Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Implementación de un servicio de atención al usuario en la Armada bajo el marco normativo del Ministerio de Defensa

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Fernando Guinea Rodriguez

DIRECTORES: Miguel Ángel Ares Tarrío

Norberto Fernández García

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Implementación de un servicio de atención al usuario en la Armada bajo el marco normativo del Ministerio de Defensa

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Las Fuerzas Armadas tienen como misión principal la defensa de la soberanía nacional por tierra, mar y aire. Uno de los pilares fundamentales para alcanzar este objetivo son las Tecnologías de las Información y las Comunicaciones (TIC). Una buena Gestión de los Servicios TIC permite a los miembros de las Fuerzas Armadas centrarse en su misión principal y no en los medios o procedimientos para alcanzarla.

En este Trabajo Fin de Máster (TFM) mostraré el estado actual de la Gestión de Servicios en la que se encuentra el Ministerio de Defensa, su evolución y su alcance e identificaré la ausencia de un servicio de atención al usuario como tal. Como aclaración, en el Ministerio de Defensa, se definen dos tipos de información baja clasificación, incluye información de Uso Público y Uso Oficial, y la de alta clasificación, de Difusión Limitada a Secreto, esta memoria se centra en los servicio para la baja clasificación y más concretamente en los de Uso Oficial.

En el presente TFM se expondrá una metodología para implementar un servicio de atención al usuario en la Armada ya que actualmente no cuenta con ella. La elección de la Armada como caso de estudio se debe a la amplia variedad de unidades con las que cuenta; desde buques navegando al otro lado del mundo, que necesitan recibir servicios desde el territorio nacional, hasta Cuarteles Generales equiparables al órgano de dirección de una gran empresa; presenta una gran casuística que debe cumplir con la normativa emanada por el Ministerio de Defensa en lo que a Gestión de los Servicios se refiere. Otro motivo por el que se ha elegido la Armada es porque veremos que el nivel que alcanza la Gestión de servicios en el Ministerio de Defensa no es el suficiente para satisfacer las necesidades de los miembros de la Armada.

En el desarrollo se expondrá, de manera lo más resumida posible, la actual normativa en vigor, incluyendo la estructura TIC desde el Ministerio de Defensa hasta la Armada, y la implementación de la Gestión de Servicios en las FAS usando como base la normativa del Ministerio de Defensa así como los estándares y metodologías que pueden ser de utilidad.

En la parte final se realizará una propuesta realista de implementación de un servicio de atención al usuario en la Armada bajo el marco de gestión normativo del Ministerio de Defensa. Esta propuesta abarcará los recursos humanos, procesos y tecnologías con el objetivo de alcanzar los tres pilares de un servicio TIC.

PALABRAS CLAVE

ITIL, Atención al usuario, Servicio, Normativa, Armada.

AGRADECIMIENTOS

A Miguel y Norberto por su paciencia y flexibilidad durante la tutorización de esta memoria.

A Carlos Delgado Huertas, José A. Verdú Rico y Juan Jose Yañez Urbano sin los cuales no podría haber comprendido lo importante que es el usuario (ese gran desconocido y denostado), trabajar en equipo y sobre todo el compañerismo sin distinción de graduación o puesto.

Pero especialmente quiero agradecer a mi mujer, Patricia, ya que mientras preparaba esta memoria fuimos padres y se ha encargado en mis periodos frente al ordenador, de cuidar de nuestras mellizas, Victoria y Matilda, nacidas el 6 de septiembre de 2022.

CONTENIDO

Contenido 1

Índice de Figuras 4

Índice de Tablas 6

1 Introducción y objetivos 1

1.1 Introducción. 1

1.2 Gestión de servicio en el Ministerio de Defensa 2

1.3 Organigrama CCEA 2

1.4 Sistema de Control de Acuerdos de Nivel de Servicio 3

1.4.1 Elementos de organización 4

1.4.2 Objetos 5

1.4.3 Roles 5

1.4.4 Subsistemas de SCANS 6

1.4.5 Subsistema de atención al usuario (SAU) 7

1.5 Gestión de servicio de la Armada 10

1.5.1 Organización de la estructura de apoyo CIS a las autoridades, mandos y unidades de la Armada 10

1.5.2 Grupo de Centros de Explotación de Sistemas de Información y Telecomunicaciones (GRUCECIS) 11

2 Estado del arte 17

2.1 ITIL 17

2.1.1 ITIL V3 18

2.1.2 ITIL 4. 26

2.2 UNE-ISO/IEC 20000:2018. Gestión de Servicios de TI 29

2.2.1 Especificaciones 30

2.2.2 Código de buenas prácticas 30

2.3 DevOps 31

2.4 PRINCE2 33

2.4.1 Principios PRINCE2 33

2.5 SCRUM 34

2.5.1 Los equipos o roles en SCRUM 34

2.5.2 Eventos 35

2.5.3 Los artefactos son: 36

2.6 KANBAN 37

2.7 Gestión de Servicio en el Ministerio de Defensa 38

2.7.1 Infraestructura Integral de Información para la Defensa (I3D) 38
2.7.2 Lotes 39
2.7.3 Gestión de servicios 41
2.7.4 Acuerdos de nivel de servicios. 43
2.7.5 Parámetros de medida del Acuerdo de Nivel de Servicio 45
2.8 Proactivanet. 46
2.9 Herramientas ITSM en la AGE 49
3 Desarrollo del TFM 51
3.1 ITIL para SAU-AR 51
3.1.1 Estrategia del Servicio 51
3.1.2 Diseño del Servicio 52
3.1.3 Transición del Servicio. 53
3.1.4 Operación del Servicio 53
3.2 Aplicación ITSM 64
3.3 Implantación del servicio 64
3.3.1 SCRUM 64
3.3.2 KANBAN 66
4 Resultados 68
5 Conclusiones y líneas futuras 70
5.1 Conclusiones. 70
5.2 Líneas Futuras 71
6 Bibliografía 72
7 Anexo I: Severidad 74
8 Anexo II: Plazos, Disponibilidad y Compromisos 76
1. Plazos aplicables en la gestión de incidencias y peticiones 76
2. Disponibilidad de activos y servicios 78
2.1. LOTE 1: Servicios e infraestructuras de datos, telefonía y localización de la I3D 79
2.2. LOTE 2: Servicios e infraestructuras de comunicaciones móviles de la I3D. 79
2.3. LOTE 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D 79
2.4. LOTE 4: Servicios e infraestructuras de acceso a Internet de la I3D 80
2.5. LOTE 5: Servicios e infraestructuras de Telemedicina de la I3D 80
2.6. LOTE 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D 80
3. No disponibilidad de un activo 80
3.1. Lote 2: Servicios e infraestructuras de comunicaciones móviles de la I3D 80
3.2. Lote 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D 80

3.3. Lote 4: Servicios e infraestructuras de acceso a Internet de la I3D.....80
3.4. Lote 5: Servicios e infraestructuras de Telemedicina de la I3D.....81
3.5. Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D.....81
4. Compromisos.....82
4.1. Lote 1: Servicios e infraestructuras de datos, telefonía y localización de la I3D.....82
4.2. Lote 2: Servicios e infraestructuras de comunicaciones móviles de la I3D.....85
4.3. Lote 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D.....88
4.4. Lote 4: Servicios e infraestructuras de acceso a Internet de la I3D.....91
4.5. Lote 5: Servicios e infraestructuras de Telemedicina de la I3D.....95
4.6. Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D.....98

ÍNDICE DE FIGURAS

Imagen 1.- Interfaz SCANS (Fuente: SCANS) 3
Imagen 2.- Interfaz petición incidencias (Fuente: SCANS) 4
Imagen 3.- Ejemplo tipos incidencias (Fuente: SCANS) 4

Ilustración 1.- Distribución Geográfica CECIS (Fuente: propia) 12
Ilustración 2.- Interfaz GESCAI (Fuente: propia) 15
Ilustración 3.- Organigrama CESIN y roles CCEA (Fuente: propia) 16
Ilustración 4.- Ciclo ITIL V3 (Fuente: ITIL V3 Axelos) 18
Ilustración 5.- Service desk local (Fuente: propia) 23
Ilustración 6.- Service desk centralizado (Fuente: propia) 24
Ilustración 7.- Service desk virtual (Fuente: propia) 24
Ilustración 8.- Dimensiones de la gestión de servicios (Fuente: propia) 26
Ilustración 9.- Sistema de Valor del Servicio (SVS) en ITIL 4 (Fuente: propia) 28
Ilustración 10.- Principios PRINCE2 (Fuente: www.axelos.com) 33
Ilustración 11.- Relación Eventos, entrada y salida (Fuente: propia) 36
Ilustración 12.- Módulos Proactivanet (Fuente: propia) 46
Ilustración 13.- Proceso de gestión de incidentes (Fuente: propia) 54
Ilustración 14.- Categorías en GLPI (Fuente: propia) 55
Ilustración 15.- Gestión de problemas (Fuente: propia) 58
Ilustración 16.- Ciclo de vida de una petición (Fuente: propia) 60
Ilustración 17.-Alta Disponibilidad GLPI en Armada (Fuente: Carlos Delgado Huertas) 61
Ilustración 18.- Estadísticas de encuestas de calidad en GLPI (Fuente: propia) 63
Ilustración 19.- Relación Eventos, entrada y salida (Fuente: propia) 65
Ilustración 20.- SCRUM (Fuente: propia) 66
Ilustración 21.- Tablero KANBAN para GLPI (Fuente: propia) 67
Ilustración 22.- Ejemplo de tarjeta tablero KANBAN GLPI (Fuente: propia) 67
Ilustración 23.- Dashboard GLPI (Fuente: propia) 68

Organigrama 1.- CCEA (Fuente: propia) 2
Organigrama 2.- Jefatura CIS (Fuente: propia) 10
Organigrama 3.- Organigrama Grupo CIS de la Armada (Fuente: propia) 11
Organigrama 4.- Centro de Sistemas de Información (Fuente: propia) 13

Gráfico 1.- KPI Incidencias (fuente: Propia) 69

ÍNDICE DE TABLAS

Tabla 1.- Topología sedes (fuente: PPT [1]) 44
Tabla 2.- Prioridad de una petición 45
Tabla 3.- Prioridad de las incidencias 45
Tabla 4.- CSF y KPI Gestión de Incidentes 57
Tabla 5.- CSF y KPI Gestión de Problemas 59
Tabla 6.- Tiempos de actuación para las Peticiones de Servicio 83
Tabla 7 Tiempos de actuación para Cierre de incidencias 84
Tabla 8.- Tabla de compromisos de respuesta y resolución de peticiones de administración y provisión del Servicio de Comunicaciones Móviles 85
Tabla 9.- Tabla de compromisos de respuesta y resolución de peticiones de administración y provisión del Servicio de Comunicaciones Móviles 86
Tabla 10.- Compromisos de Tiempo máximo de respuesta ante incidencias para el Servicio de Comunicaciones Móviles 86
Tabla 11.- Tiempo Máximo de Entrega de Informes de Resolución de Incidentes de Seguridad 86
Tabla 12.- Número máximo de incidencias de seguridad mensuales 87
Tabla 13.- Compromisos de Disponibilidad en %. 87
Tabla 14.- Tiempos de actuación para las Peticiones de Provisión y Administración 88
Tabla 15.- Compromisos de Tiempo máximo de respuesta ante incidencias 89
Tabla 16.- Tiempo Máximo de Entrega de Informes de Resolución de Incidentes de Seguridad 89
Tabla 17.- Número máximo de incidencias de seguridad mensuales 89
Tabla 18.- Compromisos de Disponibilidad en %. 90
Tabla 19.- Tiempos de actuación para las Peticiones de Servicio 91
Tabla 20.- Tiempos de actuación para Cierre de incidencias 92
Tabla 21.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias 92
Tabla 22.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad 93
Tabla 23.- Número máximo de incidencias de seguridad mensuales 93
Tabla 24.- Compromisos de Disponibilidad en %. 94
Tabla 25.- Tiempos de actuación para las Peticiones de Servicio 95
Tabla 26.- Tiempos de actuación para Cierre de incidencias 96
Tabla 27.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias 96
Tabla 28.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad 96
Tabla 29.- Número máximo de incidencias de seguridad mensuales 97
Tabla 30.- Compromisos de Disponibilidad en %. 97
Tabla 31 .-Tiempos de actuación para las Peticiones de Servicio 98

Tabla 32 .- Tiempos de actuación para Cierre de incidencias.....99
Tabla 33.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias.....99
Tabla 34.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad 99
Tabla 35.- Número máximo de incidencias de seguridad mensuales.....100
Tabla 36.- Compromiso de Disponibilidad en %.....100

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción.

Tras 3 años trabajando en un puesto donde se proporcionan servicios TIC en la Armada la conclusión es que nos hemos quedado muy por detrás de las nuevas tendencias y metodologías. Seguimos trabajando como hace 10 años. Si bien hay que decir que trabajamos de una manera eficaz pero no de manera eficiente, véase se alcanzan los objetivos pero no de manera priorizada siendo el objetivo, en muchas ocasiones, generar y resolver incidencias sin importar en la resolución la satisfacción del usuario. Esto nos ha llevado a centrarnos más en las estadísticas internas que en la satisfacción de los miembros de la Armada.

El principal objetivo de este trabajo es entregar valor al cliente, pero esto en la Armada resulta difícil ya que no somos una empresa y demostrar que se puede entregar valor no es fácilmente cuantificable de manera económica. La única forma de dar valor al cliente es con algo más valioso que el dinero, con tiempo, si un militar pierde un día en resolver su incidencia y está pendiente de ella es tiempo que no ha dedicado a su principal misión.

Para entregar ese valor a los miembros de la Armada debe haber una estructura, unos procedimientos y la tecnología que permita esa entrega de valor. Actualmente se hace pero con una normativa y estructura que no están en consonancia con las nuevas tecnologías ni con el estado del arte.

En los últimos años se han sufrido muchos cambios en empresas y organizaciones debido a la necesidad de satisfacer las necesidades de sus clientes pero no por la satisfacción de la empresa de tener al cliente contento. La evolución de las empresas se puede resumir en dos frases conocidas: “el cliente siempre tiene la razón” y “la información es poder”, pero, actualmente con un cambio “el cliente tiene la información” y “la información es dinero”. Las empresas quieren cuantos más clientes satisfechos mejor para conseguir su información y por ende dinero. Pero esta motivación es difícil de trasladar al mundo militar, lo que nos mueve es la eficacia y la eficiencia, véase alcanzar nuestros objetivos y de la manera más rápida.

Pero la Armada no es una “empresa” independiente donde se tiene autonomía para decidir las líneas de actuación. El Ministerio de Defensa es el encargado de dar un marco normativo a todas las acciones que toman el Ejército de Tierra, la Armada o el Ejército del Aire y en el caso de las TIC no iba a ser menos. En mayo del año pasado se firmó el Pliego de Prescripciones Técnicas que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D) [1].En marzo de 2022 formalizó del mismo por un periodo de 3 años.

La Armada tiene la necesidad apoyar y aportar valor al usuario acorde con el despliegue geográfico mediante la implantación de un servicio de atención al usuario especifica (SAU-AR) pero todo ello bajo el marco normativo del Ministerio de Defensa. Para poder fundamentar esta implementación se ha desarrollado la presente memoria, estructurada de la siguiente manera: En este Capítulo 1 de introducción, y para ponernos en situación, describiré la estructura actual de apoyo al usuario de forma directa en el Ministerio de Defensa y de la Armada. A continuación, en el Estado del Arte del Capítulo 2, expondré las metodologías, herramientas, marcos normativos, bibliotecas así como el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa y su manera de ejecutarlo mediante los Pliegos de Prescripciones Técnicas (PPT) del MINISDEF que pueden ser de utilidad para alcanzar el fin deseado. En el Capítulo 3 describiré la metodología que se usó para definir e implementar de manera ágil un Servicio de Atención al Usuario en la Armada (SAU-AR) así como la aplicación ITSM (*Information Technology Service Managemet)* elegida para la gestión de servicios de tecnología de la información o ITSM). En el Capítulo 4 explicaré los resultados de la implementación de la ITSM GLPI en la Armada y en el último capítulo expondré las conclusiones y líneas futuras para el uso del GLPI en la Armada.

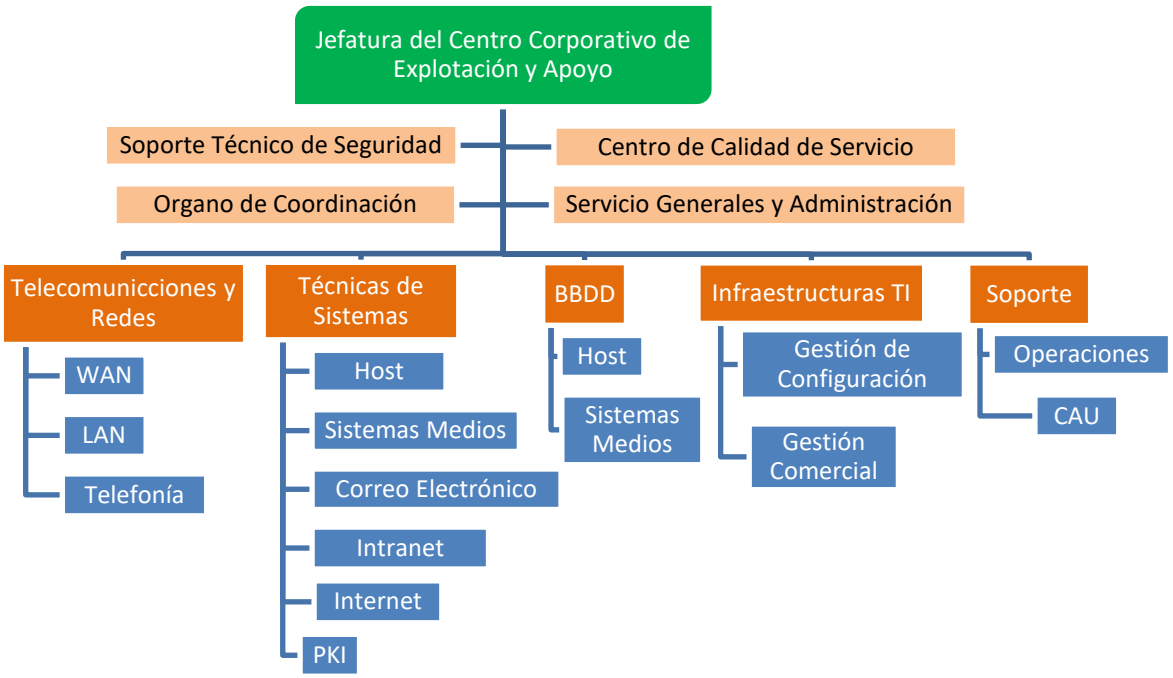
1.2 Gestión de servicio en el Ministerio de Defensa

El Centro Corporativo de Explotación y Apoyo (CCEA) [2] tiene la misión de asumir la dirección de la gestión y explotación de los sistemas de información, de la plataforma informática y de las telecomunicaciones del Ministerio de Defensa. Dentro de sus cometidos generales está dar Servicio de Atención al Usuario (SAU) de los siguientes Servicios/Sistemas:

- Servicios de Telecomunicaciones integrados en la Red Privada Virtual (RPV) de voz y en la Red de Área Extensa Corporativa de Propósito General (en adelante, WAN-PG).
- Servicios Informáticos relacionados con el software (SW) / hardware (HW) de Propósito General que no es específico de aplicaciones o sistemas de información de Mando y Control.

1.3 Organigrama CCEA

Para alcanzar estos cometidos se define el organigrama, ver Organigrama 1, en el CCEA [3]:



Organigrama 1.- CCEA (Fuente: propia)

En este organigrama hay un punto muy importante, el Centro de Atención a Usuarios (CAU), como núcleo especializado en la atención a usuarios, cuyo objetivo es proporcionar un nivel de servicio adecuado y uniforme para todos los usuarios de la red de Propósito General (WAN-PG) , tanto en datos como en telefonía y sistemas (infraestructura tecnológica).

1.4 Sistema de Control de Acuerdos de Nivel de Servicio

En 2003, se concibe el Sistema de Control de Acuerdos de Nivel de Servicio (SCANS-DEF) [4], coloquialmente conocido como SCANS, como herramienta informática con la finalidad de dar cobertura funcional a los siguientes requerimientos particulares:

- Atención y gestión de llamadas.
- Consultas y sistema de información de las guías públicas y privadas del MINISDEF (a través de una interfaz web).
- Gestión del presupuesto y control del gasto en telefonía.
- Gestión de incidencias.
- Gestión de peticiones.

