normas de referencia de diversos marcos y metodologías; algunas ya implantadas parcialmente en ciertas redes y sistemas propias, que proporcionará un lenguaje común y homogéneo y dará orientación para mejorar la eficacia, la eficiencia y la

[7] Norma Interna de Organización 01/2018, del CESTIC, Concepto de Operación (CONOPS). En revisión, versión 2.0 enero 2021.

seguridad de la información. Este modelo proporcionará la posibilidad de adoptar y utilizar las mejores prácticas disponibles para los procesos funcionales y operativos.

Dispondrá de una organización que le permita prestar servicios, como proveedor único del MDEF, con el mejor uso de los recursos y de acuerdo a los siguientes principios de actuación en la gestión de Servicios CIS/TIC:

- Gestión única a través de procesos estandarizados, funcionales y operativos, de forma centralizada y orientada a servicios, garantizando su provisión, integración y agilidad.
- Proporcionar los Servicios de acuerdo a los niveles acordados en los SLA, disponiendo de capacidad de negociación que garantice el uso eficiente de las tecnologías.
- Controlar centralizadamente la correcta provisión de servicios CIS/TIC que garantice la óptima asignación de recursos.

Para ello el CESTIC se divide en dos estructuras, la Estructura de Gobierno y la Estructura de Gestión como se puede apreciar en la siguiente figura 1-3.

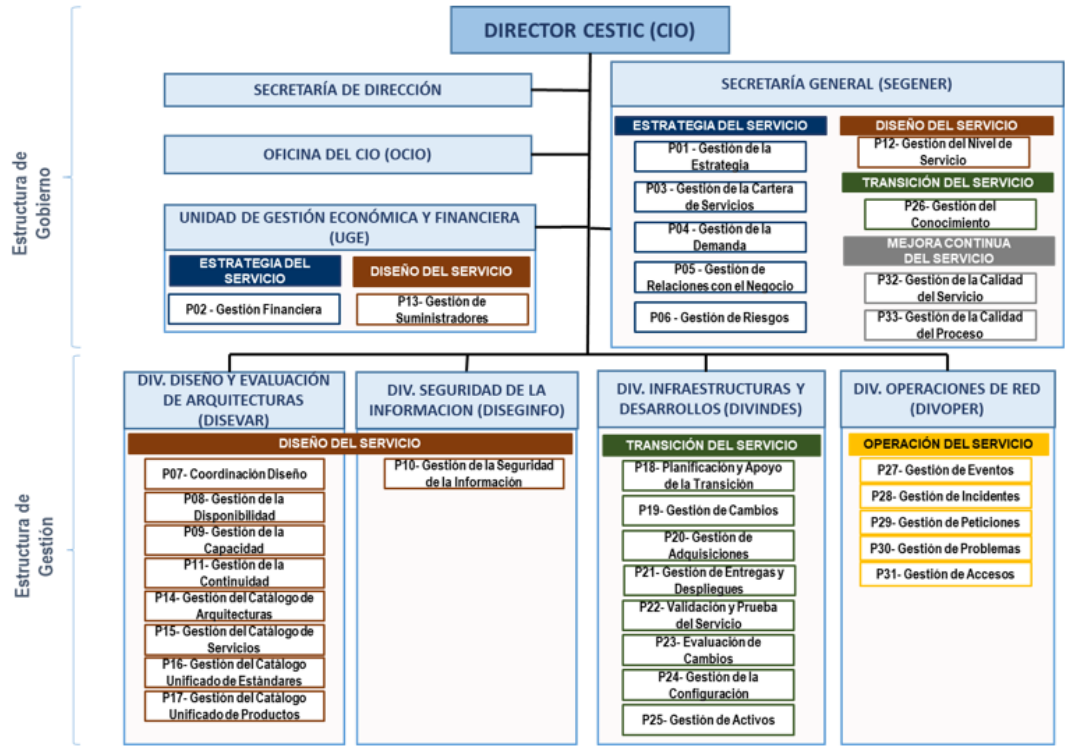

Figura 1-3. Organigrama y responsabilidades sobre procesos de Gestión de Servicios del CESTIC

Revisaremos en mayor detalle ciertos apartados del documento de referencia íntimamente relacionados con la Gestión de Servicios y con la finalidad de este trabajo, que no es otra que la de establecer una metodología a menor nivel para los Centros de Explotación CIS de la Armada.

1.3.1 Estructura de Gobierno

Como CIO, el DICESTIC pertenece a la Comisión Ejecutiva CIS/TIC, con responsabilidades sobre la supervisión y control de los resultados de métricas e indicadores de rendimiento obtenidos de

la explotación y prestación de servicios del Catálogo, así como sobre la coordinación del desarrollo de los procesos de gestión del cambio.

La Oficina del CIO desarrolla las estructuras de gobernanza y control de la GIC en la estructura del Centro, definiendo y comunicando las estrategias y marcos de referencia para la gestión, gobernanza, calidad y analítica de datos del MDEF y participando en el proceso de definición de servicios y sistemas, estableciendo los requisitos que aseguren la calidad y seguridad de los datos. También identificará aquellas acciones que pudieran mejorar los procesos o servicios y llevar a la práctica las válidas; función común a otras oficinas, como la Unidad de Gestión económica (UGE), que directamente apoya en la codificación y valoración económica de los servicios incluidos en el Catálogo y de su prestación según se especifique en los SLA.

La Secretaría General (SEGENER) debe desarrollar un modelo de Gestión de Servicios CIS/TIC, con la finalidad de cubrir las necesidades de los órganos del MDEF, dando prioridad a las FAS, y en especial al Mando y Control Militar. También debe desarrollar y mantener la Cartera de Servicios, estructurada en los de ámbito sectorial del MDEF y en los compartidos con la AGE.

Además, gestiona los recursos del CESTIC necesarios para llevar a cabo el Modelo de Gestión de Servicios CIS/TIC, identifica a los responsables y gestores de sus procesos y procedimientos y propone, inicia y gestiona cualquier plan de mejora de la Organización o del citado modelo.

La SEGENER también prioriza el desarrollo de los servicios que aseguren las capacidades C2 e Inteligencia de las FAS, e identifica y analiza patrones de actividad y perfiles de usuario para realizar una previsión de la demanda y poder asegurar los recursos adecuados disponibles para cumplir dicha previsión, siempre justificando el coste del servicio con el valor que aporta.

- Desarrolla los Acuerdos de Nivel de Servicio entre el CESTIC y los usuarios que recibirán los servicios CIS/TIC en el ámbito del MDEF, revisando frecuentemente el alcance de los servicios y los acuerdos de nivel operacional y de soporte para velar por su cumplimiento.
- Identifica los indicadores medidores de eficacia y eficiencia de los procesos y servicios CIS/TIC.
- Controla y supervisa la implementación de las mejoras propuestas, con el apoyo del resto de la estructura del CESTIC, así como la gestión de riesgos en todo el ciclo de vida de los servicios y sistemas.

1.3.2 Estructura de Gestión

Son cuatro los departamentos o Divisiones que encontramos, según la anterior figura 1-3, donde se detallan los procesos vinculados a la Gestión de servicios que a cada una competen (descarto DISEGINFO por no ser de mayor relevancia en el desarrollo de este trabajo).

I. DISEVAR es responsable de los procesos de Gestión de la Disponibilidad, de la Capacidad y de la Continuidad, y de la Gestión de los Catálogos de Servicios, Estándares y Productos.
    - Enlaza con la industria externa en busca de soluciones tecnológicas para proveer herramientas para la gestión de Servicios CIS/TIC.
    - Incluye los nuevos servicios, estándares y productos que han sido aprobados para inserción y/o actualización en los catálogos.
    - Diseña los citados catálogos definiendo sus estructuras y relaciones.
    - Realiza el informe de evaluación de los cambios antes de su diseño y desarrollo.
    - Verifica la existencia de capacidad para cumplir con los niveles de servicio requeridos de los nuevos y existentes.
    - Revisa periódicamente los planes de continuidad y evalua los posibles problemas de continuidad de cada servicio.

II. DIVINDES es responsable de la Gestión de Cambios, de la Configuración y de los Activos.

- Planifica el proyecto de creación o modificación de un servicio, así como los resursos y pruebas necesarias para ello.
- Coordina la comunicación de la entrega del servicio nuevo o modificado, incluyendo la gestión del mismo.
- Desarrolla la documentación de nuevos servicios y modificados, comprobando que cumple con los requisitos técnicos y operativos acordados con los receptores.
- Define la estructura del sistema de gestión de la configuración y recopila, gestiona, controla y mantiene un inventario único de activos CIS/TIC con HW, SW, licencias, servicios e infraestructuras.

III. DIVOPER es responsable de los procesos relacionados con la Gestión de Eventos, Incidentes, Peticiones, Problemas y Accesos; y para ello posee un Centro de Gestión de Servicios (CEGES).

- Responsable de servicios en producción ante usuarios y resto de la organización, garantizando su operatividad y especificando y monitorizando su operación.
- Punto de contacto principal de los servicios ante incidencias, peticiones y gestiones de accesos para el usuario.
- Es primer nivel de soporte para eventos, no de seguridad, de incidencias, errores repetitivos y peticiones de usuarios, registrándolas, analizándolas, resolviéndolas y /o escalándolas cuando sea necesario.
- Controla que los procesos de recuperación del normal funcionamiento y la resolución de errores repetitivos cumplen con los niveles acordados.
- Proporciona informes de capacidad y rendimiento de los servicios, identificando oportunidades de mejora para cumplir los objetivos de nivel de servicio.
- Colabora en la elaboración de SLAs y contratos con suministradores con la SEGENER, proporcionando informes de nivel de servicio e investigando los posibles incumplimientos para prevenir y corregir según el caso.

1.3.3 Ciclo de vida de los Servicios

Siguiendo modelos y metodologías de referencia estandarizados como ITIL e ISO, ampliamente conocidos en la gestión de servicios y aplicados en la Adminstración y empresas, el CESTIC también desarrolla los procesos de su responsabilidad relativos a funcionalidad y operatividad de los Servicios que provee siguiendo un ciclo de vida de 5 fases, según se muestra en la figura 1-4.

- **Estrategia del Servicio CIS/TIC**. Alinear los Servicios CIS/TIC con los objetivos y necesidades del MDEF a través de Estrategias, Políticas y Planes, priorizando los requerimientos de los usuarios con una orientación a Servicios, no al "cómo".
- **Mejora Continua del Servicio CIS/TIC**. Identificar e implementar mejoras en los servicios y procesos para mantener los Servicios CIS/TIC en línea con la evolución y los cambios en las necesidades del MDEF.
- **Diseño del Servicio CIS/TIC**. Asegurar que los Servicios CIS/TIC satisfacen las metas y objetivos definidos por la Estructura de Gobierno (Estrategia CIS/TIC) a través de procesos que además permitan su empleo en otros entornos garantizando la entrega de servicios de calidad y satisfactorios para el usuario.

- **Transición del Servicio CIS/TIC**. Asegurar que las metas y objetivos definidos por la Estructura de Gobierno se tienen en cuenta en el desarrollo de los Servicios CIS/TIC previamente diseñados y que además apoyen al diseño a medida que estos evolucionan del desarrollo a la implantación, a la modificación y finalmente a su retirada.
- **Operación del Servicio CIS/TIC**. Aquellos orientados a la coordinación e implementación de actividades y procesos necesarios para la entrega y el mantenimiento de los Servicios CIS/TIC en los niveles acordados en los SLA con los organismos receptores.

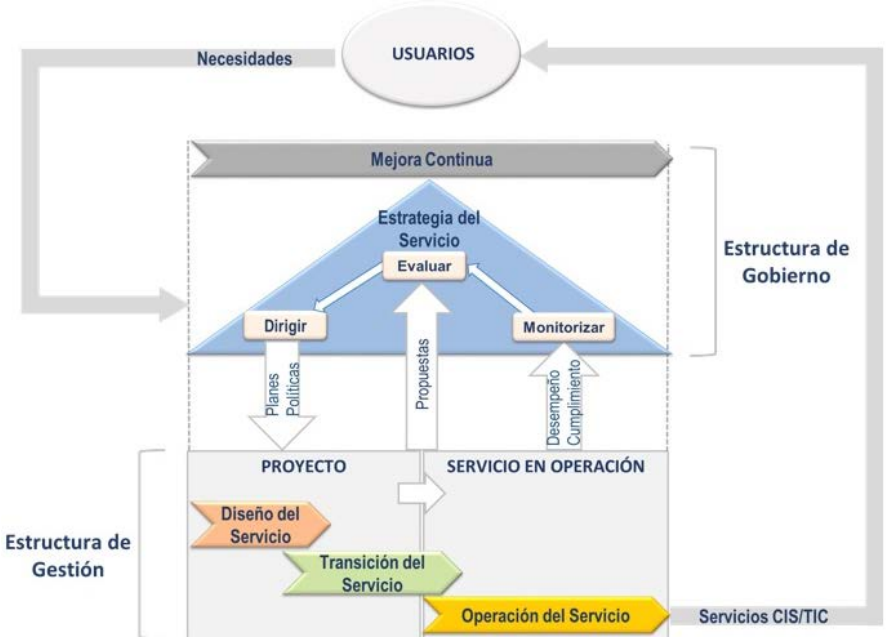

Figura 1-4. Ciclo de Gestión de Procesos

El propósito de todos los procesos es proveer de Servicios de muy alta calidad a los usuarios y a continuación veremos los principales relacionados con la operación, incidencias y cambios:

- **Gestión de la Demanda.** Comprender la demanda de los usuarios sobre un servicio y prever el suministro de la capacidad y otros aspectos del soporte para el servicio, tratando de reconocer proactivamente la carga de trabajo (demanda) de los receptores de los servicios con los recursos disponibles (capacidad), con análisis, tendencias y previsiones.
- **Gestión de la Disponibilidad.** Asegurar que la disponibilidad de los recursos CIS/TIC aprobados se cumple o se supera consistentemente, así como satisfacer futuras necesidades de disponibilidad de una base de nuevos servicios o extendidos de forma rentable.
- **Gestión de la Capacidad.** Lograr que la capacidad del servicio y sus componentes cumplan con los requisitos y niveles acordados de rendimiento y en el futuro.
- **Gestión de la Continuidad**. Analizar los riesgos que podrían afectar a los servicios vitales y asegurar la recuperación de los niveles mínimos de servicio acordados para la continuidad de las actividades MDEF, en los plazos acordados necesarios.
- **Gestión del Nivel de Servicio.** Entregar un marco de contacto frecuente entre el usuario de los servicios y el CESTIC como proveedor, para negociar y documentar los objetivos y responsabilidades de las partes. Los SLA y los Acuerdos de Nivel Operacional (OLA) expresan las metas específicas y medibles del nivel de calidad del servicio.
- **Gestión del Catálogo de Servicios.** Proporciona una fuente de información autorizada, consistente y comprensible sobre todos los activos disponibles y asegurar que esté accesible para aquellos autorizados a verla.

- **Gestión de Cambios.** Conseguir que todos los cambios sean evaluados, aprobados, implementados y revisados de forma controlada, garantizando que, ya sea por adición, modificación o supresión de un servicio o componente, vaya en consonancia con la estrategia global del MDEF, facilitando métodos estandarizados para el manejo rápido y eficiente de los cambios técnicos, minimizando el impacto de los incidentes relativos al cambio en la calidad del servicio y mejorando las operaciones diarias de la organización.
- **Evaluación de Cambios.** Efectuar la evaluación formal previa a la ejecución de cualquier cambio importante, entregando información precisa al proceso de Gestión de Cambios sobre su probable impacto y efecto en la capacidad de servicio, antes de que sea aceptado.
- **Gestión de Activos.** Gestionar los activos CIS/TIC (hardware, software, licencias e instalaciones / infraestructuras) durante su ciclo de vida, desde la adquisición pasando por el despliegue, el uso y las mejoras, hasta su retirada o reutilización y la eliminación. Se diferencia de la Gestión de la Configuración en que ésta se ocupa de las relaciones entre los elementos de configuración en que se sustentan los servicios, mientras que la Gestión de Activos gestiona los activos y sus atributos (los costes, el cumplimiento, etc).
- **Gestión del Conocimiento.** Proporcionar el mecanismo que ayude a capturar, crear, compartir y actuar sobre la información mejorando de forma medible la entrega y el soporte de los Servicios CIS/TIC y asegurando su entrega en tiempo y forma al destinatario apropiado para la toma de decisiones que mejoren el rendimiento y la efectividad.
- **Gestión de Eventos.** Reconocer y priorizar los eventos que suceden en la infraestructura CIS/TIC y establecer la respuesta apropiada, monitorizando, filtrando y notificando las acciones y los eventos que afectan a los servicios proporcionados de forma proactiva y reactiva.
- **Gestión de Incidentes.** Reestablecer la operación normal del servicio lo antes posible minimizando el impacto negativo en las operaciones de los usuarios, asegurando los mejores niveles posibles de calidad, seguridad y disponibilidad del servicio. El objetivo es reducir la duración y las consecuencias de las interrupciones del servicio desde la perspectiva de los usuarios, más que en localizar la causa del incidente.
- **Gestión de Problemas.** Evitar que sucedan problemas e incidentes, eliminar los recurrentes y minimizar el impacto de los que no puedan evitarse, con las tareas necesarias para diagnosticar su causa raíz, determinar la resolución de esos problemas y proporcionar soluciones temporales a la Gestión de Incidentes.
- **Gestión de Peticiones.** Atender las peticiones de servicio de los usuarios dirigiendo cada petición al proceso de gestión apropiado dentro de los niveles de servicio acordados, responsabilizándose de todo el ciclo de vida de la petición.
- **Gestión de la Calidad del Servicio.** Basado en las cuatro fases del ciclo de Deming (Planificar, Hacer, Comprobar y Actuar) permite visualizar el grado de satisfacción de los usuarios y el rendimiento de los servicios, a través del seguimiento de la información y de las métricas relevantes obtenidas de procesos funcionales y operativos. Los resultados permiten desarrollar planes correctivos y ajustes que aseguren el rendimiento deseado.
- **Gestión de la Calidad del Proceso.** Basado en el mismo enfoque de cuatro fases anterior, permite evaluar los procesos regularmente, identificando las áreas en las que no se cumplen los indicadores clave de rendimiento (KPI) establecidos, así como comparativas, auditorías, evaluaciones de madurez y revisiones de procesos.

1.3.4 Responsabilidades en los procesos funcionales y operativos

Establecidos los procesos es necesario designar al personal, sección o área responsable de un modo u otro, así como la asignación de cometidos en su ciclo de vida; los llamados roles.

- **(R) Responsable de ejecución.** Quien efectivamente realiza la tarea.
- **(A) Responsable del encargo.** Se responsabiliza de que la tarea se realice y bien, rindiendo cuentas al superior jerárquico. Sólo puede haber uno.
- **(C) Consultado.** Aquel que posee información o capacidad necesaria para efectuar la tarea (comunicación bidireccional).
- **(I) Informado.** Será informado del avance y resultados de la ejecución (comunicación unidireccional).

Según estos roles, la estructura establecida en el CESTIC se muestra en la siguiente tabla 1-3

			ROLES					
ESTRUCTURA ORGANIZATIVA	FASE DEL SERVICIO	PROCESO FUNCIONAL/OPERATIVO	UGE	SEGENER	DISEVAR	DISEGINFO	DIVINDES	DIVOPER
Gobierno CIS/TIC	Mejora Continua CIS/TIC	Gestión de la Calidad del Servicio	C	A/R	C	C	C	C
		Gestión de la Calidad del Proceso	C	A/R	C	C	C	C
	Estrategia CIS/TIC	Gestión de la Estrategia	I	A/R	I	I	I	I
		Gestión Financiera	A/R	C/I	C	C	C	C
		Gestión de la Cartera de Servicios	C	A/R	I	I	I	I
		Gestión de la Demanda	I	A/R	I	I	I	I
		Gestión de Relaciones con el Negocio	-	A/R	-	-	-	C
		Gestión de Riesgos	C	A	C	R	C	R
Gestión CIS/TIC	Diseño CIS/TIC	Coordinación del Diseño	-	-	A/R	C	-	-
		Gestión de la Disponibilidad	-	I	A/R	-	-	R
		Gestión de la Capacidad	-	I	A/R	-	-	R
		Gestión de la Seguridad de la Información	-	I	I	A/R	I	R
		Gestión de la Continuidad	-	I	A/R	R	I	R
		Gestión del Nivel de Servicio	C	A	C	-	-	R
		Gestión de Suministradores	A/R	C	C	C	C	C
		Gestión del Catálogo de Arquitecturas	-	I	A/R	C	I	I
		Gestión del Catálogo de Servicios	-	I	A/R	I	I	C
		Gestión del Catálogo Unificado de Estándares	-	I	A/R	C	I	I
		Gestión del Catálogo Unificado de Productos	-	I	A/R	C	I	I
	Transición CIS/TIC	Planificación y Apoyo de la Transición	-	-	-	C	A/R	C
		Gestión de Cambios	-	I	C	C	A/R	C
		Gestión de Adquisiciones CIS/TIC	R	C	C	C	A	C
		Gestión de Entregas y Despliegues	-	-	-	I	A/R	C
		Validación y Prueba del Servicio	-	-	-	R	A/R	I
		Evaluación de Cambios	-	-	C	C	A/R	C
		Gestión de la Configuración	I	I	I	I	A/R	I
		Gestión de Activos	I	I	I	I	A/R	I
		Gestión del Conocimiento	I	A	C	I	R	I
	Operación CIS/TIC	Gestión de Eventos	-	-	-	-	-	A/R
		Gestión de Incidentes	-	I	-	R	C	A/R
		Gestión de Peticiones	C	C	C	C	C	A/R
		Gestión de Problemas	-	I	C	C	C	A/R
		Gestión de Accesos	-	-	-	C	-	A/R

Tabla 1-3. Matriz RACI de responsabilidades en la Gestión de procesos de Servios del CESTIC.

1.4 Organización de la Armada y su estructura CIS

La organización de la Armada se centra en las personas y en el conocimiento, basándose en la gestión de procesos y en proyectos como metodologías principales para elaborar su actividad[8], y subdividiéndose en su Cuartel General, la Fuerza y el Apoyo a la Fuerza según la naturaleza de su misión principal.

El principal cambio experimentado respecto a la estructura anterior, desarrollada por Instrucciones y disposiciones del año 2019 y anteriores, desde el punto de vista CIS/TIC y de interés para este trabajo, es la reestructuración de nuevos órganos con responsabilidad en materia de conocimiento,

[8] Instrucción 15/2021, de 11 de marzo, del Almirante Jefe de Estado Mayor de la Armada, por la que se desarrolla la Organización de la Armada.

información y telecomunicaciones dentro de la composición del Cuartel General de la Armada, ubicado en Madrid.

1.4.1 Cuartel General de la Armada

El Almirante Segundo Jefe del Estado Mayor de la Armada (2º AJEMA) establece las políticas de los Sistemas y Tecnologías de la Información y las Comunicaciones (CIS/TIC) de la Armada, derivadas de las establecidas por el MDEF, manteniendo relaciones directas en este aspecto con DICESTIC. Asume la Jefatura del Estado Mayor de la Armada (EMA) bajo la dirección del AJEMA.

El Estado Mayor de la Armada, principal órgano asesor del mando, se compone a su vez de diferentes órganos que asumen las competencias asignadas al mismo, siendo la Secretaría General del EMA (SEGEMAR) la encargada de impulsar, coordinar y controlar la implantación del modelo de gestión de las actividades centrado en el conocimiento y en la transformación digital, y de la innovación y de la política CIS/TIC, estructurada según la figura 1-5.

La Sección GIC vela por lograr la evolución hacia una gestión corporativa inteligente del conocimiento de la información y de los datos, desarrollando, ejecutando y supervisando políticas, normas y procedimientos de gestión y gobernanza de datos, garantizando su disponibilidad, seguridad y calidad suficiente para soportar procesos de trabajo y la toma de decisiones.

Elabora y mantiene atualizado el "Plan GIC de la Armada" coordinando con el CESTIC las necesidades de desarrollo de herramientas para la gestión de la información y el conocimiento y colaborando con la Dirección de Enseñanza Naval en la elaboración de planes de formación del personal en materia GIC.

Por su parte, la Sección de Tecnologías de la Información y Telecomunicaciones (SECIS) apoya y asesora en política CIS/TIC nacional e internacional y en su planeamiento derivado. Participa en el desarrollo de las AR de los sistemas CIS/TIC permanentes y dirige la elaboración de la arquitectura y objetivo de los medios CIS/TIC desplegables de la Armada.

Figura 1-5. Estructura de la Secretaría General del EMA.

1.4.2 Jefatura de Sistemas de la Información y Telecomunicaciones (JECIS).

La Instrucción que desarrolla la Organización de la Armada da lugar a normas posteriores que establecen la composición y funcionamiento de los Organos de Apoyo a la Acción Orgánica (OAAO), bajo la autoridad del 2º AJEMA, con la responsabilidad de proporcionar los servicios y apoyos de su competencia para facilitar la acción orgánica en la estructura de la Armada, como técnicos en su materia específica y asesorando al EMA en la elaboración de las políticas de su ámbito.

Como OAAO CIS/TIC tenemos la Jefatura de Sistemas de la Información y Telecomunicaciones[9] (JECIS), figura 1-6, que gestiona y proporciona servicios CIS en el nivel adecuado de eficacia, relacionados con los sistemas de información y telecomunicaciones de su ámbito de responsabilidad, a las unidades y organismos de la Armada, supervisa la aplicación de la normativa de seguridad de la información (SEGINFO), la protección de datos personales y garantía de derechos digitales, y dirige y gestiona la adquisición y empleo de la capacidad de ciberdefensa en la Armada.

Se relaciona con la Jefatura de Apoyo Logístico (JAL) para la modernización y sostenimiento de los medios CIS y con la Flota (Fuerza) para contribuir y ayudar en su correcto empleo. En cuanto al ámbito conjunto, mantiene relaciones con el CESTIC y el Mando Conjunto del Ciberespacio (MCCE) en sus competencias CIS/TIC y Ciberdefensa.

En su labor de supervisión del cumplimiento de la normativa SEGINFO, mantiene relaciones con la Oficina Nacional de Seguridad (ONS) y con el Centro Criptológico Nacional del Centro Nacional de Inteligencia (CNI).

Figura 1-6. Organigrama de la JECIS

- SETEC. Secretaría Técnica. Asiste al Almirante (AJECIS) efectuando estudios y análisis técnicos relativos a la organización, nuevas tecnologías y sistemas CIS, y elaborando la documentación resultante.
- GRUCIBER. Grupo de Ciberdefensa. Ejecuta y planea las acciones de seguridad de defensa de las redes y sistemas de información y de operación específicos de la Armada a su nivel. Monitoriza, previene y detecta incidentes de seguridad en los sistemas de la Armada al objeto de garantizar la confidencialidad, integridad y disponibilidad.
- GRUSEGINFO. Grupo de Seguridad de la Información. Vela por la seguridad de la información en personas, instalaciones y documentos y coordina el cumplimiento de la normativa relativa a la protección de datos de carácter personal de la Armada.
- GRUCECIS. Grupo de Centros de Explotación de Sistemas de Tecnología de Información y Telecomunicaciones. Proporciona los servicios CIS/TIC de apoyo a las unidades de la Armada implementando y manteniendo los requisitos de seguridad aprobados. Gestiona, controla y explota los CIS/TIC de su entorno de responsabilidad, corporativos y conjuntos, dando asesoramiento técnico CIS.

[9] Norma Permanente de Organización núm. 03/2021, de 4 de mayo, del 2º AJEMA, por la que se desarrolla la Organización del EMA y de los Organos de Apoyo a la Acción Orgánica (OAAO).

1.4.3 Grupo de Centros de Explotación de Sistemas de Información y Telecomunicaciones (GRUCECIS).

Actualmente se encuentra en desarrollo la Norma Permanente[10] que desgrana la estructura de la Jefatura CIS a partir de los dos documentos de referencia vistos hasta este subapartado, la Instrucción 15/20021 sobre Organización de la Armada y la Norma Permanente 03/2021 de Organización del EMA y de los Organos de Apoyo a la Acción Orgánica (OAAO).

De la estructura interna de la JECIS, figura 1-7, nos centraremos en el GRUCECIS, en su composición y en el desarrollo de sus competencias con el fin de proponer un plan dinámico y funcional, acorde a las referencias y estándares internacionales, para la provisión de servicios CIS/TIC de calidad desde sus Centros de Explotación.

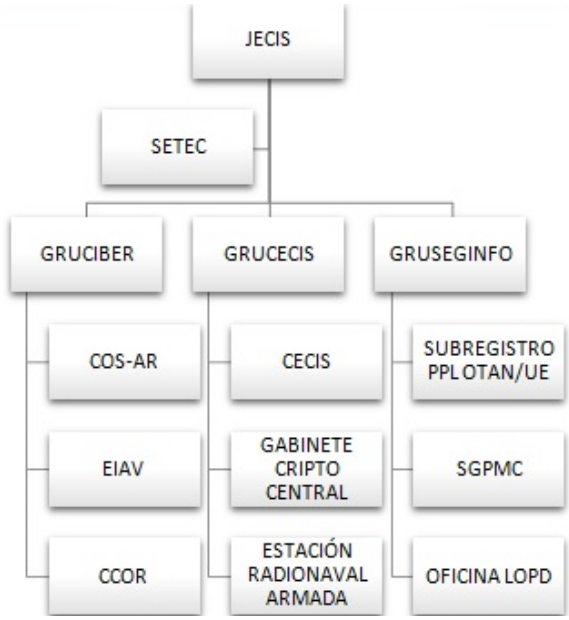

Figura 1-7. JECIS y estructura GRUCECIS

El Grupo, Figura 1-8, tiene los siguientes cometidos particulares:

- Dirige y controla la actividad de los Centros de Explotación CIS (CECIS) para la correcta explotación de los CIS/TIC específicos de la Armada y de los corporativos del MDEF en nuestro ámbito.
- Genera, difunde y controla la ejecución de la normativa técnica a aplicar por los CECIS.
- Coordina y gestiona las peticiones y necesidades que los CECIS requieren de otros órganos CIS de ámbito conjunto y en la Armada.
- Elabora y mantiene el catálogo e inventario de la configuración de los componentes hardware y software de los sistemas CIS/TIC, en colaboración con la Sección CIS de la Dirección de Sostenimiento de la Jefatura de Apoyo Logístico (JAL) y coordina la distribución de este material informático a los CECIS.
- Coordina a nivel técnico con los órganos CIS de la JAL y Flota para asegurar la explotación eficaz de los sistemas CIS.

[10] Norma Permanente de Organización 01/2021, del Almirante Jefe de Sistemas de Información y Telecomunicaciones, por la que se desarrolla la estructura de la Jefatura de Sistemas de Información y Telecomunicaciones.

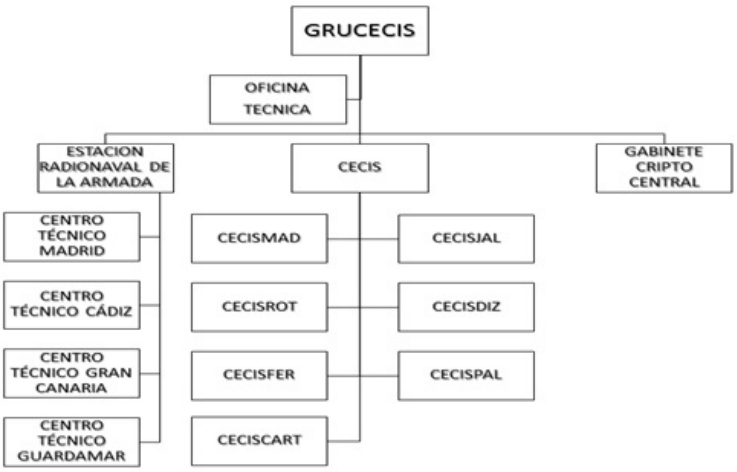

Figura 1-8. GRUCECIS y Centros de Explotación CIS establecidos

En particular, los Centros de Explotación de Sistemas de Información y Telecomunicaciones (CECIS), facilitan a mandos y unidades de su localización geográfica los servicios CIS, el acceso a los Sistemas que requieren para el ejercicio de sus funciones y apoyo técnico para su empleo. Para el reparto de competencias y desarrollo de sus cometidos se dividen en dos, el Centro de Comunicaciones (CECOM) y el Centro de Sistemas de Información (CESIN). Sus cometidos son:

- Asegurar la continuidad de los enlaces entre sistemas y usuarios garantizando rapidez, seguridad, confianza y flexibilidad.
- Apoyar a las unidades en la instalación, configuración y actualización de los sistemas CIS prestando asesoramiento técnico CIS.
- Controlar, administrar y distribuir el equipamiento informático hardware y software, manteniendo el inventario actualizado.
- Prestar los servicios de cifra, distribuir y controlar el material cripto y apoyar en el mantenimiento del equipamiento criptográfico.
- Colaboran en la definición de los requisitos de los nuevos sistemas, en la elaboración de la doctrina sobre su empleo, en la realización de pruebas y estudios para su implantación y en el desarrollo de nuevas aplicaciones informáticas.
- Colaborar con el CESTIC y el MCCE en el mantenimiento de los niveles de servicio adecuados de los sistemas CIS del MDEF.

2 ESTADO DEL ARTE

En este capítulo se comentarán diferentes estándares, normas, y procedimientos en vigor, relevantes y relacionados con el desarrollo del proyecto en el ámbito de la gestión de servicios de TI; así como algunas herramientas software facilitadoras de la gestión en si y de uso extendido.

2.1 ITIL

Information Technology Infraestructure Library es un conjunto de publicaciones que contiene una amplia serie de "buenas prácticas" orientadas a la gestión de servicios de TI que facilitan a las organizaciones la gestión de sus infraestructuras TI y dan apoyo a sus objetivos de negocio.

Este manual nació en los años 80 como referencia para hacer más eficiente el trabajo en las oficinas del sector público británico y hoy en día se ha convertido en una herramienta aplicable a cualquier organización para la gestión de muchas otras materias como son la seguridad de la información, los niveles de servicio, de sus activos, software y aplicaciones, por ejemplo, tratando de crear un punto de unión entre la gestión de la TI y la gestión empresarial, basado en otros estándares como ISO o EFQM (*European Foundation for Quality Management*, modelo que permite la mejora integral de la gestión, relaciones, sociedad, personas, recursos y liderazgo en las organizaciones).

Se caracteriza por haberse desarrollado sin derechos de propiedad y por tanto ser de uso libre y público, adaptándose a las características de cada necesidad organizacional y estando en continuo crecimiento con otras buenas prácticas recopiladas por expertos y profesionales del sector, favoreciendo así la estandarización internacional en el empleo de terminología, lenguaje y documentos. Está en vigor en su versión 4, compuesta por 5 libros o volúmenes, que definen el ciclo de vida ITIL (Figura 2-1).

Figura 2-1. ITIL *lifecycle*

A continuación se describe, no en su totalidad por su gran extensión, el contenido de los volúmenes, organizado en 34 procesos o prácticas entendidas como "conjuntos de recursos organizacionales diseñados para realizar un trabajo o lograr un objetivo", que es dar soporte y valor al negocio desde un punto de vista TI, y que no todos tienen por qué realizarse en una organización; principal diferencia con otros procesos estandarizados que sí buscan la certificación, como es ISO.