Dentro de SCANS, como podemos ver en la Imagen 1 e Imagen 2, se identifican tres subsistemas para cubrir los requisitos anteriores:

- Subsistema de Atención a Usuarios (SAU). Este sistema estará integrado por los siguientes módulos:
  - Gestión de Incidencias (Imagen 3).
  - Gestión de Peticiones.
- Subsistema de Control de Gasto e Inventario de recursos contratados por el Concurso Público (SCGI).
- Subsistema de Información de Guía Telefónica.

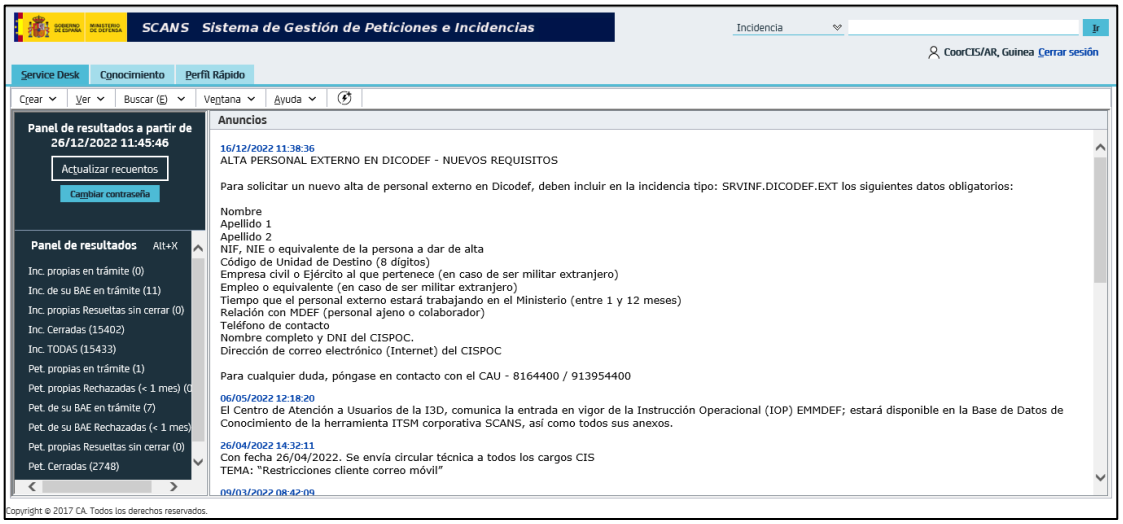


Imagen 1.- Interfaz SCANS (Fuente: SCANS)

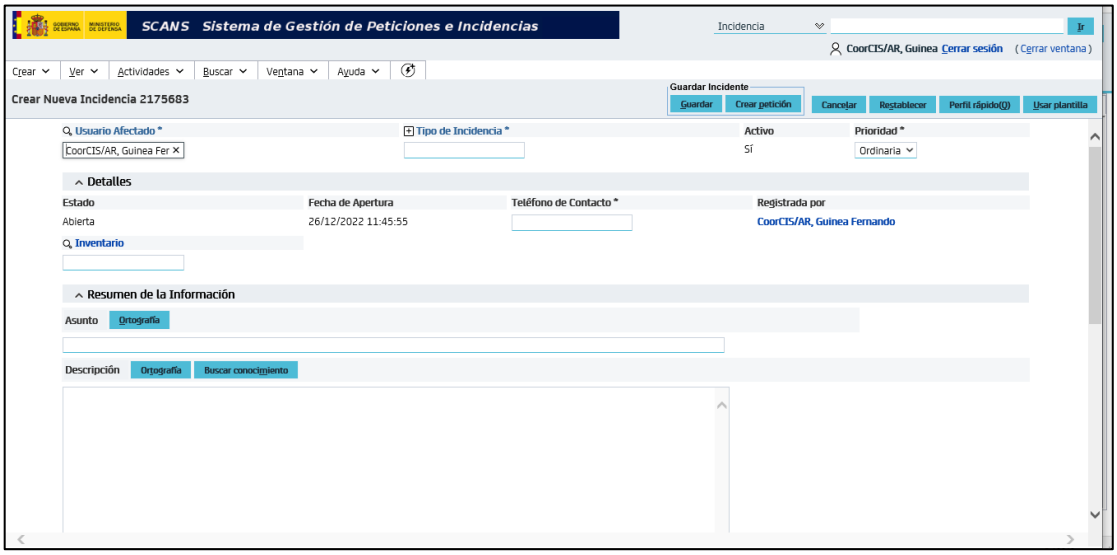


Imagen 2.- Interfaz petición incidencias (Fuente: SCANS)

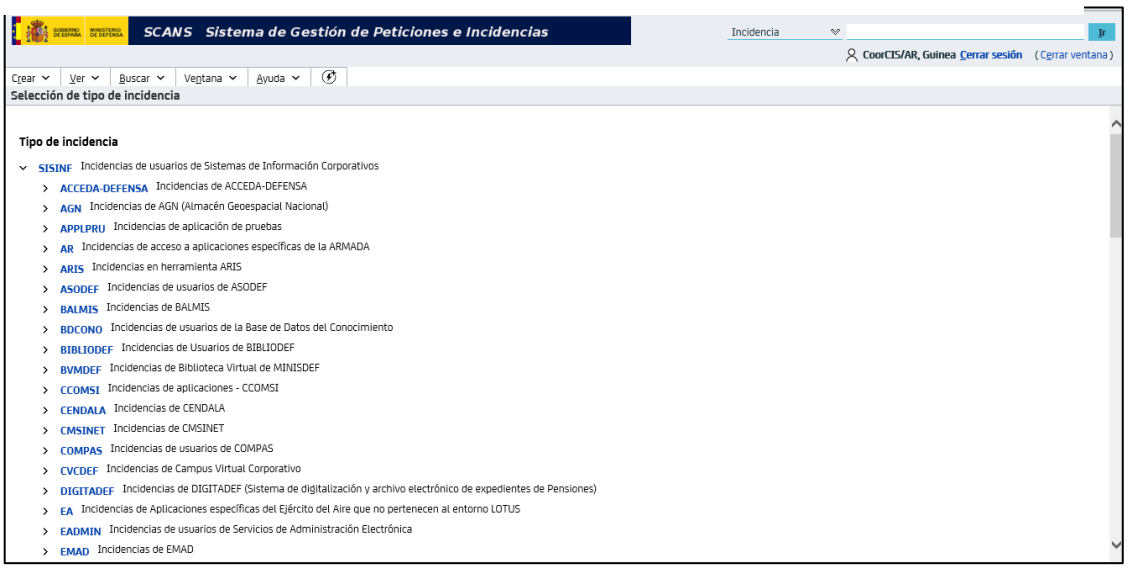


Imagen 3.- Ejemplo tipos incidencias (Fuente: SCANS)

Además de definir este sistema el CCEA define unos procesos de trabajo en [4] que son soportados por el sistema pero para ello antes se definen los siguientes elementos de la organización, los objetos y los roles implicados.

1.4.1 Elementos de organización

- Organización: Organismo o Ejército al que pertenecen los emplazamientos y diferentes unidades de destino. P.ej.: Órgano Central, Ejército de Tierra, Instituto para la Vivienda de las Fuerzas Armadas (INVIFAS), etc.
- Emplazamiento: Edificación, acuartelamiento, o recinto perteneciente a una organización, que puede albergar una o varias dependencias. P.ej.: Base Naval de Rota.
- Unidad: Elemento organizativo de la jerarquía del MINISDEF al que se le asigna una misión dentro del MINISDEF. Disponen de entidad propia por la misión y preparación específica que desarrollan. Habitualmente una unidad tiene asignada una dependencia de un único emplazamiento, aunque puede darse el caso de que una unidad pueda estar repartida en varias dependencias de distintos emplazamientos. P.ej.: Cuartel General de la Flota (con emplazamiento en la Base Naval de Rota).

- Dependencia: Cada uno de los organismos en los que se encuentra divida una unidad. P.ej. Tercio de la Armada (perteneciente a la unidad del Cuartel General de la Flota y con emplazamiento en el Poblado Naval de San Fernando).

1.4.2 Objetos

- Petición: Solicitud de servicios de infraestructura tecnológica, suministro de material informático, o paradas programadas incluidas dentro de una topología definida. Para su concesión es necesaria la aprobación por parte de un responsable designado.
- Incidencia: Solicitud de soporte para la eliminación de fallos, malfuncionamientos o inadecuados niveles de servicio. A diferencia de la petición no se necesita aprobación para su resolución.
- Consulta (o petición de información): Solicitudes de información o ayuda sobre la utilización de un servicio, sistema o infraestructura tecnológica. A diferencia de la petición no se necesita aprobación para su resolución.

1.4.3 Roles

- Usuario: Persona que en el desempeño de su función utiliza los servicios o recursos del MINISDEF.

- CIS-POC: Persona designada por el Jefe de la Dependencia como punto de contacto (POC) con el CCEA. Inicialmente habrá que distinguir diferentes funciones que podrán ser asignadas a uno o varios usuarios CIS-POC, en función del tamaño de la dependencia:
  - Punto de contacto CIS para peticiones: Responsable de la gestión y seguimiento de peticiones.
  - Punto de contacto CIS para telefonía fija: Responsable de la gestión y seguimiento de las peticiones e incidencias relacionadas con telefonía fija.
  - Punto de contacto CIS para telefonía móvil: Responsable de la gestión y seguimiento de las peticiones e incidencias relacionadas con telefonía móvil.
  - Punto de contacto CIS para sistemas informáticos: Responsable de la gestión y seguimiento de las peticiones e incidencias relacionadas con sistemas, aplicaciones, servicios o infraestructura tecnológica del MINISDEF.

- OACIS: Órgano de Apoyo CIS. Órgano o uniones de órganos que actualmente realizan el apoyo CIS al emplazamiento (P.ej. Centro de Comunicaciones (CECOM), Servicio de Apoyo Técnico (SAT), etc.). Siendo su función principal coordinar a los usuarios CIS-POC que pudiera existir en el emplazamiento.
  Se trata de un órgano ejecutor, recibirá copia de las peticiones de los usuarios CIS-POC de su emplazamiento y podrá incluir comentarios a las mismas (no filtra, únicamente informa si lo considera oportuno).

- Coordinador CIS: En caso de que en el emplazamiento no haya un OACIS, el Jefe del Emplazamiento nombrará un coordinador (CIS-POC) que se encargue de auxiliar el CCEA en la implantación del Concurso Público de Telecomunicaciones. Al igual que el OACIS recibirá copia de las peticiones e incidencias que hayan tramitado los usuarios y CIS-POC de su emplazamiento y podrá incluir comentarios a las mismas.

- Controlador intermedio: Persona u órgano encargado de realizar el control de alguno de los siguientes aspectos: gasto telefónico, incidencias, peticiones e información de guía. En algunos casos, el rol de controlador será asumido por el CIS-POC de la dependencia, en otros, será responsabilidad de personas u órganos intermedios que agrupen a varias Unidades de la organización del MINISDEF.

- Operador CAU: Persona situada en la primera línea de atención del CAU, encargada de la atención y gestión de llamadas telefónicas, proporcionando un nivel de servicio adecuado y uniforme para todos los usuarios de la red de propósito general y cuyas funciones serán las siguientes:
  - Asistencia a usuarios (Help-Desk): Registro y seguimiento centralizado de incidencias e insatisfacciones de los usuarios del dominio de propósito general del MINISDEF en relación con la utilización de los servicios e infraestructura tecnológica. La petición / incidencia / insatisfacción puede ser resuelta por el soporte técnico de primer nivel del CAU o dirigida al soporte de segundo nivel.
  - Soporte técnico: Asistencia técnica directa a usuarios acerca de la instalación, operación, mantenimiento y seguridad de los elementos de la infraestructura tecnológica.
  - Gestión y seguimiento de incidencias: Seguimiento y verificación de la resolución de incidencias no resueltas directamente por el CAU.
  - Información telefónica (Call-Center): Servicio de información telefónica de consultas de usuario. Desarrollará también la función de centralita remota de aquellos emplazamientos que se determine.
  - Peticiones: Centralización de todas las solicitudes y peticiones, a través de las personas designadas con potestad para hacer peticiones (CIS-POC).

Una vez definidos los elementos, objetos y roles podemos volver a las especificaciones funcionales de los subsistemas que tiene SCANS

1.4.4 Subsistemas de SCANS

En este apartado solo se entrará en detalles del Subsistema de Atención al Usuario (SAU) y del Subsistema de Control de Gasto e Inventario de recursos contratados por Concurso Público (SCGI) ya que el Subsistema de Información de Guía Telefónica no es relevante para esta memoria ya que es un sistema orientado, principalmente al control de gasto de telefonía asociado a cada organización y el mantenimiento del presupuesto.

Si bien el Centro de Atención al Usuario (CAU) es el núcleo especializado en la atención a usuarios,

1.4.4.1 Centro de Atención al Usuario (CAU)

Constituye la primera línea de un soporte organizado en tres niveles o líneas de atención y utilizará el Sistema de atención a Usuarios de SCANS [4]:

1.ª Línea de Atención: Se encargarán de la atención y del registro de las llamadas recibidas. Para la funcionalidad de gestión de incidencias, dispondrán de un árbol de decisión que les guíe en la resolución de las mismas. En caso de que la incidencia salga de sus atribuciones, o no pueda ser resuelta por esta primera línea de atención, la escalarán a segundo o tercer nivel.
Para la funcionalidad de soporte, se encargarán de solucionar las dudas de los usuarios relativas al uso de la guía telefónica de la intranet, de proporcionar los números de teléfonos contenidos en la Guía Telefónica que soliciten los usuarios y de registrar y, en algunos casos, resolver las cuestiones / dudas de usuarios relativas telefonía fija.

2.ª Línea de Atención: La segunda línea de atención estará dividida en las dos siguientes:

2ª Línea Sistemas: Se encargará de las resoluciones de incidencias o soporte que requieran un cierto nivel de acceso a los sistemas.

2ª Línea Comunicaciones: Se encargará de las peticiones, incidencias, y soporte relacionado con telefonía fija, móvil y las comunicaciones de datos e Internet.

3.ª Línea de Atención: Integrado por el personal técnico de los distintos órganos y núcleos del CCEA.

1.4.5 Subsistema de atención al usuario (SAU)

El Subsistema de Atención a Usuarios (SAU) está integrado por los siguientes módulos:

- Gestión de Peticiones: orientado a soportar la gestión de peticiones de información y de recursos CIS, desde su apertura hasta el cierre.
- Gestión de Incidencias: orientado a soportar la gestión de incidencias, insatisfacciones, etc., de usuarios relativas a servicios de la plataforma tecnológica del MINISDEF (telefonía, datos, sistemas, aplicaciones, SW y HW)

El análisis funcional de los diferentes módulos se concreta en los apartados siguientes.

1.4.5.1 Gestión de peticiones

Se trata de una aplicación que permite registrar, gestionar y controlar las peticiones relativas a servicios y recursos CIS. Su funcionalidad da cobertura a los siguientes requerimientos generales:

- Gestión y control de peticiones de forma completa, desde su apertura hasta el cierre.
- Gestión de peticiones relativas a paros pre programados debidos a mantenimiento. Estas paradas tienen que estar autorizadas por el CCEA y el emplazamiento correspondiente.
- Registro de peticiones a través de su propia interfaz, así como la recepción de mensajes de correo electrónico o acceso web.
- Las peticiones de usuarios finales serán revisadas y valoradas por el CIS-POC de cada dependencia que, con el criterio establecido por su jefe de unidad, aprobará o denegará la solicitud.
- El sistema habrá de facilitar la valoración de la operadora correspondiente a cada petición. Toda petición tiene que estar valorada.
- Facilidades de escalado de peticiones. Facilidad de configuración de reglas de escalado.
- Funciones de automatización de procesos y alarmas.
- Priorización / clasificación de peticiones.
- Asignación de recursos a una petición.
- Notificación por diversos medios a usuarios de la herramienta. Pudiendo ser éstos: llamada del CAU, e-mail, etc.
- Elaboración y distribución de informes que aporten la información necesaria que permita realizar un control de las actuaciones realizadas. Informes según diferentes criterios de selección y diseño de informes a medida. Estadísticas de gastos de peticiones por organización.
- Soporte a la gestión de la relación con proveedores externos.
- Generación de argumentarios de ayuda a los agentes del CAU, basados en reglas de *Workflow* e integrados con la información de la base de datos de conocimiento, de forma que se eviten errores en la entrada de datos y la respuesta de los agentes sea uniforme y estandarizada.
- Capacidad de realizar consultas a través de la intranet, por parte de los usuarios, de las peticiones realizadas, el estado de las mismas, etc.
- Posibilidad de que los responsables de las organizaciones intermedias (controladores) y los responsables de gestión de peticiones del CCEA dejen las peticiones recibidas temporalmente detenidas. Inclusión de un nuevo estado: Peticiones en estudio.
- Capacidad de soportar estructuras de control de peticiones, que podrán estar formadas por una o varias dependencias / unidades agrupadas y cuya función será la de realizar el seguimiento y control de peticiones a través del rol de Controlador Intermedio.
- Acceso a la aplicación, por parte de los técnicos de soporte presencial, de los usuarios CIS-POC y los Controladores Intermedios de peticiones.
- Integración con las aplicaciones: Guía Telefónica y SCGI.

Siendo los canales de interacción con el usuario mediante el SAU, Web (intranet) o Correo electrónico.

El proceso de gestión de peticiones de usuarios CIS-POC al CCEA tendrá las siguientes consideraciones (ver Figura 1):

- Los usuarios CIS-POC de cada emplazamiento realizarán sus peticiones al CCEA. Estos usuarios se encargarán de realizar, gestionar y controlar todo tipo de peticiones (Punto de contacto CIS para Peticiones).
- Los usuarios OACIS y/o los Coordinadores CIS recibirán copia de las peticiones realizadas por los CIS -POC de su emplazamiento, pudiendo incluir comentarios a las mismas. No podrán vetar la petición, únicamente podrán informar.
- La petición realizada por el usuarios CIS -POC podrá ser vista tanto por el OACIS / Coordinador CIS correspondiente al emplazamiento, como por todas las organizaciones intermedias situadas entre el emplazamiento solicitante y el CCEA.
- Las organizaciones intermedias podrán vetar la petición realizada por el usuario CIS-POC, momento a partir del cual esta petición se queda en suspenso (siendo archivada en el sistema). Además, tendrán la opción de detenerla temporalmente (petición en estudio). El usuario de la organización intermedia tendrá la posibilidad de incluir los comentarios que considere oportunos.
- En el caso de que los organismos intermedios no veten la petición, ésta pasará al personal del CCEA encargado de su gestión transcurrido un plazo de tiempo determinado (procedimiento de omisión), que variará en función de la urgencia de la petición.
- Las peticiones que lleguen al CCEA sin ser vetadas por ningún organismo intermedio se tramitarán siguiendo los criterios que figuran a continuación:
  - Peticiones Menores (aquellas que no llevan coste asociado, o dicho coste es mínimo): pasarán a la segunda línea de atención del CAU que las tramitará para su resolución. P.ej.: Una solicitud de alta de usuario en una aplicación determinada se tramitará por el grupo de soporte correspondiente.
  - Peticiones Mayores (aquellas que llevan coste asociado), pasarán a los órganos del CCEA responsables de control de gasto. P.ej.: Petición de una nueva central en un emplazamiento, solicitud de un nuevo servidor o licencias de software, etc.
- Una vez que la petición llega a los órganos del CCEA responsables de control de gasto, éstos tendrán la posibilidad de aprobarla, denegarla o dejarla en estudio para su tratamiento posterior.