2.1.1 Estrategia de Servicios (Service Strategy – SS)

Diseña el plan de acción que permite implementar una estrategia empresarial en la Organización que incluya las TI desarrollando multiples areas, como son la competitividad y el posicionamiento en el Mercado, la gestión del servicio como factor estratégico, el diseño organizacional, la gestión financiera y la cartera de servicios o la gestión de la demanda. Permite graduar y alinear sus objetivos de negocio con su infraestructura TI y las necesidades de los usuarios, favoreciendo la entrega y respaldo de los servicios y productos que los clientes necesitan, fomentando la administración de los servicios de TI y el conocimiento de la red que interacciona con clientes y usuarios. Es por tanto fundamental para generar valor, que dominemos la composición de nuestro servicio. Son cinco las áreas incluidas en este proceso:

I. Gestión de la Cartera de Servicios

Su objetivo es conocer, actualizar y actuar sobre nuestros servicios cuando estos lo demanden, permitiendo ser más eficiente en el gasto optimizando el beneficio obtenido de la infraestructura con inversiones de bajo riesgo, controladas y beneficiosas por el momento y forma.

Son cuatro pasos los que se deben realizar:

- Inventariar, definir y validar los servicios contenidos en la cartera con terminología TI común en el mercado.
- Valorar los servicios para priorizar y equilibrar los recursos necesarios según criterios de ventaja y riesgo.
- Medir los servicios para conocer su dependencia como proveedores de valor y cómo los suministra la organización, a través de encuestas a los ususarios, por ejemplo.
- Justificar los proyectos de TI mostrando las oportunidades de mejora para el negocio y la validez de estas inversiones, valorando la dificultad, el coste y el beneficio esperado.

II. Gestión Financiera de Servicios de TI

Pretende ayudar a la organización a gestionar los costes de los recursos TI necesarios para suministrar sus servicios, alineando la calidad del servicio con el coste asociado. Para ello es necesario evaluar los costes directos e indirectos de la infraestructura para proveer los servicios, con el fin de tomar decisiones adecuadass y conocer el rédito que se obtendrá de tal inversión. Bien ejecutadas reducirán costes, aportarán eficacia y aumentarán la rentabilidad del negocio.

Son tres actividades las que se llevan a cabo principalmente:

- Contabilidad que nos permita atribuir costes a los trabajos realizados desde el departamento TI.
- Presupuestos que permitan a la organización planificar costes e inversiones así como una valoración de la financiación para mantener los servicios TI.
- Fijación de precios para asignar un valor real al trabajo que supone cada servicio y su infraestructura. Se puede utilizar para el cálculo de los costes de mantenimiento y preparar presupuestos para los servicios a clientes.

III. Gestión de la Demanda

Se trata de optimizar el empleo de los recursos TI, tanto a corto como a medio y largo plazo. A corto plazo conociendo las prioridades estratégicas actuales de la empresa y evitando incidencias que afecten a procesos críticos y disminuyan la capacidad de reacción, ya sea por fallos en la integridad del servicio debido al aumento imprevisto de la demanda o por interrupciones de servicio por errores HW o SW.

Y a medio y largo plazo para que las inversiones se efectúen de forma racional. En determinadas situaciones puede parecer que se necesita un aumento de la capacidad, cuando realmente con un reparto inteligente de la carga sobre la infraestructura podríamos mantener la calidad del servicio. Esto se consigue monitorizando nuestra infraestructura para rentabilizar el servicio y así evitar inversiones innecesarias.

IV. Gestión de Relaciones Comerciales

Permite a los servicios de TI informar e implementar la estrategia y la selección de servicios, tratando de establecer una relación con los clientes que permita comprender sus requerimientos de servicio. El indicador de rendimiento clave (KPI) de este proceso es la satisfacción del ciente, y son tres aspectos los que se deben considerar en su implementación:

- Asegurar que los servicios proporcionados entregan el valor que el cliente espera.
- Entender el entorno del cliente para detectar nuevas oportunidades de servicio o nuevas aplicaciones de servicios ya existentes.
- Estar al corriente de las modificaciones del ambiente empresarial del cliente que puedan afectar los requerimientos del servicio.

V. Gestión de Estrategias para Servicios de TI

Pretende que la gestión de servicios de TI sea un activo estratégico más para la organización, buscando no solo alinear la TI con el negocio, sino también integrarla en él, ya sea como soporte, como apoyo o como elemento diferenciador.

Es fundamental conocer en profundidad la red que interacciona entre nuestra organización, los usuarios y los clientes y el espacio de mercado en el que opera. Saber cuáles son nuestras fortalezas y nuestras debilidades como proveedor, y qué oportunidades están disponibles, contrastando y detectando multitud de factores como la capacidad, la utilidad, la fiabilidad, continuidad, seguridad, rapidez en la entrega, etc que respondan a preguntas tales como:

- Quiénes son nuestros clientes, qué resultados empresariales necesitan y cómo apoyan esos resultados los servicios que ofrecemos.
- En qué espacio de mercado operamos y cómo podemos posicionarnos como proveedor destacado del entorno.
- Cómo podemos expandirnos a nuevos mercados o cubrir áreas no atendidas desarrollando nosotros nuevos servicios.

2.1.2 Diseño de Servicios (Service Design – SD)

Se trata de transformar la estrategia de negocio en un modelo de desarrollo del servicio, basado en diferentes niveles de gestión, donde habrá que negociar con los clientes y proveedores, mantenerlo activo y en condiciones propicias, así como velar por la seguridad del contenido y su reconstrucción en caso de incidencia. Son siete las áreas contenidas en este proceso:

I. Gestión de los Niveles de Servicio

Supone investigar y comprender los requisitos de nuestros clientes, estableciendo un marco de registro de todas las vicisitudes (un acuerdo) que nos permita proveer un servicio de TI de gran calidad a un coste asequible.

Todo el proceso sigue un ciclo de calidad similar a otras metodologías, como ISO, cerrando fases en el orden de la figura 2-2 con el objetivo de la mejora.

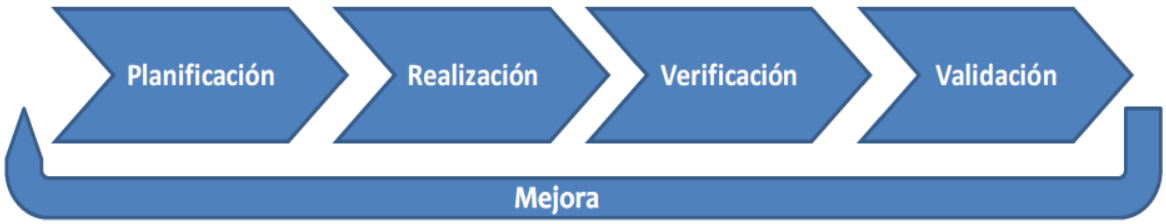

Figura 2-2. Ciclo de Gestión del Nivel de Servicio

Planificar el servicio es orientarlo en la dirección que permita ofrecer al cliente algo acorde a sus necesidades, estudiando cuáles son, cómo entregarlas, qué capacidad tenemos para lograrlo, qué nivel podemos ofertar y cómo gestionarlo.

La Realización es la tarea de ponerlo en funcionamiento para el cliente en base a la documentación desarrollada en la fase anterior con diferentes actuaciones.

Verificar supone monitorizar las actuaciones realizadas con el fin de mantener o mejorar la calidad del servicio ofertado, midiendo y estudiando ciertos indicadores de rendimiento que nos permitirán llevar a cabo la posterior Validación, a través de informes personalizados del estado del servicio.

Y por último la Mejora, cuyo fin es revisar constantemente la calidad del servicio entregado siguiendo un Programa de Mejora del Servicio.

El proceso enmarcado queda perfectamente registrado sobre una serie de Documentos de Detalle definidos para el cliente y desarrollados con él, que contienen múltiples aspectos del servicio esperado,

si no todos. Son, siguiendo las fases del ciclo, y no todos tienen obligatoriamente que ser desarrollados:

- Catálogo de Servicios. Pertenece a la Planificación y debe proceder de la identificación de nuestra Cartera de Servicios de TI, describiendo exhaustivamente los servicios ofrecidos en términos comprensibles para el cliente.
- Requisitos de Nivel de Servicio (SLR – *Service Level Requirement*). También pertenece a la Planificación y contiene las necesidades del cliente.
- Hojas de Especificaciones del Servicio (*Specsheet*). Detallan en profundidad los aspectos técnicos contenidos en los SLR, explicando cómo se gestionará cada detalle del servicio, aportando así información para el Plan de Calidad del Servicio.
- Plan de Calidad del Servicio (SQP - *Service Quality Plan*). Documento interno que rige las actuaciones que se efectuarán para el desarrollo del servicio al cliente con el objetivo de alinear los recursos personales y TI y la ejecución del servicio y sus operaciones.
- Acuerdo de Nivel de Servicio (SLA – ***Service Level Agreement***). El principal documento del ciclo, ya en la fase de Desarrollo, detallando todos los elementos internos y del Acuerdo ante el cliente para proporcionar servicios específicos al nivel de calidad definido. Este documento debe tener una profunda difusión entre la organización y la estructura de la organización del cliente, así como ser revisado y validado con cierta periodicidad.
- Acuerdo del Nivel de Operaciones (OLA – *Operational Level Agreement*). Documento muy técnico referente sobre cómo proceder con el desarrollo del servicio, desarrollando procesos y procedimientos exclusivamente internos de la organización.
- Contrato de Soporte (UC – *Underpinning Contract*). Ordena procesos y procedimientos relacionados con los proveedores externos para la adecuada entrega del servicio, acotando y asegurando sus responsabilidades en la implementación, soporte y/o suministro.
- Programa de Mejora del Servicio (SIP – *Service Improvement Program*). Documento interno conteniendo las mejoras a realizar, con sus tiempos, prioridades, costes y responsabilidades, y que alimenta al posterior informe para el cliente con las mejoras realizadas y posibles nuevos acuerdos que pudieran contemplarse en la revisión del SLA.

II. Gestión del Catálogo de Servicio

El Catálogo deriva de la Cartera de Servicios y delimita qué servicios puede ofertar a sus clientes la organización y qué nivel de desarrollo puede alcanzar. Debe dominarlo el personal que trabaja con los SLAs y en el *Service Desk* (Centro de Servicios), con el fin de dar la mejor atención a usuarios y clientes. Debe por tanto redactarse con una adecuada terminología comercial, no excesivamente técnico, exponiendo la calidad y el nivel de servicio de forma comprensible por los interesados.

III. Gestión de la Disponibilidad

Es un complejo proceso que tiene por objeto que todos los servicios y la infraestructura TI que la organización ofrece estén tal y como se acordó en los SLAs, y por tanto estará en estrecha relación con otros muchos procesos de la Gestión de Servicios. En la figura 2-3 se refleja este proceso, que responde a tres fases diferenciadas: Planificación, Control y Monitorización.

Figura 2-3. Proceso de Gestión de la Disponibilidad

La Planificación queda plasmada sobre un Plan de Disponibilidad en el que se determinan los niveles de disponibilidad de cada servicio, equilibrados entre las necesidades del cliente y lo que puede ofrecer la organización, que permita a ésta lograr sus metas, a un coste adecuado.

Forman parte de este plan el Diseño de la Disponibilidad y el Diseño del Mantenimiento, donde se incluye la reacción ante incidencias, la coordinación desde el *Service Desk* o los tipos de disponibilidad según las necesidades de horario del cliente (24/7 o 12/5 por ejemplo).

Control supone dirigir los perfiles de acceso, los accesos a servicios y las autorizaciones, determinando la Seguridad de la Disponibilidad.

Y la Monitorización se efectúa gracias a técnicas e indicadores[11] que permiten establecer qué factores intervienen en la disponibilidad. De tal modo tenemos:

- El cálculo de la disponibilidad en tanto por ciento según la siguiente fórmula:

$$\%\ \text{Disponibilidad} = \frac{\text{Tiempo de Disponibilidad Acordado (AST)} - \text{Interrupción del Servicio durante el Tiempo de Disponibilidad Acordado (DT)}}{\text{Tiempo de Disponibilidad Acordado}} \times 100$$

- Análisis de fallos de los componentes a través de una base de datos mantenida al día que contenga y reconozca el impacto de cada fallo en cada componente de la infraestructura TI.
- El análisis de la interrupción del servicio nos permite obtener las causas de los fallos detectados y se pueden proponer soluciones.
- Con el análisis del árbol de fallos podemos estudiar de dónde proceden y cómo se desarrollan, permitiendo entender y medir las consecuencias sobre la disponibilidad.

Finalmente, la correcta gestión de la disponibilidad se compone de tres fases: detección, respuesta y recuperación, donde será fundamental la detección temprana, el registro y diagnóstico en el mínimo tiempo, y la obtención de una solución o puesta en marcha de nuevo del servicio lo antes posible.

[11] Indicadores son la muestra de la medición de las incidencias, los tiempos de resolución y los tiempos transcurridos y calificados como fallos de disponibilidad del servicio, en un formato comprensible por el cliente.

IV. Gestión de la Seguridad de la Información

Supone la adecuada gestión de todo lo que implica poner en marcha un servicio TI con respecto a la seguridad de la información, protegiendo su disponibilidad, integridad, confidencialidad y legalidad, cumpliendo los requisitos de seguridad acordados en terminos de legislación, políticas externas y contratos en los SLAs.

De nuevo aplicaremos un ciclo con fases de planificación, ejecución y seguimiento, estableciendo los objetivos de la Política y Plan de seguridad, evaluando y actualizando los procesos definidos en ellos y activando las mejoras extraídas del seguimiento y evaluación gracias al empleo de indicadores de rendimiento y auditorías de seguridad. Todo ello permitirá mejorar eficacia y eficiencia en las respuestas a incidencias de seguridad.

Es muy importante difundir las necesidades de seguridad, los protocolos establecidos y cómo actuar en cada caso, designando una autoridad y responsables en la organización.

V. Gestión de Proveedores

Busca la externalización de ciertos procesos para evitar cargas o sobrecostes en la organización, de manera que determinados proveedores den apoyo al servicio que el cliente requiere o a la infraestructura propia, ya sea a través del suministro eléctrico, del suministro de banda ancha, HW o SW, ciertos mantenimientos u otras gestiones; todo ello detallado en contratos de soporte (UCs).

Tras identificar los aspectos que tienen mayor relevancia para la organización y qué se espera de los proveedores, se suele establecer una valoración de estos, registrar las incidencias de sus productos, las ventajas y servicios postventa que ofrece cada uno, reevaluarlos anualmente y prescindir de los servicios de aquellos que no estén a la altura.

VI. Gestión de la Capacidad

Tiene por objeto que el servicio posea la capacidad de almacenamiento, rendimiento y eficiencia necesaria en el instante que se demande, reduciendo gastos por ineficiencia y manteniéndose alineada con los requisitos del cliente y la estrategia de la empresa. Todo ello monitorizando el rendimiento y alcance de la infraestructura para soportar nuevos servicios y planificando situaciones futuras con un Plan de Capacidad.

Las ventajas de tener una adecuada gestión de la capacidad serán el control de los recursos y del rendimiento reduciendo así el riesgo de disminuir la calidad del servicio, mayor eficacia en la respuesta y flexibilidad ante nuevas necesidades y finalmente la reducción de costes y el control del gasto. La figura 2-4 muestra las entradas del proceso y la documentación de salida que produce.

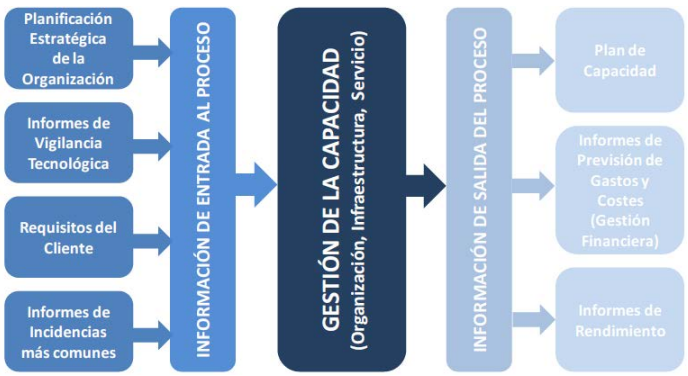

Figura 2-4. Proceso de Gestión de la Capacidad

La información de entrada se empleará para determinar qué necesidades de Capacidad hay en la organización en forma, lugar y tiempo a través de tres subprocesos de capacidad:

- De la Organización, que analiza las tendencias de Mercado y del negocio, previsiones futuras y tamaño de la organización, el volumen de negocio y los requisitos, para generar informes de gastos y costes estimados a futuro.
- De la Infraestructura, estudiando su capacidad y la de los recursos, para observar e informar sobre el empleo actual y futuro de los componentes y medios.
- Del Servicio, analizando e informando sobre el ejercicio y rendimiento de cada servicio.

Las salidas del proceso serán varios documentos e informes con recomendaciones y ajustes, entre los que destaca el ajuste del SLA en vigor, permitiendo ofrecer una mayor capacidad de la infraestructura y agrandar el abanico de servicios, o por el contrario reducir la entrega pactada ante las necesidades del cliente.

VII. Gestión de la Continuidad

La Gestión de la Continuidad (IT Service Continuity Management - ITSCM) trata de asegurar que la infraestructura y servicios vitales de la organización estén preparados para recuperar la normalidad tras un desastre natural, provocado o informático, en el mínimo tiempo posible y siguiendo dos posibles vías, la preventiva o la reactiva. Este proceso debe integrarse y ser coherente con la Estrategia de Continuidad del Negocio, que no son lo mismo; y sigue las fases de la figura 2-5.

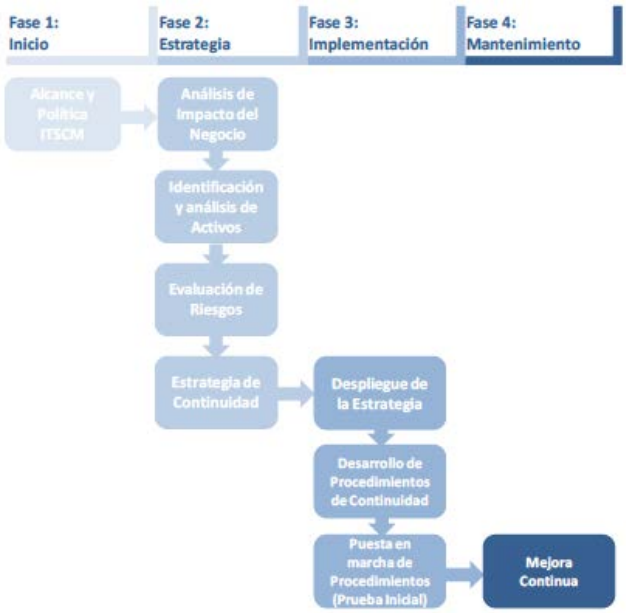

Figura 2-5. Proceso de Gestión de la Continuidad

Con el análisis de impacto se evalúa cuánto costaría al negocio la interrupción de un servicio, siendo aconsejable haber realizado previamente una valoración de los activos de los mismos, los recursos, componentes, personas, SW, etc. Habrá que determinar a qué riesgos están expuestos, conociendo sus puntos débiles y posibles amenazas; medidas que serán de utilidad para establecer las Estrategias de Prevención o Recuperación. La suma será la Estrategia de Continuidad.

El mantenimiento o mejora se consigue a través de dos vías, la formación continua del personal en nuevas amenazas, soluciones, vigilancia, gestión de conflictos y tiempo, etc, y por otro lado, a través de auditorías internas y externas.

2.1.3 Transición de Servicios (Service Transition – ST)

Se trata de un proceso que ayuda a planificar y gestionar el cambio de estado de un servicio durante su estado de vida, evitando sobrecostes, pérdidas de tiempo por adaptación, por fallos de previsión o por no haber vuelta atrás en caso de fallos de implementación.

Este volumen de ITIL se compone de los siguientes subprocesos:

I. Gestión del Cambio

Tiene objetivo hacer que los cambios producidos por la entrada en funcionamiento de nuevas aplicaciones o elementos SW/HW sean lo menos traumáticas posibles para las personas afectadas, planificando, analizando y evaluando los cambios a realizar, asegurando procesos eficientes y eficaces, para proporcionar continuidad y calidad de servicio. Todo ello generando documentación y procedimientos asociados al cambio de la infraestructura.

Es fundamental centralizar la información y almacenarla en una base de datos constantemente actualizada (*Change Management Data Base* – CMDB) que recopile todas las peticiones de cambio (*Request for Change* - RFC). La figura 2-6 es ilustrativa de la complejidad del proceso y la Gestión del Conocimiento necesarios a través de diferentes bases de datos, que aportan reducción de incidentes, poder regresar fácilmente a configuraciones previas estables gracias al establecimiento de planes de recuperación, una mejor aceptación de los cambios y proactividad del personal y mejora la estimación de costes entre muchos otros beneficios.

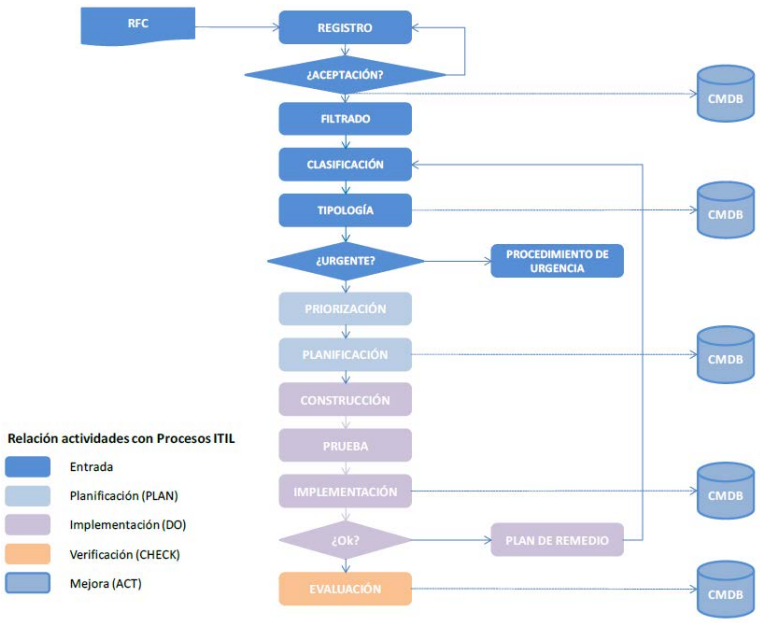

Figura 2-6. Proceso de Gestión del Cambio.

Para dirigir la gestión del cambio hay dos entes fundamentales, el Gestor de Cambios, responsable en la organización de quien depende aceptar y clasificar las RFCs, y el Consejo Asesor del Cambio (*Change Advisory Board* – CAB), que evalua, planifica y prioriza los cambios a realizar en base a datos numéricos sobre dificultad, coste, tiempo, recursos y necesidad.

En primer lugar se deben analizar las necesidades de recursos y el impacto del cambio. Durante las pruebas se evaluará la funcionalidad, usabilidad, accesibilidad e integración. En la implementación se realizará seguimiento para comprobar plazos, calidad del SW y documentación, aplicando el plan de comunicación al cliente previamente a la realización del cambio como aviso. Y finalmente la evaluación de los resultados se extrae de los indicadores de rendimiento del proceso.

II. Gestión de la Configuración

Se trata de mantener actualizada la información de la infraestructura TI de la organización, sus elementos de configuración (CI) y relaciones en la infraestructura. Son: HW, SW, personas, componentes de red y líneas de negocio.

Este objetivo se logra a través de:

- Entregar documentación e información suficiente para cooperar e interactuar con el resto de procesos de gestión.
- Controlar objetivamente los componentes de la infraestructura, produciendo informes que permitan reconocer y verificar las versiones de los CI.
- Monitorizar frecuentemente la configuración de los sistemas para cotejarla con la almacenada en la CMDB.

La comunicación entre la gestión del Cambio y la gestión de Versiones es permanente y bidireccional con la gestión de la Configuración, retroalimentando una base de datos común. Solo quedan registrados los CI autorizados, al realizar un cambio en las características registradas o en las relaciones de éste con otros componentes de la infraesructura.

III. Gestión de Versiones y Despliegues

Tiene por objeto controlar la distribución y puesta en marcha del SW y HW en el entorno de producción que haya sido autorizado en la gestión del cambio, estableciendo canales de comunicación con clientes y usuarios sobre las nuevas funcionalidades y cooperando en la actualización de la CMDB, donde se centraliza todo el conocimiento relativo a los procesos de cambio, configuración y versiones. Este proceso debe desarrollar además el plan de recuperación junto con el proceso de gestión del cambio que nos permita regresar a versiones estables anteriores en caso de fallo.

Las pruebas previas a producción serán de tipo unitarias, de funcionalidad, operativas, de integración y de rendimiento. Y tras la verificación por parte del equipo desarrollador, será el CAB, quien valide la versión final.

La implantación se podrá realizar por etapas o de manera integral (completa y todas las localizaciones al unísono), y el Centro de Servicios deberá mantener al corriente de las quejas y reclamaciones que se produzcan al proceso de gestión de versiones para su análisis. Se considera muy buena práctica desarrollar herramientas que instalen de forma automática las actualizaciones SW, así como proveer de formación a los usuarios de las nuevas versiones tras la instalación.

2.1.4 Operación del Servicio (Service Operation – SO)

Se trata de un conjunto de buenas prácticas orientadas a asegurar la prestación de servicios eficaz y eficiente, cumpliendo con las peticiones de los usuarios, solucionando posibles errores, eliminando problemas y aplicando medidas comerciales de acercamiento tanto a usuarios como a clientes. La herramienta fundamental para este fin es el Centro de Servicios.

I. Centro de Servicios

Su razón de ser es actuar como centro de operaciones, herramienta de control y coordinación de todos los procesos que soportan el servicio, punto de contacto para los usuarios aportando soluciones ante errores, registrando y siguiendo las incidencias, canalizando las peticiones de cambio y manteniendo actualizada la base de datos de configuraciones; todo, en busca de beneficios que incrementen la satisfacción del cliente. Su implementación puede ser en tres diferentes formas:

- Centro de Llamadas (*Call Center*), que recibe y transfiere a los terceros adecuados todas las llamadas entrantes de los clientes. Si además recibe emails, fax o correo postal se denomina *Contact Center*.
- Centro de Soporte (*Help Desk*), como primer escalón técnico de resolución de incidencias, problemas y dudas.
- Centro de Servicios (*Service Desk*), que suma ambas funciones anteriores y se convierte en referente único para clientes y usuarios, centralizando los procesos de gestión, canalizando las peticiones y monitorizando los SLAs.

La generación de un centro de servicios requiere un estudio previo, el sondeo a los clientes, fijar procedimientos de trabajo depurados y el compromiso de la organización a mantenerlo. Su estructura se fijará en el nivel físico (localización) y funcional (gestión). Según su ubicación, podrá ser, en función de las necesidades de continuidad, disponibilidad, por las clases de clientes, usuarios y costes:

- Local, atendiendo las necesidades de las sedes donde radican, lo cual optimiza tiempo pero no los recursos, relación entre procesos ola monitorización.
- Centralizado, atendiendo un único centro a varias sedes, lo cual reduce costes y optimiza los recursos, mejora la gestión de incidencias y la coordinación entre procesos TI. Su punto débil aparece cuando una incidencia requiere la presencia de personal técnico específico.
- Virtual, que combina las opciones anteriores, con un *service desk* virtual que dirige las operaciones. Empleado en organizaciones con sedes localizadas en ciudades y países diferentes, proporciona múltiples beneficios, pero su principal dificultad es la implantación, así como la disponibilidad y continuidad constante del servicio.

Según el servicio que definitivamente implante la organización, las opciones y funcionalidades que un *service desk* ofrecerá son: gestión de incidencias con opción a su escalado, punto de información al usuario, centro de coordinación de las actividades, lugar de contacto con proveedores y *service desk* "integral"[12].

II. Gestión de Incidencias

Este proceso busca resolver los incidentes (actuación reactiva) para recuperar con rapidez y eficacia el servicio a través del centro de servicio. Las incidencias fuera de lo común se suelen derivar a la gestión de cambios con una RFC (*Request for Change*). El proceso de gestión de toda incidencia pasa por las siguientes fases:

- Comunicación y registro, anotando detalles como servicios involucrados, causas, prioridad, impacto, recursos para la resolución y estado de la incidencia.
- Clasificación, en función del impacto y la prioridad, estableciendo un tiempo de resolución. Tiempo, impacto y urgencia podrán variar y ajustarse durante el enfrentamiento con la incidencia. La clasificación conlleva categorizar numerosos detalles, lo cual facilitará el archivo y búsqueda en la CMDB.
- Investigación y diagnóstico, comparando primero con incidencias similares en la CMDB.
- Escalado, funcional o jerárquico, cuando en primera instancia no puede darse solución a la incidencia.

[12] Service Desk "integral" es un concepto que añade un servicio de información, peticiones y resolución de incidencias interno para la organización, donde el service desk se relaciona, además de con las TI, con otros departamentos de la organización, ahorrando costes en la gestión de asuntos internos, generalmente relacionados con recursos humanos.

- Seguimiento, ya sea atendida por la Gestión de Incidencias o por la Gestión del Cambio, actualizando las bases de datos de incidencias y de configuración (CI) y comunicando la solución alcanzada a clientes y usuarios.

III. Gestión de Problemas y Errores

Trata de investigar y analizar los problemas que afectan al servicio, identificando las causas y proponiendo soluciones que faciliten evitar que se repitan, con una actitud proactiva para predecirlos.

El trabajo frecuente sobre los problemas llevará a convertirlos en errores conocidos, cuyas causas ya han sido determinadas. Hay dos caminos de actuación, el reactivo tras ocurrir el incidente y el proactivo, que monitoriza la infraestructura TI con el objetivo de prevenir las incidencias. Este último, aunque aumenta los costes iniciales por necesitar técnicos específicos, disminuye notablemente los problemas, y aporta mayores beneficios, como reducir los gastos infringidos por las incidencias.

Este proceso sigue caminos similares a otros vistos anteriormente, con las siguientes fases:

- Identificación y registro.
- Clasificación.
- Investigación y diagnóstico.

Reconocidas las causas se podrá entregar una solución temporal a la gestión de incidencias, hasta que la gestión de cambios dé con una solución definitiva. En este instante el problema es identificado y aceptado como un error conocido y pasa a pertenecer a la gestión de errores.

Este subproceso, gestión de errores, empieza al identificar un error conocido, es decir, tras localizar la configuración causante o el componente, ya sea SW o HW, y sigue fase similares al subproceso de gestión de problemas. La solución definitiva propuesta debe ser valorada para sopesar si es asumible en costes y proporciona unos beneficios contundentes.

2.1.5 Mejora Continua del Servicio (Continual Service Improvement – CSI)

Este proceso procede del mismo concepto aplicado a cualquier sistema de gestión, el Ciclo de Mejora de Deming o ciclo PDCA (*Plan, Do, Check, Act*). Se necesita conocer nuestro servicio y definirlo, para aplicarle indicadores de medición de sus actividades que nos den una referencia para mejorarlo. Hay múltiples documentos que definen el concepto "gestión por procesos", pudiendo adoptar "la aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacciones entre estos procesos, así como su gestión para producir el resultado deseado"[13].

Los indicadores de medición, o métricas, servirán para medir, analizar y revisar los servicios, la gestión de sus procesos y sistemas vinculados. Estas vendrán reflejadas en documentos como el SLA, procederán de los diferentes procesos de la gestión de servicios vistos hasta ahora y serán datos del tipo: cantidad de problemas provocados por la escasez de capacidad, cantidad de cambios para solucionar los citados problemas, número de incidentes, interrupciones de servicio en un periodo de tiempo, porcentajes de inversión en componentes por año, etc.

En resumen, todas las acciones sobre la infraestructura de TI, la organización, y las relaciones con usuarios, proveedores y clientes, se gestionan a través de procesos que han de ser pulidos mediante el análisis de indicadores que aporten información para cerrar el ciclo de mejora activando soluciones.

[13] Concepto "gestión **por** procesos" extraído de la serie ISO.

2.2 ISO

ISO, Organización Internacional de Normalización, es una federación de organismos nacionales que prepara a través de comités técnicos normas reconocidas internacionalmente. Existen normas ISO para multitud de productos y todas tratan de desarrollar una gestión por procesos que aporte calidad en el producto y en sus propios procesos, integrándolos además con procesos generales y de otros servicios, como los de recursos humanos, apoyo a la dirección o de soporte. A continuación se verán algunas de las normas relacionadas con organizaciones del sector TIC.

2.2.1 ISO 9001:2015. Gestión de la Calidad

Supone definir las actividades de la organización de una forma medible y con posibilidad de mejora, asegurando al cliente que sus procesos son gestionados de la mejor manera posible para prestar un servicio eficiente, evaluable por un agente externo y en un ciclo de mejora continua. Trata de aportar eficiencia, optimizar recursos, evitar incidencias y fallos y facilitar la toma rápida de decisiones en base a la información extraída de indicadores. Esta norma, aplicada específicamente al ámbito de desarrollo software y con una mayor profundidad técnica, se convierte en la ISO/IEC 90003:2018.

2.2.2 ISO/IEC 27001:2013. Gestión de la Seguridad de la Información

Esta norma está compuesta de múltiples procesos de gestión que generan procedimientos y documentación también vistos en ITIL, como son: la Política y el Plan de Seguridad, Evaluación de Riesgos, Gestión de Proveedores, Auditorías y Mejora Continua entre otros. Busca asegurar que la organización que la implemente proteja la información de sus procesos, localizada en servidores y documentos, en sus diferentes dimensiones (confidencialidad, integridad, disponibilidad y legalidad).

2.2.3 ISO/IEC 20000:2018. Gestión de Servicios de TI

Se trata de una norma que se puede auditar y valorar en una organización para otorgarle la certificación de su sistema de gestión de servicios (SGS) de TI. Es totalmente compatible con el modelo ITIL, con una gran diferencia: la primera se puede aplicar de múltiples formas, sin ser evaluable y a demanda, mientras que ISO supone una auditoría completa, con numerosos requisitos que cumplir para certificar a la organización, y que debe desarrollar todos los procesos y documentación que la norma contempla.

Se compone de 5 partes, de las cuales tres son informes técnicos. Las otras dos son las que describen las especificaciones (parte 1) y el código de buenas prácticas (parte 2).

I. Parte 1: Reúne los requisitos para proporcionar unos servicios de TI en línea con las necesidades del negocio, de calidad y valor añadido para los clientes, optimizando costes y garantizando la seguridad de la entrega permanentemente. Garantiza seguir un ciclo de mejora continua en la gestión de los servicios y supone en su totalidad un completo sistema de gestión basado en procesos de gestión de servicio, políticas, objetivos y controles.

Los procesos identificados en esta norma se agrupan en 5 bloques:

- Provisión del Servicio
  - Gestión de Nivel
  - Generación de Informes
  - Gestión de la Continuidad y Disponibilidad
  - Elaboración de Presupuestos y Contabilidad
  - Gestión de la Capacidad

- Gestión de la Seguridad de la Información
- Control
  - Gestión de la Configuración
  - Gestión del Cambio
- Entrega
  - Gestión de la Entrega
- Resolución
  - Gestión de Incidencias
  - Gestión de Problemas
- Relación
  - Gestión de las Relaciones con el Negocio
  - Gestión de Suministradores

II. Parte 2: Recoge un amplio conjunto de buenas prácticas, basadas de hecho en ITIL, que sirven como referencia y apoyo en la implementación de actividades de mejora del servicio y preparación ante la certificación.