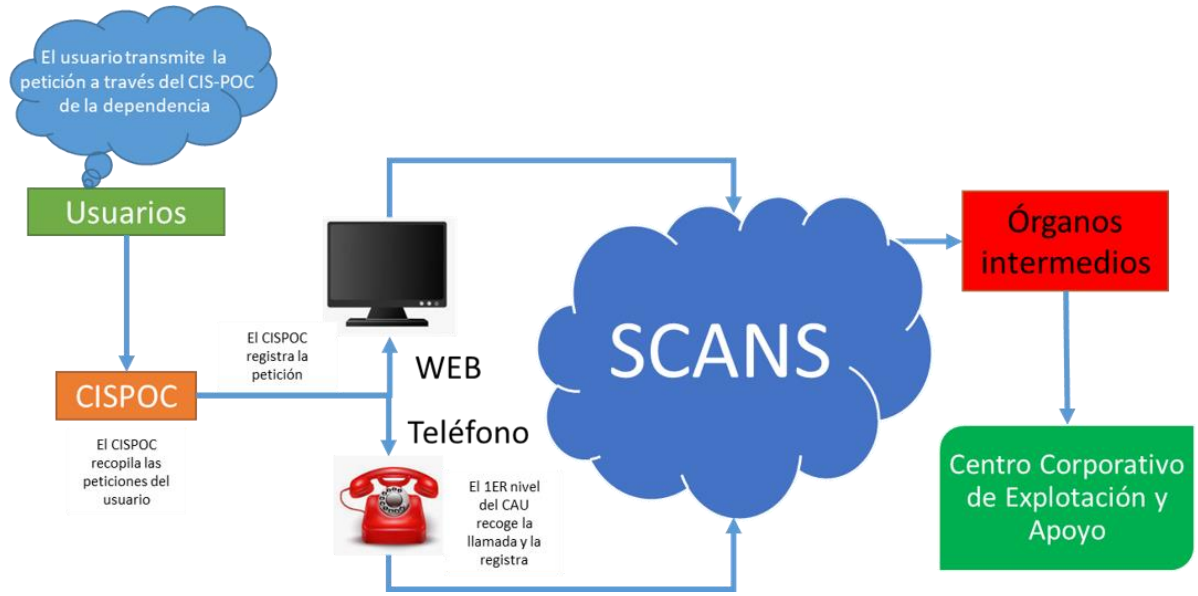


Figura 1.- Proceso de peticiones CIS-POC al CCEA
(Fuente: propia)

1.4.5.2 Gestión de incidencias:

De manera similar a la gestión de peticiones la gestión de incidencias permite registrar, gestionar y controlar las incidencias e insatisfacciones de los usuarios. Su funcionalidad da cobertura a los siguientes requerimientos generales:

- Gestión y control de incidencias e insatisfacciones de forma completa, desde su apertura hasta el cierre.
- Facilidades de escalado de incidencias y problemas. Facilidad de configuración de reglas de escalado.
- Mantenimiento de un histórico de incidencias y del histórico de cada incidencia (registro del escalado y de las modificaciones realizadas por cada usuario).
- Registro de incidencias a través de su propia interfaz, así como la recepción de mensajes de correo electrónico.
- Funciones de automatización de procesos y alarmas.
    - Incorporación de alarmas sobre incumplimientos de tiempos de resolución. El Centro de Calidad de Servicio debe poder asignar tiempos máximos de resolución de incidencias y, en caso de que se sobrepasen, se emite la alarma correspondiente en dicho Centro.
    - Gestión de los parámetros del Acuerdo de Nivel de Servicio (ANS o SLA en inglés Service Level Agreement). Emisión de la alarma correspondiente en caso de incumplimiento.
- Asignación de prioridades / clasificación de sucesos / incidencias.
- Asignación de recursos a una incidencia o problema.
- Notificación por diversos medios a usuarios de la herramienta.
- Elaboración y distribución de informes que aporten la información necesaria que permita realizar un control de las actuaciones realizadas. Informes según diferentes criterios de selección y diseño de informes a medida.
- Soporte a la gestión de la relación con operadores externos.
- Integración de operadora.
    - Gestión de la base de datos de incidencias y soluciones, de forma que dada una incidencia concreta por primera vez, las sucesivas y similares a ésta, tengan el mismo punto de encuentro para su solución, basado todo ello en el conocimiento adquirido por dicha herramienta. Base de datos de conocimiento: la herramienta proporciona el paso de ciertas resoluciones "tipo" a una base de datos de conocimiento con búsquedas de texto libre, con objeto de mejorar en el futuro la resolución de incidencias similares.
- Generación de argumentarios de ayuda a los agentes del CAU, basados en reglas de *Workflow* e integrados con la información de la base de datos de conocimiento, de forma que se eviten errores en la entrada de datos y la respuesta de los agentes sea uniforme y estandarizada.
- Capacidad de consulta, por parte del cliente del CAU del estado de sus incidencias, las que tiene abiertas y cerradas, las acciones tomadas para resolverlas, etc.
- Capacidad de soportar estructuras de control de incidencias, que podrán estar formadas por una o varias dependencias / unidades agrupadas y cuya función será la de realizar el seguimiento y control de incidencias a través del rol de Controlador Intermedio.
- Acceso web a la aplicación, por parte de los técnicos de soporte presencial y por parte de los Controladores Intermedios.

Como resumen, hasta ahora hemos visto las herramientas que utiliza el Ministerio de Defensa pero vemos que el CIS-POC es el primer punto de contacto con la incidencia. Pero el CIS-POC no es el usuario que tiene la incidencia, el CIS-POC es el "administrativo" que carga la solicitud[1] y en ningún momento le faculta para poder resolver la misma.

[1] incidencia/petición/consulta

1.5 Gestión de servicio de la Armada

El ACP-121 [5] es una publicación de la Armada donde se define la Organización de las Comunicaciones Navales y tiene por objetivo proporcionar instrucciones generales de comunicaciones sobre las siguientes materias:

- Organización de la estructura de apoyo TIC a las autoridades, mandos y unidades de la Armada.
- Organización de la estructura de explotación/operaciones TIC.

Esta publicación es de 2018 pero que ha ido sufriendo cambios siendo el último del 27 de octubre de 2020.

En esta publicación se define que la organización de la estructura TIC de la Armada debe estar alineada tanto con las estrategias, políticas e iniciativas que se produzcan en la estructura de la Administración General del Estado y en el Ministerio de Defensa para conseguir la interoperabilidad y mayor eficiencia de los sistemas CIS. En este sentido, el empleo de los medios CIS debe pasar de una arquitectura orientada a los sistemas CIS a otra orientada al usuario y basada en los servicios que discurrirán en una única infraestructura de red dentro del Ministerio de Defensa. Esta infraestructura deberá proporcionar acceso multinivel a cada uno de los usuarios de la red, según su necesidad de conocer.

Como podemos ver la organización del Armada se alinea con la política definida por el Ministerio de Defensa y para ello se distinguen funcionalmente dos estructuras: una encargada principalmente de gestionar, controlar y apoyar en la provisión de servicios CIS y otra encargada de utilizar y explotar los servicios CIS ambas bajo el ámbito de responsabilidad de la Jefatura de Sistemas de Información y Telecomunicaciones (JECIS),

1.5.1 Organización de la estructura de apoyo CIS a las autoridades, mandos y unidades de la Armada

Como se define en el ACP-121, *«la Jefatura de Sistemas de Información y Telecomunicaciones (JECIS) será responsable de la explotación, gestión y control de los sistemas de información y comunicaciones, así como de la seguridad de la información y la Ciberdefensa, en el ámbito de la Armada»*. Estas responsabilidades están más desarrolladas en los cometidos definidos en la norma [6], siendo los relacionados con esta memoria los dos siguientes:

- Gestionar y controlar los sistemas CIS en el ámbito de la Armada, incluidos los que dirige el Estado Mayor de la Defensa (EMAD) y la Secretaría de Estado de Defensa (SEDEF), así como la explotación de los servicios CIS específicos de la Armada.
- Velar por el mantenimiento del nivel de eficacia adecuado de los sistemas CIS.

Esta Jefatura depende funcionalmente Jefe de los Servicios de Telecomunicaciones e Información de las Fuerzas Armadas (JCISFAS), ubicado dentro del Estado Mayor de la Defensa, y del Centro de Sistemas y Tecnología de la Información (CESTIC) de la Secretaría de Estado de la Defensa.

A su vez de la JECIS dependen, como podemos ver en el Organigrama 2:

Organigrama 2.- Jefatura CIS (Fuente: propia)

- Grupo de Centros de Explotación CIS (GRUCECIS): Órgano responsable de la explotación, gestión, control de los Sistemas de Información y telecomunicaciones específicos de la Armada, así como de la aplicación de las normas de seguridad establecidas, y de la explotación y coordinación en el ámbito de la Armada de los medios corporativos del Ministerio de Defensa.

- Grupo de Ciberdefensa (GRUCIBER): Órgano responsable de ejecutar y supervisar la capacidad de Ciberdefensa en los Sistemas de información y Telecomunicaciones en el ámbito de la Armada.

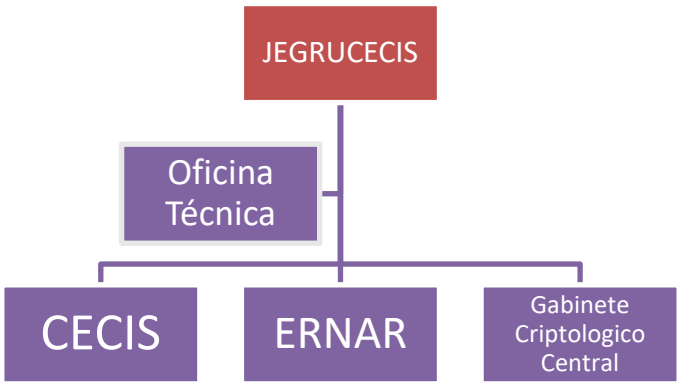
- Grupo de Seguridad en la Información (GRUSEGINFO):Órgano que centraliza todas las actividades relacionadas con la Seguridad de la Información en documentos, personas e instalaciones, tanto de material nacional como de países OTAN/UE y aquellos con los que haya acuerdos bilaterales de intercambio de información y de organizaciones internacionales.

De estos tres grupos nos centraremos en GRUCECIS ya que es el encargado, entre otras funciones, del apoyo en la provisión de servicios CIS a las Autoridades, Mandos y Unidades de la Armada.

1.5.2 Grupo de Centros de Explotación de Sistemas de Información y Telecomunicaciones (GRUCECIS)

Este Grupo es el órgano responsable de la explotación, gestión, control y aplicación de las normas de seguridad, de los Sistemas de Información y Telecomunicaciones específicos de la Armada y de los corporativos del Ministerio de Defensa en el ámbito de la Armada.

El Jefe del GRUCECIS (JEGRUCECIS), como podemos ver en el Organigrama 3, ejercerá el mando orgánico de los Centros de Explotación CIS (CECIS), de las Estaciones Radio-navales (ERNAR) y del Gabinete Criptológico Central. Ejercerá simultáneamente la Jefatura del CECIS de Madrid y contará con el apoyo de una oficina técnica para la realización de sus cometidos.



Organigrama 3.- Organigrama Grupo CIS de la Armada (Fuente: propia)

En lo que a sus cometidos particulares se refiere estos vienen reflejados en la Norma Permanente de Organización (NPOR) 1/2022 del AJECIS donde se desarrolla la estructura de la JECIS, siendo los relacionados con esta memoria los siguientes:

- Gestionar, controlar y, en su caso, explotar los sistemas de información y telecomunicaciones en su entorno de responsabilidad, incluidos los del ámbito corporativo y conjunto.
- Generar, difundir y controlar la ejecución de la normativa técnica a aplicar por los CECIS y la ERNAR.
- Coordinar y gestionar las solicitudes y necesidades que los CECIS y la ERNAR requieren de los órganos con competencias CIS en el ámbito conjunto y en el específico de la Armada.

- Gestionar, analizar e informar en relación con las solicitudes de nuevos servicios y aplicaciones CIS-TIC en coordinación con la sección de Gestión de Información y Conocimiento (GIC) y de acuerdo a la normativa en vigor.
- Elaborar y mantener actualizado el catálogo/inventario de la configuración de los componentes de la infraestructura tecnológica asociada a los sistemas de información y telecomunicaciones en el ámbito de la Armada, en coordinación con la Sección CIS de la Dirección de Sostenimiento (DISOS) de la Jefatura de Apoyo Logístico de la Armada (JAL).
- Elaborar y mantener actualizado el catálogo/inventario de las aplicaciones y servicios CIS-TIC y controlar su desarrollo, conforme a las normas que establece el CESTIC para la I3D.
- Establecer y controlar la vista técnica y de servicios de los sistemas de información y telecomunicaciones en el ámbito de la Armada.
- Coordinar la distribución del material informático (hardware y software) a los CECIS.
- Efectuar la coordinación técnica con los organismos CIS de la JAL y Flota[2], necesaria para asegurar la correcta explotación de los sistemas CIS específicos.

Los Centros de Explotación CIS son los encargados de facilitar a las autoridades y unidades que apoyan los servicios CIS y el acceso a los diferentes Sistemas de Información y Telecomunicaciones que necesitan para el cumplimiento de sus cometidos, así como el apoyo técnico necesario para su correcto empleo y funcionamiento. Como podemos ver en la Ilustración 1 el apoyo se efectuará mediante los diferentes CECIS de apoyo que hay distribuidos en la geografía española.

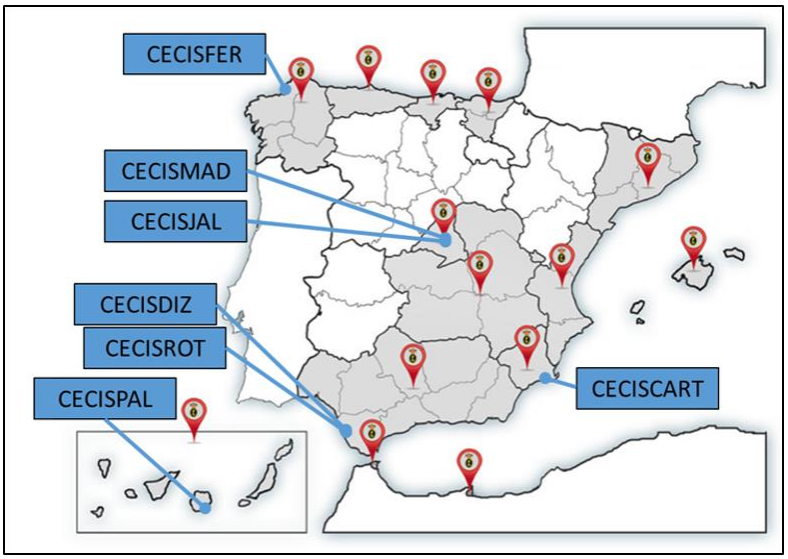


Ilustración 1.- Distribución Geográfica CECIS (Fuente: propia)

Para poder proporcionar el apoyo en las diferentes zonas geográficas los CECIS cuentan con un Centro de Sistemas de Información (CESIN) y con un Centro de Comunicaciones (CECOM). De estos dos centros nos vamos a enfocar en el CESIN ya que, como veremos, está relacionado con los servicios TIC.

Según la publicación, se denomina CESIN al conjunto de instalaciones, personal y material que, convenientemente organizado, apoya a las Autoridades, Mandos y Unidades de su ámbito geográfico en proporcionar los medios y asesoramiento técnico relacionado con las redes y sistemas de información de uso en la Armada.

[2] Se entiende por Flota a todos los buques y respectivas Jefaturas de Órdenes.

La misión del CESIN es gestionar los medios puestos a su disposición en apoyo a las Autoridades y Unidades, prestando los servicios que permitan el acceso a los sistemas de información clasificados y de propósito general requeridos para facilitar al mando el ejercicio de sus funciones.

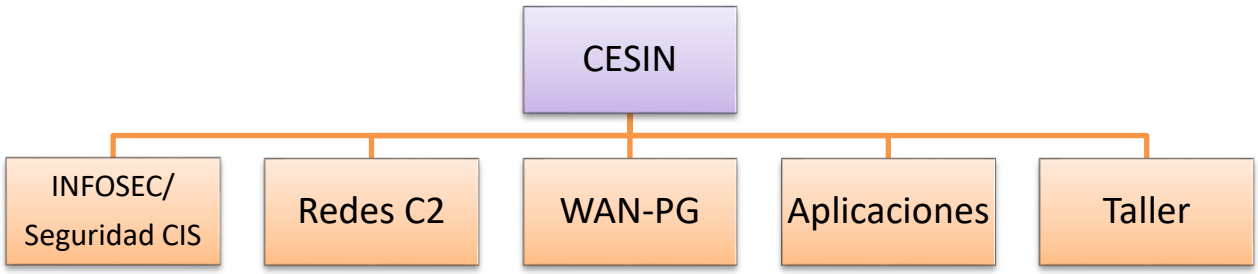
Los cometidos generales del CESIN son:

- Proporcionar los servicios de sistemas de propósito general (PG).
- Prestar asesoramiento técnico y de seguridad a las Autoridades y unidades las que apoya.
- Velar por el adecuado sostenimiento y actualización de equipos mediante el uso eficiente de los créditos disponibles para tal fin.

En lo que a sus cometidos particulares se refiere estos vienen reflejados en [6], siendo los relacionados con esta memoria los siguientes:

- Distribuir, administrar y controlar el material informático (hardware y software) de las unidades que apoyan.
- Apoyar en el mantenimiento del inventario y la configuración de los componentes de la infraestructura tecnológica asociada a los sistemas de información y telecomunicaciones, y aplicaciones específicas de la Armada en el ámbito de las unidades que apoyan.
- Colaborar en el desarrollo de aplicaciones informáticas de interés para la Armada, dentro de sus posibilidades.
- Colaborar con las diferentes divisiones del CESTIC y con el Mando Conjunto de Ciberespacio (MCCE), para mantener los niveles de servicio de los sistemas CIS del Ministerio de Defensa.
- Colaborar con el CESTIC en la resolución técnica de incidencias relacionadas con los servicios de telecomunicaciones prestados a través de la I3D.

Para lograr estos cometidos los CESIN se estructuran con los destinos indicados en el Organigrama 4:



Organigrama 4.- Centro de Sistemas de Información (Fuente: propia)

A partir de ahora nos centraremos en el CESIN de Ferrol (CESINFER) ya que para poder llevar a cabo los cometidos particulares definidos en párrafos anteriores en 2016 en CECISFER se desarrolló el Sistema de Gestión Integral del Centro de Apoyo Informático[3] (GESCAI) para: «*la gestión, aseguramiento, administración y control de los sistemas de información sobre los que tiene la competencia, con cierto volumen (medio/grande) de actuaciones/incidencias* [7]».

Para el desarrollo del GESCAI se utilizó Métrica V3, siendo esta versión de 2001, un método europeo derivado inicialmente de la metodología SSADM (*Structures Systems Analysis and Design Method*, - Análisis Estructurado de Sistemas y Métodos de Diseño), utilizada por las organismos oficiales del Reino Unido desde el año 1986, que desarrolló en España el Ministerio de las Administraciones Públicas (actual Ministerio de Hacienda y Función Pública) , siendo utilizado de forma oficial por los organismos dependientes del Estado Central, estando aun disponible en su web [8].

[3] Centro de Apoyo Informático (CAI) es la antigua designación para los actuales Centros de Sistemas de Información (CESIN).

La metodología Métrica V3 presenta un marco genérico para el desarrollo de sistemas, y como tal, representa una guía para dicho desarrollo, lo que hace necesario adecuarla al contexto del trabajo a desarrollar. Por ello, se seleccionan las tareas adecuadas, se definen documentos específicamente elaborados con una perspectiva generalista.

Para este desarrollo el GESCAI desarrollo un documento [7] . Al ser el GESCAI un Proyecto Clásico de Ingeniería, cubría dos aspectos:

- La funcional y operacional.
- La formalidad de la configuración del proyecto software a desarrollar.

Las actividades principales del sistema eran:

- Control de Inventario (hardware): Consiste en llevar a cabo una gestión, administración y control del material informático de los sistemas de información apoyados, diferenciando entre el almacenado y el de las unidades.
- Control del Software: Consiste en la gestión, la administración y el control del software instalado en los equipos de las unidades apoyadas, para que responda a las políticas del Dominio del Ministerio de Defensa.
- Ayuda de Escritorio (*Help Desk*): Se centra básicamente en la creación de un mecanismo interactivo de asistencia por el que el CAI Ferrol (actual CECISFER), por medio de la figura del coordinador y/o el técnico, se relaciona con las unidades, a través del Coordinador Informático del Destino.
- Auditoria hardware y software: Mediante las correspondientes herramientas, con la debida autorización y siempre contando con la disponibilidad de la redes, se efectuarán bajo demanda, auditorías hardware y software para mantener el control, gestionar y administrar debidamente el parque informático del CAI Ferrol (actual CECISFER).
- Compras: Esta actividad comprenderá un espacio genérico para controlar la propuesta de adquisiciones de material informático (hardware) para el apoyo a las unidades desde dos puntos de vista, que van a constituir las funciones básicas de esta actividad:
  - De cara al ejercicio siguiente, que lleve a cabo un seguimiento que muestre el nivel de cobertura respecto a la propuesta inicial en tiempo real e interactiva.
  - Respecto a las adquisiciones puntuales caso de ser preciso (reparaciones y/o sustituciones de componentes)

  Esta actividad debía mantener una importante interfaz con la actividad Control de Inventario.
- Tablón de avisos, instrucciones y notas: Se trata de mantener un espacio donde incrustar o vincular informaciones de utilidad para los usuarios del sistema. Debe llevar a cabo dos funciones básicas:
  - La de supervisión: que es la que pone a disposición del resto la información mediante interfaces ligeras e intuitivas.
  - La de consulta: espacio de consulta intuitivo, ligero y útil para los usuarios del sistema.
- Administración o gestión: Actividad que comprende la administración y gestión puramente administrativa y auxiliar respecto al resto de actividades del Sistema. Básicamente lleva a cabo su labor bajo supervisión directa, sobre todo en lo que respecta a la gestión de adquisiciones o compra de material o activos.

Como podemos ver el GESCAI era un Sistema bastante completo que necesitaba de un Coordinador Informático del Destino (denominado CIS-POC) los cuales recibían las solicitudes de los usuarios y si eran capaces de resolverlas ellos mismos lo hacían pero si no era así se creaba una incidencia en el GESCAI mediante la interfaz mostrada en la Ilustración 2:

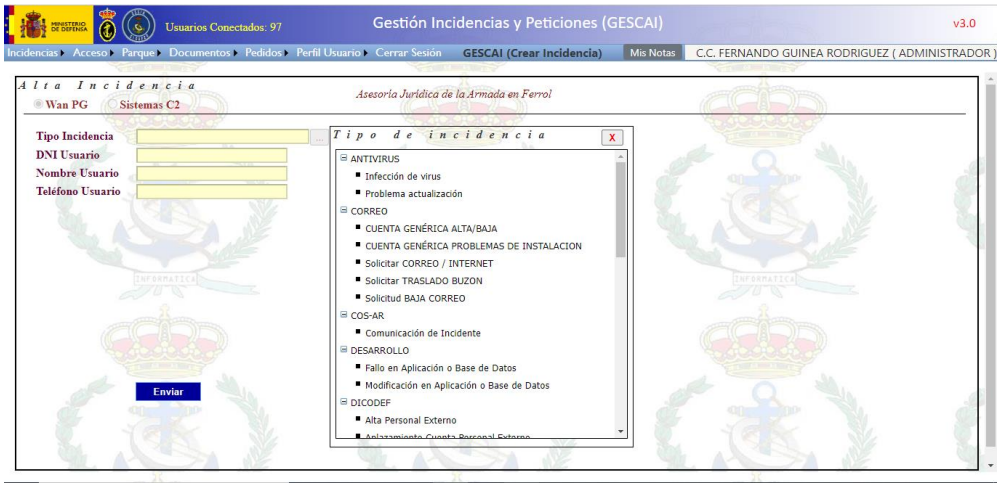


Ilustración 2.- Interfaz GESCAI (Fuente: propia)

A pesar de ser un sistema bastante completo con el paso del tiempo se identificaron ciertas flaquezas:

- Se programó con unos requisitos iniciales. Una vez finalizado ya no se podían hacer cambios/mejoras de manera sencilla ya que no se documentó suficientemente.
- Demasiado personalizada, hasta el extremo que de los 120 tipos de solicitudes que permitía de un tipo solo se creó una incidencia durante el ciclo de vida de la aplicación.
- Sin seguimiento de las incidencias por parte de los usuarios, el GESCAI solo permitía que accedieran a él los CIS-POC como nivel más bajo, debiendo los usuarios preguntar al CIS-POC por el estado de su incidencia.
- Heterogeneidad en las comunicaciones entre CIS-POC y usuarios, debido a lo comentado en el párrafo anterior, cada CIS-POC decidía como relacionarse con sus usuarios, véase, correo electrónico, llamada telefónica o presencialmente. Esto produce confusión en el usuario, consiguiendo el efecto contrario de aportar valor al usuario.

Llegados a este punto podemos ver similitudes entre la aplicación usada por el Ministerio de Defensa y la usada por el CECISFER. Pero falta un pilar importante, el personal. En el punto 1.4.3 hemos visto los roles que necesita el Ministerio de Defensa para ejercer sus funciones y en la página anterior hemos visto el organigrama de los CECIS. Ambos son compatibles como podemos ver en la ilustración 3:

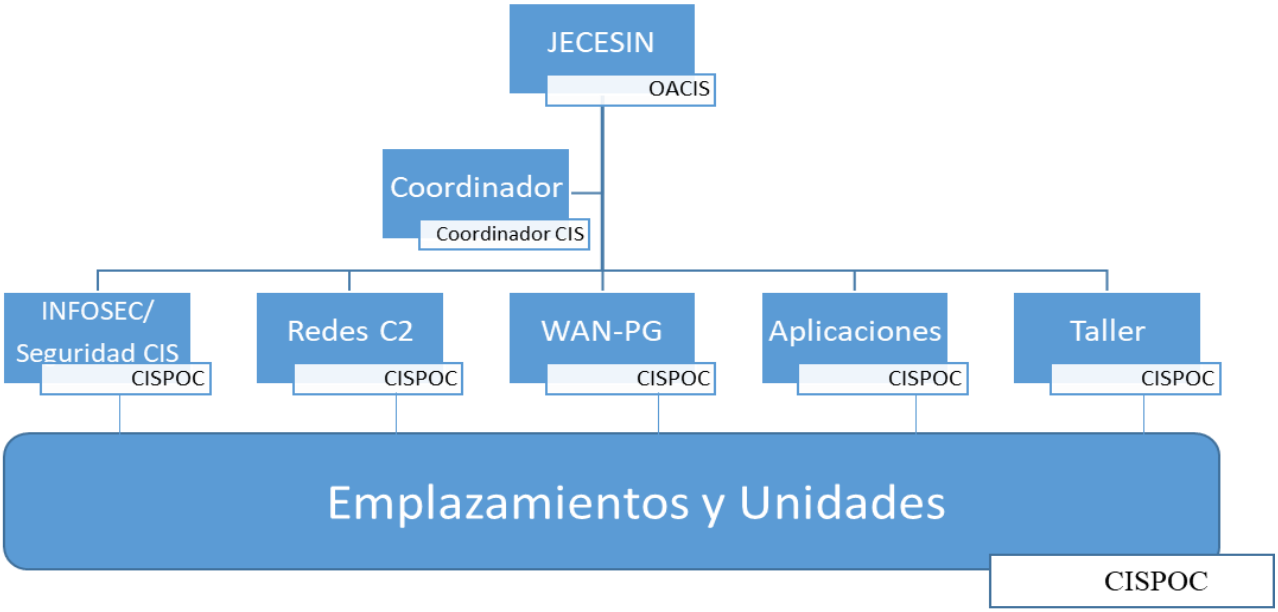


Ilustración 3.- Organigrama CESIN y roles CCEA (Fuente: propia)

Como resumen, vemos que los roles que necesita el Ministerio de Defensa son perfectamente asumibles por la organización actual de los CECIS de apoyo. También hemos visto que, tanto el Ministerio de Defensa, como la Armada dejan de lado al usuario centrándose en un CIS-POC como "concentrador" de las solicitudes. Además de esto vemos que tanto los entornos de desarrollo, en el caso del GESCAI, como las interfaces con los usuarios, en GESCAI y SCANS, no son amigables y es incluso necesario leer el manual cada vez que se quiere realizar una incidencia o hacer un seguimiento.

2 ESTADO DEL ARTE

En este capítulo se expondrá el estado del arte actual empezando por la metodología ITIL, como guía de buenas prácticas, continuando con la normativa ISO relacionada con la gestión TIC. Tras esto se expondrá la metodología DevOps, como marco de trabajo, y, aunque no es exclusivo para TI, la metodología Prince2. Tras esto se comentará, de manera muy sucinta, dos marcos de trabajo, SCRUM y KANBAN, muy útiles en desarrollos ágiles. En el último tercio de este capítulo se desarrollaran tanto la gestión como los servicios previstos en el Ministerio de Defensa y, finalmente, se describirán algunas de las herramientas ITSM que hay en el mercado y pueden satisfacer las necesidades de la Armada.

2.1 ITIL

ITIL, del inglés *Information Technology Infraestructure Library* [9], es una serie de buenas prácticas que se aglutinan en un conjunto de publicaciones. ITIL detalla un amplio conjunto de procedimientos de gestión diseñados para ayudar a las organizaciones a lograr la calidad y la eficiencia de las operaciones de TI.

ITIL nació en la década de 1980, desarrollado por la *Central Computer and Telecommunications Agency* (CCTA) del gobierno británico, como una referencia para mejorar la productividad de las oficinas del sector público del Reino Unido. Este manual, conocido como *British Standars,* es hoy una herramienta para que cualquier organización gestione muchos otros asuntos, como la seguridad de la información, los niveles de servicio, los activos, el software y las aplicaciones, como 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).

Una de sus principales características es su desarrollo sin derechos de propiedad y por tanto es 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.

En 1989 los primeros libros de ITIL fueron publicados, en 1999 ITIL publica su Versión 1 establece estándares amplios de buenas prácticas de TI. En 2007, en su Versión 2, se vuelve más accesible. Y en 2018 se publica la Versión 3, que adoptó un enfoque del ciclo de vida para la integración empresarial de TI. En 2019, se publica ITIL 4 [9] para satisfacer las complejas demandas de los negocios globalizados y las necesidades de los profesionales dentro de las organizaciones

En todas las versiones, excepto en la versión actual ITIL 4, se habla de procesos, que son un conjunto estructurado de actividades diseñadas para conseguir un objetivo específico. Un proceso tiene varias entradas (*inputs*) y las transforma en salidas (*outputs*). Los procesos tienen las siguientes características [9]:«

- *Son medibles: podemos medir el proceso de una forma apropiada. Está orientado al rendimiento. Los gestores desean medir el coste, la calidad y otras variables, mientras que los profesionales se preocupan por la duración y la productividad.*
- *Tienen resultados específicos: la razón que explica la existencia de un proceso es la entrega de un resultado específico. Este resultado debe ser identificable y cuantificable individualmente.*
- *Los procesos tienen clientes: cada proceso entrega sus resultados primarios a un cliente o interesado. El proceso debe satisfacer sus expectativas, independientemente de que sean internos o externos a la organización.*
- *Responden a eventos específicos: aunque el proceso puede ser continuo o iterativo, éste debe ser fácil de activar por un disparador concreto.»*

Como hemos visto ITIL V3 defina procesos frente a ITIL 4 que, como veremos más adelante, define prácticas. Este cambio de paradigma es el determinante para la elección del marco a usar en el desarrollo de esta memoria.

2.1.1 ITIL V3.

En la versión 3 de ITIL [10] se plantearon 26 procesos divididos en 5 etapas del ciclo de vida del servicio:

2.1.1.1 Estrategia del servicio:

En el centro del ciclo de vida del servicio está la estrategia de servicio. La creación de valor comienza con la comprensión de los objetivos de la organización y las necesidades del cliente. Todos los activos de la organización, incluidas las personas, los procesos y los productos, deben apoyar la estrategia.

Este servicio proporciona orientación sobre cómo ver la gestión del servicio, no solo como una capacidad organizativa, sino como un activo estratégico. Describe los principios que sustentan la práctica de la gestión del servicio y que son útiles para desarrollar políticas, directrices y procesos de gestión del servicio a lo largo del ciclo de vida del servicio ITIL.

Ilustración 4.- Ciclo ITIL V3 (Fuente: ITIL V3 Axelos)

Los temas tratados en este servicio incluyen el desarrollo de espacios de mercado, las características de los tipos de proveedores internos y externos, los activos del servicio, la cartera de servicios y la implementación de la estrategia a través del ciclo de vida del servicio. La gestión de las relaciones empresariales, la gestión de la demanda, la gestión financiera, el desarrollo organizativo y los riesgos estratégicos son otros de los temas principales.

Las organizaciones deben utilizar esta estrategia para establecer objetivos y expectativas de rendimiento de cara a servir a clientes y espacios de mercado, y para identificar, seleccionar y priorizar oportunidades. La estrategia del servicio consiste en garantizar que las organizaciones estén en condiciones de gestionar los costes y riesgos asociados a sus carteras de servicios, y que estén preparadas no sólo para la eficacia operativa, sino también para un rendimiento distintivo.

2.1.1.2 Diseño del servicio

Para que los servicios aporten verdadero valor a la empresa deben diseñarse teniendo en cuenta los objetivos en mente. El diseño abarca a toda la organización de TI, ya que es la organización en su

conjunto la que presta y soporta los servicios. El diseño del servicio es la fase del ciclo de vida que convierte una estrategia de servicio en un plan para alcanzar los objetivos de negocio.

El Diseño del Servicio ITIL proporciona orientación para el diseño y desarrollo de servicios y prácticas de gestión del servicio. Abarca los principios de diseño y métodos para convertir objetivos estratégicos en carteras de servicios y activos de servicio. El alcance del Diseño del Servicio ITIL no se limita a los nuevos servicios incluye los nuevos servicios. Incluye los cambios y mejoras necesarias para aumentar o mantener valor para los clientes durante el ciclo de vida de los servicios, la continuidad de los servicios, la consecución de los niveles de servicio y el cumplimiento de normas y reglamentos. Orienta a las organizaciones sobre cómo desarrollar para la gestión de servicios.

Otros temas del Diseño del Servicio ITIL incluyen el diseño, coordinación, gestión del catálogo de servicios, gestión de niveles de servicio, gestión de disponibilidad, gestión de la capacidad, gestión de la continuidad del servicio TI y gestión de proveedores.

2.1.1.3 Transición del servicio:

Este servicio proporciona orientación para el desarrollo y la mejora de las capacidades para la introducción de servicios nuevos y modificados en entornos soportados. En su tomo correspondiente se describe cómo realizar la transición de una organización de un estado a otro, controlando el riesgo y apoyando el conocimiento organizativo para la toma de decisiones. Asegura que los valores identificados en la estrategia del servicio, y codificados en el diseño del servicio, sean efectivamente transicionados para que puedan ser realizados en la operación del servicio.

La transición de los servicio describe las mejores prácticas en la planificación y el soporte de la transición, la gestión del cambio, la gestión de los activos y la configuración del servicio, la gestión de la liberación y el despliegue, la validación y las pruebas del servicio, la evaluación del cambio y la gestión del conocimiento.

Proporciona orientación sobre la gestión de la complejidad relacionada con los cambios en los servicios y los procesos de gestión de servicios, evitando consecuencias no deseadas y permitiendo al mismo tiempo la innovación.

Este servicio también introduce el sistema de gestión del conocimiento del servicio, que puede apoyar el aprendizaje organizativo y ayudar a mejorar la eficiencia y eficacia generales de todas las etapas del ciclo de vida del servicio. Esto permitirá a las personas beneficiarse de los conocimientos y la experiencia de los demás, apoyar la toma de decisiones informadas y mejorar la gestión de los servicios.

2.1.1.4 Operación del servicio

Este servicio describe las mejores prácticas para la gestión de servicios en entornos soportados. Incluye orientación sobre cómo lograr eficacia y eficiencia en la prestación y el soporte de servicios para garantizar el valor para el cliente, los usuarios y el proveedor de servicios.

Los objetivos estratégicos se alcanzan en última instancia a través de la operación del servicio, lo que la convierte en una capacidad crítica. ITIL Operación del Servicio proporciona orientación sobre cómo mantener la estabilidad en la operación del servicio, permitiendo cambios en el diseño, la escala, el alcance y los niveles de servicio. Las organizaciones reciben directrices detalladas de procesos, métodos y herramientas para su uso en dos perspectivas de control principales: reactiva y proactiva. A los gestores y profesionales se les proporcionan conocimientos que les permiten tomar mejores decisiones en áreas como la gestión de la disponibilidad de los servicios, el control de la demanda, la optimización de la utilización de la capacidad, la programación de las operaciones y la evitación o resolución de incidencias en el servicio y la gestión de problemas. Se describen nuevos modelos y arquitecturas como los servicios compartidos, la informática de servicios públicos, los servicios web y el comercio móvil para apoyar la operación de servicios.

Otros temas de este servicio incluyen la gestión de eventos, la gestión de incidentes, el cumplimiento de solicitudes, la gestión de problemas y los procesos de gestión de acceso; así como las funciones de *service desk*, gestión técnica, gestión de operaciones de TI y gestión de aplicaciones.

Dentro de la operación del servicio se definen los siguientes procesos:

2.1.1.4.1 Gestión de eventos

Un evento se puede definir como cualquier cambio de estado que tiene importancia para la gestión de un elemento de configuración (CI) o servicio de TI. Los eventos son típicamente reconocidos a través de notificaciones creadas por un servicio de TI, CI o herramienta de monitoreo.

El objetivo de la gestión de eventos es gestionar eventos a lo largo de su ciclo de vida. Este ciclo de vida de actividades para detectar eventos, darles sentido y determinar la acción de control apropiada es coordinado por el proceso de gestión de eventos

La gestión de eventos es la base para el seguimiento y control operativo. Si los eventos están programados para comunicarse información, así como advertencias y excepciones, se pueden utilizar como base para automatizar muchas actividades rutinarias de gestión de operaciones, para ejemplo ejecutando scripts en dispositivos remotos, o enviar trabajos para su procesamiento, o incluso dinámicamente equilibrar la demanda de un servicio a través de múltiples dispositivos para mejorar el rendimiento.

Los objetivos del proceso de gestión de eventos son:

- Detectar todos los cambios de estado que hayan tenido importancia para la gestión de un CI o TI Servicio
- Determinar la acción de control apropiada para eventos y asegurarse de que estos sean comunicados a las funciones apropiadas
- Proporcione el disparador, o el punto de entrada, para la ejecución de muchos procesos de operación de servicios y actividades de gestión de operaciones
- Proporcionar los medios para comparar la operación real de desempeño y comportamiento frente a los estándares y SLA
- Proporcionar una base para la garantía del servicio e informes; y mejora del servicio.

2.1.1.4.2 Gestión de incidentes

En la terminología de ITIL, un "incidente" se define como una interrupción no planificada de un servicio de TI o reducción en la calidad de un servicio de TI o un fallo de un CI que aún no ha impactado un servicio de TI (p.ej. ejemplo el fallo de un disco RAID)

La gestión de incidentes es el proceso responsable para gestionar el ciclo de vida de todos los incidentes.

Los incidentes pueden ser reconocidos por el personal técnico, detectado e informado por la herramientas de monitoreo de eventos, comunicaciones de los usuarios (generalmente a través de una llamada al *service desk*), o informado por un tercer proveedores o socios.

Los objetivos del proceso de gestión de incidentes son:

- Asegurar que los métodos y los procedimientos se usan para una gestión eficiente y rápida, análisis, documentación, en gestión en curso y novedad de incidentes
- Aumentar la visibilidad y la comunicación de incidentes a la empresa y al personal de soporte de TI
- Mejorar la percepción comercial de TI a través del uso de un enfoque profesional para resolver rápidamente y comunicar las incidencias cuando se produzcan
- Alinear las actividades de gestión de incidentes y prioridades con las del negocio.
- Mantener la satisfacción del usuario con la calidad de servicios TI.

2.1.1.4.3 Gestión de problemas

Se define un problema como la causa subyacente de uno o más incidentes.

El propósito de la gestión de problemas es gestionar el ciclo de vida de todos los problemas desde la primera identificación a través de una mayor investigación y documentación. La gestión de problemas busca minimizar el impacto adverso de los incidentes y problemas en el negocio que son causados por errores subyacentes dentro de la infraestructura de TI, y para prevenir proactivamente la recurrencia de incidentes relacionados con estos errores. Para lograr esto, la gestión de problemas busca llegar a la raíz causa de los incidentes, documentar y comunicar errores conocidos e iniciar acciones para mejorar o corregir la situación.

Los objetivos del proceso de gestión de problemas son:

- Prevenir problemas e incidentes.
- Eliminar incidentes recurrentes.
- Minimizar el impacto de incidentes que no pueden ser evitados.

2.1.1.4.4 Gestión de acceso

La gestión de acceso es el proceso de conceder a usuarios autorizados el derecho a utilizar un servicio, impidiendo el acceso a usuarios no autorizados. También se conoce como gestión de derechos o gestión de identidad.

Los objetivos del proceso de gestión de acceso son:

- Administrar el acceso a los servicios en función de las políticas y acciones definidas en seguridad de la información gestión.
- Atender con eficiencia las solicitudes de autorización de acceso a los servicios, cambiar los derechos de acceso o restringir el acceso, asegurando que los derechos que se proporciona o modifican se conceden debidamente.
- Supervisar el acceso a los servicios y garantizar los derechos que se proporcionan no se utilizan indebidamente.