Los requisitos definidos en la norma incluyen la planificación, el diseño, la entrega y la mejora de los servicios para cumplir los requerimientos y aportar valor; y la organización no puede prescindir de ninguno de ellos si pretende obtener la certificación (figura 2-7).

El sistema de gestión de

REGIMIENTO DE TRANSMISIONES 22 (Ejército de Tierra)

Avda. Radiotelevisión 6
28223 Pozuelo de Alarcón. Madrid. España

Ha sido evaluado y certificado en cuanto al cumplimiento de los requisitos de

ISO/IEC 20000-1:2005

Para las siguientes actividades

El alcance de certificación está indicado en la página 2 de este certificado.

Cualquier aclaración sobre el alcance de este certificado y la aplicación de los requisitos de la norma ISO / IEC 20000-1:2005 se puede obtener consultando a la organización.

Este certificado es válido desde 14 Mayo 2012 hasta 14 Mayo 2015 y permanece válido a condición de satisfactorias auditorias de seguimiento
Auditoria de renovación antes de 27 Abril 2015
Edición 1. Certificado desde 14 Mayo 2012

Esta es una certificación multi-emplazamiento.
Los emplazamientos adicionales se indican en la siguiente página.

Autorizado por

Álvaro Rodriguez de Roa
Director de Seguridad de la Información y Gobierno TI SGS ICS
SGS ICS Ibérica, S.A.
C/ Trespaderne 29,
28042 Madrid- España

SYSTEM CERTIFICATION ISO/IEC 20000 SGS

APMG-International ISO/IEC 20000

Figura 2-7. Ejemplo de Certificado ISO 20000

En común con otros referentes de buenas prácticas en la gestión de servicios, ISO contiene un capítulo específico de vocabulario y terminología con definiciones estandarizadas y compartidas con ITIL, como son, mejora continua, acciones correctivas, monitorización y medición en base a métricas, objetivos, proveedores externos, política y estrategia, procesos, riesgos, incidencia, problema y error

conocido, disponibilidad, catálogo de servicios, continuidad, acuerdo de nivel de servicio (SLA) y valor entre muchos otros.

Del mismo modo, muchos de los documentos de un SGS son comunes a ITIL: Alcance, política, plan y objetivos del SGS, política de gestión de cambios, de seguridad de la información y planes de continuidad, procesos del SGS, requisitos de servicio, catalogo/s de servicios, acuerdos de nivel de servicios (SLA), contratos y acuerdos con proveedores externos e internos, procedimientos requeridos por la norma y registros necesarios para demostrar su cumplimiento para la acreditación.

2.3 DevOps

Entre los referentes y estándares internacionalmente reconocidos por múltiples empresas, encontramos un método llamado DevOps, que ha demostrado ser muy eficaz para incrementar la eficiencia y mejorar los tiempos de entrega. Su nombre es acrónimo de *Development & Operations* y es la combinación de buenas prácticas y herramientas específicamente desarrolladas para incrementar la capacidad de una empresa para proveer servicios y aplicaciones SW en menos tiempo que empleando los procesos de desarrollo tradicionales, entregando mejor servicio a los clientes y siendo más competitivos en el mercado.

Este marco de trabajo busca alinear a los equipos envueltos en el desarrollo y operaciones de los productos de software, para que trabajen codo con codo desde su concepción hasta la entrega y soporte. Lo hace a través de una filosofía, maneras y herramientas que promueven la integración de las funciones de desarrollo y operaciones y que se han convertido en poco más de una década en una disciplina con procesos propios. Nació como conjunto de ideas y principios para la administración de sistemas ágiles, aplicados por primera vez en Google, donde se encuentran los inicios de la metodología actual.

A continuación repasaremos algunas de estas nuevas tendencias aplicadas al desarrollo de SW:

Para reducir o eliminar los errores humanos, los cambios implementados al desarrollo se hacen de forma automática; la compilación de código, realización de test o el análisis de calidad de código se automatizan impulsando un proceso de integración continua (C*ontinuous Integration* – CI). Esto permite la detección rápida de fallos de forma continua, aumentar la productividad del equipo, automatizar y ejecutar de inmediato los procesos y la monitorización continua de las métricas de calidad del proyecto, debiendo obtener un sistema preparado para ser lanzado. Los componentes del equipo integran diariamente su trabajo y cada integración se verifica a través de una compilación automatizada que incluye pruebas y test para detectar errores de integración lo antes posible. Así se mejora la productividad del desarrollo, reduciendo el número de fallos de integración, detectando errores pronto, efectuando cambios y entregando valor con mayor rapidez y con transparencia en el proceso.

Si todos los resultados obtenidos fueran correctos se podría activar también un proceso de despliegue continuo (C*ontinuous Deployment* – CD) que permita disponer de la nueva aplicación con sus cambios añadidos para probarla en entornos de integración de manera agil, fiable y automática, obteniendo así despliegues predecibles, automáticos y rutinarios sin tener que renunciar a la calidad y estabilidad gracias a la CI anteriormente aplicada.

Las ventajas de la integración y entrega continua se pueden enumerar en:

- Lanzamientos de incrementos o mejoras de código de bajo riesgo, en cualquier momento y según se necesite a demanda o de forma automática.
- Reducción de tiempos entre la comunicación de la necesidad de un cambio o mejora hasta que se despliega en producción para su empleo por el cliente.

- Mejora de la calidad centrando a los desarrolladores en las evoluciones gracias a la automatización de tests en la integración continua.
- Reducción de costes por realizar y entregar cambios incrementales al software, al invertir en desarrollo, pruebas y configuraciones automáticas que eliminan muchos costes fijos asociados al lanzamiento.
- Productos mejores trabajando en ciclos pequeños que permitan entregar al cliente "entregables" para su validación y llevarlo a producción. Se evitan periodos prolongados trabajando en una característica que finalmente ni interesa ni aporta valor al negocio (se aplica el concepto "falla rápido, falla barato").
- Satisfacción del personal gracias a cambios menos sufridos para el equipo, rapidez y automatización de procesos y permitiéndoles centrarse en lo que les satisface, según especialización y cometidos, para dar valor al cliente.

Los siguientes pasos serán llevar el nuevo producto a entornos de preproducción y producción mucho más estables, pues es posible que terceros lo estén empleando para integrarse con el nuestro.

Los desarrolladores emplearán su propio entorno local de programación (su IDE-*Integrated Development Environment*), para realizar desde tareas básicas como la codificación hasta las más avanzadas. Hay múltiples opciones, y se conectan y entienden a través de Git, un sistema de control de versiones distribuido, de código abierto y gratuito, que permite guardar código fuente y los cambios realizados fusionándolos con los del repositorio común entre desarrolladores.

Aplicando un modelo de desarrollo basado en diferentes ramas de Git sobre un repositorio central aplicamos Git Flow, obteniendo un importante control, mantenimiento y soporte de las distintas versiones del proyecto para volver atrás en caso necesario; siendo muy útil al trabajar en grandes características nuevas entre varios desarrolladores y evitar desarrollos incompletos. Siempre se almacenan dos ramas principales y paralelas, *master* y *develop*, sobre las que se avanza en el desarrollo, apoyadas por otras ramas de soporte con vida limitada (*feature* para el desarrollo de nuevas funcionalidades para las próximas versiones, *release* para preparar nuevas versiones de producción, pequeñas correcciones de errores y preparación de metadatos, y *hotfix* para la corrección inmediata de errores críticos en una versión de producción).

En el caso de grupos de desarrolladores muy experimentados y maduros que actúen directamente sobre la rama principal común a todos, estarán aplicando una forma de trabajar conocida como *trunck based development*, cuya ventaja principal es que las integraciones de cambios sobre la rama principal son más sencillas de resolver por ser más acotadas, al hacerse más frecuentemente, y se reduce la cantidad de errores que conllevan.

Superadas las pruebas locales el producto se traslada a entornos de integración lo más parecidos al entorno de producción, pero siempre hay diferencias y particularidades. Ante los riesgos de la introducción de parámetros manualmente y generar errores, DevOps ofrece los conceptos de integración y despliegue continuo, junto a infraestructura como código (*Infraestructure as Code* – IaC) y configuración como código (*Configuration as Code* - CaC) para que los desarrolladores se centren en desarrollar y que otras tareas como configurar entornos, subir cambios y desplegarlos sean automáticas y predecibles.

La IaC supone disponer de toda la infraestructura de la empresa necesaria para que nuestra aplicación funcione, con todos sus componentes, ya sea on premise o cloud, disponible en ficheros, y que además los mantengamos versionados en el repositorio de código con su historial de cambios. Esto nos permitirá automatizar su despliegue y regresar a versiones anteriores ante fallos. Supone un método de acopio y gestión de nuestra infraestructura mediante código que aporta un desarrollo más rápido y eficiente, permitiendo la reutilización y automatización, ofreciendo entornos estables y a escala reduciendo tiempos de paso a producción y lanzamiento a mercado.

La CaC es un proceso para administrar datos de configuración de una aplicación, es decir, "la migración formal de la configuración entre entornos, respaldada por un sistema de control de versiones"[14].

De nuevo enumeramos las ventajas de IaC y CaC:

- Trazabilidad, pudiendo regresar a versiones anteriores mientras localizamos el cambio que introdujo el fallo.
- Reutilización de las mismas configuraciones para obtener los mismos escenarios.
- Agilidad y eficiencia automatizando la administración de recursos y optimizando el ciclo de vida de desarrollo de SW.
- Escalabilidad alta pudiendo añadir instancias de aplicaciones fácilmente y rápido al trabajar con recursos cloud virtualizados, así como retirarlos tan pronto ya no sean necesarios.
- Reducción de riesgos e infraestructura invariable garantizando la uniformidad del sistema descartando errores humanos con su automatización.
- Incrementa la seguridad al repetirse las configuraciones de forma automática, por lo tanto los mimos estándares de seguridad pueden cumplimentarse.
- Mejora a la documentación ya que el propio repositorio de código nos desvela con más exactitud el contenido de cada máquina.

2.4 SRE Google

Otro concepto que también se originó como remedio para pulir los roces entre grupos de trabajadores y engranar las tareas de programadores, desarrolladores y equipos de operaciones de SW es SRE (*Site Reliability Engineering)*, que nació también en Google, con el fin de lanzar al mercado productos trabajados simultáneamente por ambos grupos desde el inicio, al igual que DevOps. Trata de solucionar la misma problemática fomentando fiabilidad, responsabilidad e innovación en los productos.

SRE es un modelo que emplea los múltiples aspectos del desarrollo del SW y lo aplica a problemas y tareas específicas en operaciones de TI. Mientras DevOps se centra en añadir eficiencia al proceso completo de desarrollo de software, SRE procura equilibrar la confiabilidad del sitio con la generación de nuevas características, convirtiéndolo en un producto altamente escalable.

Los ingenieros en este caso, además de ser responsables del entorno de producción y su estabilidad, están comprometidos en la búsqueda de nuevas funciones y mejorar la operatividad. Dentro de SRE se establecen medidas para la confiabilidad de los servicios (*Service Level Objective* – SLO), enmarcados en un acuerdo SLA y empleando una métrica específica, como puede ser el tiempo de actividad o el tiempo de respuesta. Los SLOs vienen a ser los compromisos individuales adquiridos dentro del acuerdo total o SLA.

Los técnicos SRE son responsables de la disponibilidad, continuidad, y de monitorizar y actuar ante incidentes sobre la infraestructura y servicios que la organización maneja y ofrece a sus usuarios y clientes.

Según su creador, Ben Treynor, los principios básicos de SRE Google son los siguientes:

- Contratar solo personal programador, pues la principal responsabilidad de un ingeniero SRE es escribir código. Al ponerlo a realizar operaciones intentará automatizar su labor.
- Definir para cada servicio un SLO, que será su nivel de disponibilidad.
- Emplear este SLO como medida de su rendimiento y efectuar informes.

[14] Guía completa de DevOps, v.4. para directivos y técnicos.

- Emplear un presupuesto de error como criterio de lanzamiento. Según la disponibilidad que se pretende alcanzar, el presupuesto es uno menos el SLO. Ese tiempo de indisponibilidad será el presupuesto marcado y que se puede consumir realizando lanzamientos y otras tareas de prueba fallidas sin llegar a rebasarlo. La perfección absoluta no se considera como resultado realizable, teniendo más contras que pros el intentar alcanzarla (será más caro, técnicamente complejo e inalcanzable, el usuario apenas lo notará, supondrá más tiempo de retraso en el lanzamiento y despliegue del producto, etc)
- Tanto ingenieros como desarrolladores SRE pertenecerán al mismo equipo de personal, sin separación que los diferencie, invitando a los desarrolladores a realizar tareas de ingeniero SRE y permanencer si lo desean.
- Las tareas excedentes de operaciones recaerán sobre el equipo de desarrollo.
- Organizar las tareas de los ingenieros SRE para que tengan una carga operacional del 50% y otro 50% para la automatización y mejora de la fiabilidad.
- El equipo SRE comparte un porcentaje mínimo del trabajo de operaciones con el equipo de desarrollo. Si se añaden funcionalidades que desestabilizan el sistema, el equipo SER devuelve el producto a los desarrolladores, pues no está listo para soporte, y lo asumirán a tiempo completo hasta quedar listo para ser soportado en producción.
- Organizar equipos de guardia con ocho ingenieros como mínimo o seis si se trata de dos localizaciones distintas, para garantizar un trabajo aceptable sin caer en el cansancio.
- Cada ingeniero podrá afrontar el ciclo completo de 2 incidencias como máximo en su turno (registro, actuaciones, revisión, notificación, etc). En todos y cada uno de los eventos se centrarán en el proceso y la tecnología, no en buscar culpables, ya que suele tratarse normalmente del propio sistema, el proceso, su entorno o los componentes tecnológicos.

2.5 Entrega de Servicio en la OTAN por NCIA *(Enterprise Service Delivery Model - ESDM)*

En este subapartado se presenta el modelo de entrega de servicio seguido desde 2016 en el ámbito OTAN, del cual emana un plan trianual (*Service Delivery Plan - SDP*) que es revisado anualmente. Resume cómo, aplicando los estándares de calidad de gestión de servicios vistos en los apartados anteriores, la *NATO Communications and Information Agency* (NCIA) provee servicios de ICT (*Information and Communication Tecnology*), incluyendo servicios C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*) desde sus Centros de Apoyo a Unidades (CSUs); lo cual será modelo y soporte para la propuesta realizada en este trabajo.

La Agencia emplea este documento como modelo genérico para definir modelos de entrega en particular para cada servicio de su portfolio, incluyendo los roles, responsabilidades, obligaciones y autoridades asignadas.

Los servicios que la Agencia provee son de tres tipos que, de un modo u otro, se encuentran entrelazados y con múltiples interdependencias (figura 2-8):

- Servicios de cara al cliente (lo que el cliente, los usuarios, podrían solicitar).
- Servicios de apoyo (que hacen posible muchos de los Servicios de cara al cliente). Por ejemplo, atención al cliente, redes, ciberseguridad, almacenamiento, capacidad de servidores, gestión de servicios, servicios de verificación y validación independientes, Oficina de Gestión de Programas…) pero que generalmente el cliente no solicitaría.
- Servicios facilitadores (que apoyan o controlan la entrega de los dos tipos anteriores). Por ejemplo, servicios de Adquisición, Logísticos, Financieros, Recursos Humanos, Aseguramiento de la Calidad, servicios de Arquitectura, de Gestión de Riesgos y todos aquellos que incluyen procesos como Gestión de Cambios y Gestión de Activos y Configuración del Servicio.

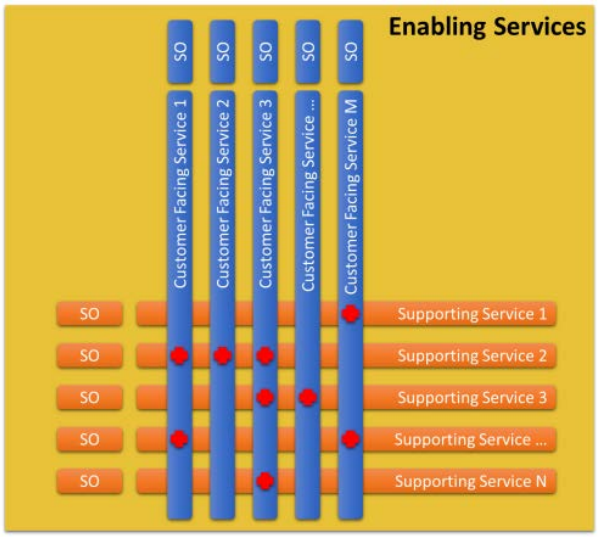

Figura 2-8. Relación entre los servicios de cara al cliente, de apoyo y facilitadores.

2.5.1 Entidades relacionadas y niveles de apoyo

Las principales unidades vinculadas en la entrega de los servicios CIS gestionados son: Los *CIS Support Units* (CSUs), el *Operations Centre* (Ops Cen), las *Service Lines* (SLs) y los elementos de apoyo de nivel 3.

Los niveles de apoyo establecidos son los siguientes:

- Nivel 0. Aquel que puede ser llevado a cabo por el usuario final sin interacción con ningún miembro del equipo técnico externo, aunque sí guiados por un servicio automático de atención al cliente (*Service Desk*).
- Nivel 1. Es el primer nivel con asistencia técnica. Todas las solicitudes de servicio y comunicación de incidentes (*Trouble Tickets* (TT)) serán cargadas, categorizadas, priorizadas, diagnosticadas y gestionadas. Servicio proporcionado por un Centro de Atención al Usuario (*Centralised Service Desk* – CSD) localizado en el Ops Centre, responsable también de la coordinación y escalado cuando sea necesario a otro nivel de apoyo.
- Nivel 2. Supone la intervención de personal técnico cualificado más allá de la aportación disponible en el nivel 1. Este nivel requiere permisos de administración completos en el equipamiento del usuario y en el del servicio afectado. Lo provee el *Service Support Centre* (SSC), unidad integrada en el Ops Cen y gestionado principalmente por personal de las SL.
- Nivel 3. Es el máximo nivel, con especialistas disponibles en la Agencia y que enlaza con proveedores de servicios y productos externos. Lo componen *Subject Matter Experts* (SME) de las SLs y proveedores externos.

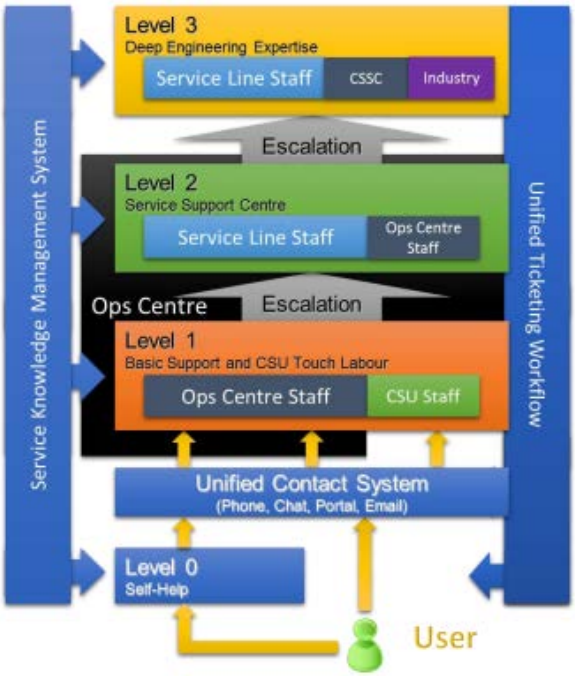

Figura 2-9. Niveles de asistencia y relaciones.

El ESDM se basa en los roles necesarios para cada servicio. Es intencionadamente genérico y con vistas a futuro, pudiendo necesitar adaptaciones individuales por servicios. Cualquier adaptación solicitada por un *Service Owner* (SO) tendrá que ser confirmada por el ESDM *owner*, el *Chief Service Strategy Innovation*.

2.5.2 Service level Agreement (SLA)

La calidad y los tipos de servicios a entregar estarán completamente definidos en un documento oficial de acuerdo entre las partes, CSU y Cliente, el *Service Level Agreement* (SLA). Este acuerdo es revisado y firmado anualmente y recoge los servicios a entregar obtenidos del catálogo ofertado por la Agencia. El ciclo de SLAs se inicia con la revisión de este portfolio, añadiendo, modificando o eliminando servicios del mismo.

El Comandante del CSU (*CSU Commander*) y su personal tendrán un papel fundamental en la Gestión de la Relación con el Cliente (*Customer Relationship Manegement* - CRM), participando directamente en la negociación de los SLAs locales, recopilando *feedback* de los usuarios y comunicando las evoluciones de los servicios al cliente.

Además de los servicios empleados en el día a día, se incluirán todos aquellos previstos para apoyar ejercicios, operaciones y actividades adicionales. La negociación de cada uno de ellos será responsabilidad del *CSU C*ommander, verificando los términos acordados con los *Service Owners* (SOs) antes de proceder a firmar cualquier acuerdo o modificación.

2.5.3Principales Roles en el ESDM

I. *Service Management Authority (SMA).*

Será quien controle la correcta cualificación del personal designado como *Service Delivery Manager* (SDM) en la Agencia, desarrollando las líneas de cualificación y experiencia para el puesto, asegurando que ejercen sus responsabilidades de acuerdo a las directivas e instrucciones en vigor y

asignándolos adecuadamente a cada servicio con el fin de mantener los mayores estándares de calidad del puesto.

II. *Service Delivery Portfolio Owner (SDPO)*

El *SL Chief*, *CSU Commander*, *CSSC Commander* u otro miembro cualificado podrá ser responsable de un portfolio de servicios asignado y a su juicio estará, en el ejercicio de tal responsabilidad, el asignar personalmente cada servicio a personal de su unidad organizacional (figuras 2-9 y 2-10).

III. *Service Owner (SO)*

Será responsable ante el *SL Chief* de los siguientes términos:

- Ciclo de vida del servicio/s asignado/s y de su Mejora Continua (*Continual Service Improvement* – CSI).
- Velar por la entrega de servicio conforme a los requisitos acordados con el cliente, supervisando las tareas del SDM responsable de la entrega de cada servicio y de los *Change-Proyect Managers* (C-PMs) que trabajen para la entrega de cambios y pequeñas mejoras de sus servicios.
- El desarrollo de la instrucciones de implementación de sus servicios, coordinar todos los cambios y mejora continua, así como la transición a nuevos servicios de las nuevas capacidades, mejoras y cambios.
- Definición e informe de los niveles *Key Performance Indicators* (KPI) alcanzados y las métricas asociadas a sus servicios de responsabilidad en coordinación con su SDM.
- Actuar como punto de decisión para el escalado de las incidencias relevantes relacionadas con su servicio.

IV. *Service Delivery Manager (SDM)*

Responderá ante el SO de la entrega diaria del servicio asignado de acuerdo a los parámetros establecidos en el SLA, así como supervisar el establecimiento y mantenimiento de su *baseline*.

Es responsable de la correcta planificación para la entrega del servicio, monitorizando e informando de los KPIs y métricas asociadas, contabilizando el tiempo dedicado a su apoyo y entrega y realizando coordinación de alto nivel para los cortes y cambios programados.

También lo es de la mejora continua del servicio y alcanzar los objetivos de eficiencia y eficacia en la entrega acordada. Monitorizará incidentes y problemas que afecten a su servicio, estará preparado para las revisiones rutinarias en representación de la Agencia y para la preparación y presentación de los informes semanales y mensuales del servicio.

V. *Change-Proyect Manager (C-PM)*

Trabajará en la introducción periódica de mejoras en el servicio, en la corrección de pequeñas deficiencias, implementación de parches, etc. Según la envergadura del cambio, ciertas categorías podrían ser delegadas en un *Change Coordinator / Manager* local, en el propio CSU.

Implementará los cambios en la *baseline* de acuerdo con la dirección del SO (costes, calidad, objetivo). Y en coordinación con el SDM planeará y entregará ñas actividades necesarias para la adecuada transición a operaciones del cambio, actualizando las instrucciones relevantes, la documentación y las necesidades de adiestramiento del personal, incluido el usuario final.

VI. SL SME Level 2

Estará localizado en el Ops Cen SSC para desempeñar sus funciones y responsabilidades ante el SDM en lo relativo a:

Resolución de problemas que superen las capacidades al alcance del Nivel 1, pero menores al 3; aplicando parches, manejando incidentes y peticiones, monitorizando servicios en el marco global de la Organización, la Gestión de Eventos, el Apoyo al Cambio en el Servicio, y la aplicación de procedimientos y soluciones de contingencia, entre otros.

Proporcionará informes precisos posteriores a la resolución de incidentes y problemas para la base de datos del sistema de Gestión del Conocimiento (*Service Knowledge Managemnt System* – SKMS).

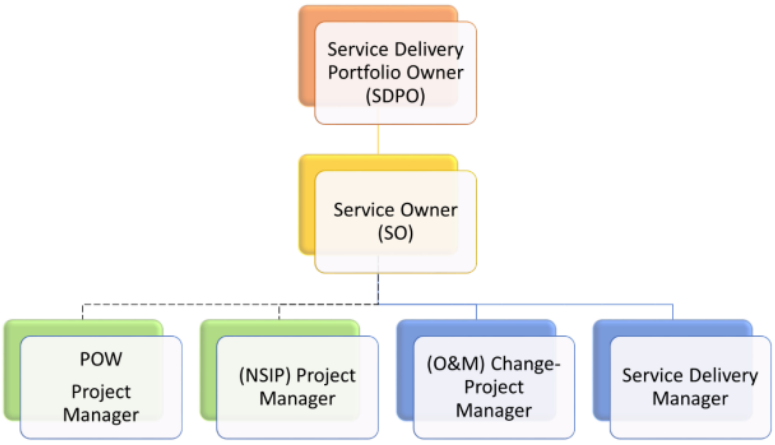

Figura 2-10. Relación entre SDPO, SO, SDM, PMs y C-PM.

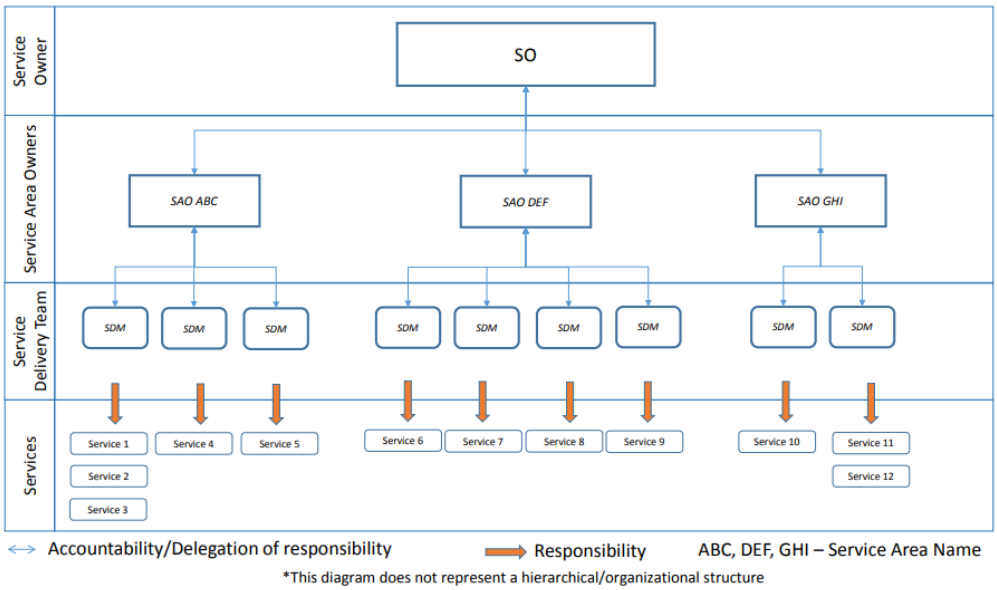

Figura 2-11. Relaciones funcionales en la operación y cambio de servicios.

VII. *Operations Centre (OpsCen) Roles.*

Posiblemente el elemento más crítico para la operación de los servicios sea el OpsCen, que debe ser flexible y sensible a las necesidades de los clientes, estar preparado para hacer de enlace entre las comunidades de usuarios y proveer los servicios de acuerdo a lo acordado en los SLAs, según las prioridades operacionales y el estado de los medios técnicos.

Se compone de tres partes: el *Operations Centre Command Cell* (OCCC), el CSD, y el *Service Support Cell* (SSC). Aunque opera como entidad única, el OpsCen, está repartido físicamente entre dos localizaciones geográficas (Mons y La Haya) y es responsable de los SOs para la asistencia de niveles 1 y 2 a los servicios.

El CSD gestiona el ciclo de vida de los TTs, asegurando que están correctamente cargados, priorizados según su relevancia en el SLA, asignados para resolución, y que el trabajo es realizado de acuerdo a los tiempos de respuesta estipulados en el acuerdo, así como cerrados en tiempo y forma. Contacta con el CSU cuando sea necesaria su asistencia para resolver incidencias que requieran la manipulación física.

Todo el nivel 2 de asistencia a servicios, monitorización, administración y resolución de incidentes será realizado desde el OpsCen, para lo que su personal necesitará los apropiados privilegios de administración. El CSD está atendido 24/7 y el OpsCen asegura la asistencia de nvel 2 y 3 para todos los servicios centralizados (aquellos comunes a todos los usuarios) 24/7/365. Será necesario el contacto estrecho para proveer una imagen exacta de la situación y resolver conflictos entre prioridades de diferentes clientes y usuarios.

VIIa. *OpsCen Duty Control Officer (DCO)*

Responde ante el *Ops Centre Chief* del desarrollo eficaz de las operaciones del centro, del informe diario de la situación, y de los incidentes de alto nivel. Coordinará la gestión de estos, verificando el correcto escalado en su gestión.

Gestiona las actividades del CSD y sus supervisores, actuando como punto de escalado de las incidencias para estos. Coordina la implementación de todos los cambios, programándolos para su ejecución en los momentos de menor impacto y riesgo para los usuarios.

Supervisa que las acciones tomadas para cada incidente son las correctas, asegurando que todos los procesos en la toma de KPIs se cumplen.

VIIb. *CSD Agent*

Será responsable de atender, monitorizar, hacer seguimiento y comunicar los incidentes, peticiones de servicio, problemas y *feedback* de los usuarios.

Analizará, identificará y categorizará los *tickets*, asignándoles una prioridad inicial de acuerdo al SLA y resolviendo los incidentes dentro de los límites de su conocimiento y adiestramiento en el nivel 1 de asistencia. Les dará escalado si fuera necesario y les hará seguimiento.

Cerrará cada incidencia a través de la aplicación de informes y gestión de incidencias, siempre tras confirmar su resolución con el usuario.

VIII. *CSU Roles*

En relación a los servicios centralizados, el CSU constituirá el último paso en la entrega de estos al usuario final. A este respecto, su personal apoyará al *Service Delivery Manager* a que los servicios alcancen los niveles contratados. También dará apoyo a los directores de proyectos (*Proyect Managers* –PM) en la entrega de cambio o mejora de los servicios.

Para los servicios entregados localmente, el CSU tendrá una mayor responsabilidad; correspondiéndole casi en su totalidad los niveles 1, 2 y 3 de asistencia a estos servicios. Normalmente los *tickets* serán elevados, encauzados y priorizados en el CSD, pero el esfuerzo por su resolución delegado a los CSUs.

VIIIa. *CSU Commander*

Será el director de Gestión de la relación con el Cliente (*Customer Relationship Management - CRM*), entre la Agencia y los usuarios locales, respondiendo ante los SDMs de la asistencia diaria en la entrega de servicios.

Supervisará la correcta dedicación en tiempo y esfuerzo de su personal a la resolución de las incidencias encomendadas y se responsabilizará de la entrega de los servicios específicos locales, tal y como se haya acordado en los SLAs.

2.6 Ejemplos de Gestión de Servicios en Defensa y en la Armada

2.6.1 Gestión de la Demanda. Solicitud de un nuevo servicio en el MDEF

Como se adelantó durante la introdución, en la Política CIS/TIC (Orden DEF/2639/2015) del MDEF se exponen los siguientes principios: la orientación a servicios, identificando la información como un valor estratégico, la centralización, estableciendo una visión global y común de los CIS/TIC; y eficiencia en la obtención y uso de los CIS/TIC, empleando productos ya desarrollados y evitar duplicidades.

Como herramienta para conseguir estos objetivos, se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa[15] (AG CIS/TIC), al objeto de imponer coherencia e integridad técnica en el desarrollo de las Capacidades CIS/TIC que el MDEF requiere. En el mismo documento se organizan los Servicios CIS/TIC en: Servicios y Aplicaciones de Usuario, Servicios de Infraestructura Tecnológica, Servicios de Seguridad de la Información y Servicios de Gestión.

A su vez, existen una serie de acuerdos técnicos entre la Jefatura CIS de las FAS (JCISFAS) y el CESTIC que regulan los pasos a seguir en las distintas fases del ciclo de vida de los servicios en el ámbito operativo, dentro del marco de la Infraestructura Integral de Información para la Defensa (I3D). Actualmente, mientras no se alcance la total operatividad de esta Infraestructura, el CESTIC ha promulgado una Instrucción Técnica (IT) que regula el proceso a seguir para solicitar nuevos servicios CIS/TIC en el MDEF[16] o cambios de gran impacto en servicios existentes, donde se incluyen peticiones para operaciones, maniobras y ejercicios de las FAS, definiendo además las relaciones entre el CESTIC y los diferentes ámbitos del MDEF a través de sus organismos autorizados.

Este proceso facilita y estandariza los trámites de cada solicitud, automatiza el control del tiempo de respuesta y atención desde el CESTIC, y encauza la correcta implementación de la Política CIS/TIC, especialmente la aplicación de los principios de centralización y eficiencia en la obtención y uso de los recursos CIS/TIC.

Al igual que se ha visto en la organización de la NCIA en el ámbito OTAN, en este proceso de solicitud también se establecen ciertos roles.

- Ambito solicitante. En nuestro caso, es la Armada uno de los siete establecidos dentro del MDEF para centralizar y comunicar con el CESTIC.
- Interlocutor del ámbito. En la Armada, ya vimos en la organización de la JECIS el COE-AR como tal interlocutor.
- Gestor de solicitudes. Pertene a la SEGENER del CESTIC.
- Jefe de Proyecto. Personal del CESTIC que coordina el análisis de la petición, y si se aprueba, proseguir, continuar su desarrollo.
- Grupo de análisis. La DISEVAR del CESTIC, en coordinación con la SEGENER, lidera al equipo designado de todas las divisiones, áreas y unidades para analizar la solicitud.
- Organo de Gobierno. Estructura que aprueba y prioriza las peticiones de servicios CIS/TIC.

El proceso de Gestión de la Demanda se divide en 3 fases, que son, Solicitud, Análisis y Aprobación, que a su vez de componen de subfases.

I. Solicitud del servicio.
   - El ámbito solicitante cumplimenta el formulario establecido de solicitud y a través de su interlocutor tramita oficialmente la petición.

[15] Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa.
[16] IT 01/20 del CESTIC "Gestión de la Demanda". Solicitud de nueva necesidad de Servicio CIS/TIC en el MDEF.

- Estudio de la solicitud. Se identifica, registra y categoriza la petición, determinando el Órgano de Gobierno según su tipología, si pertenece a Transformación Digital o no.
- Inclusión de consideraciones de otros ámbitos, si se decide ampliar el alcance de la solicitud original.
- Propuesta de Jefe de Proyecto.