2.1.1.5 Funciones de los servicio de operación

Una función es un equipo, o grupo de personas, y herramientas, u otros recursos, que utilizan para llevar a cabo uno o más procesos o actividades. En organizaciones más grandes, una función puede ser desglosada y realizada por varios departamentos, equipos y grupos, o puede estar incorporado dentro de una sola unidad organizativa (por ejemplo, una *service desk*). En organizaciones más pequeñas, uno persona o grupo de personas puede realizar múltiples funciones (por ejemplo, un departamento de gestión técnica podría también incorporan la función de *service desk*).

A continuación se hace una pequeña descripción de las funciones de los servicios de operación:

2.1.1.5.1 Gestión técnica

La gestión técnica proporciona información técnica detallando las habilidades y los recursos necesarios para apoyar la operación continua de los servicios de TI y la administración de la infraestructura. La Gestión técnica también juega un papel importante en el diseño, prueba, lanzamiento y mejora de servicios TI. En organizaciones pequeñas, es posible gestionar en un solo departamento, pero las organizaciones más grandes normalmente se dividen departamentos especializados. En muchas organizaciones, la gestión técnica también es responsable de las operaciones diarias.

2.1.1.5.2 Gestión de operaciones de TI

La gestión de operaciones de TI es la función responsable de las actividades operativas diarias necesarias para administrar y dar soporte a los servicios de TI. Esto se hace según los estándares definidos durante el Servicio Diseño. En algunas organizaciones se trata de un único departamento centralizado, mientras que en algunas ciertas actividades son distribuidas entre varios departamentos. Esta función tiene dos subfunciones que son únicas y son organizativamente distintos. Estas son:

- Control de operaciones de TI: Por lo general, cuenta con personal a turnos de técnicos lo que asegura que se llevan a cabo tareas operativas rutinarias. El control de operaciones TI también proporcionará actividades de seguimiento y control, generalmente utilizando un centro de operaciones.
- Gestión de instalaciones: Es la gestión del entorno físico de TI, generalmente centros de datos En muchas organizaciones tanto la gestión técnica como de aplicaciones se ubican junto con Operaciones de TI en grandes centros de datos. En algunas organizaciones muchos componentes físicos de la infraestructura de TI ha sido subcontratada.

2.1.1.5.3 Gestión de aplicaciones

La gestión de aplicaciones es la responsable de administrar las aplicaciones a lo largo de su ciclo de vida.

La función de gestión de aplicaciones admite y mantiene las aplicaciones operativas y también juega un papel importante en el diseño, prueba y mejora de las aplicaciones que forman parte de servicios de TI. Suele estar dividida en departamentos según la cartera de aplicaciones de la organización, lo que permite una especialización más fácil y un apoyo más centrado. En muchas organizaciones los departamentos de gestión de aplicaciones tienen personal que realiza estas operaciones diarias, al igual que con la gestión técnica, este personal forma parte de las operaciones de TI.

2.1.1.5.4 Service desk

La *service desk* o mesa de servicio es el único punto de contacto para los usuarios cuando hay una interrupción del servicio, para solicitudes, peticiones…La *service desk* proporciona un punto de comunicación a los usuarios y un punto de coordinación de varios grupos y procesos de TI. Para permitir realizar estas acciones de manera efectiva la *service desk* suele estar separado de las otras funciones de operación del servicio. En algunos casos, p.ej: donde se ofrece soporte técnico detallado a los usuarios en la primera llamada, puede ser necesario para el técnico o personal de gestión de aplicaciones para estar en el *service desk*. Esto no significa que la *service desk* pasa a formar parte de la función de gestión técnica. De hecho, mientras están en la *service desk* dejan de ser parte de la función de gestión técnica y formar parte de la *service desk*, aunque solo sea temporalmente.

Debido al objetivo de esta memoria se describirá con más detalle esta función.

Un Centro de Servicio al Usuario es una unidad funcional compuesta por un número dedicado de personal responsable de tratar diversos eventos del servicio, a través de llamadas telefónicas, interfaz web o eventos de infraestructura sobre los que se informa automáticamente

El Centro de Servicio al Usuario tiene una importancia vital en el Departamento de TI de una organización y debería ser el Punto Único de Contacto (SPOC Single Point Of Contact) diario para los usuarios de TI y tratará todas las incidencias y peticiones de servicio utilizando habitualmente herramientas de software especializado para registrar y gestionar todos esos eventos

Beneficios de un *service desk*:

- Mejora del servicio, de la percepción y de la satisfacción del cliente
- Incremento de la accesibilidad a través de un punto único de contacto, comunicación e información
- Mejor calidad y capacidad de respuesta más rápida a las peticiones del cliente o usuario
- Mejora del trabajo en equipo y de la comunicación

- Mejora del enfoque y puesta en marcha de una metodología proactiva para la provisión del servicio
- Un reducido impacto negativo sobre el negocio
- Mejora de la gestión y control de la infraestructura
- Mejora del uso de los recursos de Soporte de TI y mejora de la productividad del personal de negocio
- Información de gestión más significativa para apoyar la toma de decisiones

El objetivo principal de la *service desk* es proporcionar un único punto de contacto entre los servicios que se proporciona y los usuarios. Las responsabilidades específicas de la *service desk* incluirán:

- Registro de todos los incidentes/solicitudes de servicio relevantes detalles, asignación de categorización y códigos de priorización
- Proporcionar investigación y diagnóstico de primera línea.
- Resolver incidencias/solicitudes de servicio en la primera contactado siempre que sea posible.
- Escalar incidentes/solicitudes de servicio que no puede resolver dentro de los plazos acordados.
- Mantener informados a los usuarios sobre el progreso
- Cerrar todas las incidencias resueltas, solicitudes y otras llamadas
- Llevar a cabo devoluciones de llamada de satisfacción del cliente/usuario/ encuestas según lo acordado
- Comunicación con los usuarios: mantenerlos informados del progreso del incidente, notificándoles de cambios inminentes o interrupciones acordadas, etc.

Hay muchas formas de estructurar y ubicar los centros de atención al cliente y la solución correcta variará para diferentes organizaciones. A continuación se detallan las opciones principales, pero en realidad, una organización puede necesitar implementar una estructura que combina varias de estas opciones para satisfacer plenamente las necesidades del negocio.

2.1.1.5.4.1 Service desk local.

Ubicado junto o cerca de la comunidad de usuarios, como vemos en la Ilustración 5, que atiende esto a menudo facilita la comunicación y proporciona una presencia visible, lo cual a algunos usuarios les gusta, pero a menudo puede ser ineficiente y costoso para los recursos, ya que el personal local está ocupado esperando atender incidentes cuando el volumen y la tasa de llegada de llamadas pueden no justificarlo.

Sin embargo, puede haber algunas razones válidas para mantener un escritorio local, incluso cuando los volúmenes de llamadas por sí mismos no lo justifiquen. Las razones podrían incluir:

- Diferencias de idioma y cultura o políticas
- Zonas horarias diferentes
- Grupos especializados de usuarios
- La existencia de servicios personalizados que requieren conocimientos especializados
- Estatus de VIP/criticidad de los usuarios.

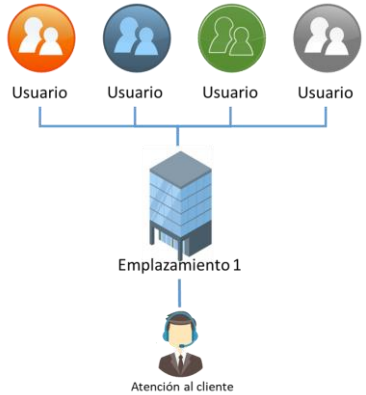


Ilustración 5.- Service desk local (Fuente: propia)

2.1.1.5.4.2 *Service desk* centralizado.

Es posible reducir el número de *service desk* fusionándolos en una sola ubicación (o en un número menor de ubicaciones) reuniendo al personal en una o más estructuras de escritorios de atención al cliente centralizados, como podemos ver en la Ilustración 6. Esto puede ser más eficiente y rentable, permitiendo que menos personal en general atienda un mayor volumen de llamadas, y también puede llevar a niveles de habilidad más altos a través de un mayor conocimiento de los eventos más frecuentes. Aún puede ser necesario mantener algún tipo de presencia local para manejar los requisitos de soporte físico, pero dicho personal puede controlarse y desplegarse desde el escritorio central.

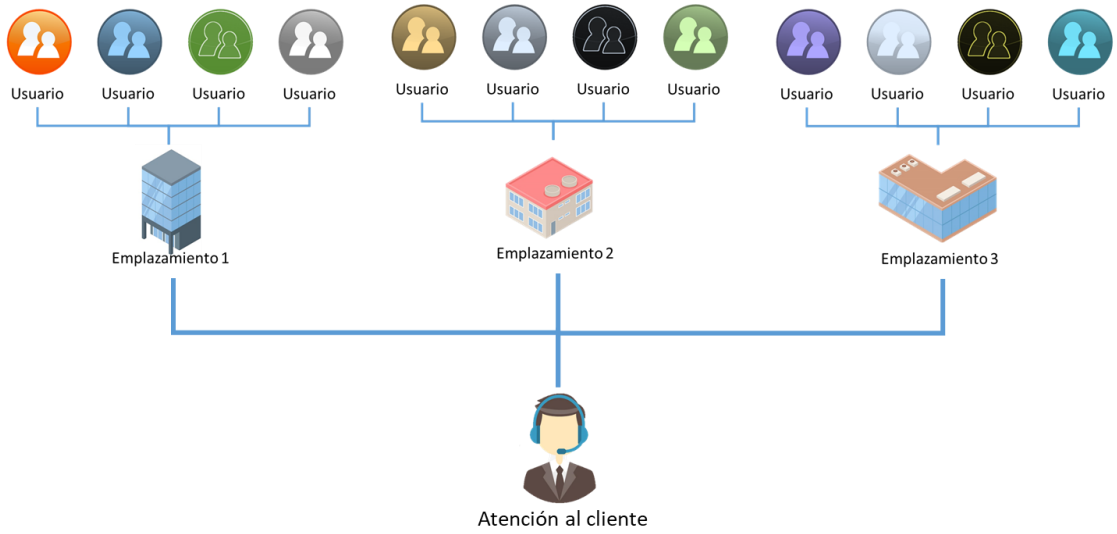


Ilustración 6.- Service desk centralizado (Fuente: propia)

2.1.1.5.4.3 Service desk virtual

Mediante el uso de tecnología y el uso de herramientas de soporte corporativas, es posible dar la impresión de un único escritorio de atención al cliente centralizado, como podemos ver en la Ilustración 7, cuando en realidad el personal puede estar disperso o ubicado en cualquier número o tipo de ubicaciones geográficas o estructurales Esto permite la opción de trabajar desde casa, grupos de soporte secundarios, externalización o tercerización, o cualquier combinación necesaria para satisfacer la demanda del usuario. Es importante tener en cuenta, sin embargo, que se necesitan medidas de seguridad en todas estas circunstancias para garantizar la consistencia y la calidad del servicio.

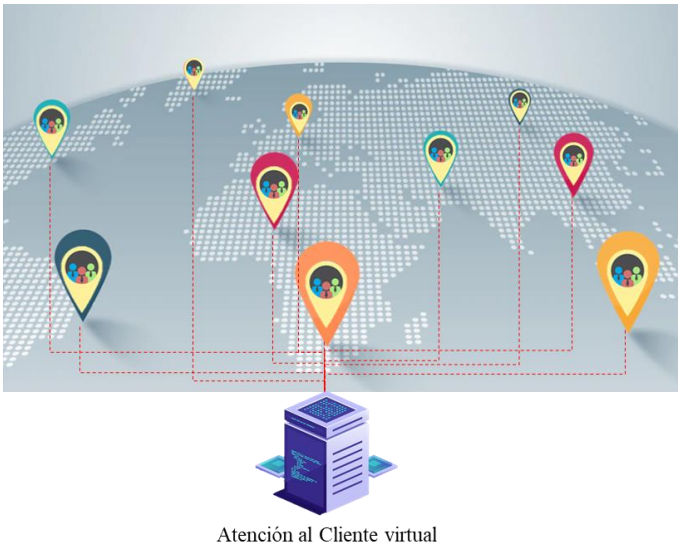


Ilustración 7.- Service desk virtual (Fuente: propia)

2.1.1.5.5 Personal del centro de atención al cliente

Los roles y responsabilidades típicas del centro de atención al cliente incluyen al gerente del centro de atención al cliente, al supervisor, a los analistas y, en algunas organizaciones, estos roles se complementan con usuarios de negocios (superusuarios) que proporcionan soporte de primera línea que actúan como puntos de contacto con TI en general y el Centro de Servicio al Usuario en particular.

2.1.1.5.6 Métricas del Centro de Servicio al Usuario

Deberían establecerse métricas *Key Performance Indicators*[4] (KPI) alineados con los *Critical Success Factors*[5] (CSF) para poder evaluar regularmente el rendimiento del Centro de Servicio al Usuario. Las métricas son importantes para evaluar la salud madurez, eficiencia, eficacia y cualquier oportunidad de mejora de las operaciones del Centro de Servicio al Usuario:

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

Dentro de estas métricas esta la satisfacción del usuario que sirven para ver cómo los usuarios sienten han sido atendidas que sus llamadas, si sienten que el operador del centro de atención al cliente fue amable y profesional, y si transmitieron confianza al usuario. Esta métrica se obtiene mediante las encuestas de satisfacción del cliente usuario.

2.1.1.5.7 Externalización del Centro de Servicio al Usuario

La decisión de externalizar el Centro de Servicio al Usuario es un aspecto estratégico para la organización. El *service desk* se puede externalizar convirtiéndolo en un Servicio, y la organización no asumiría, por definición, costes y riesgos inherente al propio servicio *service desk*.

Si el centro de atención al cliente se externaliza, se debe tener cuidado de que las herramientas sean consistentes con las que todavía se están utilizando en la organización. A menudo, la externalización se ve como una oportunidad para reemplazar herramientas obsoletas o insuficientes, solo para descubrir que hay graves problemas de integración entre la nueva herramienta y las herramientas y procesos heredados.

Por esta razón es importante asegurar que estos problemas se investiguen adecuadamente y que los requisitos del cliente se definan y especifiquen adecuadamente antes de contratar la externalización. Las herramientas no solo deben soportar el centro de atención al cliente externalizado, sino que también deben soportar los procesos y requisitos del negocio de la organización.

Idealmente, el centro de atención al cliente externalizado debería utilizar las mismas herramientas y procesos (o, como mínimo, herramientas e interfaz) para permitir un flujo de proceso suave entre el centro de atención al cliente y los grupos de soporte de segunda y tercera línea.

[4] Objetivo o umbral que permite medir el rendimiento.

[5] CSF: áreas en las que es importante obtener un alto rendimiento o éxito, las áreas que determinan el éxito de una empresa.

2.1.1.6 Mejora continua:

- Según [11] el proceso de mejora contiene los siguientes 7 pasos:«
  1. *Identificación de la estrategia de mejora.*
  2. *Definición de lo que se va a medir.*
  3. *Recopilación de datos.*
  4. *Procesamiento de datos.*
  5. *Análisis de la información y datos.*
  6. *Presentación y uso de la información.*
  7. *Aplicación de la mejora.»*

2.1.2 ITIL 4.

En 2019, se publica ITIL 4 [9] para satisfacer las complejas demandas de los negocios globalizados y las necesidades de los profesionales dentro de las organizaciones. Estos necesitan rapidez y constancia en la entrega de servicios para las organizaciones. La toma de decisiones debe ser mucho más ágil y precisa minimizando los tiempos de reacción y reduciendo el tiempo de producción y desarrollo. ITIL V3 no puede satisfacer esas necesidades pero otras metodologías ágiles sí por lo que una revisión se hace necesaria para ponerse al mismo nivel que otras metodologías agiles como puede ser SCRUM, que se explica más adelante.

Podemos decir que ITIL 4 se enfoca en las actividades de la gestión de servicios y no tanto en la tecnología, como hace la V3. Un dato significativo es que lo que la V3 llamaba “procesos” en ITIL 4 se llama “prácticas”. Según ITIL 4 una práctica es un conjunto de recursos organizativos diseñados para realizar un trabajo o lograr un objetivo. Si recordamos el significado de proceso, que son un conjunto estructurado de actividades diseñadas para conseguir un objetivo específico, vemos bien que la noción de proceso estructura las actividades con una cierta secuencialidad. Mientras que la práctica se focaliza en la realización de la tarea, independientemente del modo de llegar a ella y, sobre todo, sin una secuencia de acciones predefinidas. Con la definición de práctica, estamos en línea con las metodologías Agile.

Esta nueva versión de la publicación la podemos describir en los siguientes puntos:

- Las cuatro dimensiones de la gestión de servicios.
- El sistema de valor del servicio ITIL.
- Prácticas de ITIL 4.

2.1.2.1 Las cuatro dimensiones de la gestión de servicios

ITIL 4 define cuatro dimensiones fundamentales en el proceso de creación conjunta de valor para los clientes y otras partes interesadas. Se representan en la Ilustración 8:

Ilustración 8.- Dimensiones de la gestión de servicios (Fuente: propia)

La gestión de servicios de TI es mucho más que la gestión de tecnología. También incluye las organizaciones internas de la empresa y las personas involucradas, las relaciones de la empresa con proveedores y socios, y los diversos procesos y tecnologías utilizadas en las operaciones comerciales.

Definidas ahora como las cuatro dimensiones de la gestión de servicios, se aplican al Sistema de valor del servicio (SVS) de ITIL y tienen un impacto directo en la gestión de servicios empresariales. Interferir con estas dimensiones puede resultar en ineficiencias en los servicios. En las siguientes secciones se describen brevemente estas 4 dimensiones.

2.1.2.2 Organizaciones y personas

Las líneas jerárquicas claras y las funciones y responsabilidades bien definidas son cruciales para construir una organización bien estructurada que contribuya en gran medida a la prestación eficaz de servicios. Pero una organización sin una cultura que apoye el logro de sus objetivos adolece de falta de ambición.

Esto también afecta la forma en que se prestan los servicios en la empresa. Esta cultura está formada por personal: personal técnico y no técnico, personal administrativo, personal de administración de fincas, personal de seguridad, etc. Las personas que trabajan juntas como una unidad son el activo más valioso de una organización. La diversidad cultural que ofrecen es crucial para el funcionamiento eficiente de la empresa.

Si bien existen tecnologías y máquinas que pueden realizar muchas de las tareas que realizan los humanos, contar con las personas adecuadas en el lugar correcto puede resultar invaluable para una organización.

2.1.2.3 Información y tecnología

La dimensión de información y tecnología descrita en ITIL 4 incluye tecnologías que soportan la gestión de servicios, sistemas de gestión de flujo de trabajo, almacenes, bases de datos, herramientas analíticas y sistemas de comunicación en una organización. Además, incluye todos los datos que la organización crea, almacena, gestiona y utiliza durante la prestación de un servicio de TI.

Hoy en día, las empresas utilizan tecnologías como inteligencia artificial, aprendizaje automático, el internet de las cosas (IoT) y *blockchain* para procesar grandes volúmenes de datos, lo que requiere prácticas estrictas de gestión de datos. Las organizaciones deben tener la previsión de establecer prácticas infalibles para administrar estas cantidades masivas de datos.

2.1.2.4 Socios y proveedores

Ningún ecosistema de gestión de servicios estaría completo sin socios y proveedores de servicios. Toda organización depende en cierta medida de sus socios y proveedores para la prestación de sus servicios. Esta dimensión de ITIL 4 cubre las relaciones de la organización con otras organizaciones o individuos involucrados en el diseño, desarrollo, entrega y soporte de servicios.

Las organizaciones dependen de sus socios en diferentes niveles. Algunos se enfocan en desarrollar sus competencias básicas internamente y confían en socios y proveedores para otras necesidades. Algunos tratan de depender lo menos posible de sus parejas. En ambos casos, los socios y proveedores deben estar bien alineados con los valores fundamentales y los objetivos comerciales de la organización para garantizar un servicio fluido.

2.1.2.5 Fuentes y procesos de valor

ITIL 4 describe esta dimensión de la siguiente manera: Implica definir las actividades, flujos de trabajo, procesos y procedimientos necesarios para lograr los objetivos profesionales previstos y definir cómo las diferentes partes de la organización se conectan y trabajan juntas para permitir la creación de valor a través de productos y servicios.

De acuerdo con ITIL 4, una fuente de valor es una serie de pasos que toma una organización para crear y entregar productos y servicios a los consumidores. Esas fuentes de valor son, a su vez, posibles a través de procesos que transforman insumos en productos. Esta dimensión ayuda a definir el modelo de prestación de servicios e identificar procesos que no agregan valor a la empresa.

2.1.2.6 El sistema de valor del servicio ITIL 4

El Sistema de Valor del Servicio (*Service Value System* o SVS) de ITIL 4, como vemos en la Ilustración 9, describe jerárquicamente las entradas del sistema, los diversos elementos de la organización que están directamente relacionados con la creación de valor y las salidas (el logro de los objetivos comerciales).

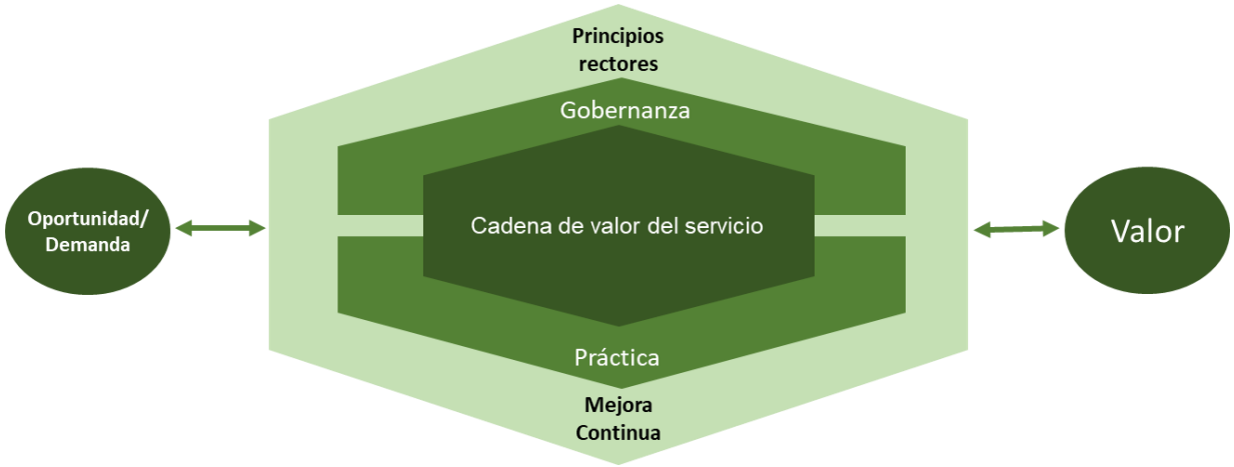


Ilustración 9.- Sistema de Valor del Servicio (SVS) en ITIL 4 (Fuente: propia)

2.1.2.7 Oportunidad/demanda

Una oportunidad representa la posibilidad de crear valor agregado para los usuarios finales. La demanda es la necesidad de productos o servicios. Estas dos entradas clave siempre están presentes en el sistema, pero la organización no siempre aprovecha las oportunidades brindadas y no cumple con todos los requisitos.

2.1.2.8 Principios rectores

Es un conjunto de recomendaciones de ITIL 4 que guían a una organización a través de su ciclo de vida de gestión de servicios, independientemente de los cambios que puedan ocurrir en las metas, estrategias o estructura de la organización. ITIL define los siguientes 7 principios clave:

1. Enfocarse en valor

La organización debe mapear el valor directa o indirectamente a las partes relevantes. Un principio centrado en el valor abarca muchos aspectos, incluida la experiencia del cliente y del usuario.

2. Comenzar desde la situación actual

Cuando se desea realizar cambios, es fácil caer en la tentación de comenzar de nuevo. Sin embargo, partir de cero puede tener más efectos negativos que positivos… En primer lugar, porque dañaría no solo el valor ya existente, sino también el trabajo en equipo. Según lo que se tenga, puede moverse rápidamente, optimizar de manera efectiva y obtener el apoyo de los socios.

3. Progresar iterativamente mediante *feedback*

Organizar el trabajo en partes pequeñas y manejables. De esa manera, se pueden implementar y completar a tiempo. Además, se deben solicitar comentarios desde el principio hasta el final de cada iteración. La retroalimentación es valiosa para garantizar que sus acciones sean relevantes y específicas.

4. Colaborar y promover la visibilidad

La cooperación de las personas adecuadas en los roles correctos aumenta la probabilidad de éxito del proyecto. Fomentar una cultura de colaboración aporta valor añadido a todas las partes implicadas. Sin embargo, la transparencia es necesaria para que esta colaboración funcione. Por eso es importante compartir información y asegurarse de que se entienda.

5. Pensar y trabajar holísticamente

Debe entenderse que la organización funciona como un todo. Cada decisión tomada por un individuo o departamento afecta a todas las demás áreas. Por lo tanto, es importante considerar cómo todas las partes crean valor antes de tomar medidas

6. Mantener las cosas simples y prácticas

Simplificar los procesos siempre que sea posible. Preguntarse si un proceso complejo realmente requiere tantos pasos. Si no, hacer lo más fácil considerando la creación de valor para las personas involucradas.

7. Optimizar y automatizar

El equipo es el recurso más valioso. El personal debe centrarse en actividades cruciales, no en tareas que puedan automatizarse. Pero antes de automatizar los procesos hay que optimizarlos. Así es como se asegura de que los procesos automatizados creen valor.

2.2 UNE-ISO/IEC 20000:2018. Gestión de Servicios de TI

Antes de desarrollar este punto merece la pena detenerse en el significado de las siglas. ISO (del inglés *International Standardization Organization*) e IEC (del inglés *International Electrotechnical Commission*) forman el sistema especializado para la normalización mundial. Los organismos nacionales miembros de ISO e IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la organización respectiva, para atender campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo.

UNE (del español Una Norma Española) es una organización privada sin ánimo de lucro legalmente reconocida en España como organismo nacional de normalización.

Tanto UNE como ISO e IEC se encargan de la normalización en sus respectivas áreas. Siendo la [12] relacionada con la Gestión del Servicio.

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. Además El estándar ISO ofrece una opción de certificación para organizaciones o empresas, mientras que el estándar ITIL es solo para particulares.

Se compone de 5 partes, de las cuales las tres primeras son informes técnicos. Las dos últimas son las que describen las especificaciones y el código de buenas prácticas.

2.2.1 Especificaciones

Esta parte cumple con los requisitos para brindar servicios de TI de acuerdo a las necesidades del negocio con alta calidad y valor agregado para los clientes, optimizando costos y asegurando constantemente la seguridad del suministro. Asegura el seguimiento del ciclo de mejora continua de la gestión del servicio y requiere un sistema de gestión integral basado en procesos, políticas, objetivos y controles de gestión del servicio. Los procesos definidos en esta norma se agrupan en cinco 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

2.2.2 Código de buenas prácticas

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.

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 (ANS) 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 [13], 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.

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 o CI (*Continuous Integration*). 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 o CD (*Continuous Deployment*) que permita disponer de la nueva aplicación con sus cambios añadidos para probarla en entornos de integración de manera ágil, 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 son:

- 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 o 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* (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 *trunk 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 o IaC (*Infraestructure as Code*) y configuración como código o CaC (*Configuration as Code*) 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 al 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.

Las ventajas de IaC y CaC son:

- 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 mismos 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 PRINCE2

Del acrónimo en inglés *PRojects IN Controlled Environments* (PRINCE) [14], es decir conversión de proyectos variables e inciertos en entornos controlados. Al Igual que ITIL, fue desarrollado por la CCTA, y originariamente fue desarrollado para proyectos TIC aunque actualmente es compatible con todo tipo de proyectos incluyendo la construcción de estadios. Su última revisión es de 2009.

Es un método estructurado de gestión de proyectos basado en las experiencias y aportes de las organizaciones para obtener buenas prácticas y experiencias de gestión de proyectos.

PRINCE2, como vemos en la Ilustración 10, se basa en 7 principios que son obligaciones y buenas prácticas que nos guían y determinan si el proyecto se gestiona correctamente y se está gestionando mediante la metodología.

Ilustración 10.- Principios PRINCE2 (Fuente: www.axelos.com)

El estar en un entorno controlado obliga a que los proyectos sean planificados de manera meticulosa antes de iniciarse y cada fase es estructurada de manera clara.

2.4.1 Principios PRINCE2

Estos son los 7 principios de PRINCE2:

- Justificación comercial continua: asegurar una razón válida para iniciar el proyecto. Las justificaciones deben ser identificadas y aprobadas y mantenidas durante la duración del proyecto. Debe haber un retorno de inversión.

- Gestión basada en la experiencia: un principio común y se puede decir que en el caso de otras metodologías es obligatorio aprender las experiencias y las lecciones aprendidas durante el proyecto. También es importante aprender lecciones de proyectos anteriores y evitar "caer dos veces en la misma piedra".

- Roles y responsabilidades definidos: este es uno de los principios más importantes para desarrollar bien desde el principio. El proyecto tiene tres *stakeholders* principales: patrocinadores comerciales, usuarios y proveedores.
  - Los patrocinadores comerciales: asegurarse de que el proyecto garantice resultados.
  - Los usuarios: utilizan y se benefician de los productos una vez creados.
  - Los proveedores: aportan recursos y experiencia al proyecto y proveen productos en primer lugar. Pueden ser internos y externos.

  Estas tres partes deben participar en la toma de decisiones.

- Gestión por fases: cada etapa del proyecto debe ser planificada, monitoreada y controlada. Hay puntos de control entre cada etapa.

- Enfoque en los productos y no en las actividades: Centra la atención en la definición y entrega de productos, es decir, un proyecto no son un conjunto de tareas a realizar, sino que entrega productos. El manual PRINCE2 afirma que: «*Un proyecto PRINCE centra su atención en la definición y la entrega de productos; en particular en sus exigencias de calidad* [11]»

- Gestión por excepción: se utiliza en cada nivel para controlar el nivel inferior. Si los informes no mencionan excepciones después de cada paso del proyecto, entonces todo va bien y no hay necesidad de preocuparse en un nivel superior. Como dicen, si no hay noticias, son buenas noticias.

- Capacidad de adaptación al entorno de proyecto: la metodología debe adaptarse al entorno, tamaño, entorno, importancia, complejidad, capacidad y riesgos del proyecto. No es lo mismo un proyecto de un pequeño taller que la remodelación del Santiago Bernabéu.

2.5 SCRUM

Este método se originó en los sectores automotriz y electrónico de Japón y Estados Unidos, donde se entendió que a pesar de los nuevos y cambiantes requerimientos, el producto debía llegar al mercado en un tiempo cada vez más corto. Por lo tanto, tenían que ser manejados con facilidad y naturalidad.

Es un marco para proyectos en entornos complejos donde los resultados deben obtenerse rápidamente y los requisitos son variables o están mal definidos. Se basa en la innovación, la competencia y la productividad.

SCRUM se basa en el desarrollo gradual de los requisitos del proyecto en bloques de tiempo cortos y fijos. La priorización de requisitos se basa en su valor para el cliente y el costo de desarrollo en cada iteración.

Por otro lado, al final de cada iteración, se muestra al cliente el resultado real obtenido para que pueda tomar las decisiones necesarias en función del contexto observado y actual del proyecto. Por otro lado, el equipo se sincroniza diariamente y hace los ajustes necesarios. SCRUM permite:

- La potenciación del equipo, que se compromete a entregar unos requisitos y para ello se le otorga la autoridad necesaria para organizar su trabajo.
- Sistematizar la colaboración y comunicación tanto entre el equipo como con el cliente.
- Sincronizar de las actividades del proyecto para apoyar la toma de decisiones y entregar resultados.

Esta metodología se basa en tres elementos y las relaciones entre ellos: Equipos (Roles), Eventos y Artefactos.

2.5.1 Los equipos o roles en SCRUM

Los equipos o roles en SCRUM son:

- Dueño del producto (PO): discute con el cliente, define el alcance del proyecto, prioriza los objetivos y equilibra el valor que aportan con sus costes.

- Equipo de desarrollo (DT): un grupo de personas que trabajan juntas para desarrollar el producto de un proyecto. Tienen un objetivo común, comparten la responsabilidad del trabajo realizado en cada iteración y proyecto. Son multifuncionales e independientes, lo que permite que los miembros del equipo tengan las habilidades necesarias para poder identificar y realizar todas las tareas que permitan al cliente cumplir con los requisitos descritos en la iteración. Deben depender lo menos posible de personas ajenas al grupo, de modo que la predicción del trabajo revisado al final de cada

iteración no se vea comprometida. Se crean sinergias y el resultado final es más rico, beneficiándose de las diversas experiencias, conocimientos y habilidades de todos, "colaboración creativa".

- SCRUM Master (SM): admite tanto al propietario del producto como al equipo de desarrollo. Esto ayuda al equipo de desarrollo a trabajar de manera inteligente y de acuerdo con los valores y principios de la metodología. Elimina los obstáculos que impiden que el equipo alcance su objetivo.

2.5.2 Eventos

Los eventos en SCRUM son:

- Planificación diaria (*Daily* SCRUM): El propósito de esta reunión es facilitar la transferencia de conocimientos y la colaboración entre los miembros del equipo para aumentar su productividad al resaltar los puntos en los que pueden ayudarse entre sí. Cada miembro del equipo revisa el trabajo realizado por los demás (dependencias entre tareas, avance hacia el objetivo iterativo, obstáculos que pueden impedir el logro de este objetivo) para hacer los ajustes necesarios al final de la reunión para hacerlo posible. adherirse a las predicciones que hicieron sobre los objetivos del equipo, que se presentan al final de la iteración (la reunión de planificación de la iteración).

- Planificación de la iteración (*Sprint planning*): Se realiza en dos partes y contestando a las preguntas Qué y Cómo:
  - Durante el Qué:
    - El cliente proporciona al equipo una lista de requisitos prioritarios para el producto o proyecto, nombra el propósito de la iteración (para ayudar a tomar decisiones sobre su implementación) y sugiere los requisitos de mayor prioridad a desarrollar en ella.
    - El equipo revisa la lista, le hace al cliente cualquier pregunta que pueda tener, agrega condiciones de satisfacción y selecciona los objetivos/requisitos clave que esperan lograr en la iteración para entregar lo que el cliente desea.
  - Durante el Cómo:
    - El equipo planifica la repetición, desarrolla tácticas que permitan lograr el mejor resultado con el menor esfuerzo posible. Esta actividad la realiza el equipo porque ellos son los encargados de organizar su trabajo y lo saben mejor.
    - Define las tareas requeridas para cumplir con cada objetivo/requisito mediante la creación de un *backlog* de sprint basado en la definición de hecho.
    - Estima colectivamente el esfuerzo requerido para completar cada tarea.
    - Los miembros del equipo autodeterminan las tareas que pueden realizar, se organizan para trabajar incluso en parejas (o grupos más grandes) para compartir información (creando un equipo más resiliente) o para resolver juntos objetivos especialmente complejos.

- Revisión de los requisitos completados (*Sprint Review*): Reunión informal donde el equipo:
  - Repasa los resultados obtenidos según el propósito de la iteración, los problemas descubiertos y su solución.
  - Presenta al cliente los requisitos cumplidos como un complemento del producto, que está listo para su entrega y uso con el menor esfuerzo posible, haciendo que el recorrido por los mismos sea lo más real posible y lo más cercano posible al objetivo deseado.

- Retrospectiva del sprint (*Sprint Retrospective*): El objetivo es mejorar constantemente la productividad y la calidad del producto que se está desarrollando, la motivación del equipo, cómo interactúan entre sí, cómo fue la última iteración o cómo avanza el proyecto... el equipo analiza cómo fue su camino, si trabajó durante la iteración, por qué está logrando o no los objetivos con los que se comprometió al comienzo de la iteración y por qué la adición del producto que acaba de mostrar al cliente era o no lo que esperaba.

2.5.3 Los artefactos son:

- Lista de objetivos (*Product Backlog*): El dueño es el *Product Owner*. Es una lista de objetivos/requisitos priorizados y representa la visión y expectativas del cliente para los objetivos y el desempeño del producto o proyecto. La lista incluye
  - Objetivos/requisitos de alto nivel para un producto o proyecto, a menudo expresados en forma de historias de usuarios. Para cada objetivo/requisito, se anota el valor que aporta al cliente y los costos de implementación esperados. Al priorizar la lista, el valor de cada requisito para la empresa se equilibra con los costos de desarrollo estimados, es decir retorno de la inversión (ROI).
  - En la lista se muestra las posibles iteraciones y resultados que el cliente espera en función de la velocidad de desarrollo del equipo que trabaja en el proyecto. Es conveniente que el contenido de cada iteración sea consistente, de forma que se reduzca la consecución de todos sus objetivos.
  - La lista también debe tener en cuenta los riesgos del proyecto y contener los requisitos o tareas necesarias para reducirlos.
- Lista de tareas de la iteración (*Sprint Backlog*): El dueño es el *Development Team*. Este es un subconjunto seleccionado de los objetivos/requisitos de la cartera de productos para la iteración actual y su plan de tareas de desarrollo. El equipo completa esta reunión de planificación de sprint y selecciona lo que espera poder completar y presentar al cliente como un conjunto de productos terminados para entregar al final del sprint.

En la ilustración 11 podemos ver la relación entre eventos, entrada y salida.

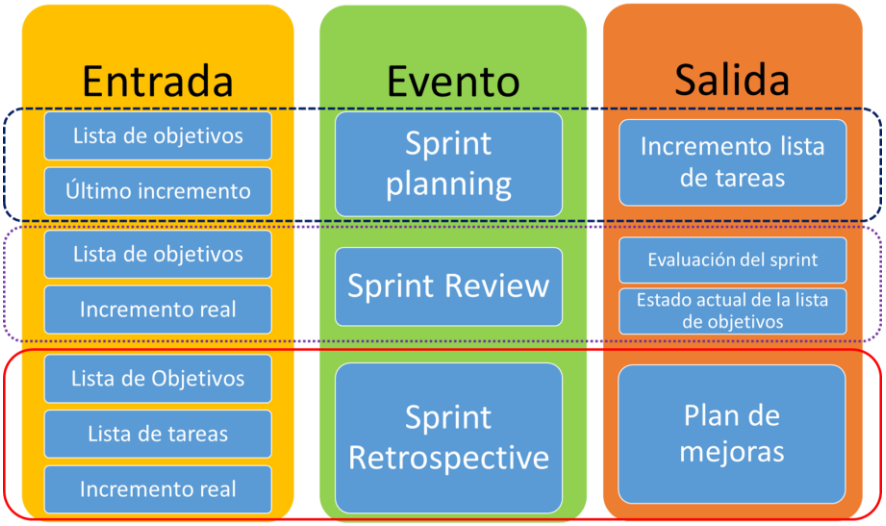


Ilustración 11.- Relación Eventos, entrada y salida (Fuente: propia)

2.6 KANBAN

Kanban es una combinación de dos palabras japonesas: 看 (Kàn), "signo" o "señal visual", y 板 (Bǎn), "tablero".

Es un método visual [13] de gestión de proyectos que permite, de forma visual en un tablero organizado por columnas, visualizar los flujos de trabajo de un proyecto. Cada columna es una etapa del trabajo. En cada columna se ubican las tarjetas donde se identifica las tareas así como el responsable o responsables de la misma. El tablero básico tiene tres columnas Tareas pendientes, en progreso y terminadas.

A principio de la década de los 2000 la metodología Kanban se adaptó al desarrollo software usando el mismo proceso de extracción o *pull*. A modo de resumen, El trabajo se "extrae" de las tareas pendientes, según la carga laboral y capacidad de cada miembro del equipo. Luego, los miembros pueden hacer un seguimiento visual del trabajo a medida que avanza a través del ciclo de vida de las tareas, representado por etapas en un tablero Kanban, hasta su finalización.

Kanban funciona como un método visual de gestión de proyectos que permite a los equipos encontrar un equilibrio entre la demanda de trabajo y la disponibilidad de los recursos del equipo.

Los principios Kanban son los siguientes:

- Comienza con lo que haces ahora

Se puede implementar esta metodología a cualquier proceso o flujo de trabajo actual. A diferencia de algunos procesos de gestión ágil más definidos como Scrum, Kanban es lo suficientemente flexible como para adaptarse a las prácticas centrales de tu equipo de trabajo.

- Acordar un cambio incremental y evolutivo

Los grandes cambios pueden ser perjudiciales para el equipo y, si se intenta cambiar todo a la vez, es posible que el nuevo sistema no funcione se esperaría. Ese es el motivo por el cual el marco Kanban está diseñado para fomentar la mejora continua y el cambio progresivo. En lugar de cambiar todo de una vez, empieza por buscar cambios progresivos para lograr que los procesos de tu equipo realmente evolucionen con el tiempo.