II. Análisis de la solicitud.

- Constituir el Grupo de análisis en el CESTIC, liderado por DISEVAR.
- Efectuar una estimación preliminar de alto nivel y remitirla al Gestor de solicitudes, tratando su viabilidad técnica, impacto en servicios ya existentes, planificación previa de desarrollo, de los recursos humanos, financieros y materiales necesarios, de necesidades formativas de mantenimiento y operación, normativa legal vinculante y análisis de riesgos.
- Comunicación de la estimación preliminar de alto nivel al ámbito interesado para concretar la aportación de recursos estrictamente necesarios por cada parte, bajo la dirección técnica del CESTIC.
- Comunicación de las aportaciones parciales de recursos al ámbito interesado, para su confirmación o corrección, así como al Gestor de solicitudes. El resultado determinará la priorización del Organo de Gobierno.
- Confeccionar una estimación definitiva de alto nivel. La realiza el Jefe de Proyecto y la remite al Gestor de solicitudes.

III. Aprobación de la solicitud.

- Solicitar aprobación y priorización de la solicitud. Acompañada de la estimación definitiva para el DICESTIC y aprobación del Organo de Gobierno competente.
- Decisión sobre el punto anterior. Aprobar o rechazar, priorizarla para el presente o próximo año y analizar y decidir sobre el impacto que conlleva sobre solicitudes previamente aprobadas y priorizadas.
- Comunicación de la decisión. Al ámbito interesado y al Jefe de Proyecto y áreas implicadas de la decisión a través del Gestor de solicitudes. Además, se comunican las repriorizaciones resultantes de incluirse en la lista de actividades.
- Solicitud de incorporación en la planificación financiera. Es necesario actualizar el plan financiero del año o del siguiente con este nuevo hito, iniciando el proceso de obtención de recursos materiales tan pronto finaliza esta tercera fase.

2.6.2Gestión del Servicio de Red Wifi de Asistencia al Personal (RAP)

Siguiendo las instrucciones de la IT 01/20, se desarrollan otras normas que regulan los servicios. Para el caso de este trabajo, la norma reguladora de la Red Wifi de Asistencia al Personal desplegado en operaciones (RAP)[17] es un ejemplo de Gestión de Servicio siguiendo los modelos estandarizados internacionalmente ya vistos, definiendo su ámbito de aplicación, asignado roles, funciones y responsabilidades, estableciendo fases para el despliegue y puesta en producción del servicio e incluyendo un procedimiento de gestión de peticiones, incidencias y control de la configuración.

Así pues, esta IT 03/21 fija el procedimiento para gestionar los servicios de navegación por internet, servicios de entretenimiento, servicios de formación, de telefonía y multimedia y servicios de la AGE tanto en territorio nacional (RAPNA) como en zona de operaciones (SAPZO). El conjunto se denomina RAP. El documento regula la coordinación entre diferentes roles establecidos, procedentes de ámbitos distintos y respetando su dependencia funcional del CESTIC.

[17] Norma 03/21 del CESTIC, de 2 de marzo de 2021, sobre la Gestión del Servicio de Red Wifi de Asistencia al Personal (RAP).

La gestión de la red se centraliza en el CESTIC, a través de un Nodo de Gestión Centralizada, entregando así un servicio homogéneo a todas la unidades desplegadas, compartiendo una base de datos única de control de cuentas de usuarios, de eventos de acceso, de conexión y control de dispositivos, navegación y eventos importantes (logs) para el posterior análisis forense en caso de incidentes de seguridad.

I. Roles en la Gestión de la RAP.

Al igual que en los modelos ya vistos, se definen una serie de roles en el proceso (figura 2-12):

- Administrador Central. El CESTIC actua como único punto de contacto para gestionar peticiones e incidencias a través de su Centro de Atención al Usuario (CAU). Despliega configuraciones y políticas de empleo de manera global. Es el único punto de almacenamiento de cuentas de usuario e identidades. Monitoriza los depliegues de equipos WiFi en las unidades, generando alertas según umbrales para localizar casos de servicios degradados.
- Jefe de Unidad. Responsable de la seguridad física del equipamiento, pudiendo solicitar la desactivación de cuentas al Gestor de Cuentas.
- EMAD y ámbitos. Reciben los sevicios entregados por la RAP en las unidades de su responsabilidad, según los SLAs que se acuerden. De su Jefatura CIS dependen los autorizadores, centralizadores y canalizadores de las peticiones relativas a la gestión de cuentas de usuario, de emplazamiento, SAPZO y cuentas receptoras de nuevas altas.
- Gestor de Emplazamiento. El Centro de Comunicaciones de la Unidad, responsable CIS, responderá de los detalles técnicos básicos de operación de la RAP, supervisando y realizando mantenimiento sencillo en la Unidad.
- Gestor de Cuentas de Usuario. Organo que monitoriza el ciclo de vida de cada usuario en el servicio, como gestor de la calidad de vida en el propio emplazamiento.
- Gestor de Cuentas SAPZO. Organo de gestión de altas de usuario en la RAP, así como bajas y recuperación de contraseñas. Este rol y el anterior se pueden unificar en uno solo.
- Responsable de Ejército. Unico/s autorizado a gestionar peticiones e incidencias, y con acceso a las aplicaciones SCANS / SGPI para: poder editarlas, rechazar o dar conformidad, resolución, visualizarlas y cerrar las que haya creado, y con acceso a estadísticas.
- Usuario. Personal individual y expresamente autorizado al uso de la RAP en sus dispositivos personales aceptando las condiciones de navegación establecidas. Podrá ser habitual o itinerante, según su permanencia en la unidad.
- Empresa que proporciona soporte. Aquella que realiza una función externa en la gestión y/o soporte de la RAP, dotada de un Centro de Atención al Cliente (CEX) en comunicación permanente con el CAU del CESTIC.

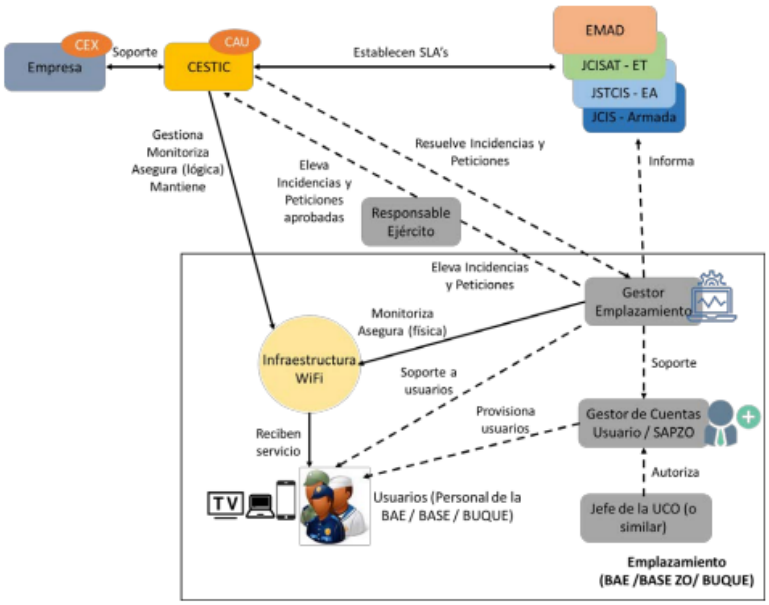

Figura 2-12. Roles en la Gestión de la RAP

II. Gestión de Peticiones.

Por una parte quedan delegadas en el Gestor de Cuentas del Emplazamiento las peticiones de altas, bajas, el soporte a usuarios finales o la gestión de credenciales entre otras peticiones que puedan atenderse localmente por su sencillez.

Para otras peticiones, más allá de este tipo, deberán cargarse en la aplicación SCANS a través del CISPOC de la Unidad para que el CESTIC las resuelva, y los Gestores de Emplazamiento podrán actuar como controlares intermedios. Así mismo deberán comunicar al CAU cuantas modificaciones sobre el servicio sean necesarias, teniendo a su disposición email y teléfono 24/7/365.

Estas serán, por ejemplo, peticiones en relación al cambio en la asignación de roles en la Unidad, la solicitud de activar el servicio satélite o el acceso remoto a la infraestructura, relativas a equipamiento y configuración, y aquellas sin capacidad de resolución local.

Por su especificidad, en la norma se detalla el procedimiento a seguir para:

- Solitud de activación del servicio satélite según tenga la unidad terminal satélite con capacidad limitada o sin terminal SECOMSAT. Y para aquellos con terminal SECOMSAT de gran capacidad y COMSAT IGX.
- Peticiones de activación y desactivación de cuentas de telefonía IP en ZO a través de SCANS por parte del Gestor de Emplazamiento, ya sea para usuarios permanentes en la Unidad o aquellos transeúntes con duración menor, estrictamente la misión.
- Solicitud de activación de cuentas para acceder a través de VPN desde ZO, diferenciando entre unidades con Gestor de Emplazamiento o usuarios individuales, para aquellos casos donde no existe SAPZO.

III. Gestión de Incidencias.

Al igual que en el subproceso anterior, aquí también la tipología de las incidencias se agrupa en dos. Por un lado el Gestor de Cuentas de cada Unidad se responsabilizará de la gestión de las incidencias que afecten al soporte a usuarios, ya sea altas, bajas, o credenciales, por ejemplo. Si no fuera capaz de dar resolución, la elevará al Gestor de Emplazamiento, quien podrá elevarla al CESTIC si tampoco puede resolverla.

Y por otra parte están las incidencias que superan el mantenimeinto preventivo y correctivo del emplazamiento RAP y que no pueden ser resueltas por el Gestor del Emplazamiento como responsable. Los CISPOC generarán las incidencias SCANS para resolución del Gestor de Emplazamiento o que éste las remita al CESTIC. Entre éstas están:

- Errores de acceso de sesión, de conexión o de acceso a herramientas.
- Averías en los puntos de acceso, en equipamiento HW o simplemente de su configuración.
- Errores de conectividad, problemas con el servicio de internet, telefonía IP o entretenimiento multimedia.

Cómo debe atender cada incidencia el Servicio de Atención al Usuario, empleando el Sistema de Gestión de Incidencias y Peticiones (SCANS/SGPI) según la tipología de la misma, se desarrolla en una Instrucción Operacional[18] que amplía la presente Norma. En ella se agrupan las incidencias en:

- Incidencias de usuarios.
- Incidencias relativas al acceso a la red.
- Incidencias relativas al equipamiento.
- Incidencias relativas a las comunicaciones.
- Incidencias relativas al servicio.
- Peticiones de altas, bajas y modificaciones de usuarios.
- Peticiones de altas, bajas y modificaciones de servicio de comunicaciones.
- Peticiones de contenido multimedia.
- Peticiones de equipamiento.

Cada una de las incidencias consideradas como posibles están desarrolladas, explicando qué información cargar en la herramienta, cómo identificarla y actuar en busca de su resolución.

En todo caso deben cumplirse los siguientes requisitos para una adecuada gestión de incidentes:

- Mantener un registro actualizado de cada incidente de operación o de la gestión del Nodo de Gestión Centralizada y de los emplazamientos.
- Clasificar los incidentes por prioridad de resolución según los SLAs establecidos.
- Monitorizar el ciclo completo de cada incidente, con procedimientos de escalado y notificación explícitos.
- El procedimiento completo estará definido en la herramienta de gestión y control SCANS.

IV. Gestión de la Calidad del Servicio.

A través de correo electrónico hay contacto permanente entre el CESTIC (DIVOPER) con todos los Gestores de Emplazamiento donde se ofrece el servicio RAP. Por esta vía se solicita periódicamente el envío de la evaluación de la calidad del servicio prestado, haciendo uso de una plantilla establecida en esta Norma en los plazos que se establezcan.

Se trata de una encuesta de satisfacción que hace especial hincapié en el acceso a internet en territorio nacional, y en el acceso a internet, a la telefonía IP y al servicio de entretenimiento multimedia desde zona de operaciones.

La supervisión de los servicios se centraliza en el Nodo de Gestión Centralizada del CESTIC, comprobando y verificando el estado de equipos, realizando el mantenimiento preventivo y evolutivo, monitorizando los componentes, analizando los niveles de servicio ofrecidos en comparación con los requeridos y extrayendo informes de la calidad de servicio de la red satélite suministrados por los órganos de gestión.

Además, se generan informes de control sobre el servicio de gestión de incidentes y sobre el control de la capacidad y disponibilidad de los componentes del Nodo de Gestión Centralizada de la RAP, donde los emplazamientos incluirán estudios de tendencias, rendimientos, cargas y empleo de los servicios ofrecidos.

[18] IOP-01-CESTIC-01/20.

V. Gestión de la Configuración y Control de Inventario.

El Control de la Configuración se mantiene desde la DIVOPER del CESTIC al objeto de proporcionar los servicios del Nodo de Gestión Centralizada de la RAP, debiendo cumplirse los siguientes términos:

- Existe un inventario de productos que debe mantenerse actualizado a través de la implantación y gestión del sistema GESTIONAL por parte de la DIVOPER.
- Todo cambio en la infraestructura debe reflejarse en la base de datos de Control de la Configuración, con las versiones HW y SW actualizadas.
- Se solicita periódicamente y de manera oficial a los emplazamientos la actualización de los recursos.
- Se mantiene actualizado el archivo de incidencias y peticiones de cada emplazamiento.
- Se archivan copias de seguridad de configuraciones y datos que permitan recuperar el servicio al máximo nivel.

2.6.3Gestión de la infraestructura TIC en la Armada

En este apartado se expondrá procedimiento actualmente seguido en el ámbito de la Armada para el control del catálogo e inventario de material informático, así como de su adquisición para las redes.

I.Gestión del Catálogo e inventario informático en la Armada.

Las directrices a este respecto proceden de la Jefatura CIS[19], responsabilizando al JEGRUCECIS de su elaboración y mantenimiento, apoyado por los CECIS periféricos del Grupo.

Como herramienta de cálculo se emplea una hoja excel que refleja las cifras de equipamiento HW, de las redes clasificadas y sin clasificar, que se asignan a cada CECIS para que las unidades a las que dan apoyo puedan desempeñar sus misiones.

A cada CECIS se le atribuye la responsabilidad de confeccionar y actualizar el "Catálogo de material informático" de su área de competencias, mostrando el reparto asignado a cada unidad, y sin superar las cifras máximas establecidas por AJECIS en el documento "Material informático principal de la Armada", el cual cumple los criterios establecidos por el EMA, pudiendo redistribuir o modificar los componentes de sus catálogos en caso de necesidades operativas de la Unidades, pero sin sobrepasar el máximo antes indicado.

Ambas hojas, la principal actualizada por la JECIS y el catálogo por cada CECIS, serán revisadas anualmente, manteniéndolas al día en la web de Sharepoint de la red de Sistema de Mando Naval (red clasificada específica de la Armada). En este proceso de control se tiene en cuenta el Plan de Renovación Tecnológica, que pretende la renovación del equipamiento cada 8 años, lo que implica la renovación de un 12% del parque al año. Los CECIS desarrollan las instrucciones particulares necesarias para hacer más fácil el control de su inventario distribuido entre las Unidades.

Aparte, el catálogo de la Armada podrá ser revisado por las siguientes circunstancias:

- A propuesta razonada de las Unidades que requieran su modificación. Estas propuestas serán estudiadas por el CECIS y elevadas a JEGRUCECIS, que realizará una propuesta de modificación consolidada a la JECIS para su aprobación, si la hubiera.
- A iniciativa de los propios CECIS ante las demandas de las Unidades apoyadas, cuando consideren que se dan las circunstacias.
- Por orden de la JECIS cuando se considere necesario. La JECIS resolverá anualmente las propuestas y comunicará la autorizaciónes pertinentes.

[19] Instrucción de JEGRUCECIS 06/17

II.Procedimiento de adquisición de material informático para la WAN PG y redes clasificadas.

Al objeto de optimizar la gestión del material informático de las redes CIS operando en la Armada, hay establecido un procedimiento específico para su adquisición que facilita la labor de JEGRUCECIS como gestor responsable[20]. Esta instrucción es de cumplimiento para los CECIS y las unidades a las que apoyan, afecta a las redes clasificadas y la red de propósito general (WAN PG), y engloba todo el HW y SW (licencias, ordenadores, componentes, electrónica de red, servidores, impresoras y periféricos, telefonía, fax, etc).

La unidad que dispone y maneja el presupuesto para la adquisición de material informático en la Armada es la Sección de Comunicaciones y Sistemas de Información de la Dirección de Ingeniería y Construcciones Navales (SUBCIS DIC-JAL), mientras en el ámbito conjunto depende del CESTIC.

Las necesidades de las Unidades pueden ser:

- Adquisiciones de material incluido en el catálogo e inventario de la Armada. Se trata de una reposición, que puede ser ordinaria o urgente.
  Las peticiones ordinarias se remiten a JEGRUCECIS cada 1 de marzo a través de los CECIS de apoyo y siguiendo un formulario estandarizado, pudiendo recibir una priorización alta, media o baja en función de la limitación operativa que supone su pérdida.
  JEGRUCECIS consolida las necesidades y eleva la petición a la SUBCIS o al CESTIC según competencias.
  Las necesidades SW son centralizadas por el CESTIC, que supervisa el cumplimiento de los contratos establecidos con las empresas y no rebasar las licencias acordadas.
- Peticiones urgentes. SUBCIS DIC-JAL entrega a los CECIS cierta cantidad de recursos financieros para cubrir este tipo de necesidades especiales y urgentes, informando de las adquisiciones a JEGRUCECIS.
  Si el CECIS no dispone de recursos, puede consultar al resto de CECIS. En caso de disponer, se contempla el intercambio de componentes. De no tener ninguno, JEGRUCECIS, notificado de ello, realiza la petición formal a la SUBCIS de la JAL.
- Nuevas adquisiciones (no incluidas en catálogo informático). Se seguirá el procedimiento descrito en el punto I de este subapartado.

Con el fin de hacer seguimiento a todo el proceso de adquisición y entrega de equipamiento los CECIS informan anualmente al JEGRUCECIS del material recibido y pendiente, así como de las fechas en que se entregan a sus destinatarios, las unidades apoyadas, no más tarde del 20 de enero.

2.7 Herramientas para la Gestión de Servicio

A continuación se presentan diferentes herramientas para gestión de servicios empleadas en el ámbito de la Defensa y en los propios Ejércitos en particular.

2.7.1 SCANS

Comenzamos con la herramienta más conocida puesta a disposición de todos los Ejércitos para comunicar al Servicio de Atención a Usuarios (SAU) del CCEA (Centro Corporativo de Explotación y Apoyo) sus incidencias y peticiones en redes y sistemas, así como el control del gasto y facturación telefónica; SCANS, o Sistema de Control de Acuerdos de Nivel de Servicio del MINISDEF.

La aplicación es útil para la gestión de los servicios de telecomunicaciones integrados en la red de propósito general (WAN PG), sus servicios informáticos HW y SW y los sistemas de información corporativos. Los recursos con los que cuenta el SAU son, el Centro de Atención al Usuario (CAU),

[20] Instrucción de JEGRUCECIS 03/17 Cambio 1.

localizado en el CCEA, el Sistema de Gestión de Peticiones e Incidencias (SGPI) accesible a través de la aplicación SCANS y la Base de Datos del Conocimiento "*Knowledge Tools"* a través de SCANS y vía web.

El CAU es el punto único de asistencia permanente a los usuarios MDEF para el registro, gestión y resolución de incidencias en los servicios y sistemas antes mencionados 24/7/365, a través de teléfono, email, fax y web. Todas las incidencias y petiones deben ser comunicadas a través de los CIS POC de las unidades o emplazamientos.

Las tareas de los diferentes CIS POC de un emplazamiento o localización son coordinadas por un Coordinador CIS, que pertenecerá en la medida de lo posible al Organo de Apoyo CIS[21] (OACIS) del emplazamiento, con unos conocimientos técnicos adecuados para la resolución de incidencias comunes y sencillas. Además, para emplazamientos de gran tamaño es aconsejable el nombramiento de al mesos dos Coordinadores CIS, uno para atender los Servicios de Telecomunicaciones y otro para los Servicios Informáticos y Sistemas de Información.

El siguiente escalón previo al CAU es el Responsable de Ejército, quien controla y gestiona las peticiones tramitadas por los CIS POC y Coordinadores CIS, para darles conformidad, rechazar, poner en estudio o resolver aquellas para las que tiene potestad y conocimientos.

A los roles anteriores es el CCEA quien les proporciona, previa solicitud, usuario de acceso a las aplicaciones SCANS y DICODEF, si además son gestores de sistemas informáticos, con el nivel de visibilidad de pantallas y datos que les corresponda según su rol.

Cada usuario autorizado, según su rol, tiene acceso a las incidencias y peticiones propias, de su responsabilidad asignada en su propia dependencia, o aquellas cargadas por los CIS POC de su círculo de gestión y que debe tramitar; reflejadas con un estado de "abiertas". "cerradas", "en progreso", "reconocidas" o "resueltas", o simplemente puede ver "todas". El responsable de Ejército las ve todas y sólo las puede marcar como "cerradas" el usuario que las abrió o aquel a quien se asignó. El CAU las cierra en todo caso que superen dos meses resueltas y sin reclamación abierta.

Las peticiones en cambio, pueden tener los siguientes estados: "abiertas", "conforme controlador", "conforme responsable", "aprobadas en progreso", "cerradas", "en estudio", "rechazadas" o "resueltas". Para el Responsable de Ejército aparecen además las "conforme resp. Ejército" y por tanto escaladas al CCEA.

La herramienta está diseñada para realizar búsquedas sencillas y rápidas en la base de datos, buscar el historial de una incidencia/petición, así como de incidencias con interdependencias. En todas las incidencias es obligatorio cargar usuario afectado, prioridad y tipo de incidencia si queremos que se eleve automáticamente al personal de soporte adecuado que resolverá. Además, la carga de la incidencia permite asociarla a un elemento de inventario registrado (teléfonos, componentes de redes de datos, etc). La prioridad introducida en la carga será acorde a los niveles de servicio asignados y permitirá monitorizar su grado de cumplimiento. Generalmente las incidencias/peticiones urgentes se escalan automáticamente a las 24 horas y las ordinarias a las 72 horas.

La aplicación permite nombrar y describir con detalle la petición/incidencia y adjuntar documentos que ayuden a los técnicos a darle respuesta/solución. Cada incidencia queda registrada con un número de referencia. Las peticiones rechazadas no se cierran, quedando almacenadas en tal estado.

La herramienta permite asociar las incidencias a un tipo de servicio, entendido como el compromiso adquirido con el CAU a que su tramitación se haga conforme a unos tiempos

[21] Dependencia o departamento técnico que proporciona apoyo a los usuarios del emplazamiento y que suele materializarse en unidades de telecomunicaciones o informática en bases, acuartelamientos y edificios oficiales.

determinados en un Acuerdo de Tipo de Servicio; según la figura 2-13. En función del tipo de servicio se lanzan una serie de eventos asociados al alcanzar ciertos límites de tiempo.

Tipos de Servicio	Nivel de servicio
Peticiones Ordinarias	Se asigna por defecto a las Peticiones Ordinarias
Peticiones Urgentes	Sin uso
04hr resolution	Compromiso de resolución de incidencia / petición en 4 horas hábiles
06hr resolution	Compromiso de resolución de incidencia / petición en 6 horas hábiles
08hr resolution	Compromiso de resolución de incidencia / petición en 8 horas hábiles. Se asigna por defecto a las Peticiones Urgentes
12hr resolution	Compromiso de resolución de incidencia / petición en 12 horas hábiles
24hr resolution	Compromiso de resolución de incidencia / petición en 24 horas hábiles
48hr resolution	Compromiso de resolución de incidencia / petición en 48 horas hábiles
72hr resolution	Compromiso de resolución de incidencia / petición en 72 horas hábiles
10 Días tipo de servicio	Compromiso de resolución de incidencia / petición en 10 días hábiles

Figura 2-13. SCANS. Tipos de Servicio conforme a los tiempos de resolución

2.7.2 I-CIS. Sistema de Gestión de Servicios IT en el Ejécito de Tierra (ET)

Es la herramienta[22] empleada en el ámbito interno del Ejército de Tierra para comunicar las indidencias CIS al CISPOC de la Unidad y a los técnicos del Centro de Comunicaciones (CECOM). Cualquier usuario puede emplearla tras autenticar su identificación. Es una aplicación que, basada en los principios de la Gestión de Incidentes de la ISO 20000, trata de aportar a los usuarios:

- Incrementar su productividad y satisfacción, a la vez que optimiza los recursos disponibles.
- Cumplir con los niveles de servicio fijados por SLA, con mayor control de los procesos y monitorización del servicio.
- Registro de los incidentes con todos los datos necesarios para analizar el servicio suministrado por el CECOM.
- Mejor registro de las acciones realizadas durante la investigación y resolución de las incidencias.

Es responsabilidad del usuario introducir todos los datos de identificación, incidencia y destino que ocupa correctamente, así como actualizar estos últimos si se trasladara, pues será necesario para hacer el correcto seguimiento de evolución a la incidencia.

El usuario recibe emails cada vez que la incidencia es atendida, comentada, transferida o escalada. Igualmente puede añadir comentarios y reclamaciones así como conocer los datos del técnico que resuelve su inciencia (figura 2-14).

[22] http://portal.mdef.es/iCIS/

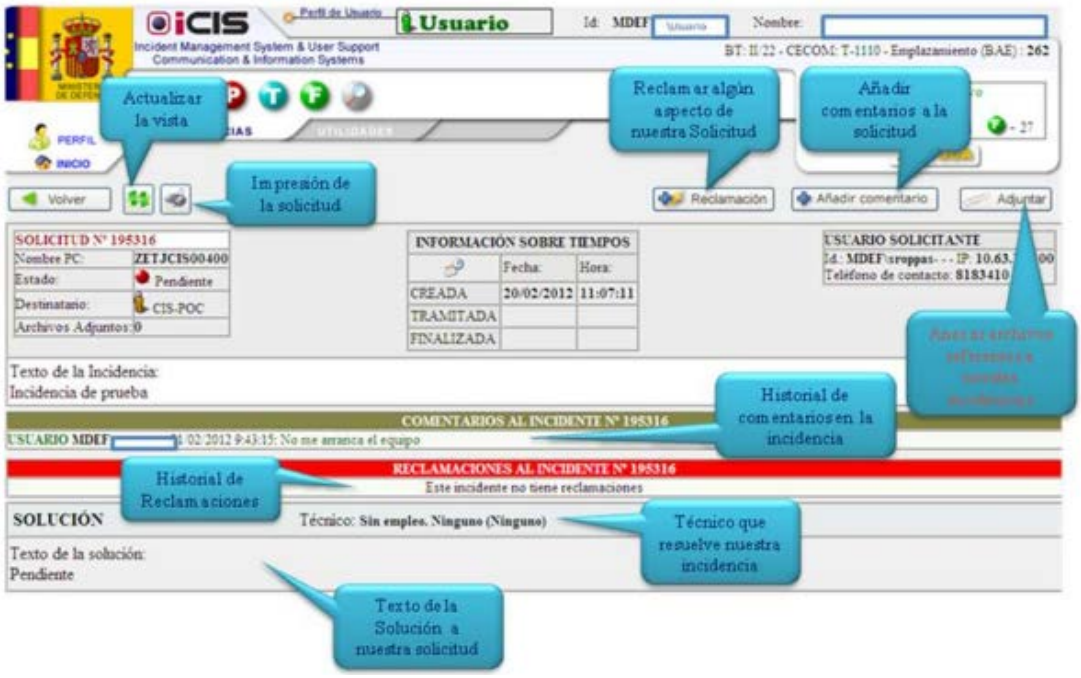

Figura 2-14. I-CIS. Seguimiento de Incidencias

2.7.3 GISMI.Gestión del mantenimiento de equipos informáticos en el ET

Esta herramienta para la Gestión de Incidencias y Saldos de Mantenimiento de Informática tiene por objeto definir el procedimiento para los mantenimientos del material de los sistemas de información y electrónica de red de las Unidades del ET dado de alta en el inventario de activos CIS (ARIET).

El empleo de GISMI responde a una cadena funcional articulada, según se explica en la Instrucción Técnica 11/05 de la Jefatura CIS y AT del ET, en los siguientes roles:

- Director de Proyecto. Será el Jefe de la Sección de Apoyo o quien determine el General Jefe de la JCIS y AT del ET.
- Subdirector de Proyecto. Desempeñado por el Jefe del Organo CIS u otro cargo del mismo, con Unidades asignadas para mantenimiento.
- Jefe de Proyecto. Seleccionado del personal de la empresa contratada para el mantenimiento y recibiendo de los Subdirectores de Proyecto las peticiones a atender.
- Empresa. La seleccionada a partir de concurso para realizar los mantenimientos del material inventariado en ARIET.
- Organo Técnico. Organos CIS tanto de antiguas como de nuevas estructuras, con responsabilidades de gestión y administración del mantenimiento de los equipos objeto de esta IT.
- Unidades de “primer nivel”. Aquellas con capacidad para atender y resolver incidencias CIS e informáticas de otras, denominadas de “segundo nivel”.
- Organo CIS de apoyo al emplazamiento (OACISE). Materializados principalmente por los CECOMs y responsabilizándose del mantenimiento GISMI de los medios asignados y de su electrónica de red. Según su plantilla podrán llegar a proveer apoyo a usuarios.

Los mantenimientos gestionados podrán ser de diferentes tipos:

- Preventivos. Revisiones y actualizaciones a impresores de red y por lotes, iniciadas por el Subdirector de Proyecto hacia la empresa.

- Correctivos. Reparaciones de equipos, de coste razonable, tramitadas a través de GISMI desde la Unidad. Las aprobadas serán remitidas por el Subdirector de Proyecto a la empresa. Si no es posible el mantenimiento se comunicará al Director.
- Perfectivo. Ampliación de prestaciones, por obsolescencia, necesidad de integración o difícil reparación. Las peticiones aprobadas se remitirán al Director que, según las instrucciones de la JCIS y AT, denegará o hará llegar a la empresa para su atención.
- Adaptativo. Adaptación de componentes para mejorar las prestaciones, ante la necesidad de mayores recursos y requisitos, que requiren la evolución tecnológica del equipo. O justificación ante de una reparación de alto coste en comparación a un equipo nuevo. Siguen los mismos pasos que el mantenimiento perfectivo, dando de baja los equipos retirsdos de inventario y de alta a las nuevas adquisiciones.

La cadena de mantenimiento del material informático, tanto de la WAN PG como de los Sistemas de Mando y Control que se determinen, será tramitada desde los CECOMs, como OACISs, y cada Unidad tendrá un Organo Técnico de referencia nombrado (cadena GISMI) a través del cual realizará su mantenimiento.

Las diferentes unidades y roles con responsabilidades en la cadena de mantenimento, haciendo uso de la aplicación Lotus Notes, acceden a la Base de Datos de Gestión de Incidencias y Saldos de Mantenimiento de Informática (GISMI). Las unidades de segundo nivel (inicialmente los CECOMs) cargan sus incidencias para ser atendidas por las de primer nivel (Batallones de Transmisiones generalmente), o rechazadas, y el Jefe del Regimiento de Transmisiones 22 (RT-22) actúa como Subdirector de Proyecto. Las solicitudes llegarán a la empresa, que reportará al Director de la solución y presupuesto según cada caso.

El proceso es finalizado por el Subdirector de Proyecto dando visto bueno a la actuación de la empresa a través de la aplicación GISMI, solicitando los informes que estime oportuno a las unidades de primer y segundo nivel. Todos los cambios en los equipos deben quedar reflejados en ARIET.

El Director de Proyecto será quien proceda a cerrar los procesos, efectuando las liquidaciones trimiestrales para control de gastos, una vez dado el visto bueno por el Organo Técnico. Estas son enviadas al JCIS y AT para seguimiento del Programa de Mantenimiento, desglosado en escalones intermedios o Subdirectores.

La herramienta permite dar un Parte de Queja cuando alguno de los usuarios de una Unidad no esté conforme con las actuaciones de la Empresa y no haya podido alcanzar una resolución satisfactoria en su negociación.

2.7.4 PROACTIVANET. Gestión en el Organo Central vía SIJE.

Es la herramienta que el Organo Central está probando desde el segundo semestre de 2021 en el entorno conjunto, en SIJE, para gestionar de manera eficiente incidencias, problemas y cambios; mantener actualizado el inventario del parque informático, así como de la aplicaciones instaladas en él, y proporcionar métricas útiles para la toma de decisiones agiles. Todo ello proporciona una notable mejoría en la gestión de las TI y del servicio suministrado, con un control eficiente de los activos y la reducción de riesgos y costes a la Institución. Se trata de una aplicación, con un precio en relación a los módulos y herramientas que la componen (figura 2-15), algunos estrechamente vinculados a otros y necesarios para su funcionamiento, así como del número de usuarios, con licencias nominales, asociadas a grupos de usuarios o mixtas.

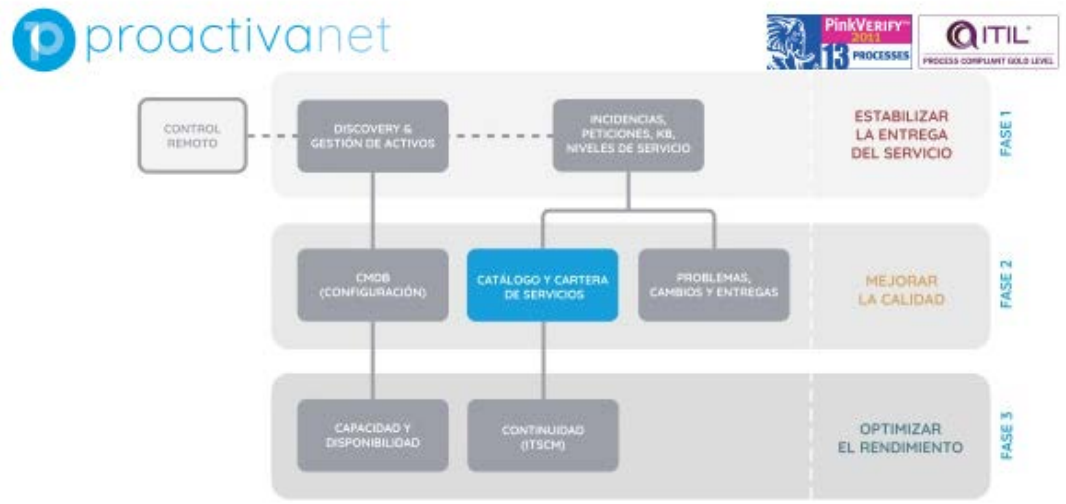

Figura 2-15. Proactivanet. Relación entre sus módulos

I. Gestión de Activos

La herramienta permite conocer en detalle y de forma automática el inventario completo del parque informático, sus licencias y configuración, ahorrando costes y mejorando la seguridad de la infraestructura. Permite controlar el empleo de las licencias SW instaladas y saber si hay escasez o exceso en las redes. Proporciona datos al resto de los procesos ITSM disponibles en la plataforma.

Se integra en los principales sistemas de virtualización, optimizando los recursos Y controlando los licenciamientos. Detecta los equipos desactualizados y comienza los procesos de descarga e instalación automática de parches.

Permite la gestión y auditoría de los teléfonos móviles corporativos (*Mobile Device Management* – MDM). También hace seguimiento de las unidades de almacenamiento y de las variaciones de los permisos de acceso a la información, detectando la instalación de cualquier SW no permitido.