- Respeta los procesos, los roles y las responsabilidades actuales.

El objetivo es obtener apoyo para Kanban en un entorno donde las personas pueden tener un interés personal en las prácticas establecidas. Esto es particularmente cierto para las organizaciones más grandes donde el cambio es más lento y más difícil de lograr.

- Fomentar el liderazgo en todos los niveles de la organización

Kanban reconoce el poder de la colaboración, pero también permite que cualquier persona se apropie de un problema y lo aborde. Armado con una fuerte justificación y datos para respaldar un argumento, cualquiera debería poder tomar medidas.

Al promover una cultura de seguridad Kanban empodera a los miembros del equipo para que lideren, asuman riesgos y crezcan profesionalmente.

Tras haber descrito las diferentes metodologías en el siguiente punto hablaré del estado del arte pero en lo que a la necesidad del Ministerio de Defensa tiene para su Infraestructura Integral de Información para la Defensa (I3D).

2.7 Gestión de Servicio en el Ministerio de Defensa

2.7.1 Infraestructura Integral de Información para la Defensa (I3D)

La Orden de Defensa 2639/2015 [16], que establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, define a la Infraestructura Integral de Información para la Defensa (I3D) como: *"una infraestructura tecnológica que mediante la convergencia de los sistemas de información y telecomunicaciones y los servicios que estos proporcionan, optimice el uso de los mismos y facilite a los organismos y usuarios el acceso eficaz y seguro a los recursos de información de Defensa. Este acceso debe poder ser independiente de la situación geográfica del usuario de si este está en movimiento, estacionario o fijo.»*

La Infraestructura Integral de Información para la Defensa (I3D) es la espina dorsal de todas la misiones que realizan nuestras FAS en tiempo de paz o guerra por lo que debe tener capacidad resiliente para adaptarse a los cambios como pueden ser catástrofes naturales que inutilicen centros de comunicaciones o acciones del enemigo que deliberadamente restrinjan nuestras infraestructuras.

En la citada orden de Defensa se tomó la decisión de organizar los servicios de la I3D según el modelo OTAN *(NATO C3 Classification Taxnomy* [17][6], actualmente en su *Baseline* 5 de agosto de 2021*)*

En la Ley Orgánica 5/2005 de la Defensa Nacional [18], se define que las Fuerzas Armadas contribuyen a la seguridad y Defensa de España y sus aliados en el marco de las organizaciones internacionales de las que forma parte como, por ejemplo la Organización del Tratado del Atlántico Norte (OTAN). Es por todo esto que los servicios e infraestructuras de la I3D deben estar vinculados con la Defensa Nacional y ser interoperables con las estructuras operativas internacionales.

También se pretende alinear la contratación de los servicio con los de la Administración General del Estado (AGE).

La Instrucción 33/2018, de 6 de junio, del Secretario de Estado de Defensa, aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa [19]. La Orden DEF/2639/2015, de 3 de diciembre, establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa [20]y define la estructura de gobierno que permite su coordinación, control y seguimiento. Esta Política CIS-TIC proporciona una visión global e integral de los recursos del Departamento en esta materia, basada en las misiones y operaciones y en las capacidades operativas del Ministerio de Defensa, poniendo énfasis en la prioridad de las Capacidades CIS-TIC para las Fuerzas Armadas y en su normalización para asegurar la interoperabilidad. El artículo 4 de [16] señala que: «*el planeamiento y obtención de los CIS/TIC, su control, organización, operación y mantenimiento, para el establecimiento y provisión de los Servicios CIS/TIC, se regirá por los principios, finalidad, ejes estratégicos y directrices de la citada Política CIS/TIC. En esta instrucción se recoge como ejes estratégicos de actuación los siguientes:*

- *Avanzar hacia una única Infraestructura Integral de Información para la Defensa, gestionada por el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC).*
- *Dar prioridad a las actuaciones orientadas a satisfacer las necesidades de Servicios CIS-TIC de las Fuerzas Armadas.*
- *Potenciar la utilización de sistemas normalizados, homogéneos e interoperables.*

[6] La Taxonomía C3 es un modelo que representa los conceptos y sus relaciones involucradas en todas las actividades del ciclo de vida para las capacidades de Consulta, Mando y Control (C3) de la OTAN. La Taxonomía C3 proporciona una herramienta y un lenguaje común para sincronizar estas actividades y mejorar la conexión del Concepto Estratégico y la Orientación Política de la OTAN a través de los niveles de ambición expresados en el Proceso de Planificación de la Defensa de la OTAN (NDPP), con la arquitectura y el diseño tradicionales de los Sistemas de Información y Comunicaciones (CIS).
.

- *Consolidar la Seguridad en los CIS/TIC.*
- *Avanzar hacia un nuevo modelo de gobierno integral de los CIS/TIC.*
- *Optimizar la gestión de los recursos humanos relacionados con los CIS-TIC y racionalizar los recursos financieros y materiales en esta materia.»*

Recientemente se ha adjudicado el Pliego de Prescripciones Técnicas que ha de regir el establecimiento de un acuerdo marco para la contratación de Servicios e Infraestructuras de Telecomunicaciones de la Infraestructura Integral de Información para la Defensa. El Objeto de este Pliego, que alcance a todo el Ministerio de Defensa y sus Organismos Públicos, es: "*la prestación de los servicios e infraestructuras de telecomunicaciones para la Defensa en Territorio Nacional y Zonas de Operaciones, necesarios para dotar a los emplazamientos del MINISDEF incluidos en el alcance de este contrato de una comunicación de calidad entre todos ellos, partiendo de la situación actual, y con el objetivo de la convergencia de las redes existentes actuales.*" [1]

El objeto de los trabajos especificados en este pliego comprende la instalación, configuración y puesta en marcha de los siguientes servicios, se mencionan solo los relacionados con esta memoria:

- La provisión y gestión de los servicios de voz y datos necesarios para todos los emplazamientos del Ministerio de Defensa.
- La prestación de los servicios de comunicaciones móviles: voz, datos y mensajería.
- La prestación de los servicios e infraestructuras asociados a la red de respaldo de fibra óptica del Sistema de Mando y Control Militar (SMCM) para completar la I3D.
- La prestación de los servicios de comunicaciones de cobertura global satelital.
- Los servicios de acceso a Internet libre para misiones de la Defensa en Territorio Nacional.
- La provisión de los servicios de soporte.
- Los servicios de videoconferencia segura entre los diversos emplazamientos del Ministerio de Defensa.
- La prestación de los servicios e infraestructuras para el seguimiento y localización de vehículos y personal militar.
- Los servicios de Apoyo Técnico-Logístico que el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) precisa para desarrollar sus funciones en materia de explotación, desarrollo técnico, mantenimiento, control de la seguridad de las comunicaciones y servicios asociados a la I3D.
- Los servicios e infraestructuras necesarios para el mantenimiento y extensión de la red WiFi de asistencia al personal.
- La implantación, explotación, gestión y mantenimiento de los servicios objeto del contrato, y de todo el equipamiento e infraestructura necesarios.

2.7.2 Lotes

Por la diferente naturaleza de los servicios de telecomunicaciones a contratar el pliego se divide en 8 lotes:

- Lote 1: Servicios e infraestructuras de Datos, telefonía y localización de la I3D del MINISDEF.
- Lote 2: Servicios e infraestructuras de Comunicaciones móviles de la I3D del MINISDEF.
- Lote 3: Servicios e infraestructuras de Comunicaciones satelitales civiles de la I3D del MINISDEF.
- Lote 4: Servicios e infraestructuras de Acceso a Internet de la I3D del MINISDEF.
- Lote 5: Servicios e infraestructuras de Telemedicina de la I3D del MINISDEF.
- Lote 6: Servicios e infraestructuras de Soporte y Atención a Usuarios de la I3D del MINISDEF.
- Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D del MINISDEF.
- Lote 8: Apoyo Técnico y Logístico a los servicios e infraestructuras de la I3D del MINISDEF.

Con objeto de ver la variedad de servicio se hará una pequeña descripción de los servicios que se necesitan en el Ministerio de Defensa para cumplir su misión y por tanto su gestión, para más adelante centrarse en el servicio relacionado con esta memoria.

- Lote 1: Servicios e infraestructuras de datos, telefonía y localización de la I3D del MINISDEF.
  Este lote presta los servicios de definición, implantación, mantenimiento y gestión de una red de datos multiservicio para la Defensa, única, global y de altas prestaciones para las sedes del Ministerio de Defensa sobre la que convergerán las diversas redes privadas virtuales para la transmisión de servicios de *Voice over IP/Text over IP* (VoIP/ToIP), datos y multimedia demandados por el MINISDEF.
  También es objeto del lote la prestación de los servicios de definición, implantación, mantenimiento y gestión del servicio de Telefonía Fija de las sedes del MINISDEF, junto con el correspondiente servicio de Gestión, Operación y Mantenimiento de la infraestructura asociada objeto del lote.

- Lote 2: Servicios e infraestructuras de comunicaciones móviles de la I3D del MINISDEF.
  Este lote comprende el suministro de dispositivos móviles junto con el tráfico de voz y datos asociados a dichos dispositivos, y los servicios de implantación, gestión y mantenimiento de la Red Privada Virtual Móvil (RPV Móvil) así como su interconexión con la Red Privada Virtual Fija (RPV fija) del Lote 1 de este pliego.

- Lote 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D del MINISDEF.
  El objeto de este lote es la prestación de los servicios de telecomunicaciones satelitales para aquellas Unidades del MINISDEF que lo necesitan en el desempeño de sus misiones, tanto en Territorio Nacional como en el extranjero.
  Se incluyen los servicios de comunicaciones de voz y datos en las distintas modalidades específicas de cada una de las constelaciones satelitales.

- Lote 4: Servicios e infraestructuras de acceso a Internet de la I3D del MINISDEF.
  El objeto de este lote es la prestación de los servicios de definición, implantación, mantenimiento y gestión de la solución de acceso directo a Internet para las sedes del MINISDEF que lo necesitan dentro del Territorio Nacional.
  Para todo ello se requiere la implantación y operación de un centro de gestión, cuyos técnicos realicen las funciones propias de la gestión del equipamiento objeto del lote y la resolución de incidencias y peticiones.

- Lote 5: Servicios e infraestructuras de Telemedicina de la I3D del MINISDEF.
  El objeto de este lote es la contratación de los servicios e infraestructuras de telemedicina de la I3D empleados por los determinados emplazamientos militares en Territorio Nacional, así como contingentes de las Fuerzas Armadas en Zona de Operaciones.

- Lote 6: Servicios e infraestructuras de Soporte y Atención a Usuarios de la I3D del MINISDEF.
  El objeto del presente lote es la prestación de los servicios de Soporte y Atención al Usuario TIC. El Servicio de Soporte TIC estará compuesto por el Centro de Atención al Usuario (CAU) y el Sistema de Control de Acuerdos de Nivel de Servicio (SCANS).

- Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D del MINISDEF.
  El objeto del presente lote es establecer las condiciones técnicas por las que se ha de regir la contratación de los Servicios de Videoconferencia de la I3D del Ministerio de Defensa.

- Lote 8: Apoyo Técnico y Logístico a los servicios e infraestructuras de la I3D del MINISDEF.
  El presente lote tiene por objeto regular y definir el alcance, contenido y condiciones de prestación, la enumeración y descripción detallada de las características de los procedimientos y metodología,

sistemas técnicos, recursos, normativa, etc., que habrán de regir (a las que debe ajustarse) la contratación y/o la ejecución de los Servicios de Apoyo Técnico-Logístico que el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) precisa para desarrollar sus funciones en materia de explotación, desarrollo técnico, mantenimiento, control de la seguridad de las comunicaciones y servicios asociados a la Red Terrena de la I3D.

2.7.3 Gestión de servicios.

La Gestión de servicios afecta a todos los lotes anteriormente mencionados e incluye la implantación del servicio; el plan de gestión del servicio, y la finalización del servicio.

De las tres fases, anteriormente indicadas, la más interesante es la de Gestión del Servicio pero es necesario explicar la fase de Implantación para contextualizar la gestión.

La fase de Implantación Comprende las actividades encaminadas a que la totalidad de los servicios asociados al contrato se presten de forma normalizada y se produzca su aceptación por parte del MINISDEF. Incluye las fases de planificación y coordinación, de instalación, de transición y migración, y de aceptación. Durante esta fase no podrá existir en ningún momento pérdida de servicio, de forma que, una vez este contrato haya entrado en vigor, el adjudicatario entrante deberá mantener el servicio prestado por el adjudicatario anterior al menos durante este periodo.

2.7.3.1 Fase de Gestión

Dada la envergadura del presente proyecto, las funciones de gestión del servicio constituyen un factor determinante para asegurar su adecuada implantación y operación.

En el PPT se menciona que cada licitador deberá proporcionar los recursos necesarios y suficientes para soportar de manera adecuada el modelo de gestión técnica, administrativa y comercial demandado, así como detallar en su oferta los canales y procedimientos oportunos que desarrollen el modelo de prestación del servicio solicitado.

La atención a usuarios en el MINISDEF para resolución de incidencias, peticiones o consultas relativas a telecomunicaciones se proporciona mediante dos líneas de atención:

- Primera línea o Centro de Atención a Usuarios (CAU): este servicio será proporcionado por el adjudicatario del lote 6.
- Segunda línea o Centro de Gestión Técnico (CGT): proporcionado por los adjudicatarios del resto de lotes.

Adicionalmente, el adjudicatario de cada lote deberá conformar una Oficina de proyecto en la cual centralizar todas las gestiones técnicas y comerciales asociadas al contrato.

El MINISDEF centralizará a través de su Centro de Atención a Usuarios (CAU) y del Sistema de Control de Acuerdos de Nivel de Servicio (SCANS) las funciones de interlocución con sus usuarios.

El Sistema de Control de Acuerdos de Nivel de Servicio (SCANS) cuenta con los siguientes subsistemas:

- Subsistema de Control de Gasto (SCG).
- Subsistema de Inventario de Telecomunicaciones (SIT)
- Subsistema de Gestión de Peticiones e Incidencias (SGPI).
- Subsistema de Información de Guía Telefónica (SIGT).
- Subsistema de Base de Datos del Conocimiento (SBDC).

Los adjudicatarios de los lotes proporcionarán con periodicidad mensual los ficheros de facturación para su carga en el SCG. El MINISDEF proporcionará en el arranque del contrato la estructura y contenidos definida para dichos ficheros.

Con independencia del registro de incidencias y peticiones que el adjudicatario realice en sus sistemas, el CGT guardará registro en el SGPI de las acciones realizadas para su resolución. Será responsabilidad del adjudicatario, registrar en este subsistema aquellas incidencias no reportadas por los usuarios e identificadas por el adjudicatario como consecuencia de la monitorización del servicio. Los Acuerdos de Nivel de Servicio tomarán como fuente de información básica los datos recogidos en este subsistema.

El CGT proporcionado por el adjudicatario actuará como segunda línea de atención al usuario. Los licitadores deberán contemplar en su oferta un servicio de asistencia técnica 24 horas x 7 días a la semana para recogida y tramitación de incidencias, consultas técnicas relacionadas con el servicio y peticiones de usuarios.

La oferta propondrá un Plan de Gestión del Servicio, que detallará todos los planes y necesidades de los siguientes subapartados: Plan de Operación, Plan de Mantenimiento y Plan de Evolución. Corresponderá al personal del MINISDEF la supervisión y validación de las soluciones propuestas, así como de los trabajos de implantación realizados, y su aceptación.

- Plan de Operación

Dentro de la fase de Gestión del Servicio se proporcionará un Plan de Operación, donde se definan los procesos, procedimientos, actividades y responsabilidades encaminadas a asegurar el correcto y continuo funcionamiento de todos los servicios demandados, siguiendo las buenas prácticas de ITIL.

Estos procesos deberán integrarse con los procesos definidos a tal efecto y las herramientas que los sustentan en cada Sede, debiendo ser posible relacionar incidencias y/o cambios (entre otros) relativas al servicio de este contrato con incidencias y/o cambios (entre otros) generados en servicios verticales responsabilidad de cada Sede. Además deberán integrarse con las herramientas que tenga el MINISDEF y se indiquen durante la ejecución del contrato.

- Plan de Mantenimiento

Dentro de la fase de Gestión del Servicio se proporcionará un Plan de Mantenimiento, con objeto de definir los procedimientos de mantenimiento de todo el equipamiento hardware y software suministrado por el adjudicatario, de los servicios de conexión con las redes públicas, y de todos los servicios de valor añadido, incluidos sus componentes y dispositivos adicionales ofertados.

- Plan de Evolución

Dentro de la fase de Gestión del Servicio se incluirá un Plan de Evolución que presentará las previsiones necesarias para evolucionar el servicio durante los años de su prestación, y de acuerdo a las condiciones establecidas en el presente pliego y en el PCAP (Pliego De Cláusulas Administrativas Particulares).

El plan debe contemplar la ejecución de las variaciones en los servicios contratados en cada lote incluyendo las condiciones técnicas y administrativas (plazos, trámites...), así como parámetros de cualquier otra índole que hayan de tenerse en consideración ante la solicitud de cualquier cambio.

En base a las condiciones económicas establecidas en el PCAP, el MINISDEF podrá ir solicitando modificaciones y ampliaciones de capacidad en el objeto de suministro.

Este contrato debe permitir la prestación por el MINISDEF de los servicios en el tiempo fijado, por ello este plan debe incluir de forma clara y concreta, el dato del plazo cerrado (medido en días naturales) de provisión del servicio para una nueva sede. Este plazo incluirá todas las provisiones necesarias, incluyendo las de terceros, obra civil, licencias o cualquier otro extremo que el adjudicatario precise para proveer el servicio, contándose desde la aceptación del servicio por el MINISDEF hasta su puesta en marcha en pleno orden de funcionamiento.

El plazo propuesto vinculará al adjudicatario y generará de forma inmediata las penalizaciones correspondientes de las relacionadas en el PCAP respecto a los niveles de servicio descritos. Aun cuando el adjudicatario realice subcontratación del servicio, siempre en los términos autorizados por la legislación vigente, estará obligado a cumplir el plazo que haya ofertado sin que pueda transferir los retrasos a terceros.

Si durante el período de vigencia del contrato el adjudicatario hubiera introducido en el mercado innovaciones tecnológicas que impliquen, a juicio del MINISDEF, obsolescencia técnica del servicio inicialmente contratado, el MINISDEF se reserva la decisión de introducir dicha tecnología en la red ya operativa, previo acuerdo con el adjudicatario.

En cualquier caso, a la finalización del contrato todo el equipamiento de la solución deberá quedar actualizado a la última versión de su software liberada por el correspondiente fabricante y homologada por el adjudicatario.

Asimismo, el adjudicatario se coordinará con los adjudicatarios del resto de lotes y con el MINISDEF, a fin de asegurar la viabilidad y correcta ejecución de los respectivos Planes de Evolución, mediante la coordinación de las planificaciones de despliegues para caminar hacia una solución de convergencia y racionalización de servicios.

- Inventario

Con el fin de controlar el equipamiento instalado, al inicio de la migración del servicio el adjudicatario contará con una herramienta de CMDB que durante la fase de operación mantendrá una relación exhaustiva del equipamiento existente en cada centro. Esta relación servirá de base para la prestación del servicio y será actualizada reflejando, en un plazo máximo de 24 horas, las modificaciones que se realicen a lo largo de la vigencia del contrato. Abarcará todos los equipos, terminales, dispositivos, enlaces, interfaces, software, etc. Todos con su marca, modelo, identificación (incluyendo número de serie, IMEI en su caso, etc…).

Esta herramienta de CMDB deberá ser interoperable con el Subsistema de Inventario de Telecomunicaciones (SIT) del Sistema de Control de Acuerdos de Nivel de Servicio (SCANS) del Lote 6.

Se etiquetarán todos los elementos de forma clara y estandarizada, documentando a las Sedes del MINISDEF cada uno de los elementos componentes del equipamiento y líneas, de forma que la resolución de incidencias se haga de forma sencilla en caso de tener que solicitar colaboración del personal de la propia sede, o desplazar a personal del adjudicatario a la sede. En caso de modificaciones, el etiquetado y equipamiento inventariado debe mantenerse actualizado permanentemente.

2.7.4 Acuerdos de nivel de servicios.

El acuerdo de nivel de servicio habitualmente referido como SLA por acrónimo en inglés *(Service Level Agreement*) constituirá el mecanismo cuantitativo y cualitativo básico de seguimiento y control de la calidad del servicio, sin que ello suponga perjuicio alguno en el establecimiento de otros mecanismos de control periódicos o extraordinarios con el objetivo de asegurar que el compromiso de calidad se cumpla en la práctica.