Todas estas tareas mejoran la productividad de los técnicos de soporte, liberándolos de tareas básicas, sencillas y repetitivas, y agilizando las auditorías de SW. También mejora la productividad de los usuarios finales al disminuir los tiempos de diagnóstico y resolución de peticiones e incidencias y en general aportando valor al negocio con una mayor disponibilidad de los servicios y mejor administración de la infraestructura en continua evolución.

Posee un módulo para la Gestión de Proveedores y Contratos, en línea con las mejores prácticas ITIL (*ITIL Compliant*) e ISO para la prestación de servicios, que permite el registro y seguimiento de los proveedores y los contratos para la compra de HW y SW y la contratación de servicios.

II. Gestión de Incidencias, Peticiones, Conocimiento (KB) y Niveles de Servicio (SLAs, OLAs y UCs)

Estos módulos entregan las herramientas necesarias para implementar un Centro de Servicios (*Helpdesk*), permitiendo al usuario final la gestión de sus propios tickets, la correcta priorización en base a niveles de servicio y la personalización según las necesidades específicas de la organización; completamente alineados con las mejores prácticas ITIL y norma ISO 20000.

Pone al servicio del usuario una excelente vía de comunicación, reduciendo los tiempos de estudio y resolución de incidencias y generando una base del Conocimiento que le permite evitar la generación

de tickets innecesarios, que además consumen tiempo de los técnicos de primera línea. Pone a disposición de técnicos y usuarios la información necesaria para minimizar los tiempos de diagnóstico y resolución de incidencias.

A través de la Gestión de Niveles de Servicio se pueden medir los tiempos de respuesta y reparación y localizar cuellos de botella en el sistema de atención a incidencias y peticiones. Se pueden modelar los flujos de autorización para que haya un escalado específico, monitorización y proceso de aprobación a tiempo, sin demoras, con avisos automáticos.

Prioriza la gestión de las incidencias críticas e introduce lecciones aprendidas que habilitan la mejora continua, proporcionando la gestión integral del ciclo de vida completo de las incidencias y peticiones. Permite gestionar y monitorizar los niveles de servicio establecidos con usuarios, internos y con proveedores, así como el ciclo de vida de los acuerdos de nivel de servicio de principio a fin.

III. Gestión de la Configuración y Activos (CMDB)

Es un módulo de la aplicación fundamental para implementar el proceso de Gestión de la Configuración de ITIL e ISO 20000, actuando como repositorio de información central para todos los elementos de configuración de la empresa y sus interrelaciones, automatizando y reduciendo el esfuerzo en mantenimientos mientras incrementa el aporte de valor a otros procesos.

Es una herramienta esencial para localizar los puntos aislados de fallo en nuestra infraestructura (*Single Point of Failure* – SPF) que pudieran dañar la disponibilidad y la capacidad de los servicios, de una manera muy intuitiva a través de gráficos.

Su integración con el *Service Desk* permite a los técnicos de peticiones e incidencias acceder a la CMDB y su fuente de conocimiento, agilizando la resolución de éstas.

También ayuda a quienes no son muy técnicos a entender las inversiones realizadas en IT como inversiones positivas para la prestación de nuevos servicios al negocioo o mejorar los ya existentes, es decir, a aceptarlas como inversiones en procesos de negocio y no como un mero gasto en tecnologías.

Este módulo ayuda a detectar la infraestructura infrautilizada y poder reorientar su uso y futuras inversiones; así como la infraestructura obsoleta que podría poner en compromiso la confidencialidad de la información. También a disminuir el número de incidencias consecuencia de cambios realizados sin antes un adecuado análisis de impacto.

IV. Gestión de Problemas, Cambios y Entregas

Este módulo tiene como objetivo la reducción del número de incidencias y el tiempo para resolverlas, ayudando a identificar puntos débiles y de mejora en la empresa de una manera proactiva, antes incluso de aparecer los problemas. Si la resolución definitiva requiere un cambio, la Gestión de Cambios y Entrega permitirá su aplicación ordenada, dirigida y planificada, minimizando los riesgos y promoviendo la evolución continua.

Junto con la Gestión de la Configuración y Activos se pueden controlar los cambios de principio a fin, atendiendo a los detalles que ITIL aconseja y simplificando la ejecución de análisis de riesgos detallados.

Requiere ser instalado e integrado con el módulo de Gestión de Incidencias, Peticiones, KB y SLM, y permite a los técnicos ver en la CMDB el Calendario de Cambios Programados del inventario y el historial de cambios experimentados por cada ítem incluido en la base de datos. La herramienta permite establecer criterios de escalado y asignaciones perfectamente definidos y automáticos, indicando qué Consejo Asesor del Cambio (CAB) es el idóneo para la toma de decisiones y el criterio de votación para su aprobación final. En definitiva, esta herramienta también es un buen paso para sentar las bases de la Gestión de Proyectos en la organización.

Finalmente, aporta informes avanzados, completamente personalizados y cuadros de mando (*dashboards*) representando gráfica e interactivamente la información útil del proceso.

V. Catálogo y Cartera de Servicios

Este módulo también requiere la instalación previa del módulo de Gestión de Incidencias, Peticiones, KB y SLM. Aporta una visión completa y precisa de los servicios de TI a todas las áreas del negocio y usuarios, definiendo al personal técnico las expectativas de soporte esperadas. La Gestión de la Cartera de Servicios o Portfolio dirige el ciclo de vida completo de los servicios, permitiendo encaminar las inversiones y la planificación estratégica de nuevos servicios alineada con las necesidades de la organización.

La herramienta premite priorizar los servicios relevantes para la organización y ayuda a reprogramar las inversiones. Ayuda a la priorización correcta de los tickets de incidencias y peticiones que cargan los usuarios, lo que finalmente ayudará a minimizar los tiempos de resolución.

Que toda la organización conozca en detalle los servicios que se prestan y su impacto en los procesos de negocio, permitirá la priorización de las inversiones y de las tareas orientadas a mejorar la disponibilidad y continuidad de aquellos definidos como críticos.

VI. Gestión de la Capacidad y la Disponibilidad

Este módulo específicamente requiere disponer del módulo de Gestión de la Configuración (CMDB), optimizando y monitorizando los servicios TI en su funcionamiento correcto e ininterrumpido, a un coste razonable, siendo además reforzados por unos recursos adecuadamente dimensionados. Todo ello reduce drásticamente los tiempos de caída del servicio con una detección temprana e incluso anticipada.

Enfoca Capacidad y Disponibilidad sobre los servicios, no solo a la infraestructura que los proporciona, automatizando la creación y cierre de incidencias en situaciones de falta de disponibilidad o de capacidades comprometidas, controlando el nivel de cumplimiento de los SLAs.

Permite medir los niveles de demanda y así poder adaptar nuestra infraestructura para evitar colapsos por falta de capacidad o disponibilidad; también hacer simulaciones de futuras demandas que permitirán definir planes de infraestructura. Igualmente, permite conocer la disponibilidad histórica y la tendencia de los servicios.

Toda esta información se puede extraer en informes avanzados y en detalle con cálculos reales de tiempos 24/7, que permitirán obtener métricas de valor para analizar el grado de cumplimiento de los SLAs y otros acuerdos de la organización y con proveedores.

VII. Gestión de la Continuidad

Este módulo requiere la instalación previa del Catálogo y Cartera de Servicios, como puede verse en la figura 2-15, dedicándose a impedir que una interrupción de servicios no prevista y grave provoque serias consecuencias en la empresa, en línea con las mejores prácticas de ITIL e ISO 20000, empleando medidas proactivas que impidan y minimicen las consecuencias, y tareas reactivas para la reanudación del servicio lo antes posible.

Permite tener control total y automático de los tiempos de restauración y la visualización del impacto de la discontinuidad en la CMDB, así como seguir la implantación de los planes de contingencia negociados en los acuerdos de nivel de servicio.

Esta herramienta permite a los técnicos conocer las incidencias potencialmente críticas y planificar las actuaciones para tal caso, así como la detección de incomptibilidades entre dichos planes de contingencia y la infraestructura real que posee la organización, lo cual facilitará su adaptación.

La Gestión de la Continuidad nos facilita identificar y diferenciar los componentes críticos, que requerirán medidas proactivas para impedir su colapso y caída del servicio, de los componentes de menor relevancia, y que por tanto con establecer un plan reactivo podremos atender su recuperación.

El poder hacer simulaciones de caídas de servicio nos permitirá valorar el impacto real en las pérdidas del negocio y fomentar así una política proactiva de análisis de riesgos continua entre empleados y usuarios, que lleven a la implantación de acciones de mejora justificadas y regular los procesos de creación de planes de continuidad.

3 DESARROLLO DEL TFM

3.1 Estrategia GIC de los Centros de Explotación CIS de la Armada

Se ha explicado al comienzo de este trabajo la importancia de establecer en la Armada una Estrategia de Gestión del Conocimiento (GIC) que aporte valor a la entrega de servicios desde nuestros Centros de Explotación CIS (CECIS), alentando el desarrollo de mayor información y mejor conocimiento.

El personal del CECIS y los usuarios de la organización deberán poder acceder fácilmente a este conocimiento, a las herramientas colaborativas y a los activos relevantes para el desarrollo de su trabajo, de carácter interno y externo a su ámbito, y que puedan utilizar estas capacidades en su entorno de trabajo cumpliendo con los requisitos de seguridad establecidos en Defensa y organizaciones internacionales a los que pertenecemos, la OTAN y la UE.

Entenderemos por Conocimiento la Información en acción. En el contexto del negocio, conocimiento es lo que los empleados saben sobre las diferentes disciplinas relacionadas con su actividad, sobre los productos, los procesos, de sus clientes, de sus compañeros, así como de los errores y éxitos del pasado[23].

Hay que moverse de la idea "la información es poder" a un nuevo concepto, "el conocimiento es poder, cuando se comparte". El conocimiento es ya uno de los mayores activos de competitividad en los negocios. Por este motivo la estrategia planteada deberá estar enfocada no sólo en integrar los procesos de gestión del conocimiento en las aplicaciones y herramientas tecnológicas clave, sino también en otras áreas habilitadoras como son la gestión completa de servicios (ITIL), la gestión de programas y proyectos, en los procesos de las operaciones y ejercicios (como ejemplo, Lecciones Aprendidas), así como en la propia arquitectura y gobernanza de TI (COBIT[24]).

Los fundamentos principales para esta Estrategia son:

- Que los CECIS facilitarán la reutilización de la información y la experiencia que ya reside en la organización, evitando duplicar esfuerzos, promoviendo y propiciando una cultura de creación e intercambio de conocimientos así como también a través de la búsqueda y recuperación más ágil de los activos.

[23] Glosario de *Knowledge Management* del *American Productivity and Quality Center* (APQC) https://www.apqc.org/

[24] *Control Objectives for Information and Related Technology*. https://www.isaca.org/resources/cobit

- Que esta reutilización de la información dará valor, conduciendo a un aumento general de conocimiento, y que retornará en eficiencia a la hora de gestionar y desarrollar las capacidades de la Armada.
- Que esta mejora en el ciclo de creación, intercambio y reutilización del conocimiento también mejorará la entrega de servicios, acelerando y mejorando los procesos internos para la toma de decisiones.
- Que este movimiento hacia una perspectiva más transparente y una cultura de intercambio de conocimiento, acompañada del desarrollo de la autonomía y experiencia del personal, conducirá a disponer de una plantilla más productiva, satisfecha consigo misma y comprometida con su labor, y en consecuencia, a incrementar la entrega de valor a los clientes de TI. En general, para todas las partes interesadas, el CECIS será percibido como un atractivo productor de capacidades innovadoras y proveedor de servicios de primera categoría.

Los supuestos anteriores estarán orientados a lograr los siguientes resultados:

- Adaptar, mejorar y fortalecer la Gestión de proyectos, programas y cartera de servicios, así como la capacidad de entrega de estos, aumentando la satisfacción de clientes y proveedores.
- Fortalecer la toma de decisiones en la Armada mediante un mejor uso de la información, explotar el "big data", el empleo de la IA y las técnicas y herramientas *machine learning* en beneficio de la Defensa.
- Optimizar la colaboración con los órganos de Dirección para la mejora de políticas y procesos de adquisición de recursos, logrando una obtención más inteligente del equipamiento HW/SW capacitado para un uso intenso.

3.1.1 Misión, Visión y Ambición estratégica

La Misión de la Estrategia GIC del CECIS será ofrecer al personal un entorno moderno, eficiente y transparente de gestión, acelerando los procesos internos de toma de decisiones y mejorando la conducción del negocio de TI.

La Visión será convertirse en un referente de conocimiento en la Armada, facilitador del acceso a información y experiencia y con una política organizacional de transparencia, intercambio de activos y colaboración.

El acceso a los recursos de información y conocimiento y la experiencia debe estar asegurado con independencia de la localización geográfica y de la pertenencia organizacional. Todo el personal estará igualmente habilitado para desarrollar su experiencia, generar nuevo conocimiento y tomar mejores decisiones.

El Plan GIC deberá revisarse al menos anualmente, garantizando que se mantiene lo relevante y apropiado e incorporando las nuevas tecnologías facilitadoras de IKM emergentes y que la organización pueda implementarlas para cumplir con los requisitos estratégicos de la Armada y Defensa.

Es evidente que la estrategia debe expandirse en consonancia con la modernización de las TI (ITM) y es por tanto necesario establecer un marco de referencia para medir el grado de madurez GIC que desarrollan nuestros CECIS. Un modelo referente lo establece el Centro Americano de Productividad y Calidad (American Productivity and Quality Center - APQC[25]), y que emplea actualmente la NATO Communications and Information Agency (NCIA) en el ámbito OTAN.

[25] http://www.apqc.org/knowledge-base/download/275450/K04060_Measure_Across_Levels_KM_maturity.pdf

3.1.2 Metas estratégicas

El Plan estratégico GIC propuesto para el CECIS tendrá las siguientes cinco metas orientadas a lograr la entrega de Servicio más eficaz:

- Que se reconozca la información y el conocimiento como activos corporativos de máxima relevancia, así como a su plantilla como vehículos del propio conocimiento, conservando su experiencia cuando se marchen o se produzcan reestructuraciones.
- Asegurar que la información y el conocimiento son gestionados con precisión, garantizando que los datos se manejan exactamente de acuerdo con las directrices de la Armada.
- Asegurar que además sean fácilmente accesibles dentro del GRUCECIS, mejorando la experiencia de los usuarios a través de tecnologías de conexión online. En este sentido, se incrementará la integración de los sistemas GIC, permitiendo el acceso y replicación de bases de datos autorizadas, fomentando el intercambio inteligente de datos entre sistemas, evitando duplicidades en la incorporación de datos y su mantenimiento, y minimizando los errores.
- Facilitar al personal autorizado el intercambio de conocimiento entre los CECIS y con los clientes externos, fomentando las interacciones personales y potenciando las tecnologías que faciliten la asistencia a salas de reunión virtual, videochats y otras conexiones online.
- Alentar y apoyar la creación y desarrollo de nueva información y conocimiento, así como el acceso a las herramientas colaborativas y activos relevantes para desarrollar su trabajo. Todo ello en un entorno seguro que fomente su uso más eficaz, al objeto de impulsar en la estructura del GRUCECIS la colaboración más eficientemente y emprendedora hacia proyectos innovadores, desafiantes y complejos.

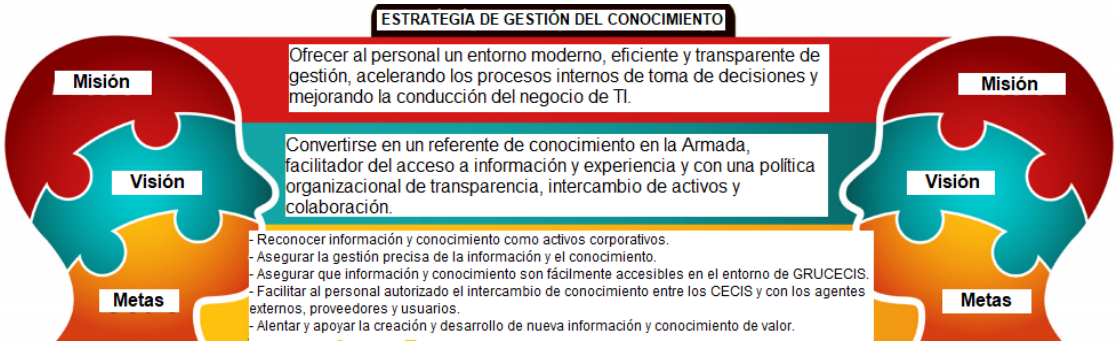

Figura 3-1. Estrategia GIC del CECIS.

3.2 Aplicación de ITIL e ISO a la Gestión de Servicios de un CECIS

Como se expuso en el Subapartado 1.4.3, cada CECIS se subdivide en CECOM y CESIN. Podríamos por tanto reducir la tipología de servicios ofrecidos y gestionados por los Centros en dos clases, radio y redes. Según la Instrucción 58/2016 del SEDEF por la que se aprueba la Arquitectura General TIC (AGSTIC) del MDEF, y dejando a un lado los servicios que gestiona el CESTIC con la colaboración de los CECIS, tenemos en la siguiente tabla 3-1 el Catálogo de Servicios específicos que la Jefatura CIS de la Armada gestiona desde sus CECIS, con el apoyo de los CISPOC de las unidades.

Categoría del servicio	Servicio ARMADA	Servicios de Gestión del CECIS	Necesidades de coordinación
Servicios de Información de las Comunidades de Interés	• Acceso a SACOMAR • SACOMAR (acceso a la red, mantenimiento de la red y su equipamiento, y encaminamiento de	• La Gestión de acceso a Sistemas Clasificados se hace conforme a Procedimientos específicos CO-DRES-POS de cada nodo. • La Gestión de peticiones e incidencias SACOMAR se hace a	• Terminales usuario y documentación clasificada deben mantenerse dentro ZAR acreditada conforme IPSEG 308 • Para manejar sistemas clasificados el AOSTIC Local debe solicitar

	los mensajes). • SACOMAR (tramitación de mensajes). • Acceso a SMN • Terminales Clasificados Aislados • Terminales Aduana entre diferentes redes • Servicios de sincronización	través de la herramienta GLPI. • Gestión de incidencias de Sistemas Clasificados se coordina por mensajes SACOMAR. • Configuración y administración local de los servidores y terminales SACOMAR de los buques y Unidades del área de responsabilidad geográfica con apoyo Tercer escalón. • Configuración y administración local de los terminales de los Sistemas Clasificados (SACOMAR, SMN, Terminales Aislados) • Configuración y administración local y de periféricos (impresoras, teléfono VOIP, VTC) y electrónica de red (switches, UPS, etc) de los Sistemas Clasificados. • Supervisión y control del tráfico SACOMAR a través de canales TX/RX desde el nodo CECIS a los NODOS subordinados. • Efectuar funciones de CEMEN de unidades que no dispongan de SACOMAR • Control del Inventario y Catalogo de equipos (HW y SW) Sistemas Clasificados.	previamente la acreditación del nodo conforme IPSEG 302 • Usuarios redes clasificadas deben disponer HPS y conocer POS • Solicitud acceso usuarios corresponde a Jefe UCO valorando necesidad conocer • Servidores asignados a las unidades deben permanecer dentro ZAR Clase I • Administración remota de servidores SACOMAR por Tercer escalón apoyo • Administración servidores nodo fijo SMN autoridades por CECIS (AS) • Apoyo configuración y administración servidores / TU´s nodos desplegables SMN autoridades por Administradores CIS unidades desplegables con apoyo CECIS de apoyo respectivo • Acceso buques y nodos desplegables a SMN según Procedimiento Operativo GRUCECIS 01/17.
Servicios de Información de Núcleo	• Desarrollo aplicaciones.	• Desarrollo de aplicaciones para elaborar herramientas o gestionar su obtención a través del CESTIC o Tercer Escalón.	
Servicios de Telecomunicaciones	• Telefonía Satélite Portátil (ISATPHONE, IRIDIUM, THURAYA) • Administración centralizada de routers y firewalls. • Terminales TETRAPOL (RSD Y SIRDEE).	• Gestión de peticiones e incidencias por mensajería SACOMAR. • CECIS controla y distribuye los terminales portátiles satélite. • CECIS configura los routers SACOMAR y es responsable de la configuración de los routers de nodos fijos SMN (con derechos temporales administración). • CECIS gestiona el transporte a la AGRUMAD/JAL para la reparación y configuración terminales TETRAPOL.	• Las Unidades deben cumplimentar lo dispuesto en la IPCIS 01/08 AJEMA en relación a las autorizaciones y el control del gasto de telefonía satélite. • Los routers de los nodos desplegables de SMN son configurados por los administradores CIS de las unidades desplegables con apoyo del CECIS respectivo.
Servicios de Seguridad de la Información	• Administración centralizada cifradores y cambio claves telegestión. • Cifrado/descifrado SICOFAR • Servicios automáticos de Backup	• La subcuenta Cripto CECIS controla y distribuye los equipos cripto de las UCO´s del área de responsabilidad geográfica • Gestión de incidencias Cripto de las UCO´s del área de responsabilidad geográfica. • Depósito Cripto de claves futuras, de reserva y “pool” equipos Cripto para su área de responsabilidad. • Transporte de material Cripto entre la cabecera de distribución y su área de responsabilidad. • El CECIS apoya cifrado/descifrado mensajes de aquellas unidades que no dispongan de SICOFAR • CECIS configura y controla el servicio Backup de los servidores y TRT´s SACOMAR con apoyo del Tercer escalón y la supervisión de los CISPOC de las UCO´s • CECIS asesora a las UCO´s en la elaboración de documentación de seguridad Nodos Clasificados y otros aspectos SEGINFO • JEFE CECIS actúa como ASS-D de los Sistemas Clasificados específicos de la Armada (SS-D contemplado en la IPSEG 300)	• Las Unidades deben tener nombrados Cripto-Custodios. • Equipos cripto asignados a las unidades deben permanecer dentro de Zonas de Acceos Restringido (ZAR) Clase I. • Backup local de Sistemas Clasificados conforme CO-DRES-POS de cada nodo. • AOSTIC-L (UCO ó emplazamiento) debe designar un Oficial Infosec (ASS-L ó SS-L), RSA´s, Administrador Local (AS-L) y que elevará la documentación de seguridad del Nodo. • Administradores de Autoridades (Flota, FIM y otros) actúan como AS-L de los nodos SACOMAR-SMN Fijo y AS-L de los Nodos SMN Desplegables. • CISPOC actúan como AS-L de los diferentes Nodos, apoyados en sus funciones por los AS del CECIS.

		• Administradores CECIS actúan como AS Nodos SACOMAR y SMN Fijo	
Servicios de Gestión	• Gestión de servicios distribuida	• Servicios verticales de gestión CECIS incluidos en esta columna. • Atención a las incidencias CIS 24/7 por la Guardia de Comunicaciones y Seguridad del CECIS y CECISMAD para buques en la mar.	• Necesidades de coordinación y gestiones delegadas a incluir en los posibles acuerdos de prestación de servicios (SLA).

Tabla 3-1. Catálogo de Servicios CIS, voz y datos, gestionados por los Centros de Explotación CIS de la Armada.

Para el correcto funcionamiento de los servicios, el Centro debe poseer un área o núcleo de Provisión de servicios que haga seguimiento de cada solicitud y supervise todos los pedidos asociados al servicio, ya sean altas, modificaciones, traslados, bajas parciales o totales. Finalizadas las propias actuaciones, el Centro debería comprobar que cada cliente tiene instalada la solución a su incidencia o petición, revisando la configuración e informando al cliente de las acciones realizas tanto a nivel datos/redes como radio. Si es posible, también es beneficioso el explicarle a los CISPOC de las Unidades las dudas que pudieran tener sobre el servicio, con el fin de que puedan en ciertas ocasiones autogestionar la resolución de incidencias internas; facilitándoles manuales o el acceso a una base de conocimiento con preguntas frecuentes (FAQ), por ejemplo.

El CECIS tendrá un Centro de Atención a Usuarios (CAU) capaz de atender incidencias vía telefónica, por email y a través de una completa aplicación de gestión de incidencias y peticiones, derivando las entradas al área de competencia y si es posible, al propio responsable del servicio tratado en su organigrama. Todo con el fin de recuperar los servicios en el menor tiempo posible, de acuerdo al nivel de servicio acordado y en base a unos KPIs definidos, medido generalmente en horas para la resolución según el horario de atención que ofrezca el Centro.

3.2.1 Estrategia del Servicio. Célula de Mantenimiento

Como parte fundamental de la política de mejora continua del Centro, es necesario perfeccionar la prestación de servicios de mantenimiento, entendiendo este concepto no como la reparación y subsanación de incidencias a posteriori, sino como tareas proactivas para mantener el servicio operativo y en unos niveles de entrega satisfactorios en previsión a posibles fallos.

La atención de solicitudes, incidencias, averías y problemas diarios alcanza cifras altísimas y los tiempos de resolución se incrementan a medida que se trata de clientes individuales y aislados, frente a casos de afección genérica; y por tanto aquéllos requieren de un trato más dedicado y personalizado para cada caso específico. Afrontar cada incidencia de manera reactiva, actuando exclusivamente en situaciones de averías a nivel de red, líneas, aplicaciones, etc, a la larga, demuestra que el tiempo de dedicación, la atención a los clientes y en general el nivel de satisfacción empeora.

Es por ello que se recomienda instaurar internamente en el CECIS una Célula de Mantenimiento que efectúe una gestión proactiva de los servicios, además de atender todas las consultas, incidencias, averías y solicitudes, aportando valor al usuario con la misma atención inmediata vía telefónica o telemática, mejorando el valor estratégico del CECIS, alineando las peticiones de los clientes con su debido tratamiento, y mejorando los tiempos y niveles de resolución.

Esta célula debe ser capaz de gestionar el conocimiento de todos sus integrantes, quienes gestionan todas las incidencias y deben tener la información necesaria para poder afrontarlas y la experiencia en su tratamiento y escalado. Igualmente, debe ser capaz de adaptarse a múltiples escenarios cambiantes. En la planificación para la implementación de la célula se deberán considerar los siguientes aspectos:

- Definir funciones a realizar y asignar responsabilidades en ella.
- Establecer los perfiles de sus integrantes y si fuera necesario, atraer personal externo.

- Definir la estructura del centro, tanto física como funcional y las herramientas y aplicaciones que necesitará para su operación (HW y SW).
- Definir las métricas a emplear para la medición del rendimiento alcanzado.
- Establecer una base de datos con HW y SW de los servicios, procedimientos propios de actuación y configuraciones.
- Definir y dar acceso al Catálogo de Servicios, manteniéndolo actualizado y disponible para usuarios y clientes.

Además, el CECIS debe estar equipado con la infraestructura debida para hacer frente a la demanda:

- Herramientas para dar la correcta atención telefónica, con sistema de grabación y monitorización de los puestos de atención.
- Espacio dimensionado para coordinadores y operadores, con cabida para su puesto informático conectado a las diferentes redes manejadas.
- Operadores y coordinadores de área con acceso a las bases de datos con los detalles de los usuarios, apoyados por herramientas que les permitan modificar las configuraciones de red.
- El adecuado reparto de clientes o Unidades a ser atendidas entre los diferentes Centros de Explotación según el área geográfica o localidad de pertenencia.
- Empleando las herramientas de detección y alarma adecuadas que permitan monitorizar con los filtros adecuados el correcto funcionamiento de las diferentes Unidades; si las líneas están activas, tiempo de permanencia en el estado actual y si ha experimentado cortes o interrupciones en un plazo determinado; todo ello para disponer de la adecuada métrica de nivel y calidad de servicio.

Para definir la cantidad de personal necesaria en el CECIS para atender la demanda normal de incidencias y peticiones, es necesario revisar la cartera y el catálogo de servicios de cada organización o unidad apoyada, y así poder establecer un cálculo aproximado de clientes/sistemas que son atendidos y enfrentarlo a la media mensual de incidencias y averías comunicadas por cualquier medio y al tiempo medio estimado de resolución de cada incidencia. Este cálculo nos permitiría conocer la cifra aproximada de personal técnico cualificado que nuestro CECIS debiera tener en plantilla.

3.2.2 Diseño del Servicio

El Centro será accesible por vía telefónica y telemática y estará dimensionado en función de la cantidad de incidencias atendidas en años anteriores, a raíz de las estadísticas obtenidas con objetividad. En base a la cobertura real de plantilla que contemplan nuestros CECIS actualmente, podría plantearse:

- Un coordinador global de la actividad, con responsabilidad en la redacción de informes de seguimiento de la actividad y que actúe ante las incidencias muy críticas y de máxima prioridad y aquellas que hayan superado el margen de tiempo de resolución convenido.
- Un grupo de soporte a operadores y de apoyo al coordinador en cada CECIS, responsable también de la recopilación de información para los informes antes indicados.
- Según el CECIS que se trate, el número de operadores diferirá en función del número y envergadura de las unidades a las que den su apoyo; siendo distribuidos entre los 7 Centros establecidos en la actualidad (figura 1-8 en la pág. 21).

La preparación del Centro para dar los servicios debe incluir un Paquete de Diseño de Servicio (*Service Design Package* - SDP), incluyendo por supuesto la Célula de Mantenimiento propuesta.

Este paquete de diseño debe atender a sus requisitos intrínsicos, el propio diseño del servicio, una valoración previa de la organización para saber si está preparada para su implementación y por último un Plan de Ciclo de Vida del Servicio. Cada uno de estos capítulos del Paquete estará compuesto por subcategorías alineadas con las buenas prácticas ITIL expuestas: requisitos funcionales, de nivel de servicio, plan de transición, evaluación de riesgos y criterios de aceptación.

Siguiendo los procesos de la fase de diseño se proponen las siguientes acciones:

I. Gestión de Niveles de Servicio.

Es necesario hacer acopio de toda la información del paquete de nivel de servicios que se haya desarrollado en la fase anterior, Estrategia del Servicio, y que nos facilite:

- Un Catálogo de Servicios.
- Requisitos de Nivel de Servicio, al objeto de cumplir el nivel acordado, a través de medidas como:
  - reforzar la formación del personal del Centro y en especial de la Célula de Mantenimiento propuesta,
  - disponer de material en stock para atender la demanda,
  - disponibilidad de aplicaciones y herramientas que permitan una ágil configuración y cambio de los equipos y matenga actualizada la base de datos de conocimiento.
- Hojas de especificaciones de los Servicios, donde se definan sus componentes y se debe compartir en la biblioteca de conocimiento.
- Acuerdos de Nivel de Servicios (SLAs) que especifiquen cómo actuar y la atención a proporcionar ante incidencias, tiempos de resolución según servicios y prioridades, periodos de atención y método a seguir según el horario laborable, días hábiles o inhábiles.
- Un programa de mejora del servicio que gestione la implantación de cada servicio revisando los errores y fallos de arranque incial con el fin de corregirlos, lo cual requiere tener un conocimeinto profundo del servicio y sus componentes.
- Un plan de calidad del servicio que contenga objetivos y estrategias del Centro y su célula de mantenimiento, el modelo de gestión de calidad que seguirá y pasos para lograrlo.
- Un Acuerdo de Nivel de Operaciones que exponga los KPIs pactados para las diferentes Unidades y sus servicios, así como la actuación de apoyo y el escalado de las incidencias en los plazos precisos.
- Contactos de soporte con los proveedores, tanto logísticos como de servicios que aporten valor, y que podrían ser compañías propietarias de HW y SW vinculadas a antivirus, a paquetes Office, u otras herramientas.

Es fundamental levantar estadísticas semanales con los datos de llamadas y *tickets* de incidencias recibidas, atendidas, tiempos de resolución y periodos de tiempo en cada estado intermedio hasta finalizarla; aí como realizar reuniones de trabajo para revisar el estado del Centro y adoptar las medidas oportunas que permitan corregir disfunciones organizativas, operativas o administrativas.

Igualmente, será necesario programar reuniones con los CISPOC de las Unidades “cliente” mensual o trimestralmente, para analizar los informes generados en los periodos entre las mismas y ver en detalle la disponibilidad y fiabilidad proporcionada, así como los detalles estadísticos de la atención a las incidencias de distinta índole.

En base a la existencia de tantos tipos diferentes de incidencias, es muy importante que el centro tenga documentado el tratamiento y atención a cada grupo, incluyendo la denominación de la unidad que suele informar, fechas, número de versión por si varía, cambios realizados, ámbito, etc. En apartados posteriores se propondrán acuerdos de nivel de servicio y tiempos de resolución tipo.

II. Gestión del Catálogo de Servicio.

Será un proceso con el objetivo de actualizar y dar accesibilidad a la información necesaria para levantar los servicios, y que para el Centro se enfocará en refrescar todo lo relativo a su mantenimiento, incluyendo las modificaciones a los catálogos de objetivos y técnicos de cada servicio, soporte, infraestructura, software, funcionamiento de las aplicaciones y datos.

Será necesario actualizar el catálogo del servicio, empleando la información que durante el proceso de estrategia se haya generado para su diseño, o sea, la actualización del portfolio. También se actualizarán las dependencias de las Unidades apoyadas y los procesos contenidos en el catálogo.

III. Gestión de la Disponibilidad.

El CECIS debe garantizar un nivel de disponibilidad de servicios igual o mayor a lo acordado con las diferentes unidades apoyadas en los SLAs. Para lograrlo, el personal de la célula de mantenimiento tendrá que monitorizar, realizar mediciones, analizar, efectuar informes y revisar la capacidad de los servicios de forma frecuente. Investigará sus interrupciones, sus componentes y tomará las acciones correctivas oportunas. Deberá planificar, diseñar y mejorar la disponibilidad de manera proactiva.

La disponibilidad se podrá medir en dos niveles: uno garantizando el funcionamiento del servicio en su totalidad, y otro a nivel componente, cuando un elemento falle pero el resto de la infraestructura trabaja correctamente. Nos centraremos en la disponibilidad total a nivel servicio, midiendo este concepto en relación al tiempo activo menos el tiempo no disponible dividido por el tiempo activo.

Otras métricas conocidas que empleará el Centro serán la fiabilidad y la capacidad de mantenimiento, aplicable a la célula propuesta; cuyos valores también serán útiles para evaluar la Capacidad de los servicios.

IV. Gestión de la Seguriad de la Información.

Este proceso supondrá para la nueva Célula de mantenimiento propuesta el asegurar que la información de los procesos internos de las Unidades apoyadas y de la propia organización cumple con los principios de disponibilidad, confidencialidad e integridad. Esto se conseguirá aplicanto estrictas medidas internas en cuanto a:

- Control de acceso a la información con permisos adecuados al nivel de cada operador.
- Control de contraseñas con cambio obligatorio de las mismas con periodicidad mensual.
- Reglas de formato para el correo, relativas al asunto e identificación de destinatarios y remitentes.
- Restricciones en el aceso a contenidos específicos según qué redes se manejen.
- Carga y actualización de antivirus incluidos en listas de SW admitidas por la organización.
- Asegurar contenidos impidiendo la extracción de documentos por puertos USB u otros.
- Facilitando el acceso seguro a los servicios desde el exterior mediante plataformas.

V. Gestión de la Capacidad.

Nuestro CECIS debe ser capaz de atender las incidencias y peticiones entrantes y poseer conocimientos y experiencia suficiente para resolverlas. Tendremos que establecer un procedimiento para medir el rendimiento obtenido en la atención a los usuarios con indicadores precisos y adoptando medidas proactivas, todo reflejado en informes de rendimiento y capacidad que retroalimentarán el Plan de Capacidad del Centro.

Como ejemplo de medidas para la mejora y que formarán parte de este plan:

- Se realizarán revisiones periódicas de los rendimientos y capacidades del Centro, midiendo las consultas por franjas horarias y adaptando la atención en función de la demanda.
- La mejora continua del control de incidencias y del servicio ofrecido.
- Estudiar, negociar y documentar los nuevos requisitos, estableciendo niveles de servicio a alcanzar.
- Planear una nueva capacidad en caso de detectarse que no se provee un servicio con la calidad suficiente.

VI. Gestión de la Continuidad.

El CECIS periférico actualmente no provee de atención 24/7, sino que da cobertura exclusivamente en horario laborable los días hábiles, manteniendo un mínimo servicio de urgencia localizado telefónicamente con personal que atiende emergencias locales. Fuera de este horario se recibe atención centralizada desde CECISMAD en el caso de operaciones y ejercicios en la mar.

Por consiguiente, debe afianzarse un plan que, combinando la atención telefónica y telemática ofrezca un servicio de apoyo sin necesidad de visitar a las Unidades y abierto al escalado de la solicitud hacia el CECIS principal, dotado por este motivo de mayor plantilla, con el fin de asegurar la provisión de los servicios prioritarios 24/7 y reedactándolo en este sentido en el SLA con cada Unidad.

Todo este plan debe quedar reflejado en detalle en el llamado Plan de Continuidad del Centro, donde se concreten los detalles aplicables a la Célula de Mantenimiento. El responsable designado para el seguimiento de este plan deberá actualizarlo con los diferentes cambios, principalmente de infraestructura TI que se produzcan.

El plan deberá ponerse a prueba de forma periódica programando actividades de carga de los servicios que nos permitan conocer sus límites y ajustar a la realidad los niveles acordados. Cada prueba generará el informe de resultados útil para efectuar dichos ajustes y emprender las reformas de infraestructura necesarias para proveer el servicio que realmente necesitan las Unidades.

3.2.3 Transición del Servicio.

I. Gestión del Cambio.

Será necesario, al implementar la Célula de Mantenimiento propuesta dentro de la organización actual del Centro, hacer seguimiento al proceso de cambio desde la estructura actual, manteniendo informados a todos los que puedan verse implicados y/o afectados por el cambio.

Será necesario programar paso a paso el cambio de modelo de atención a incidencias y peticiones, que incluya los siguientes pasos:

- Realización de pruebas sobre prototipos en el Centro con menor número de Unidades y usuarios atendidos, por ejemplo sobre una red no clasificada de poca entidad.
- Se analizará el impacto y se realizarán las adaptaciones necesarias en la organización.
- Se preparará un plan previo de comunicación de cara a los usuarios, Unidades y organización, notificándoles del cambio de gestión y de los nuevos procedimientos para la atención de sus necesidades.
- Se adapatará la formación de los operadores técnicos a las nuevas necesidades a través de cursos de formación.
- Se reforzarán las pautas para el escalado de las incidencias dentro de la estructura de la Célula y del propio Centro, así como las necesidades de formación a todos los niveles.

- Se valorará si los recursos disponibles para atender todas las incidencias son suficientes y se planificará la actualización para su logro.
- Se mantendrá actualizada la base de datos de gestión del cambio, supervisando la eliminación de errores en los documentos e incorporando lo que pudiera ser de utilidad.

La valoración del proceso se afianza contactando con los clientes a la finalización de las incidencias y peticiones atendidas al objeto de conocer de primera mano el grado de satisfacción alcanzado. Los informes conteniendo toda la información relativa a los pasos antes detallados, la percepción de los clientes, los niveles reales de servicio que se han alcanzado y los informes de la gestión de los procesos internos serán elevados a la dirección del Centro piloto y la Jefatura de los Centros (JEGRUCECIS) para evaluar su implementación en el resto de Centros.

El Centro es una Unidad más, que sufre por tanto variaciones de personal en el tiempo; y consecuentemente es necesario nombrar un gestor del cambio que se responsabilice de toda modificación que experimente la organización y su estructura, principalmente en los nombramientos de responsables y la distribución de responsabilidades en cada área; comunicando a las Unidades clientes estas variaciones a tiempo a través de comunicados en el portal de la intranet, WANPG.

Este proceso de cambio y su gestión se aplicará igualmente a la infraestructura de red desplegada para el bien de las Unidades. Se realizarán pruebas aisladas dirigidas por el gestor del cambio con el fin de comprobar una línea, o solo ciertos componentes. Obtenidos los resultados, verificará si se producen mejoras a partir de esta actualización, midiendo la calidad según los parámetros disponibles; y así mismo por comparación medirá la mejora en disponibilidad, capacidad y fiablidad del servicio, línea o equipo/s.

Hecha esta valoración, podrá elevar una petición de cambio al responsable de la Célula de Mantenimiento del Centro, al objeto de programar su presentación al pleno asesor de cambios (*Change Advisory Board* – CAB), de tratarse de un cambio crítico que afecte a un número importante de equipos, y acto seguido proponer al Jefe del Centro su implementación para todas las Unidades de su responsabilidad geográfica.

Este cambio se implementará tras hacer un breve informe de comunicación previa a los clientes, en este caso las Unidades apoyadas, indicando las fases que se seguirány sus pasos, y el plan de marcha atrás de ser necesario. Siendo así conocedores de posibles interrupciones de servicios que pudieran producirse durante el cambio. También se redactará un informe interno posterior a la implementación para que el resultado sea conocido y evaluado por los diferentes gestores del Centro, del Cambio, de la Capacidad, de la Disponibilidad, de los Niveles de Servicio, y la propia Dirección.

II. Gestión de la Configuración y de versiones.

Tendríamos que dividir este proceso en base a las responsabilidades de dos partes diferenciadas de la infraestructura.

Por un lado, en la infraestructura de nuestras unidades cliente, mantener una base de datos con las múltiples configuraciones y versiones de sus equipos, al objeto de recuperar a la mayor brevedad la configuración original en caso de producirse un error o por petición propia.

Por otra parte, en los casos de cambio de configuración de la infraestructura interna del Centro de Servicios, si se categoriza como crítico efectuaremos un plan de comunicación de los cambios de configuración que se efectuarán, detallando fecha, hora y duración, además de tener un apartado de vuelta atrás si fuera necesario.

Ambas bases de datos deben ser accesibles por la Célula de Mantenimiento del Centro para trabajar en planes de previsión de carácter proactivo y aplicar cambios en caso necesario.

3.2.4 Operación del Servicio desde la Célula de Mantenimiento.

Es necesario adoptar nuevas medidas para nuestra Célula, con el objetivo se implementar las buenas prácticas de ITIL vistas en el capítulo anterior, y que serán del tipo:

- Nombramiento y difusión del gestor responsable de la Célula en cada CECIS.
- Definir los requisitos del CECIS para la mejora de la organización y de los servicios a los clientes en la gestión de incidencias y primer soporte.
- Supervisar que la calidad del servicio es adecuada a los acuerdos alcanzados con las unidades cliente (SLAs), apoyándose en herramientas de supervisión y gestión de incidencias. Para el caso de esta metodología propuesta se hará referencia a la herramienta GLPI (Gestión Libre del Parque Informático), aplicación para la gestión de incidencias e inventario informático cuyo prototipo se está implementando en CECISFER (Ferrol).
- La adecuada gestión de las peticiones y consultas de los usuarios y la realización de encuestas de satisfacción, para efectuar mensualmente informes con la información extraída de éstas y del sistema de monitorización.
- Cargando en la web corporativa WANPG el formulario adecuado para que las Unidades puedan realizar consultas sobre los servicios, y que darán lugar al correspondiente aviso en la célula del CECIS para ser atendido según las prioridades del SLA.
- Alimentando las bases de datos del Conocimiento y de Gestión del Cambio con todos los procedimientos de comunicación a consultar por Unidades, usuarios y propios operadores de todas las áreas empleando herramientas de trabajo colaborativo como SharePoint de WANPG o de la red clasificada según la clasificación de su contenido.
- Adiestrando al personal del Centro en la gestión de incidencias, atendiendo debidamente los tickets generados a través de la herramienta de incidencias incorporada.

I. Gestión de Eventos.

Para ofrecer un servicio de calidad es imprescindible dominar el funcionamiento de la nueva herramienta de monitorización, determinando los eventos que empleará la Célula para garantizar la disponibilidad de las comunicaciones. El Centro estará atento a dos tipos de eventos principalmente:

- Perdida del acceso a un servicio por las Unidades: Se abrirá un ticket en la aplicación de gestión de incidencias y se establecerá contacto con el CISPOC de la Unidad para comprobar si es corte de alimetación, apagado del propio cliente o una avería del circuito.
  Si es avería de circuito, la célula de mantenimiento coordinará la supervisión presencial del mismo. De no detectarse avería en el circuito, se escalará la incidencia al departamento responsable de la red de acceso. Podrá tratarse del CECISMAD o el propio CESTIC.
- Interrupciones intermitentes en el acceso: También se abrirá un ticket inicial para gestionar la incidencia desde la Célula de Mantenimiento y se mantendrá informado al cliente a través de la misma aplicación con los cambios de estado, incorporando novedades a cada paso. En todo caso se informará periódicamente del avance de la incidencia a la unidad.

La tipología de eventos que la célula atiende y el centro opera irán incrementando a medida que la base de datos del conocimeinto y de gestión de incidencias se vaya nutriendo con nuevos eventos y detecciones, lo cual enriquecerá nuestro proceso de mejora continua.

II. Gestión de Peticiones.

Las peticiones y consultas que realicen los usuarios de las diferentes Unidades se encaminarán a la Célula de Mantenimiento, quien las gestionará siguiendo el procedimiento que establezcamos. Estas

peticiones serán relativas a la modificación en el ámbito de los datos o de la voz, dos grandes grupos en los que diferenciamos los servicios facilitados desde el CECIS.

III. Gestión de Incidencias.

Lo más eficiente será nombrar un responsable del proceso de gestión de incidencias, quien se responsabilizará de supervisar que se realizan las siguientes actividades:

- Gestionar las incidencias y la asistencia de soporte para su diagnosis en primera instancia y darles tratamiento. Si es necesario las escalará a las áeras responsables según su tipología.
- Supervisar el grado de cumplimiento de los niveles acordados en los SLAs establecidos.
- Clasificar los incidentes según supongan corte de servicio, avería de componentes sin perdida de comunicación y avería de área local del cliente y que le supone incomunicación.
- Realizar informes particulares y periódicos de la gestión de incidencias, apoyándose en las métricas obtenidas de la herramienta de gestión empleada, cubriendo los procedimientos de comunicación con los usuarios y los escalados realizados por sus responsables.

Los operadores necesitan tener acceso al registro histórico de incidencias de un mismo cliente para acelerar los trámites en caso de su repetición. Esta misma base de datos históricos será de utilidad para el gestor de problemas, pudiendo así reconocerlos y evaluar el riesgo que suponen según la cantidad de averías que comparten diagnóstico.

Las tareas eminentemente proactivas que nuestra Célula de Mantenimiento realizará en aras de reducir el número de incidencias serán:

- Mantenimientos de routers, switches y puntos de acceso por fallos de SW, actualizaciones de versiones o sustitución de partes o por completo por su mal funcionamiento.
- Mantenimiento de líneas en las diferentes secciones de su cableado, terminaciones y rosetas de conexión.
- Modificaciones en la configuración de las Unidades cliente que requieran presencialidad.

Para todas ellas habrá un procedimiento prestablecido según el tipo de equipo de la infraestructura afectado y que será seguido por el operador en la atención de cada incidencia, paso a paso.

IV. Gestión de Problemas.

Ya vimos que las incidencias repetitivas finalmente se definían como problemas. Igualmente al caso anterior, se nombrará a un responsable del proceso de gestión, responsable de las incidencias reiterativas para uno o varios clientes con la misma afección, así como de los errores bien conocidos.

ITIL nos orienta hacia la aplicación de una solución al menos parcial al problema, mientras la Célula de Mantenimiento trabaja por encontrar la solución final más adecuada.

3.2.5 Mejora Continua del Servicio desde la Célula de Mantenimiento

En el Centro nombraremos un gestor de mejora continua, quien deberá revisar el estado de los servicios y de la gestión de cada uno. Para desempeñar esta función necesitará:

- Realizar informes de punto de situación a partir de las métricas obtenidas en la fase de operación y poder evaluar la gestión interna de las incidencias y la valoración de los clientes sobre dicha gestión. Seguidamente auditorías internas permitirán obtener conclusiones de referencia.
- Evaluar si debemos cumplir los objetivos de servicio marcados u otros nuevos según la estrategia de la Jefatura CIS o de la propia Armada.

- Confeccionará una lista con las acciones de mejora continua admisibles según los resultados que obtenga, para su validación por la Jefatura del GRUCECIS.
- Comprobará si mejoran los resultados con las acciones validadas por la estructura CIS, basándonos de nuevo en los KPIs marcados para cada servicio y proceso y en los informes de cada gestión. Deberá generar de manera cíclica planes de mejora del servicio y actualizar la lista de acciones.

3.3 Service Level Agreement (SLA) de un CECIS

Como se ha explicado en sucesivos apartados hasta este punto, todas las condiciones relativas al método en que se gestionarán y proveerán los servicios a las Unidades apoyadas deberían quedar plasmadas sobre un documento firmado por ambas partes. Por un lado la Jefatura del Grupo de Centros de Explotación (JEGRUCECIS), y por otro el Mando de la Unidad apoyada. En caso de pertenecer la Unidad a una Escuadrilla o conjunto de unidades del mismo tipo en el área geográfica, podría elaborarse un único acuerdo de nivel de servicios común a todos.

En este apartado del Capítulo 3 no se pretende incluir un modelo fijo y completo de SLA, sino expresar con ejemplos los diferentes conceptos vistos a lo largo del trabajo, siguiendo los procesos de gestión y buenas prácticas de ITIL e ISO, y que deberán detallarse en el acuerdo entre las partes involucradas.

En primer lugar, el documento comenzará con la recopilación de las diferentes referencias en las que estará basado el acuerdo entre las partes, como por ejemplo la Organización de la Armada y su Estructura CIS, las relaciones de dependencia de la Unidad apoyada y los Servicios de voz y datos que debe disponer, los contratos establecidos con proveedores de servicios externos, el plan anual de ejercicios y operaciones en los que la Unidad participará y que supondrán servicios, dedicación y prioridades extra por parte del CECIS, las necesidades de adiestramiento del personal CIS de la Unidad y que serán impartidas por el personal de la Célula de Mantenimiento del CECIS, un listado de servicios centralizados por el CESTIC y fuera del ámbito de este SLA particular o con un mínimo nivel de apoyo por parte del CECIS como intermediario o interlocutor con su proveedor.

3.3.1 Servicios proporcionados y/o apoyados por el CECIS.

A continuación incluiremos una tabla con los servicios que el Centro provee a las unidades de su ámbito (tabla 3-1 del Apartado 3.2) y otra con los servicios centralizados en el CESTIC, donde el CECIS de apoyo actúa como intermediario y coordinador de zona (tabla 3-2, a continuación).

Categoría de servicio	Servicio	Servicios de Gestión CECIS	Necesidades coordinación
Servicios de Usuario (acceso a aplicaciones de usuario)	• Acceso WAN-PG • Correo corporativo • Acceso Internet a través de la WAN-PG • TEMD/PKI	• Gestión peticiones e incidencias se realiza vía SCANS • CECIS resuelve incidencias a su nivel y actúa como controlador intermedio SCANS • Gestión Local tarjetas e incidencias TEMD/PKI	• UCO´s deben mantener actualizados CISPOC´s para gestión peticiones e incidencias vía SCANS
Servicios de Información de Comunidades de Interés	• Acceso SIMENDEF • Acceso Internet Libre • Acceso Extranet • Acceso Red Wifi M&W • Acceso Red SARA • Acceso SIJE • Acceso SICOMEDE • Acceso NSWAN • Acceso SICONDEF. • Acceso BICES.	• Administración Local SIMENDEF y gestión incidencias vía aplicación CECISMAD • Gestión peticiones e incidencias Sistemas NO Clasificados se realiza vía SCANS • Gestión de acceso a los Sistemas Clasificados se hace conforme a procedimientos específicos POS	• Gestión peticiones e incidencias Sistemas NO Clasificados se realiza vía GLPI • Terminales Usuario (TU) y documentación clasificada deben mantenerse dentro ZAR acreditada conforme IPSEG 308 • Para manejar Sistemas Clasificados el AOSTIC Local debe solicitar previamente la acreditación del nodo

	• Acceso CENTRIXS. • Acceso SIGLO. • Acceso HERCULES.	• Gestión de incidencias Sistemas Clasificados se coordina por mensajería SACOMAR • Configuración y administración local de TU´s Sistemas Clasificados (NSWAN) y NO Clasificados (Internet Libre, Extranet) • Configuración y administración local periféricos (impresoras, escaner, etc) y electrónica de red (switches, UPS, etc) de los Sistemas Clasificados (NSWAN) y No Clasificados (Internet Libre)	conforme IPSEG 302 • Usuarios Sistemas Clasificados deben disponer HPS y conocer POS • Solicitud acceso usuarios corresponde a Jefe UCO valorando necesidad conocer • Acceso buques a SMN,SIJE y NSWAN según Procedimiento Operativo GRUCECIS 01/17
Servicios de Información de Núcleo	• Administración centralizada de servidores • Administración centralizada de terminales de usuario • Servicio de monitorización • Servicio de sincronización	• Configuración y administración local servidores WAN-PG buques y UCO´s área responsabilidad geográfica (excepto servidores de correo) • Monitorización servidores WAN-PG • Configuración y administración local de TU´s WAN-PG • Configuración y administración local periféricos (impresoras, escaner, etc) y electrónica de red (switches, UPS, etc) conectados a WAN-PG • Control Inventario y Catalogo de equipos (HW y SW) Sistemas NO Clasificados	• Servidores asignados a las unidades deben permanecer dentro de zonas protegidas o restringidas
Servicios de Telecomunica-ciones	• Telefonía Fija • Telefonía Móvil • Conexión terrena I3D / IPC2 • Conexión satélite • Interconexión con OTAN (pendiente) • Administración centralizada de routers y firewalls	• Gestión peticiones e incidencias telefonía se realiza por unidades vía GLPI (PENDIENTE) y por el CECIS con el CAU vía SCANS • Gestión peticiones e incidencias conexión terrena por mensaje SACOMAR (JECOE AR) • CECIS resuelve incidencias a su nivel y actúa como controlador intermedio SCANS • CECIS controla y distribuye los terminales móviles y los equipos FAX • CECIS supervisa actualizaciones Guía Telefónica MINISDEF en su área responsabilidad geográfica • CECIS administra y controla la infraestructura LAN de los Sistemas CIS Clasificados y NO Clasificados • CECIS actúa como 2do escalón de asistencia y soporte técnico infraestructura LAN-CIS • CECIS actúa como coordinador conexión terrena I3D/IPC2 en área responsabilidad geográfica • CECIS actúa como supervisor asentamientos RCT dentro de su ámbito de responsabiliad. • CECIS apoya configuración router WAN-PG buques con satélite	• Gestión peticiones e incidencias telefonía se realiza por unidades vía GLPI. • UCO´s deben mantener actualizados CISPOC´s para gestión peticiones e incidencias telefonía (SCANS), conexión terrena (SACOMAR) e infraestructura LAN´s (peticiones por SIMENDEF e incidencias a su CECIS. • CISPOC debe mantener actualizada su UCO en la Guía Telefónica del MINISDEF • UCO actúa como primer escalón mantenimiento (supervisión red interior telefonía / LAN, supervisión asentamiento RCT, arranque generadores emergencia STM, etc.) • CEZMAN actúan como 2do escalón de asistencia y soporte técnico conexión terrena I3D/IPC2 • UCO gestiona peticiones e incidencias conexión satélite por mensaje SACOMAR (JECOE AR) • Necesario contemplar un recurso económico para atender incidencias infraestructura LAN-CIS y red interna telefonía
Servicios de Seguridad de la Información	• Administración centralizada cifradores y cambio claves • Servicios centralizados de Backup (SIMENDEF, correo) • Gestión centralizada Incidencias Ciberdefensa	• Subcuenta Cripto CECIS controla y distribuye equipos cripto de las UCO´s del área responsabilidad geográfica • Gestión de incidencias Cripto de las UCO´s del área de responsabilidad geográfica. • Deposito Cripto de claves futuras, de reserva y “pool” equipos Cripto para su área de responsabilidad. • Transporte de material Cripto entre la cabecera de distribución	• UCO´s deben tener nombrados Cripto-Custodios • Equipos cripto asignados a las unidades deben permanecer dentro ZAR Clase I • CISPOC´s y administradores WAN-PG delegados de las UCO´s colaboran en la supervisión sistema Backup de sus nodos WAN-PG locales • Backup local de Sistemas Clasificados conforme CO-DRES-POS de cada nodo

		y su área de responsabilidad. • CECIS configura y supervisa el servicio Backup de los servidores de WAN-PG de las UCO´s área de responsabilidad geográfica • CECIS actúa como Responsable Gestión Incidencias Ciberdefensa (RGI) del área de responsabilidad geográfica, en coordinación con COS-AR	
Servicios de Gestión	• Gestión de servicios centralizada	• Servicios verticales de gestión CECIS incluidos en esta columna • Atención a incidencias CIS 24/7 por Guardia Comunicaciones y Seguridad CECIS	• Necesidades de coordinación y gestiones delegadas a incluir en posibles SLA

Tabla 3-2. Servicios que gestiona el CESTIC en colaboración con los CECIS y CISPOC de las Unidades apoyadas.

A continuación de los servicios proporcionados y asistidos por el CECIS local, el SLA suele contener un desglose del equipamiento hardware entregado a la Unidad, según catálogo de servicios, vinculado a todos y cada uno de estos. Será responsabilidad de la Unidad, desde la firma del Acuerdo, la contabilidad y buen uso del mismo. Otra opción es su inclusión como anexo al final del documento.

3.3.2 Prioridades en la Gestión de incidencias.

En el Acuerdo habrá un capítulo reservado a indicar cuáles son las prioridades establecidas por la Unidad apoyada, el cliente, y que tendrán una atención específica según los parámetros pactados. Los siguientes servicios específicos son solo un ejemplo, indicando su código, nombre, Unidad, Urgencia e Impacto de la incidencia, nivel de prioridad y condición/es para ser atendida según el Acuerdo.

Código del Servicio	Nombre del Servicio	Unidad de aplicación	Urgencia	Impacto	Nivel de prioridad	Condición para aplicar el nivel de prioridad
CEC008	Infrastructura de almacenamiento de datos en redes WANPG y clasificadas	CGMAD	Alta	Alto	P1	Pérdida completa de Servicio de las bases de datos en WANPG y SMN
CEC005	Apoyo a la Ciberseguridad por expertos	CGMAD	Alta	Alto	P1	Incidente Ciber que afecta a la totalidad de la Unidad
CEC002	Acceso a internet local	CGMAD	Alta	Alto	P1	Pérdida de acceso a internet del personal de servicio
CEC001	Presentación operacional continua	CGMAD	Alta	Alto	P1	COP de SMN
CEC004	Portal Sharepoint de WANPG y SMN	CGMAD	Alta	Alto	P1	Perdida completa de acceso en el CGMAD
CEC006	Servicio de Radiodifusión de submarinos (VLF)	CGMAD	Alta	Alto	P1	Pérdida del Servicio en el CGMAD
CEC006	Apoyo al Servicio de HF	CGMAD	Alta	Alto	P1	Pérdida completa del Servicio de HF
CEC004	Servicio ICC Nacional	CGMAD	Alta	Medio	P2+	Pérdida de acceso para el personal de guardia
CEC005	Apoyo a la Ciberseguridad por expertos	CGMAD	Alta	Medio	P2+	Necesidades de parcheo crítico

Código del Servicio	Nombre del Servicio	Unidad de aplicación	Urgencia	Impacto	Nivel de prioridad	Condición para aplicar el nivel de prioridad
CEC008	Servicio de aprovisionamiento de repuestos esenciales	CGMAD	Media	Medio	P3	CECISROT proveerá apoyo de primel nivel de repuestos HW
CEC004	Aplicaciones principales de Servicio de localización cartográfica	CGMAD	Media	Medium	P3	
CEC004	Aplicaciones de gestión de la información de inteligencia	CGMAD	Media	Medio	P3	
CEC003	Conexión local de los teléfonos BICES de voz Segura IP (VoSIP)	CGMAD	Media	Medio	P3	Mantenimiento de la conectividad por fibra apoyada por el CECIS.

Tabla 3-3. Prioridades en la Gestión de incidencias

Ambas partes negociarán uno a uno los servicios y las condiciones para la priorización de cada uno de ellos. Serán revisadas regularmente y cambiadas según se solicite a través de los procesos establecidos entre el CECIS y las Unidades.

Es posible que se imponga una repriorización sobre los servicios de una Unidad en base a los requisitos operativos sobre ésta, llegando incluso a anteponerse a otros servicios críticos de otras Unidades apoyadas por el mismo CECIS. Por ejempo, durante el alistamiento operativo de un buque previo a su despliegue en misión internacional.

Ambas partes son conscientes de este hecho y aceptan el posible impacto de las operaciones sobre el SLA, dando lugar a una posible degradación o cambio repentino de la demanda de servicios CIS. No sólo las operaciones se contemplan, sino también ejercicios nacionales e internacionales programados. Por ello, el SLA contendrá también el apoyo específico CIS que recibirá la Unidad en la preparación y desarrollo de los ejercicios previstos durante el año, con información de cantidad y capacidad requeridas. Se detallarán las necesidades de personal y equipamiento extra con una antelación de al menos 30 días a su comienzo y las horas extra de apoyo técnico para determinados servicios que pudiera prever.

3.3.3 Términos y Condiciones

En este cápitulo del SAL se desarrollan los términos del acuerdo entre las partes, con diferentes apartados y las condiciones que les vincularán para los servicios previstos. Así, podemos encontrar la siguiente información:

- Se identifica al CECIS como el principal proveedor de servicios de las Unidades clientes basadas en la misma zona geográfica, quedando reguladas las relaciones entre ambos por el presente acuerdo de nivel de servicio. Se entenderán ambas como Partes del acuerdo.
- Desde un punto de vista cualitativo y cuantitativo los servicios provistos serán considerados con independencia de su procedencia y serán de dos tipos: catalogados y no catalogados.
- Los puntos de referencia para la monitorización, toma de medidas e informes de la Calidad de los Servicios se establecerán en los puntos de acceso a la Unidad apoyada y cotejados desde la unidad de gestión de incidentes en la Célula de Mantenimiento del CECIS.
-

I. Horario laborable de la Unidad apoyada

Días de la semana	***Horas de trabajo (Periodo para la medida de Calidad del Servicio)***
Lunes - Viernes	*08:00 – 15:00*
Fines de semana y festivos	*No*

Lunes-Domingo	*24/7* *(Sólo el Centro de Operaciones Marítimas)*

II. Entrada en vigor, duración y marco del acuerdo.

Lo normal será una duración anual, de 1 de enero a 31 de diciembre, siendo posible su extensión de mutuo acuerdo por escrito (esta situación se puede dar cuando la renovación no se realiza en plazo por no alcanzar de común acuerdo una solución para las futuras condiciones deseadas). Cualquier cambio a este acuerdo especificará en un anexo todas las diferencias acordadas a partir de la fecha de firma y aceptación del cambio.

El marco vendrá definido por los servicios catalogados principalmente, y contendrá su definición, nivel de servicio base (*baseline*) y esfuerzo descrito en horas de dedicación. Aquellos servicios que no estén catalogados pero históricamente sea probado que se han entregado hasta la fecha, se considerarán incluidos en el marco de este acuerdo. Cualquier variación o adición a cualquier servicio existente seguirá el proceso de gestión de peticiones (*Customer Request Form* – CRF).

Por otro lado, la solicitud de servicios dentro del catálogo de servicios del CECIS pero no entregados a la unidad hasta el momento, podrán ser solicitados fuera del marco de este acuerdo a través del proceso de Solicitud de nuevos servicios (*New Service Request* – NSR). Ambos procesos serán objeto de aprobación de las autoridades citadas en el documento del acuerdo.

III. Autoridades.

Las personas autorizadas a realizar modificaciones o cambios que pudieran encontrarse fuera del marco del presente acuerdo y cuya firma es impresicindible sobre los requisitos por escrito, son los siguientes:

- Del cliente, el Comandante de la Unidad, COMCGMAD.
- Del proveedor, el Almirante Jefe CIS (AJECIS).

Las personas autorizadas a realizar modificaciones o cambios que estén dentro del marco del presente acuerdo, de mutuo acuerdo entre las partes y siendo responsables del control y la coordinación de los requisitos del mismo, son;

- Del cliente, el Jefe del Estado Mayor del CGMAD.
- Del proveedor, el Jefe del Grupo de CECIS (JEGRUCECIS).

Las personas autorizadas para la coordinación diaria como autoridad de la gestión de servicios, con capacidad para programar la provisión y entrega de los servicios, así como coordinar, monitorizar, informar y controlar su nivel, son:

- Del cliente, el Jefe de la Sección CIS (N6).
- Del proveedor, el Jefe del CECIS de apoyo (JECECISROT).

Todas las notificaciones y comunicaciones entre las partes se intercambiarán empleando las direcciones oficiales de los anteriormente indicados. Además, están abiertas las vías de diálogo y coordinación diario entre las partes a través de sus representantes técnicos con el fin de coordinar, monitorizar, informar y controlar la gestión de la calidad de los servicios reflejados en el acuerdo. En este caso son:

- Del cliente, el CISPOC de la Unidad en su Sección CIS (N6).
- Del proveedor, el Jefe de la Célula de Mantenimiento del CECISROT.

En toda Unidad y CECIS se nombrará un *Service Level Manager* – SLM, responsable de la redacción del Acuerdo entre las partes, así como del seguimiento de su ejecución y aquellas actividades orientadas a la coordinación, control e información sobre los servicios facilitados.

IV. Roles y responsabilidades

A continuación se exponen algunos de los puntos que deben considerarse en la coordinación de las actividades entre las partes del acuerdo, y que se incluirán en la redacción del documento vinculante.

Por un lado, la Unidad cliente permitirá al CECIS desarrollar sus operaciones en la entrega del servicio garantizándole el apropiado acceso a las zonas y sistemas sin retrasos fuera de lo razonable.

Dará las instrucciones, información, priorizaciones o decisiones razonablemente necesarias para que el CECIS pueda hacer entrega de sus servicios.

Mantendrá al CECIS informado de los cambios en las prioridades operarivas que pudieran afectar a los requisitos CIS o tener impacto en la capacidad del CECIS para mantener los niveles de servicio acordados.

Será la unidad cliente la responsable de definir y validar los requisitos CIS locales, así como de obtener la autorización de sus órganos superiores para su obtención e instalación. Así mismo, será el principal responsable en la definición de la ejecución e informes de la gestión de servicios (Service Management Performance and Reporting).

Notificará siempre que sea posible y con antelación suficiente sus necesidades de servicios, teniendo en consideración para la planificación, programación y desarrollo del presupuesto anual las interconexiones que pudiera haber entre diferentes servicios.

La Unidad priorizará las actividades y el empleo de los recursos, observando los compromisos adquiridos con el CECIS y las consecuentes acciones que ya se hayan podido desarrollar por tal acuerdo.

Apoyará en la revisión periódica y actualización del acuerdo para asegurar que el CECIS y la organización a la que pertenece y su personal reciben el suficiente apoyo para la ejecución del acuerdo.

Por otra parte, el CECIS proveedor entregará los servicios de acuerdo con este documento y de una forma consistente y fiel a los estándares nacionales y OTAN, a sus políticas, y códigos de buenas prácticas.

El CECIS mantendrá informadas a las Unidades de los estudios y evoluciones que pudieran afectar al nivel de servicio entregado bajo el marco del presente acuerdo. Les informará de cualquier retraso conocido o amenaza que pudiera afectar a la disponibilidad de cualquier servicio incluido en el acuerdo, así como de las medidas adoptadas para mitigar sus consecuencias.

Desarrollará los acuerdos contractuales necesarios para proveer los servicios acordados a través de terceros y asesorará a las Unidades en sus previsiones y solicitudes de requisitos anuales.

Proveerá de un Servicio Centralizado de atención al usuario con horario 24/7, facilitando la capacidad y disponibilidad necesarias para que pueda desarrollar plenamente sus funciones operativas, tal y como se hayan definido en los SLA.

Asistirá a las unidades en las gestiones necesarias para tramitar nuevas solicitudes de servicios no previstas en el acuerdo inicial, a través del diseño del proyecto, su orientación y objetivos, de la descripción de los paquetes de trabajo, misiones y entregables, detallando los esfuerzos para conducir los servicios y definiendo la previsión temporal de implementación y previsión del gasto.

El CECIS mantendrá la provisión de servicios esperada y las herramientas operativas de planificación a disposición de las unidades apoyadas y en el nivel de alistamiento adecuado para que puedan afrontar la demanda operacional que sus mandos pudieran exigir.

En relación a la propiedad y gestión del equipamiento CIS desplegado en las unidades, todos los medios y la infraestructura son adquiridos bajo el amparo de la organización CIS y por tanto pertenecen a la Jefatura CIS de la Armada.

Las Unidades apoyadas nombrarán a un responsable de la contabilidad del equipamiento, que generalmente será el CIS POC principal (de la sección o destino CIS), y que custodiará, controlará y velará por la seguridad del equipamiento CIS inventariado que se le ha entregado a su Unidad.

Este responsable vigilará que el equipamiento se mantenga en condiciones de empleo adecuadas y coordinará con el resto de CIS POC internos, de las restantes secciones y destinos, para la reparación, sustitución, puesta fuera de servicio y baja de los equipos según las incidencias.

Además realizará recuento anual del inventario bajo su responsabilidad y notificará a la mayor brevedad del equipamiento extraviado, dañado o destruido; así como presentará todos los hechos que obren en su poder para justificar tal incidente. La Unidad será responsable económicamente de los daños ocasionados por un maltrato demostrado.

V. Informes.

El CECIS de apoyo se reunirá trimestralmente con la Unidad apoyada, en concreto con su representante para el SLA al objeto de revisar, entre otros aspectos:

- El estado de la entrega de servicios de acuerdo con el SLA.
- La situación de los requisitos actuales y los nuevos.
- La previsión de actividades actuales y a futuro para la entrega de servicios.
- La situación de personal e impacto sobre la entrega de servicios.

Igualmente a final de año rendirá un informe completo que detalle el nivel de entrega de servicios alcanzado, aquellos que no han superado las expectativas y niveles acordados y una estimación de cara al año siguiente para la renovación del acuerdo en función de las actividades previstas por las unidades y los nuevos requisitos oportunamente notificados en las reuniones trimestrales anteriores.

Los desacuerdos serán tratados y resueltos siempre que sea posible al nivel más bajo de participación entre los representantes de ambas partes, a través de negociación y discusión, sin necesidad de llegar a recurrir a estamentos o autoridades superiores que tengan que mediar. En el caso de ser imposible alcanzar un acuerdo, serán las autoridades firmantes las que en último caso llegarán a un punto medio que les satisfaga por igual.

3.3.4 Gestión de Servicios

Es en esta sección del Acuerdo donde se redactarán los procesos que se seguirán para la gestión de los servicios concertados, en base a las buenas prácticas de estándares internacionalmente reconocidos y a procedimientos de trabajo puestos en práctica en múltiples empresas gestoras de TI, asignando responsabilidades e incluyendo al menos los siguientes apartados:

I. Procedimientos conjuntos para la entrega de servicios.

En este apartado se redactarán todas aquellas actividades relacionadas con la entrega de servicio en la que tanto la Unidad como el CECIS puedan tener una participación conjunta, como por ejemplo los roles que debe asumir cada CIS POC en la entrega de servicios.

También se suelen describir procedimientos diversos, como las actuaciones aprobadas ante el silencio por parte de usuarios a consultas, y también misiones y responsabilidades compartidas en el proceso de gestión del cambio.

II. Descripción del Ops Centre.

El Centro de Operaciones proveerá atención 24/7 a través del *Service Desk* centralizado y será responsable del proceso de gestión de incidencias. En nuestro caso esta centralización se realizará en el

CECISMAD, con su personal de guardia fuera de horario laboral y atendidas localmente en el horario laborable desde la Célula de Mantenimiento del CECISROT.

Será responsable de la gestión de incidencias, gestión de accesos, autorizador en la gestión de peticiones de Cambio y gestión de Eventos durante su ciclo de vida completa, así como responsable del inicio de la gestión de Problemas.

Será también responsable de notificar a la Unidad el escalado de las incidencias en cada caso, al objeto de alcanzar los niveles de Calidad de Servicio planificados.

III. Niveles de apoyo.

Quedarán definidos en el Acuerdo los diferentes niveles de apoyo que el CECIS proveerá a las Unidades. Por ejemplo, se proponen los siguientes:

- Nivel 0. El apoyo puede ser llevado a cabo por el propio usuario final o el CIS POC de la Unidad implicada sin participación física de ningún especialista IT del CECIS. Se reduce a soluciones que requieran exclusivamente los permisos del usuario final, el reseteo de claves o cuestiones incluidas en las preguntas frecuentes de los clientes (*Frequently Asked Questions* – FAQ). Podrá ser atendida por un servicio automático o teleoperador. Tiene por objetivo reducir la interacción directa de los clientes con el *service desk* del CECIS, a través de una herramienta sencilla que solucione las cuestiones más básicas y rutinarias que dan lugar a consulta diaria. Este nivel no engrosaría las estadísticas de peticiones de servicios o creación de incidencias.
- Nivel 1. Sería la primera línea de atención técnica que comunicará directamente con los usuarios afectados. Este nivel incluye recibir, categorizar, diagnosticar y resolver incidencias y eventos relacionados con CIS y Ciberseguridad. La atención es proporcionada por la Célula de Mantenimiento del CECIS, que se responsabilizará de las gestiones necesarias con su estructura organica para dar solución a la incidencia de principio a fin, incluyendo la coordinación con los niveles 2 y 3 de apoyo y del cierre definitivo de las peticiones de servicio y de todos los incidentes. Será también responsable del escalado de los incidentes al nivel 2 cuando su personal técnico no pueda resolverlos.
- Nivel 2. Este nivel proveerá el apoyo técnico para la investigación y diagnóstico de los incidentes, estudiando de extremo a extremo el servicio, tomando las acciones oportunas para su resolución y recuperando el servicio afectado. En caso de no ser capaz de darle solución, podrá escalar la incidencia y los problemas identificados al nivel 3.
- Nivel 3. Este nivel supone un servicio de especialistas y agentes, algunos externos, específicamente cualificados para un servicio o sistema concreto. Generalmente es necesario para probar e implementar cambios en los sistemas o en la *baseline* del servicio. Suelen ser expertos en la materia (*Subject Matter Experts* – SME) integrados en la línea del propio servicio o procedentes de proveedores externos.

Todas las actividades realizadas desde el nivel 1 al 3 serán almacenadas en la herramienta de gestión de servicios IT que emplee el CECIS en su labor como proveedor de servicios. Se ha visto en el capítulo anterior las diferentes herramientas que se están empleando actualmente en el ámbito del CESTIC y de otros Ejércitos, dejando para un apartado posterior la herramienta que para nuestro ámbito naval se propone.

Sirve la figura 2-9. Niveles de asistencia y relaciones, del apartado 2.5.1, como buen ejemplo gráfico de esta clasificación de niveles de apoyo a aplicar en nuestro CECIS, siguiendo el modelo aplicado por la OTAN en sus Centros de Apoyo.

IV. Horario de asistencia.

Para atender los servicios rutinarios y de gestión básica diaria, el CECIS deberá dar asistencia a los incidentes que surjan, de acuerdo a un plan de cobertura de personal y atención que quede reflejado y bien claro para los usuarios de la Unidad apoyada en el SLA. A modo de ejemplo, se propopone la siguiente tabla:

Días de la semana	**Horas de Asistencia**		
	Nivel 1[26]	**Nivel 2**	**Nivel 3**
Lunes - Jueves	24/7	08:00 – 17:00	08:00 – 16:30
Viernes	24/7	08:30 – 16:00	08:30 – 14:00
Fuera de horario laboral, fines de semana y festivos nacionales	24/7[27]	Limitado / Localizable [28]	Localizado (UC[29])
Excepciones			
Elementos apoyados	**Requisitos de apoyo CIS**		
Centro de Operaciones Marítimas	Asistencia 24/7 presencial dando cobertura de nivel 1por personal del CECIS de apoyo. EL propio CECIS será quien solicite la asistencia de nivel 2 o 3.		

Tabla 3-4. Horario de asistencia del CECIS

El nivel 1 de apoyo, aunque esté centralizado en el Centro de atención a usuarios (*Centralized Service Desk*), sera cubierto y atendido por el personal técnico del CECIS geográfico, que se desplazará a la unidad apoyada para afrontar y manipular la incidencia de ser necesario. En el caso de requerir aistencia de nivel 2 ó 3, sera la Célula de Mantenimiento del Centro quien lo solicite o la línea del servicio en cuestión.

V. Gestión de Incidencias.

El propósito será restaurar la operatividad normal del servicio de acuerdo a los tiempos de restauración acordados, o tan pronto como sea posible al objeto de minimizar el impacto adverso en la mision de la Unidad. El término (First-Call Resolution – FCR) se refiere a la atención y reparación de una incidencia a traves de la primera y única llamada del usuario a la Célula de Mantenimiento, sin necesidad de contacto posterior o asistencia técnica superior.

Se detallarán en este apartado las Prioridades consideradas para la reparación y subsanación de incidencias, donde se asignará una primera valoración a cada ticket abierto en función de los valores proporcionados inicialmente por la tabla 3-3 del subapartado 3.3.2.

Como algo excepcional, una Unidad podrá solicitar que se eleve la prioridad de un ticket en concreto. Solo los representantes incluidos en la lista acordada entre el CECIS y la Unidad podrán hacer esta petición. Será estudiada y en cualquier caso estará supeditada a que sea posible su ejecución en el momento, así como confirmada por el representante nombrado como autoridad en el apartado Terminos y Condiciones del Acuerdo (subapartado 3.3.3, párrafo III).

[26] Asistencia 24/7 proporcionada por el Servicio Centralizado de atención del CECIS.

[27] Fuera de horario laborable y en festivos, la Célula de Mantenimiento está disponible 24/7 con los mimos objetivos de calidad de servicio acordados, asumiendo que el volumen de incidencias y llamadas del cliente serán mucho menores.

[28] Limitado / Localizable cuando se trate de una atención fuera del rango de los expertos en la Célula de Mantenimiento. No obstante, el CECIS pondrá todos los medios disponibles para dar la asistencia debida en estos periodos.

[29] UC son los contraltos con terceros para dar apoyo al CECIS en la asistencia de ciertos servicios.

El CECIS deberá proveer a la Unidad de acceso a la funcionalidad de escalado en la herramienta de gestión de servicios IT empleada, al objeto de poder ver en tiempo real el estado de las incidencias, así como datos históricos de cada incidencia grabada en relación a sus servicios. Será aquí donde el representante autorizado podrá redactar sobre el ticket el cambio que se solicita y el motivo. Hecho esto lo comunicará a la Célula de Mantenimiento al objeto de ponerlo en conocimiento del responsable de gestión de incidencias.

La repriorización de un ticket también puede verse influida por la valoración del gestor de incidencias de la Célula de Mantenimiento, en coordinación con el representante de la Unidad, justificando así una desviación lógica de la tabla de clasificación de referencia; y también por el *feedback* de la Unidad durante el proceso de recuperación.

Es normal establecer una tabla de tiempos como la siguiente, conteniendo los objetivos de reparación de los servicios en función de la prioridad identificada previamente.

Tiempo desde la apertura de la incidencia hasta su asignación	P0 = 30mins de reloj	P1 = 1h de reloj	P2+ =1h En horario laboral P2- = 2h En horario laboral	P3 = 9h En horario laboral o 1 día de trabajo	P4 = 18h En Horario laboral o 2 días de trabajo
Tiempo desde la apertura de la incidencia hasta que el servicio es restablecido (con independencia de la resolución del fallo)	1h de reloj	4h de reloj	P2+ = 8h de reloj P2- = 8h de horario laboral	P3=18h De horario laboral o 2 días de trabajo	P4=27h De horario laboral o 3 días de trabajo
Definiciones subyacentes	Servicio alternativo listo como plan de continuidad; y las capacidades de backup alistadas	Servicio alternativo listo como plan de continuidad; y las capacidades de backup alistadas	Reacción inmediata al aviso (*on call* fuera de oficina)	Para el siguiente día laborable	Al final de la lista de prioridades

Tabla 3-5. Tiempos de reparación según prioridades

Se considerarán incidencias importantes aquellas que supongan una interrupción significativa de servicios o riesgo sobre las capacidades CIS de la Unidad y que conlleven una grave limitación para ejecutar sus cometidos, originando informes específicos. Serán atendidos con la mayor premura y su escalado sera casi inmediato; lo que permitirá a los especialistas ofrecer su asistencia desde muy temprano para recuperar el servicio lo antes posible y poder ejecutar los planes de recuperación y de continuidad CIS (*Disaster Recovery & CIS Continuity Plans*), cuando y donde sea necesario.

VI. Gestión de la Configuración.

JEGRUCECIS sera responsable, en apoyo a todas las unidades la Armada, de llevar a cabo el control de la configuración de la arquitecturas y baselines de los sistemas de su ámbito (reflejados en la tabla 3-1 en el Subapartado 3.2). Esta tarea irá intimamente ligada a la Gestion del Cambio (*IT Change Management*) que controla los cambios de configuración de los componentes.

Bajo ningún concepto se autorizará a las unidades apoyadas a variar su version actual sin la

aprobación de su solicitud de cambio (*Change Request* - CR), y llegado el caso, la autoridad proveedora podrá autorizar a la Unidad solicitante a efectuarlo a través de su personal técnico y con conocimiento del CISPOC, delegándole los permisos de manera apropiada. De no ser possible, el CECIS de apoyo es quien físicamente, a través de su Célula de Mantenimiento, la ejecutaría.

VII. Cortes programados e interrupciones de servicio aprobadas.

Es frecuente introducir en el acuerdo entre las partes un plan de acciones preventivas de mantenimiento y mejora del equipamiento de cara a mantener la calidad de los servicios propoporcionados. A veces, estas tareas conllevan un corte programado y no prolongado de servicios para hacer las tareas previstas y también atender imprevistos que surjan en su desarrollo. Todos estos trabajos serán cargados en el Módulo de Gestión del Cambio de Infraestructura por el CECIS.

Durante estos periodos de interrupción del servicio aprobados (*Approved Service Interruptions* - ASI) se permite al CECIS realizar cambios y mantenimientos sin que las Unidades puedan abrir tickets de incidencias por ello ni que el tiempo transcurrido contabilice para los KPI/KQI de incidentes. Serán programados de acuerdo con el plan de Gestión del Cambio del CECIS, o del GRUCECIS en caso de ser algo centralizado, no comenzando sin la aprobación inicial de la Unidad/es que se verán afectadas.

Estos cortes programados serán los mínimos posibles y preferentemente llevados a cabo fuera del horario laboral de la Unidad afectada. Deberán ser oficialmente solicitados y completamente coordinados con tiempo de antelación, al objeto de evitar, por ejemplo, conflictos con el desarrollo de misiones o ejercicios.

Una vez pactados estos eventos sobre el calendario, los tiempos de aviso se fijarán en un plazo de 10 días de preaviso, 5 días antes, y horas antes de su ejecución, por ejemplo. Esta misma responsabilidad del CECIS, la asumirá en caso de que el mantenimiento o corte de servicio se deba a tareas de terceros subcontratados. Si por necesidades de la Unidad el evento planeado no pudiera ser acometido, podrá proponer su reprogramación con al menos 2 días de antelación.

Además, el CECIS lanzará un mensaje genérico de aviso previo a todos los usuarios, por ejemplo hacienda uso de correo corporativo WANPG, avisando del mantenimiento programado y su impacto sobre los servicios.

Por su parte, las Unidades serán responsables de informar al CECIS al menos con 5 días de antelación de cualquier proyecto o evento que vaya a ejecutarse en relación a otros servicios de apoyo, como aires acondicionados y electricidad, que potencialmente pudieran afectar a componentes o partes del servicio proporcionado bajo su Acuerdo.

Cuando se traten de Interrupcioones de emergencia, al objeto de prevenir una caída total de servicios, recuperar la estabilidad de un servicio en concreto o como reacción ante un incidente de seguridad, no será obligatoria la aprobación por la Unidad afectada, pero si deseable el preaviso tan pronto sea posible. El procedimiento de emergencia será comenzado por el personal de servicio de la Célula de Mantenimiento del CECIS, enviando el correo genérico antes propuesto, y el SLM de la Unidad deberá ser informado lo antes posible.

En todo caso sera responsabilidad del CECIS hacer seguimiento de las actividades relacionadas con las tareas no programadas de emergencia y proveer del informe posterior a la Unidad. Así mismo, la duración de estas interrupciones de emergencia sí serán tenidas en cuenta en el cálculo de los KPI/KQI.

El Acuerdo podrá establecer que, dando cobertura a ambas partes, cuando la interrupción se deba a causas de fuerza mayor, ningún participante en el SLA sera responsable directo de fallos o retrasos en la recuperación, por tratarse de motivos más allá de su control razonable.

VIII. Gestión de la Entrega y Despliegue.

El CECIS tendrá por objetivo de esta tarea planificar, programar y controlar el proceso de lanzamiento de versiones de prueba y producción. La prioridad será proteger la integridad de los servicios en producción y que se lanzan los componentes y aplicaciones adecuadas.

El CECIS revisa y autoriza, o JEGRUCECIS si es una versión colectiva, la documentación relativa a las pruebas de validación y verificación donde se establece el nivel de las pruebas requerido para cada entrega de versiones. También revisará los informes finales tras las pruebas y valorará si la nueva version está lista para despliegue.

Por ultimo, confirmado que todo está correcto para el lanzamiento y puesta en producción, se asegurará de que el plan trazado para la implementación es correcto, está actualizado e incluye una estrategia de respaldo y retorno a la normalidad antes de comenzar la ASI.

IX. Monitorización, Medidas e Informes.

- Calidad del Servicio (*Quality of Service* - QoS).

El SLA tiene entre muchos objetivos, establecer un marco de Gestión de Servicios robusto entre las partes, donde la Calidad del Servicio esté especificada y monitorizada, y sea gestionada, valorada y notificada para asegurar la mejor entrega de servicios en relación coste-eficiencia para las necesidades operativas de la Unidad.

Por la escasa plantilla de efectivos con la que cuenta un CECIS, el nivel de partida para este marco de gestión debe ser bajo, y los estándares de calidad establecidos en el Acuerdo estarán basados en los razonables esfuerzos que el Centro realizará para proveer los servicios acordados con todas las unidades de su estorno geográfico con la mejor de sus intenciones y actuación profesional.

Todos los servicios incluidos en el Acuerdo estarán activos y funcionando a lo largo del año, a menos que se haya pactado otro detalle, y el CECIS realizará la monitorización y las medidas necesarias para la elaboración de informes de la Calidad del Servicio (QoS).

Los estándares de calidad de los servicios provistos se especificarán a través de una combinación de KQI y KPI, acordados entre ambas partes, y toda intención de mejora de los mismos será nogociada entre las autoridades involucradas delegando los detalles en sus SLM.

El KQI es un indicador acordado para valorar la percepción por parte del usuario final sobre la calidad de entrega de un servicio. Para cada servicio debe negociarse un KQI junto con su método de cálculo y valoración. La fórmula detallará cómo se consideran, añaden y valoran los KPI que dan por resultado el KQI. Cuando no haya posibilidad de obtener KQI de algún servicio, el CECIS deberá elaborar un informe cualitativo propio e informar del estado de la medición dentro de su plan de Monitorización e Informe de Calidad de Servicios; contando con el beneplácito de la Unidad cliente en relación al contenido y parámetros de este informe.

Para cada KQI el Acuerdo debe identificar un nivel objetivo a alcanzar, que será referencia para medir el nivel de entrega del CECIS a lo largo de un periodo de tiempo pactado.

Para cada KQI el Acuerdo contendrá uno o varios KPI, que son el parámetro medible y empleado como referencia para establecer el criterio de entrega de un sistema o servicio; medirlo e informar de él. La calidad, cantidad, requisitos mínimos de entrega, requisitos de apoyo y mantenimiento, así como las horas de esfuerzo para cada Servicio estarán detallados en el Acuerdo entre las partes. Por ello, con el propósito de medir, monitorizar e informar, el CECIS tiene la responsabilidad de identificar y proponer cómo medirá cada KPI con la tecnología disponible.

Como ejemplo de estos indicadores de referencia KPI/KQI para la gestión de los servicios proporcionados por nuestro CECIS, o actuando éste como intermediario, se propone la siguiente tabla 3-6, con valores KPI/KQI estándar para los servicios comunes a las unidades basadas en Rota.

Nombre del servicio	Código del Servicio	KPI	Objetivo	Indicadores de logro/puntuación	Informe
Servicio de los dispositivos gestionados	WPS001	Disponibilidad de SMN	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Disponibilidad de SACOMAR	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Disponibilidad de WANPG	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Tiempo de Respuesta (*Service Response Time* - SRT)	≤ 1 min	EDD ≤ 1m = GREEN EDD > 1m = RED	
Servicio de Correo	WPS002	Disponibilidad en SMN	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Retraso en la entrega de correo SMN	≤ 1 min	EDD ≤ 1m = GREEN EDD > 1m = RED	
		Disponibilidad en WANPG	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Retraso en la entrega de correo WANPG	≤ 2 min	EDD ≤ 2m = GREEN EDD > 2m = RED	
		Tiempo de aduana de WANPG a SMN (*Service Response Time* - SRT)	≤ 1 min	EDD ≤ 1m = GREEN EDD > 1m = RED	
Herramienta colaborativa VTC Skype Empresarial	WPS003	Disponibilidad en WANPG	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
Serivicio de copia, impresión y scanner	WPS004	Disponibilidad de periféricos de impresión, y scaner	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
Ops Centre	WPS005	Tiempo en responder las llamadas por el Ops Centre	75% en 20 sg	TAC ≤ 20 = GREEN TAC > 20 = RED	QSLR

Nombre del servicio	Código del Servicio	KPI	Objetivo	Indicadores de logro/puntuación	Informe
			80% en 30 sg	TAC ≤ 30 = GREEN TAC > 30 = RED	QSLR
			85% en 60 sg	TAC ≤ 60 = GREEN TAC > 60 = RED	QSLR
		Resolución en la primera llamada	75% en 20 mins	Av ≥ 75% = GREEN Av < 75% = **RED**	
Servicio de telefonía	WPS006	Móvil y fijo no clasificado	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
VTC SMN	WPS007	Disponibilidad de VTC en SMN	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Tiempo de respuesta del C.Control VTC	75% en 10 sg	TAC ≤ 10 = GREEN TAC > 10 = RED	
			80% en 15 sg	TAC ≤ 15 = GREEN TAC > 15 = RED	
			85% en 30 sg	TAC ≤ 30 = GREEN TAC > 30 = RED	
Voc segura en SMN (SVoIP)	WPS008	Disponibilidad en SMN	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
NSWAN Pico Point of Presence (PoP)	WPS009	NSWAN	99.80%	Av ≥ 99.8% = GREEN Av < 99.8% = **RED**	QSLR
Acceso a internet	WPS010	Internet	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
Servicio de infraestructura de almacenamiento	WPS011	Tiempo de recuperación de datos	≤ 5 sg (2MB)	TAC ≤ 5 = GREEN TAC > 5 = RED	
		Almacenamiento NSWAN	99.90%	Av ≥ 99.9% = GREEN Av < 99.9% = **RED**	
Servicio SATCOM	WPS012	Comms	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
Servicio de información WEB y Portal	WPS013	Disponibilidad en SMN	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Tiempo de respuesta en SMN (SRT)	≤ 5 sg	SRT ≤ 5s = GREEN SRT > 5s = RED	

Nombre del servicio	Código del Servicio	KPI	Objetivo	Indicadores de logro/puntuación	Informe
		Disponibilidad en WANPG	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
		Tiempo de Respuesta en WANPG (SRT)	≤ 10 sg	SRT ≤ 10s = GREEN SRT > 10s = RED	
Servicio MCCIS	WPS014	Disponibilidad en SMN	99.50%	Av ≥ 99.5% = GREEN Av < 99.5% = **RED**	QSLR
		Tiempo de respuesta al usuario tras logging	≤ 30 sg	T ≤ 30s = GREEN T > 30s = RED	
Servicio NCOP	WPS015	Disponibilidad en NSWAN	99.50%	Av ≥ 99.5% = GREEN Av < 99.5% = **RED**	QSLR
		Tiempo de respuesta al usuario tras logging	≤ 30 sg	URT ≤ 30s = GREEN URT > 30s = RED	
Sistema de mensajería MHS (SACOMAR)	WPS016	NS Availability	99%	Av ≥ 99% = GREEN Av < 99% = **RED**	QSLR
Herramienta SHAREPOINT	WPS017	NS Availability	99%	Av ≥ 90% = GREEN Av < 90% = **RED**	QSLR

Tabla 3-6. KPI/KQI Estándar a las Unidades.

Además, será conveniente añadir una tabla específica con los valores acordados para cada unidad en concreto. Por su especificidad, para nuestro Estado Mayor, podríamos proponer la siguiente tabla 3-7 con los valores KPI/KQI a alcanzar:

Nombre del Servicio	Código del Servicio	KPI	Objetivot	Indicadores de puntuación y logro	Informe
Todos los servicios incluidos en el SLA local específico	N/A	Numero de incidencias resueltas del SLA	80%	≥80% = **GREEN** <80% = **RED**	QSLR
		Incident Mean Time to Respond - MTRp	P4	MTRp ≤ 2wd = **GREEN** MTRp > 2wd = **RED**	QSLR
			P3	MTRp ≤ 1wd = **GREEN** MTRp > 1wd = **RED**	QSLR
			P2	MTRp ≤ 2h = **GREEN** MTRp > 2h= **RED**	QSLR
			P1	MTRp ≤ 1h = **GREEN** MTRp > 1h = **RED**	QSLR
		Incident Mean Time to Resolve	P4	MTTR ≤ 3wd = **GREEN** MTTR > 3wd = **RED**	QLSR
			P3	MTTR ≤ 2wd = **GREEN** MTTR > 2wd = **RED**	QLSR
			P2	MTTR ≤ 8h = **GREEN** MTTR > 8h = **RED**	QLSR
			P1	MTTR ≤ 4h = **GREEN** MTTR > 4h = **RED**	QLSR

		Number of Service Requests resolved in SLA	80%	≥80% = **GREEN** <80% = **RED**	QSLR
		Service Request Mean Time to Resolve - MTTR	Simple	MTTR ≤ 1wd = **GREEN** MTTR > 1wd = **RED**	QLSR
			Normal	MTTR ≤ 10wd = **GREEN** MTTR > 10wd = **RED**	QLSR

Tabla 3-7. KPI/KQI específicos de CGMAD

- Plan de Monitorización e Informes de la Calidad de Servicio.

Al menos tres meses antes de entrar en vigor el Acuerdo entre las partes, el CECIS debe remitir a la Unidad su Plan de monitorización e informes de QoS. El documento sera analizado y discutido en las reuniones previas a la formalización del Acuerdo.

En este plan el CECIS deberá proponer, donde no tenga medios técnicos para recoger, analizar o informar de datos relevantes de entrega, otros mecanismos de valoración cualitativos que considerará como suplemento a sus informes cuantitativos. Los servicios que carezcan de mecanismos de monitorización deberán incluirse en este apartado.

El plan incluirá la fuente de procedencia de los datos, los métodos de obtención y la frecuencia con que se anotarán; así como el proceso para revisión y validación de los datos. Además se detallará el formato estándar seguido para informar de cada KQI y la forma de obtener cada KPI.

Este plan se irá adaptando convenientemente a medida que se vayan desarrollando proyectos, se reciba *feedback* de cada reunion trimestral de revisión del SLA y de los acuerdos alcanzados en los grupos de trabajo de KQI y KPI.

- Informes del Nivel de Servicio (*Service Level Reporting* – SLR).

La frecuencia con la que la Unidad apoyada recibirá informes o notificaciones sobre el nivel de Servicio proporcionados por el CECIS podrá ser diversa.

a) Diaria, si así se require.

El CECIS debería hacer llegar a cada Unidad un breve informe diario de situación (*Situation Report* – SITREP), elaborado por su personal de guardia en la Célula de Mantenimiento. Las unidades, si así lo desean, podrán asistir a la reunión interna diaria de coordinación, mantenida en el CECIS.

Además, cuando sea técnicamente posible y acordado mutuamente, la Unidad podrá tener acceso a los informes automáticos del estado de los sistemas que recibe el CECIS, sin intervención humana, como signo de transparencia en la calidad del servicio proporcionado.

b) Semanalmente, si se require.

A petición de la Unidad, el CECIS atenderá semanalmente, o en la periodicidad que ambas partes acuerden, a las reunions que la Unidad convoque a nivel SLMs.

c) Mensualmente.

El CECIS hará llegar un informe mensual a las Unidades a las que da soporte, la primera semana de cada mes, sobre la calidad del servicio proporcionado por los Servicios Centralizados dependientes del CESTIC y aquellos del própio ámbito que se centralizan en el CECISMAD como CECIS dependiente del JEGRUCECIS.

d) Trimestralmente.

A los 15 días de finalizar cada trimestre, el CECIS hará entrega de un informe completo de revisión trimestral del nivel de los servicios a la Unidad (*Quarterly Service Level Review* – QSLR). Posteriormente, la Unidad concertará una reunión entre las partes del SLA para su análisis y discusión. En esta reunión se tratarán los siguienetes apartados:

- Informes cualitativos y cuantitativos de todos los servicios que le ha proporcionado.
- Informe de valoración del nivel de entrega de servicios del SLA.
- Comentarios y quejas de la Unidad, incumplimientos al Acuerdo y motivos para no haber alcanzado algún nivel previsto.
- Propuestas de mejora de algún servicio concreto, principalmente como solución a una queja importante al SLA o su incumplimiento.
- Tareas de mantenimiento que pudieran afectar a la *baseline* de algún servicio.
- Revisión de los cambios a *baselines* entregados y proyectos para el siguiente trimestre.
- Revisión del informe de QoS, viendo cada nivel de servicio a través de los KPI y KQI resultantes y el nivel de satisfacción de la Unidad, en base a los mecanismos de valoración cualitativos acordados en el Plan de Monitorización e Informes de QoS.
- Ciberseguridad y aspectos de seguridad CIS, incluyendo las reacreditaciones de seguridad previstas para el siguiente trimestre y sustituciones de equipos.

X. Mejora continua del Servicio.

Tanto la Unidad como el CECIS tendrán por objetivo común la mejora de la calidad de los servicios y la relación coste-eficacia de los mismos. Con este fin el Jefe del CECIS desarrollará, en coordinación estrecha con el representante de la Unidad para el SLA, una estrategia de mejora continua del Servicio que proporcione una hoja de ruta para la mejora de la Gestión del Servicio y las capacidades de control.

El CECIS llevará a cabo encuestas de satisfacción aleatorias y bianuales a las unidades para medir y hacer seguimiento a cómo de satisfechos están los usuarios con la infraestructura, la organización y funcionamiento CIS de su entorno. Del mismo modo, a la hora de cerrarse una incidencia a través de la herramienta de gestión proporcionada a los clientes, estos recibirán una breve encuesta de satisfacción que permita al CECIS revisar y entender su percepción de la entrega de servicios de calidad.

Estas actividades estarán ligadas a otros proyectos de investigación programados y planificados, así como a programas de transición CIS de la JECIS, al objeto de establecer una gestión de la capacidad de extremo a extremo eficaz y fijar un proceso cíclico para la Mejora Continua del Servicio.

3.4 GLPI. La herramienta de Gestión de Servicios del CECIS.

En el apartado 2.7 se expusieron diversas herramientas empleadas en el ámbito del MDEF, CESTIC y otros ejércitos para la gestión de incidencias y control de inventario. Actualmente, en el segundo semestre de 2021, ha comenzado a probarse una herramienta totalmente compatible con ITIL en el ámbito de la Armada con los mismos objetivos, y que hasta el momento se encontraba exclusivamente disponible en la red de gestión de mensajes oficiales SACOMAR, y limitada en sus aplicaciones. Estas pruebas se están efectuando en la zona geográfica noroeste, con CECISFER como Centro banco de pruebas.

Esta herramienta es GLPI (Gestión Libre del Parque Informático), una solución software libre de código abierto, editado en PHP y que se distribuye bajo una licencia GLP. Se trata de una aplicación

web ITSM para gestión de incidencias e inventario de una plataforma informática completa, aportando otras múltiples funcionalidades a base de ampliaciones que aportan:

- Inicio y seguimiento de incidencias, fallos, averías y solicitudes de servicio sobre el equipamiento.
- Comunicación y seguimiento de problemas generales en la red informática.
- Planificación y programación de actuaciones sobre la red, permitiendo el control de la configuración y de las distintas versiones SW a integrar en la red.
- Creación de roles estructurables al objeto de escalar incidencias, peticiones, problemas.
- Comienzo y desarrollo de informes de estado y seguimiento.
- Facilidad de integración con otras herramientas para la automatización de los catálogos e inventarios.
- Creación y alimentación de una base de datos del Conocimiento (GIC), conteniendo la mayor cantidad de información y referentes para la resolución de problemas rápida y eficiente. Además contendrá un banco de preguntas frecuentes disponible para los usuarios, que cada vez requieren un acceso más rápido a las soluciones y reforzará el apoyo de nivel 0.

La aplicación quedará instalada en los servidores principales de las redes a gestionar, se emplea a través de IP y se requiere navegador Mozilla Firefox para su correcto funcionamiento, y al igual que se vió con SCANS, I-CIS, GISMI y Proactivanet, a continuación se expondrán las particularidades que hacen especial e idónea esta aplicación para nuestro ámbito.

I. Tipos de usuarios.

Al igual que se ha visto en las otras herramientas en uso y en los niveles de apoyo establecidos en nuestro SLA, lo normal sería establecer una tipología de usuarios acorde a estos, de modo que podamos organizar la atención a las incidencias de forma similar y realizar el escalado entre ellos. Y según el tipo, las opciones accesibles y la presentación de su pantalla variará. Cada nivel estará capacitado para generar usuarios, dar bajas y/o realizar modificaciones. Los 4 niveles establecidos son:

- Nivel 1, *do yourself*, donde los propios usuarios de los sistemas podrán generar incidencias y acceder a la base de conocimiento y FAQ para tratar de resolverlas. De no poder solucionarlas podrán escalarlas al nivel 2 y hacer seguimiento sobre las acciones que se realicen en ellas.

- Nivel 2. Conformado por el personal de la Célula de Mantenimiento, autorizado para generar incidencias y atender las recibidas en su zona desde el Nivel 1. Igualmente capacitados para el escalado al siguiente en nivel si no fueran capaces de darle solución.

- Nivel 3. Será el personal del CECIS central, CECISMAD, que tendrá acceso a todas la incicencias y atenderá aquellas que le sean reenviadas por imposibilidad de solución local, pudiendo enviarlas a agentes externos del siguiente nivel en caso de no poder dar solución.

- Nivel 4. Ultimo nivel de asistencia, compuesto por el personal técnico especialidado perteneciente a las líneas de los servicios concretos y a empresas subcontratadas.

II. Acceso, apertura y seguimiento de incidencias.

El acceso a la aplicación es común, requiriendo identificación con usuario y contraseña. Todos los accesos y la actividad realizada quedarán registrados mientras se mantenga la sesión abierta, y

únicamente podrán actuar en el perfil de usuario configurado para su autorización en el nivel. Todos los paneles de usuario son diferentes según niveles, pero comparten la misma barra superior desde que acceden a las opciones habilitadas.

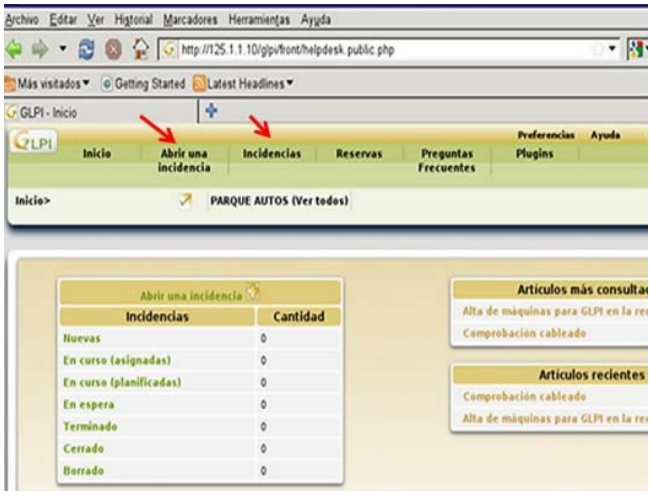

Figura 3-2. GLPI. Panel usuario Nivel 1

La forma en que se abren las incidencias depende también del nivel que lo haga, variando desde el nivel 1 que solo puede abrirla, hasta el nivel 4 que la puede convertir en problema para que reciba otro tipo de gestión.

El alta de una nueva incidencia supone rellenar una serie de desplegables identificativos que ayudarán a su reconocimiento y localización. Son:

- Tipo. Un incidencia o una solicitud, según queramos comunicar un mal funcionamiento de equipamiento o software, o pedir algún tipo de material.
- Categoría. Diferenciando de qué tipo de componente se trata.
- Urgencia. Acorde a las prioridades reflejadas en el SLA, serán 1 muy alta, 2+ alta, 2- media, 3 baja, 4 muy baja.
- Título y descripción. Detallarán la comunicación de la manera más detallada posible, incluso anexando un fichero con información relevante.

Cuando se proceda a la búsqueda de incidencias, éstas aparecerán definidas por los cuatro caracteres anteriores y listadas por la selección de "Estado" que hagamos. Estos criterios serán: nueva, en curso (asignada), en curso (planificada), en espera, resuelta, cerrada, sin resolver, sin cerrar, en curso, resuelto y cerrado, todos.

La herramienta, al seleccionar la incidencia buscada nos desplegará en pantalla las vicisitudes e historial de la misma, ofreciendo a pie de página añadir un nuevo seguimiento.

Los usuarios de nivel 2 y 3, aparte de tener presentaciones con accesos a diferentes opciones, podrán seleccionar los niveles inferiores que de ellos dependen, estando habilitados para realizar cambios y añadir seguimientos en las incidencias de esas Unidades. A mayor nivel, mayor es el detalle con que debe completarse cada incidencia.

Se añade aquí un nuevo desplegable identificativo, actores, que serán los usuarios que intervienen en el desarrollo de la incidencia y cómo lo hacen.

- Solicitante. Usuario que abre la incidencia y el grupo al que pertenece.
- Supervisor. Usuario que supervisará el desarrollo y el grupo al que pertenece.
- Asignada. Usuario-técnico encargado de resolverla y el grupo al que pertenece.

Tras cada cambio de estado que se realice habrá que actualizar los siguientes campos:

- Origen de la solicitud. Forma en que se ha conocido la incidencia: Help Desk, llamada, email, o por uno mismo.
- Solicitud de validación. Usuario o técnico que comprobará que ha sido resuelta correctamente.
- Elemento asociado. Detallamos el componente de inventario afectado.
- Título. Definición aún más clara de la incidencia creada o atendida.
- Descripción y fichero. Más detalles, observaciones e incluso documentos anexos explicativos.

III. Tareas.

Al localizar la incidencia y proceder a su resolución, el técnico del CECIS tendrá que especificar los siguientes datos de las tareas efectuadas sobre ella (figura 3-3):

- Categoría. Qué tipo de trabajo ha realizado.
- Estado. En qué estado se encuentra, terminada o no.
- Duración. Tiempo invertido en realizar la tarea.
- Privacidad. Podrá marcarla como "privado" y la tarea no aparecerá en el histórico de seguimiento del usuario que generó la incidencia.

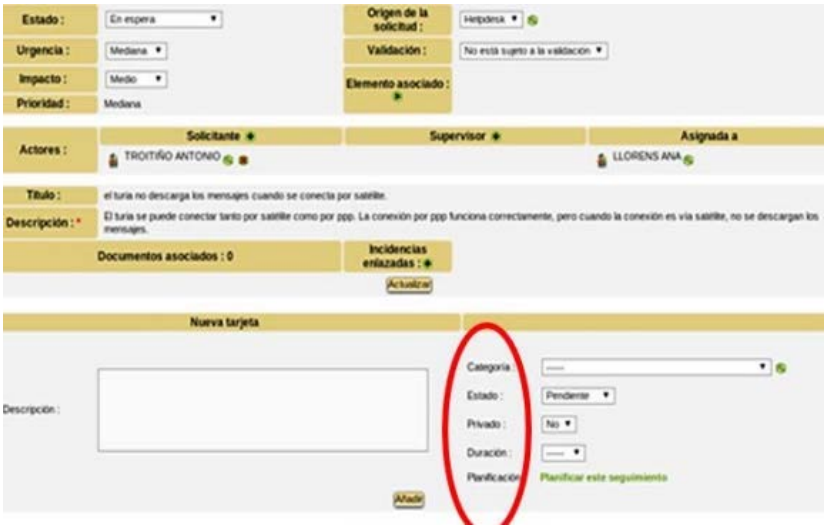

Figura 3-3. GLPI. Tareas sobre las incidencias

IV. Base de Conocimiento.

Esta sección de la herramienta nos permite acceder y visualizar todas las soluciones aplicadas a incidencias previas que hayan ocurrido y otros asuntos que puedan ayudar a resolver las nuevas que surjan. Supone un repositorio de experiencias previas que está en continua actualización. Solo los usuarios del CECIS con los permisos adecuados podrán acceder a esta opción, añadir entradas desde seguimientos sobre incidencias ya terminadas y cerradas, o directamente desde su menú.

Una vez dentro se pueden buscar entradas por categorías y temas, y al cargarlas se pueden añadir a las Preguntas más Frecuentes públicas (FAQ) para darles visibilidad a los usuarios de nivel 1 como referencias de ayuda.

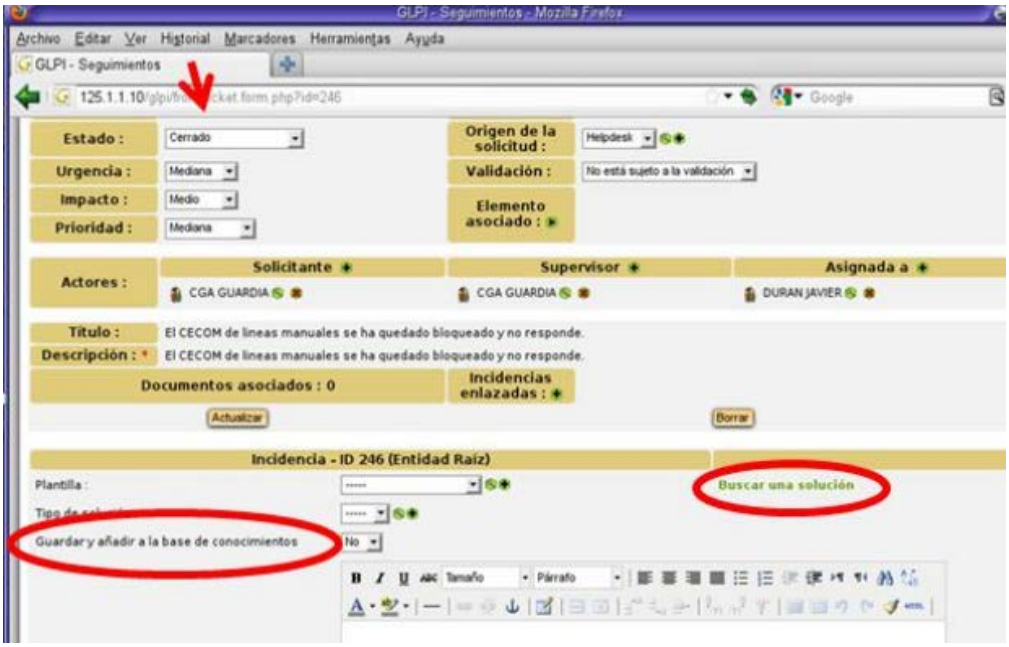

Figura 3-4. GLPI. Acceso a soluciones y guardar en FAQ.

V. Inventario.

Esta herramienta permite a los CECIS desarrollar su labor de Gestión de la Configuración a través del Control de Inventario. Mientras los usuarios de las Unidades (nivel 1) no tienen acceso, y los de nivel 2 y 3 solo de consulta, son los usuarios de nivel 4 los únicos que pueden modificarlo. Al acceder aparece un menú desplegable donde se puede elegir el tipo de componente a consultar, como puede verse en la figura 3-5.

Figura 3-5. GLPI. Desplegable de inventario

La última opción, “Estados”, permite conocer la situación en que se encuentran los diferentes elementos de equipamiento; ya sea en uso, averiado, revisión, etc.

Los usuarios autorizados podrán introducir nuevos componentes junto con todos sus datos y características técnicas, así como eliminarlos. Todos los tipos de componente abren un desplegable como el de la figura 3-6 donde se puede indicar hasta el ultimo detalle que permita identificar y localizar a cada uno.

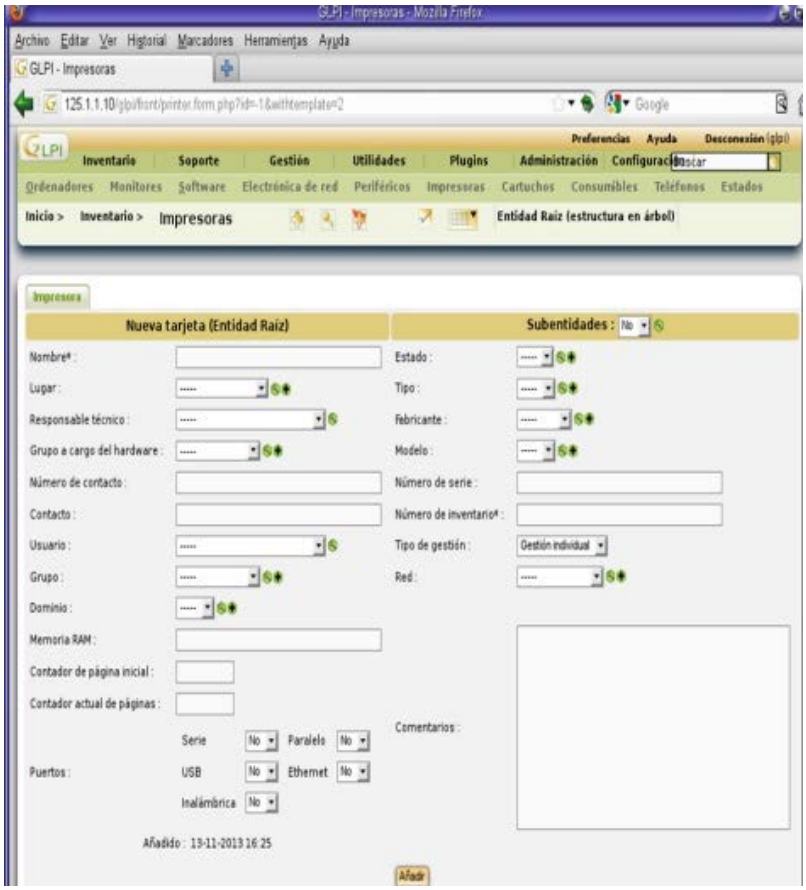

Figura 3-6. GLPI. Características de inventario

4. CONCLUSIONES Y LÍNEAS FUTURAS

4.1 Plan de Implementación de la Metodología de Gestión

Los Centros de Explotación de Sistemas de Información y Telecomunicaciones (CECIS) tienen, entre otros muchos, los siguientes cometidos:

- Apoyar a las unidades en la instalación, configuración y actualización de los sistemas CIS de acuerdo con sus necesidades.
- Distribuir, administrar y controlar el material informático (hardware y software) de las unidades que apoyan.

Para realizar estos cometidos, en el ámbito de la JECIS se están utilizado muy diversas herramientas que van desde una complicada pero básica tabla de cálculo, el uso del correo electrónico y el teléfono, a programas construidos ad-doc, cuyo mantenimiento es extremadamente complejo. La mayor parte de estas herramientas no produce un óptimo aprovechamiento de los recursos materiales y humanos ni comparte datos e información con otras. Además su disparidad impide el trabajo conjunto y una gestión centralizada que sería de gran aprovechamiento para la toma de decisiones. Es por tanto fundamental disponer de una única herramienta que englobe todas nuestras necesidades.

En el ámbito comercial existen actualmente soluciones que permiten una automatización de los procesos de inventariado y gestión interna para la resolución de incidencias y peticiones del usuario. Entre todas ellas se ha seleccionado la herramienta “Gestión Libre del Parque Informático” (GLPI), herramienta de software libre que se utiliza ampliamente y es gratuita, lo que permite un desarrollo específico y adecuado a las necesidades de la Armada, que engloban entre otras:

- Gestión multi-entidades.
- Gestión de incidencias por parte de los usuarios.
- Gestión administrativa y financiera.
- Funcionalidades de inventario.
- Gestión de expedición de tickets y solicitudes, funcionalidades de monitoreo.
- Gestión de problemas y de cambios.
- Gestión de licencias.
- Atribución de material: ubicación, usuarios y grupos.
- Interfaz simplificada permitiendo a los usuarios finales rellenar un ticket de soporte.
- Generador de informes activos y Helpdesk: hardware, red o intervenciones (soporte).

Para su implantación se ha creado un grupo de trabajo que dirige CECISFER y en el que participan todos los CECIS con la intención de hacer confluir todas las funcionalidades de las diferentes herramientas utilizadas hasta ahora en el GLPI, para su sustitución por esta aplicación, buscando la uniformidad de procesos de gestión del inventario y resolución de incidencias.

Para su implantación se consultó previamente al CESTIC, concluyendo que la herramienta en cuestión tiene muchas posibilidades de superar una auditoría, en estos momentos no hay otra en el ámbito de los Ejércitos que sea igual de "explotable" y GLPI tiene además la ventaja de estar avalada, al encontrarse incluida en el software de la Administración General del Estado (AGE).

Mientras tanto, CESTIC se encuentra inmerso en la federación de redes clasificadas nacionales de los diferentes ámbitos, para alcanzar la red denominada SC2N[30] conjunta. La contribución de la Armada a este propósito es la conversión de nuestro Sistema de Mando Naval (SMN) en una parte, denominada SC2N-Ar, para posteriormente integrarla en la SC2N final. En este macroproyecto, la herramienta de gestión de servicios que CESTIC integrará será Proactivanet, y una vez logrado se llevará también al ámbito corporativo, a la WANPG, para lo que se requerirá una empresa externa para su desarrollo y mantenimiento. Esto puede llevar de dos a tres años; de ahí el interés en implementar a nivel particular en la Armada una herramienta propia desde ya, con independencia del desarrollo de Proactivanet y su posterior relevo.

El plan de implementación debería comenzar con la instalación de GLPI en un único servidor virtual donde se alojaran todas las bases de datos de todos los CECIS. Se ubicaría en el CECISFER, con intención de alojarlo en el futuro en máquinas de CECISMAD o CECISJAL. Los recursos de demanda de este servidor inicial serían pequeños, por lo que una máquina sencilla serviría.

Actualmente la implantación de la herramienta está bastante avanzada, gracias a que se obtuvieron recursos económicos para su desarrollo y que una empresa externa de Pontevedra, TICGAL, pueda realizar auditorías sobre los avances del CECISFER en el proyecto. Además, ya se está trabajando con el CESTIC para obtener su beneplácito en relación a la seguridad.

Habría que comenzar la formación de administradores en el manejo de la Aplicación y en el ámbito de cada CECIS designar dos unidades de pequeña entidad para comenzar con el manejo de la aplicación, probar la gestión de incidencias y la confección de inventarios internamente.

El siguiente paso sería la formación de los CISPOC de las unidades, probar los accesos al sistema desde las unidades, y pruebas de redescubrimiento de la red. A continuación pruebas de gestión de incidencias SW y pruebas de incidencias HW desde las unidades piloto. A partir de ese momento habría que depurar la aplicación con los problemas que se vayan detectando, e ir incorporando poco a poco más unidades al programa.

Esta implementación se extendería a toda la estructura de GRUCECIS de manera centralizada y jerarquizada, en base a la estructura organizativa de los CECIS y a la relación funcional con las autoridades y unidades a las que apoyan.

La herramienta permitirá, por un lado, llevar un control automático del inventario. Audita y realiza el inventario de todo el parque informático automáticamente, así como toda la electrónica de red y las licencias SW. Proporciona la información de forma inmediata, y en tiempo real, a la persona o personas autorizadas para su empleo.

[30] El SC2N dispondrá de una herramienta ITSM denominada Proactivanet, que lleva un coste de licencias asociado y su implantación será llevada a cabo por parte del CESTIC a través de un contrato externalizado que ya ha salido a licitación. El CESTIC no pretende extender PROACTIVA-NET a la red corporativa a corto plazo y ha alentado a la Armada en la implantación de GLPI.

Por otro, dispone de una potente herramienta que permite realizar la gestión de incidencias, peticiones, problemas, cambios, entregas y niveles de servicio desde su registro inicial por parte del usuario hasta su cierre, optimizando la resolución de las incidencias facilitando la comunicación directa del usuario que tiene el problema con la Célula de Mantenimiento del CECIS de apoyo que ha de resolverlo.

El disponer de toda la información en el mismo entorno permitirá el control del ciclo de vida del parque informático que facilitará la toma de decisiones sobre el mismo, niveles de reposición, obsolescencia del HW, renovación de SW, empleo efectivo de los activos de la red, y otras muchas ventajas.

La implantación de GLPI entregará las siguientes ventajas:

- Mejor atención al usuario.
- Optimización del trabajo en los CECIS mediante la aplicación de procesos automatizados de gestión de incidencias y peticiones.
- Capacidad de disponer al instante el inventario de todo el parque informático, software instalado, licencias y configuraciones de manera automática y desatendida.
- Facilidad para la gestión centralizada mediante una visión global de todos los recursos disponibles.
- Mejoras en seguridad en los sistemas y servicios de la red de propósito general (WANPG).
- Facilidad de formación de los operadores de los CECIS en una única aplicación.
- Interoperabilidad con aplicaciones de terceros como puede ser el Centro Corporativo de Explotación y Apoyo (CCEA) del CESTIC.

4.2 Situación final deseada

La implementación completa de esta herramienta en la Armada supondría un único servidor con GPLI como gestor global que capacite lo siguiente:

- Gestión de incidencias. Permitirá la tramitación de incidencias ONLINE en cualquier parte desde cualquier lugar. Lo cual abre las puertas a la posibilidad de una nueva forma de optimizar y rentabilizar el trabajo:
  - Con un gran equipo de gestores y operadores deslocalizados que resuelve las incidencias de cualquier sitio e incluso las producidas en buques navegando.
  - Un pequeño equipo in situ, que resuelve las incidencias que requieran presencia de personal.
- Gestión de material. Un usuario con privilegios podría consultar los equipos disponibles en funcionamiento y en stock de todos los CECIS. Se podría entonces:
  - Hacer listados y estadísticas.
  - Asignar nuevos equipos directamente incorporándolos a la herramienta.
  - Facilitar auxilios de material entre CESIS. Control centralizado de un gran almacén de material distribuido en pequeños almacenes por toda la geografía y buques.
- Resolución de averías.
  - Ante una avería la red el sistema es capaz de señalarnos una primera aproximación del impacto. No es una aplicación específica para esto, pero puede ser muy útil en la toma de decisiones.
  - El uso de un sistema centralizado como su base de conocimiento permite el apoyo inter-CECIS en la resolución de incidencias graves de red.

GLPI sustituirá a las actuales herramientas tan dispares que estamos empleando, no teniendo sentido alguno mantenerlas al mismo tiempo, y todos los CECIS convergerán en su empleo colectivo y centralizado desde CECISMAD.

La herramienta única GLPI debe ir enfocada al dato único con servidores centralizados y llegar a ser escalable hasta el CESTIC, que proporciona la mayoría de los servicios CIS y tiene el recurso económico. En un futuro, cuando llegue el momento de ser relevada por Proactivanet, el CESTIC podrá implantarla con el apoyo del personal técnico que necesite para su mantenimiento, gracias al recurso económico y de personal que tiene a su disposición. A la herramienta deberán acceder con su correspondiente perfil y derechos tanto los CECIS como todos los CISPOC de las unidades, y no debería afectar a la dinámica de trabajo ya implantada hasta ese momento.

Mientras la herramienta sea sólo de la Armada, igualmente habría que emplear servidores centralizados y que fuera escalable hasta la JECIS de forma que en todo momento conozca el estado de las incidencias y la distribución del material, sin tener que realizar continuas consultas a los CECIS periféricos. GLPI permitirá gestionar los catálogos HW y SW de las unidades y sus variaciones periódicas, de forma que los CECIS podrán determinar sus necesidades HW y SW sin tener que realizar constantes consultas a las Unidades.

Pero está claro que tener una herramienta común no será suficiente. Además de trabajar con GLPI y después acoger Proactivanet, es necesario realizar una adaptación de la organización del Grupo de CECIS para ser más eficientes en la gestión de los recursos de material y humanos. Por ejemplo, organizando el trabajo por áreas funcionales. Sirva de ejemplo la creación de un CAU único para la resolución de incidencias, centrado en el CECISMAD, donde se concentrará nuestro Big Data, todas las incidencias y la Base de Conocimiento. Y por otra parte, interna y propia desde cada CECIS, estableciendo la Célula de Mantenimiento y una metodología de trabajo fundamentada en SLAs reconocidos y publicados, acordes con las necesidades de las Unidades a las que dan soporte.

Como conclusión de este trabajo por tanto, se puede afirmar que los objetivos propuestos de inicio son alcanzables e implementables, estando a día de hoy disponible una herramienta capaz de centralizar toda la gestión de servicios que facilitan nuestros Centros de Explotación (GLPI en nuestro caso), siendo totalmente viable la reestructuación funcional interna de los propios Centros configurando una Célula de Mantenimiento preventivo que aporte valor al usuario que vele por el correcto funcionamiento de redes y sistemas con antelación suficiente a posibles incidencias y problemas; y por último documentando su dinámica de trabajo y servicio en un marco legal establecido por Acuerdos de Nivel con las unidades apoyadas y terceros, a través de los conocidos como *Service Level Agreement*.

4.3 Mejora Continua y líneas futuras.

En los CECIS actualmente se gestionan las incidencias con lentitud a través de mensajes por sistemas clasificados, por teléfono y con correos electrónicos a una dirección genérica incidenciascecisrot@mde.es, por ejemplo, al no disponer de ninguna aplicación adecuada para su gestión. La carencia de aplicaciones adecuadas para el control del material de microinformática y la gestión de incidencias se ha notificado a los Organos Superiores a través de escritos, plenos y reuniones en los últimos cinco años, resaltando:

- Las dificultades en convivencia de la gestión de incidencias y peticiones de usuarios a través de la herramienta SCANS para la resolución por los CECIS o elevación al CCEA del CESTIC.

- La necesidad de una aplicación de gestión incidencias a nivel local con posibilidad de escalado a nivel superior. Ya sea GLPI, planteada por la Armada, o la herramienta propuesta por el CESTIC, deben estar orientadas hacia el dato único.

La normativa que estructura la JECIS y de los CECIS se desarrolla en las diferentes Instrucciones expuestas en el Apartado 1 de este trabajo, desglosando los Centros en CECOM y CESIN. Además, la organización de las comunicaciones navales se desarrolla en el ACP 121 ESP NAVY, donde en su capítulo 2 se describe la organización de la estructura de apoyo CIS a las Autoridades y Mandos, recalcando la estructura de la JECIS, GRUCECIS y los CECIS periféricos, así como sus cometidos y los de cada uno de sus órganos. Y en el capítulo 3 se incluyen párrafos totalmente nuevos que reflejan cómo se organiza la Armada para explotar los Sistemas de Información a su disposición.

A partir de aquí, en los CECIS de la Armada no tenemos desarrollado en la actualidad ningún proceso de trabajo de gestión de servicios CIS que, por la organización del MDEF y con la distribución de competencias expuestas, correspondería a la dirección de la "empresa" su generación (CESTIC o en su defecto la Armada acotándonos al ámbito), pero aquí nos encontramos con ciertos obstáculos, ya sea porque los procesos desarrollados en el portal de procesos de la Armada son más teóricos que prácticos, y muchas veces el intento de mejora continua choca con el inmovilismo y cierta comodidad de la rutina, o hay diferentes opiniones respecto a competencias y responsabilidades, que dificultan el avance.

Una de las principales carencias a la hora de administrar los servicios CIS, además de la no puesta en práctica de las buenas maneras ITIL, es la falta de personal, ya endémica en la Armada. En el caso de ciertos CECIS, su cobertura Plantilla Orgánica ya reducida un 25% en el año 2012, se encuentra actualmente al 25% de oficiales, 54% de suboficiales, 75% de Cabos 1 y al 100% de Cabos/Marineros. Y de todos ellos, solo un programador de sistemas y un solo gestor de redes. Este sería uno de los principales limitantes a la propuesta de este trabajo, de no estar la plantilla cubierta al 100%.

La figura 4.1 reforzaría el sustento de la propuesta de Metodología para la Gestión de Servicios desde un CECIS expuesta en este documento, donde no solo el dato, la información, los sistemas, son esenciales para el plan, sino también la plantilla de personal dimensionada, capacitada y experimentada.

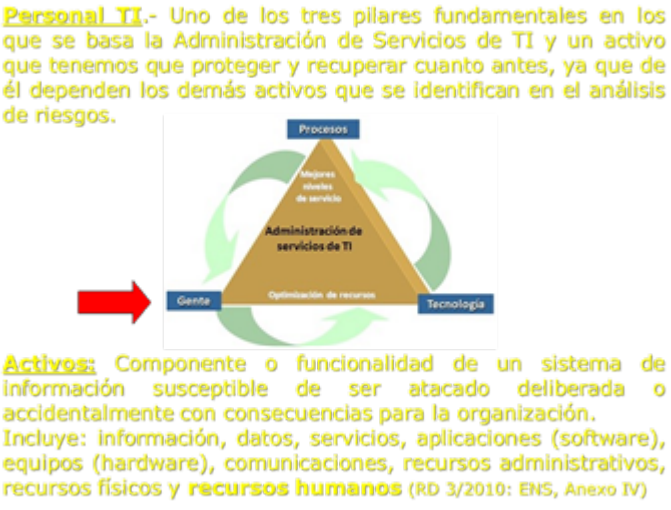

Figura 4-1. Pilares de la Gestión de Servicios de TI.

A nivel MDEF las incidencias se gestionan con la herramienta SCANS, con tickets iniciados por los CISPOC´s de las UCOS y donde los CECIS/OACIS hacen de coordinador Intermedio, como quedó expuesto en el subapartado de herramientas de gestión.

Los intentos de los CECIS de poder entrar en la aplicación SCANS como "resolutores" de incidencias no han tenido todo el éxito deseado por la escasez de licencias y fondos económicos para extender y desarrollar en profundidad la aplicación a nivel OACIS/CECIS, de forma que las incidencias se pudieran resolver o elevar en todo el panorama de los ámbitos. Todas las incidencias de los CISPOC van directamente al CESTIC y sólo son las peticiones las que estudian y elevan los Coordinadores CIS de los CECIS. Las numerosas incidencias que se resuelven a diario a nivel local simplemente no entran en el sistema y no se contabilizan, lo cual merma la capacidad de informar, controlar y retroalimentar el proceso para dar mejora continua y, en definitiva, valor a los usuarios.

A nivel CESTIC ya se es consciente de la necesidad de una aplicación "más ITIL" que el anticuado SCANS, que permita la gestión integral de todos los servicios CIS (no solo de los que ahora entran en SCANS) y que podría aparecer en un plazo de no menos de 2 años. Proactivanet es la herramienta ITIL valorada por el CESTIC. Mientras tanto la Armada, liderada por la JECIS en este campo, implanta una aplicación local, desarrollada por CECISFER y basada en GLPI. La herramienta "casa" totalmente con los principios básicos de ITIL y es gratuita.

En relación a la gestión de servicios, el que va más avanzado es también el CESTIC, que tiene las ideas a este respecto bastante claras, y las ha plasmado en un documento aún no difundido, su Instrucción Técnica 01/2021 del CESTIC, donde prácticamente todos los servicios estarán centralizados.

El futuro, ligado al recurso económico que cada vez maneja más el CESTIC en detrimento de los ejércitos, podría pasar por la unificación de todos los servicios por el CESTIC y la desaparición de los servicios específicos de la Armada. Por ejemplo, la red clasificada SMN y de mensajería SACOMAR podrían ser absorbidos por el SC2N con una aplicación para la gestión de mensajes llamada MEFO. Quizás, como apunte personal, los ejércitos deberíamos ser menos reacios al cambio, tener miras hacia lo conjunto y trabajar por esa centralización de servicios.

Resumiendo, expuesta la relevancia del conocimiento y su gestión como aporte de valor a los usuarios e Institución, las herramientas y prácticas que gentilmente otros ámbitos y el CESTIC me ha proporcionado en esta labor de investigación y comparación, la línea de mejora que tenemos que superar y que, a mi juicio podría considerarse como líneas futuras, una vez alcanzados los objetivos propuestos en este documento, son:

- Establecer unos procesos centralizados y estandarizados (SLA) desde el CESTIC y que se hagan efectivos en el manejo de una aplicación ITIL común que contrate, implante y mantenga el CESTIC durante todo su ciclo de vida: ¿Proactivanet?. No considero que GLPI pueda coexistir en el futuro con esa herramienta ITIL, con sus procedimientos que implantación y que mejore continuamente el CESTIC, pero si sería vital que el personal CIS de todas las UCOS, sus CISPOC´s, y de los OACIS/CECIS (Administradores y Coordinadores Intermedios) pudieran acceder a esa aplicación ITIL común y centralizada,

y crear resolver y/o elevar las incidencias del ámbito local para una buena gestión de servicios y entrega de valor.

- Extender esta Metodología propuesta al resto de CECIS de la Armada al objeto de afianzar el proceso propuesto en todo el entramado organizacional de la Institución y darlo a conocer a todos los miembros de la Armada.

I. BIBLIOGRAFÍA

[1] Instrucción General 01/10 del Componente CIS del Sistema de Mando y Control Militar (SMCM), de enero de 2010, del JEMAD.

[2] Instrucción Técnica para la Gestión de la Calidad del Servicio en la Red IPC2 del STM, de 13 de julio de 2015, del JESPREMAD.

[3] Acta del Pleno de la Junta CIS (JUCIS) de la Armada, de mayo de 2021 sobre la nueva Organización CIS de la Armada.

[4] Concepto de Operaciones (CONOPS) del CESTIC, de enero de 2020.

[5] Orden Defensa 2639/2015 sobre Política CIS/TIC del MDEF, de 10 de diciembre.

[6] Instrucción 37/2019, para la Coordinación de la Gestión de la Información y el Concimiento (GIC), de 9 de julio, del SEDEF.

[7] Instrucción 06/17 de Control del Catálogo e Inventario del material informático de la Armada, del JEGRUCECIS.

[8] Instrucción 01/17 Cambio 1 sobre Procedimiento de adquisición de material informático para la red de propósito general y redes clasificadas, del JEGRUCECIS.

[9] Instrucción técnica 01/20 de la Gestión de la Demanda, del CESTIC.

[10] Norma 03/21 de la Gestión del Servicio de red WiFi de asistencia al personal, del CESTIC.

[11] Instrucción Operativa para la Gestión de Incidencias y Peticiones en las redes RAPNA y SAPZO, del CESTIC.

[12] Manual Integro ITIL v3 de B-able, Biable Management, Excellence and Innovation.

[13] ITIL for dummies, edición de 2011, de Peter Farenden, publicación de John Wiley and Sons, Ltd.

[14] Norma Española UNE-ISO/IEC 20000-1, de diciembre 2018, del Comité Técnico CTN71 Tecnología de la Información.

[15] Enterprise Information and Communicaction Technology Service Delivery Model, de 30 de

noviembre de 2016, de la NATO Communications and Information Agency (NCIA).

[16] Enterprise Service Delivery Model Implementation Plan 2019, de 17 de octubre de 2018, de NCIA.

[17] Manuales de las aplicaciones de Gestión de Servicios SCANS, iCIS, ARIET y GISMI extraídos de la Red Corporativa de Propósito General (WANPG).

[18] Manual de la aplicación de Gestión de Servicios Proactivanet, de Gartner Peer Insights.

[19] Manual de la aplicación de Gestión de Servicios GLPI extraído de la red de mensajería oficial de la Armada, SACOMAR.

[20] ITIL. Apuntes y clases magistrales de la asignatura COM3 del Máster DIRETIC 2020-2021 del Centro Universitario de la Defensa (CUD).

ANEXO I: GLOSARIO DE TÉRMINOS

AG	Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (se emplea indistintamente AG y AG CIS/TIC).
AGE	Administración General del Estado.
AO	Arquitectura Objetivo.
AOS	Autoridad Operacional de los Sistemas.
ASI	Approved Service Interruptions.
AR	Arquitectura de Referencia.
C3	Mando, Control y Comunicaciones.
CAB	Change Advisory Board.
CCEA	Centro Corporativo de Explotación y Apoyo.
CDO	Responsable del Dato (en inglés, Chief Data Officer).
CDSIDEF	Consejo de Dirección de Seguridad de la Información del Ministerio de Defensa.
CESTIC	Centro de Sistemas y Tecnologías de la Información y las Comunicaciones.
CIO	Director de Sistemas y Tecnologías de Información y Comunicaciones (en inglés, Chief Information Officer).
CIS	Sistemas de Información y Telecomunicaciones (en inglés, Communications and Information Systems).
CISO	Responsable de Seguridad de la Información.
CMI	Cuadro de Mando Integral.
CONOPS	Concepto de Operación.
COTS	Productos Comerciales (en inglés, Commercial Off-The-Shelf).
CPD	Centro de Procesos de Datos.
CPM	Consulta Preliminar de Mercado.

CR	Change Request.
CRF	Customer Request Form.
CTO	Responsable de Planificación y Ejecución de Programas y Responsable de Tecnologías (en inglés, Chief Technology Officer).
CUE	Catálogo Unificado de Estándares CIS/TIC.
CUP	Catálogo Unificado de Productos CIS/TIC.
DGAM	Dirección General de Armamento y Material.
DICESTIC	Director del Centro de Sistemas y Tecnologías de Información y Comunicaciones.
DIGENECO	Dirección General de Asuntos Económicos.
DIGENIN	Dirección General de Infraestructuras.
DISEGINFO	División de Seguridad de la Información.
DISEVAR	División de Diseño y Evaluación de Arquitecturas.
DIVINDES	División de Infraestructuras y Desarrollos.
DIVOPER	División de Operaciones de Red.
DRES	Declaración de Requisitos Específicos de Seguridad.
DSIDEF	Director de Seguridad de la Información del Ministerio de Defensa.
EMAD	Estado Mayor de la Defensa.
FAQ	Frecuently Ask Questions.
FAS	Fuerzas Armadas.
FCR	First Call Resolution.
GLPI	Gestión Libe del Parque Informático.
I3D	Infraestructura Integral de Información para la Defensa.
ISO	Organización Internacional de Normalización (en inglés, International Organization for Standarization).
ITIL	Biblioteca de Infraestructuras de Tecnologías de Información.
JEMAD	Jefe del Estado Mayor de la Defensa.

KPI	Key Performance Indicator.
KQI	Key Quality Indicator.
MDEF	Ministerio de Defensa.
NCIA	Agencia de Información y Comunicaciones de la OTAN (en inglés, NATO Communications and Information Agency).
NDA-ESP	Acuerdo de Confidencialidad (en inglés, Non-Disclosure Agreement).
NISP	Estándares de Interoperabilidad de la OTAN (en inglés, NATO Interoperability Standards and Profiles).
NSR	New Service Request.
OACIS	Organo de Apoyo CIS
OCCP	Oficina Central de Control de Procesos.
OCIO	Oficina del CIO.
OTAN	Organización del Tratado del Atlántico Norte (en inglés, NATO).
PAC	Plan Anual de Contratación.
PATD	Plan de Acción del MDEF para la Transformación Digital.
PECIS	Plan Estratégico de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.
POS	Procedimientos Operativos de Seguridad.
QoS	Quality of Service.
QSLR	Quarterly Service Level Review.
RD	Real Decreto.
RENEM	Red Nacional de Emergencias.
SECOMSAT	Sistema Español de Comunicaciones Militares por Satélite.
SEDEF	Secretaría de Estado de Defensa.
SEGENER	Secretaría General.
SEGINFO	Seguridad de la Información.
SEGINFODOC	Seguridad de la Información en los Documentos.

SEGINFOEMP	Seguridad de la Información en poder de las Empresas.
SEGINFOINS	Seguridad de la Información en las Instalaciones.
SEGINFOPER	Seguridad de la Información en las Personas.
SEGINFOSIT	Seguridad de la Información en Sistemas de Información y Telecomunicaciones.
SIM	Sistema de Información Militar.
SITREP	Situation Report.
SLA	Acuerdo de Nivel de Servicio (en inglés, Service Level Agreement).
SLM	Service Level Manager.
SLR	Service Level Reporting.
SME	Subject Matter Expert.
SMN	Sistema de Mando Naval.
STM	Sistema de Telecomunicaciones Militares.