En cada lote se definen los Acuerdos de nivel de servicio. Todos los lotes tienen en común las definiciones que se detallan a continuación.

2.7.4.1 Tipología de sedes

Las sedes son las unidades, centros u organismos del MINISDEF y depende del tipo de sede este tendrá unas capacidades determinadas en la Tabla 1:

Tipología Sedes	Ancho de banda	Número de emplazamientos
Tipo 0-CPD	10 Gbps	2
Tipo 0	10 Gbps	7
Tipo 1	1 Gbps	3
Tipo 2	1 Gbps	9
Tipo 3	100 Mbps	13
Tipo 4	100 Mbps	163
Tipo 5	10 Mbps	370
Tipo 5s	300 Mbps	3

Tabla 1.- Topología sedes (fuente: PPT [1])

Las Sedes Tipo 0 incluyen enlaces de fibra más críticos de mayor capacidad tanto principal como de respaldo (10 Gbps).

Las Sedes Tipo 1 incluyen enlaces de fibra de gran capacidad tanto principal como de respaldo de 1 Gbps.

Las Sedes Tipo 2 incluyen los enlaces de fibra de alta capacidad (1 Gbps) y respaldos de 100 Mbps.

Las Sedes Tipo 3 incluyen enlaces principales y respaldo de fibra de 100 Mbps.

Las Sedes Tipo 4 incluyen enlaces de fibra de 100 Mbps y respaldos de 10 Mbps.

Las Sedes Tipo 5 incluyen enlaces principales de 10 Mbps y de respaldo heterogéneos (Fibra, cobre, VSAT, móvil).

Las Sedes Tipo 5s enlaces principales a 300 Mbps, con tecnología *Fiber To The Home* (FTTH), y respaldo a 14,4 Mbps, con tecnología móvil *Long Term Evolution* (LTE).

2.7.4.2 Peticiones

- de Provisión: Se entiende por Petición de Provisión de servicio aquella en la que se realiza una solicitud de alta o baja de una línea, o bien de modificación de las características contractuales asociadas a una línea o servicio y, por tanto, con reflejo en la facturación de la misma. La sustitución o reparación de dispositivos por avería de los mismos también se considerará como una petición de provisión.
- de Administración: Se entiende por Petición de Administración de servicio aquella en la que se solicita una modificación en el perfil de un servicio o funcionamiento de una línea, sin que ello tenga repercusión en la facturación de la misma.

La Prioridad de Resolución de una Petición, viene determinada por dos factores, la urgencia de la petición y la criticidad de la sede, activo o servicio afectado de acuerdo a lo indicado en la Tabla 2.

Prioridad		Urgencia de la petición		
		Alta	**Media**	**Leve**
		Peticiones definidas de forma explícita por el MINISDEF como de urgencia alta	Peticiones definidas de forma explícita el MINISDEF como de urgencia media	Resto de peticiones
Criticidad sede, activo o servicio	Extrema (Nivel 0)	0	1	2
	Alta (Nivel 1)	1	2	2
	Media (Nivel 2)	1	2	3
	Baja (Nivel 3)	2	2	3

Tabla 2.- Prioridad de una petición

2.7.4.3 Incidencia:

Interrupción no planificada de una Solución Técnica (de voz o datos) o reducción en la Calidad de una Solución Técnica objeto del contrato.

La Prioridad de Resolución de una Incidencia viene determinada por dos factores, la severidad (ver Anexo II) de la incidencia y la criticidad del activo o servicio afectado de acuerdo a lo indicado en la Tabla 3.

Prioridad		Severidad incidencia		
		Alta	**Media**	**Leve**
Criticidad sede, activo o servicio	Extrema (Nivel 0)	0	1	2
	Alta (Nivel 1)	1	2	2
	Media (Nivel 2)	1	2	3
	Baja (Nivel 3)	2	2	3

Tabla 3.- Prioridad de las incidencias

2.7.5 Parámetros de medida del Acuerdo de Nivel de Servicio

En el Pliego de Prescripciones Técnicas [1] se definen los plazos aplicables en la gestión de incidencias y peticiones, Disponibilidad de activos y servicios, así como la disponibilidad de los activos que se incluyen como anexo II de esta memoria.

Ese mismo Pliego de Prescripciones Técnicas el Ministerio de Defensa se define el estado del arte de este tipo de servicios donde se contempla el sistema de Gestión de Servicios (SGS) basado en

metodología ITIL e ISO2000, obligando a Telefónica a adaptarse según evolucione el SGS y/o el marco normativo del MINISDEF hacia una infraestructura integrada.

A pesar de lo explicado en las secciones anteriores hay dos definiciones que no quedan perfectamente definidas que son la de usuario y cliente. Durante todo el Pliego se confunde al usuario con el cliente cuando el cliente seria el Ministerio de Defensa y los Usuarios los miembros de las Fuerzas Armadas.

Como hemos visto en el Punto 2.6.4.6 el Lote 6 se habla de la prestación de los servicios de Soporte y Atención al Usuario TIC. Pero si recordamos, a día de hoy, esta prestación de servicios se realiza mediante las aplicaciones que he descrito en la Introducción de esta memoria. Tanto SCANS como GESCAI son, desde el punto de vista del usuario, poco amigables. Además GESCAI es, desde el punto de vista del administrador y técnico, una aplicación poco flexible. En el mercado existen múltiples aplicaciones para la administración de servicios de TI (ITSM) que satisfacen las necesidades, tanto de técnicos como usuarios de la Armada. Me he centrado en Proactivanet y GLPI.

2.8 Proactivanet.

Es la herramienta ITSM que el Ministerio de Defensa ha probado en el Sistema de Información del Jefe del Estado Mayor de la Defensa (SIJE) y está prevista que se utilice en la futura Red de Mando y Control Nacional (SC2N), esta red se considera de alta clasificación, por lo que por ella circula información desde Difusión Limitada. Se trata de una aplicación con un precio que depende de los activos con los que cuente la red como a los módulos y herramientas que la componen algunos estrechamente vinculados a otros y necesarios para su funcionamiento (Ilustración 12).

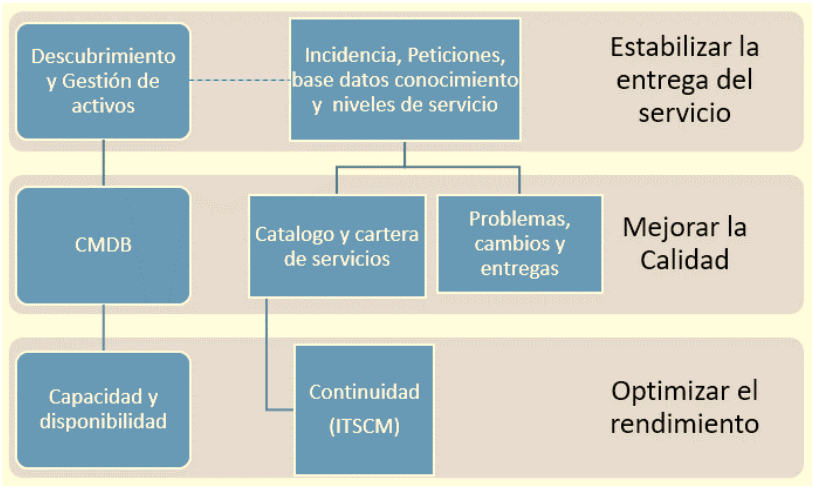


Ilustración 12.- Módulos Proactivanet (Fuente: propia)

A continuación se van a describir los diferentes módulos o funcionalidades que Proactivanet ofrece:

- Descubrimiento y Gestión de Activos

Mediante un agente se permite conocer detallada y automáticamente el inventario completo de los activos, tanto hardware como software. 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.

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.

- Gestión de Incidencias, Peticiones, Conocimiento (KB) y Niveles de Servicio.

Estos módulos entregan las herramientas necesarias para implementar un Centro de Servicios (*Helpdesk*), permitiendo al usuario final la gestión de sus propias incidencias, 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 de conocimiento que le permite evitar la generación de incidencias innecesarias, 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.

- 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 mantenimiento mientras incrementa el aporte de valor a otros procesos.

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

Su integración con el s*ervice desk* permite a los técnicos encargados de gestionar peticiones e incidencias acceder a la CMDB y su fuente de conocimiento, agilizando la resolución de éstas.

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 haber llevado a cabo antes un adecuado análisis de impacto.

- 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.

Este módulo 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 que el Consejo Asesor del Cambio CAB (*Change Advisory Board*) 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.

- 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 permite 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.

- 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 SLA y otros acuerdos de la organización con los proveedores.

- Gestión de la Continuidad

Este módulo requiere la instalación previa del Catálogo y Cartera de Servicios 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 incompatibilidades 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, en los que es suficiente con establecer un plan reactivo para atender a 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.

2.9 Herramientas ITSM en la AGE

El Centro de Transferencia de Tecnología (CTT) es un portal para la difusión y reutilización de soluciones técnicas de interés para el desarrollo de la administración electrónica. Este CTT constituye una base de conocimiento de información técnica de la administración electrónica dirigida a la Administración General del Estado, Comunidades Autónomas, Entidades Locales, etc. En este portal podemos encontrar la aplicación ITSM *Gestionnaire Libre de Parc Informatique* (GLPI), utilizado en el Ministerio de Presidencia, en el Ministerio de Educación y Formación Profesional, Ministerio de Trabajo, etc.

Como menciona el CTT [21] GLPI es de código abierto implementado en PHP y distribuido bajo una licencia GPL.

Como la mayoría de las aplicaciones de ITSM cuenta con las siguientes funcionalidades descritas en [21]:

- Compatibilidad con ITIL.
- Interfaz intuitiva y simple tanto para administradores, como técnicos y usuarios finales.
- Inventario automatizado: permite la recogida de gran parte de la información de forma automática.
- Búsquedas: la aplicación dispone de potentes búsquedas que permiten localizar registros en base a numerosos criterios y combinaciones de éstos.
- Gestión de conexiones: se pueden interconectar de forma lógica los equipos entre sí de forma que se puede tener de un vistazo los equipos relacionados entre sí permitiendo un análisis de impacto.
- Integración con localizaciones: se puede personalizar la ubicación de los equipos para su fácil localización física.
- Licencias software: además del parque informático se pueden gestionar las licencias de software utilizadas y relacionarlas con el los equipos físicos.
- Datos de gestión económica: se puede incluir información administrativa relacionada con los equipos como son expedientes, proveedores, datos de garantía, de envío, etc.

A nivel de administración también se incluyen una serie de características de utilidad como son:

- Sistema de permisos: permite crear distintos perfiles para el acceso a las distintas opciones de la aplicación
- Gestión centralizada o distribuida: se puede mantener la información de forma centralizada o delegar parte de esta a cada sede el mantenimiento de su propio inventario a través del sistema de permisos comentado anteriormente.
- Autenticación local o vía *Lightweight Directory Access Protocol* (LDAP): la autenticación se puede realizar mediante usuarios locales o importar usuarios de un directorio LDAP de forma que no existan distintos identificadores de usuario para distintas aplicaciones.
- Gestión de estados: permite la definición de estados para facilitar el seguimiento de la vida útil de los equipos.

Otras utilidades interesantes que aporta la aplicación son:

- Reservas de equipamiento: hay una gestión de reservas de equipos para controlar el material que es usado por distintos usuarios, como pueden ser portátiles, cañones para presentaciones, etc.
- Base de conocimiento: se puede incluir todo el tipo de documentación que se desee en una base de conocimiento de forma que se pueda acceder fácilmente a ésta para poder resolver cualquier duda o necesidad.
- Notificaciones y alertas: permite la configuración de alertas y avisos para notificar los finales de garantía y expiraciones de contratos.

3 DESARROLLO DEL TFM

A continuación describiré la metodología para definir e implementar un SAU-AR, la aplicación ITSM a utilizar y por último la metodología para hacerlo de una manera ágil.

3.1 ITIL para SAU-AR

Como hemos visto en apartados anteriores hay diferentes metodologías que se pueden utilizar en la implantación de un servicio de atención al cliente en la Armada y entre las distintas opciones hemos elegido la metodología ITIL V3. El motivo por el que se ha elegido ITIL V3 en lugar de ITIL 4 es porque las prácticas se focalizan en la realización de la tarea, independientemente del modo de llegar a ella y, sobre todo, sin una secuencia de acciones predefinidas y esto no se alinea con el pensamiento militar. Por el contrario ITIL V3 sí que se adapta a las necesidades, ya que para una entrada se busca una salida o lo que es lo mismo buscar un conjunto estructurado de actividades diseñadas, con una cierta secuencialidad, para conseguir un objetivo específico y esto se consigue con los procesos en ITIL V3 que tienen las siguientes características, mencionadas anteriormente en esta memoria:

- Son medibles porque podemos medir el proceso de forma adecuada. Está orientado al rendimiento. Esto permite medir el costo, la calidad y otras variables, mientras que los profesionales se preocupan por la duración y la productividad.
- Tienen resultados específicos: la razón que explica la existencia de un proceso es la consecución de un resultado específico. Este resultado debe ser individualmente identificable y medible.
- Tienen clientes porque cada proceso produce resultados primarios para un cliente o parte interesada.
- Debe cumplir con sus expectativas, ya sean internas o externas a la organización.
- Responden a eventos específicos: aunque el proceso puede ser continuo o repetitivo, debe ser fácil de activar con un disparador específico

Como veremos a continuación muchos de los diferentes servicios ITIL V3 ya están definidos por el Ministerio de Defensa.

3.1.1 Estrategia del Servicio

En el centro del ciclo de vida del servicio está la estrategia del servicio. La creación de valor comienza aquí mediante la comprensión de los objetivos de la organización y necesidades del cliente. Cada activo de la organización incluyendo personas, procesos y productos debe apoyar la estrategia.

La estrategia de servicio ITIL proporciona orientación sobre cómo para ver la administración de servicios no solo como una capacidad organizativa sino también como un activo estratégico.

Como se menciona en la Política de los Sistemas y Tecnologías de la Información y Comunicaciones (CIS/TIC) de Ministerio de Defensa [20], la información debe ser, por su valor estratégico, un activo 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) [19].

Para la consecución de la PECIS [19] se estructuran en seis Ejes Estratégicos (EE) y tres Objetivos Estratégicos (OE) eje, destacando los siguientes:

- EE 3. Potenciar la utilización de sistemas normalizados, homogéneos e interoperables, con empleo preferente de productos ya desarrollados en el ámbito nacional o aliado, en convergencia con el proceso de transformación digital de la AGE e incorporando las estrategias, las políticas y las iniciativas de la OTAN y la UE.
  - OE 3.1. Continuar el desarrollo del Proceso de Transformación Digital del MDEF, en el marco de la AGE.
  - OE 3.2. Consolidar la Normalización e Interoperabilidad de los Sistemas CIS-TIC del MDEF.
  - OE 3.3. Integrar en los procedimientos y soluciones del MDEF la Política y Estrategia de Normalización e Interoperabilidad de Organizaciones de las que el MDEF forma parte, tanto a nivel Nacional como Internacional (AGE, OTAN y la UE).
- EE 5. Avanzar hacia un nuevo modelo de gobierno integral de los CIS/TIC, buscando la máxima eficacia y eficiencia en su definición, dirección, planeamiento y gestión.
  - OE 5.1. Consolidar el funcionamiento del Consejo de Gobierno CIS-TIC y de la Comisión Ejecutiva CIS-TIC y proceder a la implantación de los Comités CIS/TIC.
  - OE 5.2. Definir e implantar el Modelo de Gobierno CIS-TIC del MDEF que complemente el marco estructural definido en este sentido.

Como hemos visto esta fase está perfectamente definida por el Plan Estratégico CIS-TIC (PECIS) [19] y si nos centramos en el Eje Estratégico 3 donde se define la potenciación en la utilización de sistemas normalizados, homogéneos e interoperables, con empleo preferente de productos ya desarrollados, como hemos visto en el Estado del Arte. Esto permite alcanzar el Objetivo Estratégico 3.2, consolidado la normalización e Interoperabilidad, por lo menos en la Armada, de los Sistemas CIS-TIC.

3.1.2 Diseño del Servicio

Los requisitos especiales se definen durante el diseño del servicio. En esta planificación de servicios se desarrollan soluciones adecuadas a esos requerimientos, se planifican nuevos servicios y se modifican y/o mejoran los existentes.

En el Pliego de Prescripciones Técnicas, que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la Infraestructura Integral de Información para la defensa (I3D) [1] descrito en esta memoria se diseñan nuevos servicios así como cambia y mejora los existentes.

Pero en este punto hemos visto como el PPT se alinea con las buenas prácticas de ITIL así como con la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa[7] pero en los requisitos del PPT nos encontramos Instrucciones sobre el Servicio de Atención al Usuario del CCEA que son de 2007 y se incluyen como guía.

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

3.1.3 Transición del Servicio.

Proporciona orientación para el desarrollo y mejora de las capacidades para introducir servicios nuevos y modificados. Este servicio describe cómo se transiciona en una organización de un estado a otro mientras se controla el riesgo. Esta transición es el paso del modelo actual a la I3D y viene definido por el Apéndice III de la PECIS [19] donde se busca asegurar que la transición desde la situación actual a la situación objetivo, en la que la I3D se encuentre implantada y en operación ofreciendo todas sus capacidades, se produce de la forma más eficiente posible. Para ello, a lo largo de esta transición se debe: «

- *Hacer uso de la experiencia acumulada y de las infraestructuras disponibles, racionalizándolas en aquello necesario antes que desarrollando o adquiriendo nuevas soluciones.*
- *Asegurar la coexistencia de soluciones actuales con las nuevas durante la implantación de éstas.*
- *Configurar un proceso de transición lo más transparente posible para los usuarios finales de la infraestructura.*
- *Evitar completamente cualquier tipo de impacto sobre el desarrollo de las misiones y cometidos del Ministerio de Defensa y especialmente de las FAS en él integradas.*
- *Elaborar los adecuados planes de formación para el personal militar que le permita alcanzar al menos el mismo nivel de ejecución y gestión de los sistemas CIS-TIC que se posee actualmente, en las nuevas tecnologías que requieran los sistemas CIS-TIC de la I3D. »*

3.1.4 Operación del Servicio

La Operación del Servicio es responsable del desempeño de todas las tareas operativas asignadas. Garantizar la prestación eficaz y eficiente de los servicios de TI. Esto incluye satisfacer las solicitudes de los usuarios, resolver interrupciones del servicio, solucionar problemas y realizar operaciones normales. Como hemos visto este es el servicio que se identifica en por la política de defensa pero no está aún desarrolla ni en la situación actual ni en la futura es por ello que nos centraremos en él. Los objetivos de las operaciones del servicio son:

- Proporcionar valor

  Este valor, en el caso de la Armada, es evidente ya que proporciona al usuario tiempo para dedicarse a su tarea principal. Pero hay desafíos que pueden poner en riesgo el valor entregado. Una vez diseñado, probado y en funcionamiento el servicio es muy difícil conseguir presupuestos para mejorar el servicio, solucionar los imprevistos o formar a los técnicos responsables del mismo. Esto se ha mitigado con contratando a una empresa externa. TIC.GAL, que proporciona el apoyo en la solución de imprevistos, mejora del servicio y formación a técnicos.

- Optimizar el rendimiento

  Esta optimización se puede realizar de dos maneras:

  - Mejora incremental a largo plazo: se basa en la evaluación del desempeño y salida de todos los procesos de operación del servicio, tecnologías, funciones y resultados a lo largo del tiempo. Este tipo de mejora no se podría implementar en el caso del SAU-AR mediante los servicios de diseño y transición a nivel MDEF ya que estos están en un nivel superior al de la Armada y esta no forma parte de ellos de manera activa. Esto no quiere decir que no se puedan realizar, ya que empleando algunas metodologías (que veremos en el siguiente punto) sí que se pueden hacer mejoras a largo plazo.
  - Mejora incremental a corto plazo: son las mejoras realizadas en prácticas de trabajo dentro de los procesos, funciones y tecnologías que sustentan la operación del servicio en sí mismo. Este tipo de mejoras son de fácil implementación gracias a las metodologías que se utilizarán en la implantación del GLPI.

3.1.4.1 Procesos dentro del Servicio de Operación

Hay una serie de operaciones de servicio clave que deben vincularse entre sí para proporcionar una estructura de soporte de TI global eficaz y estas son las siguientes.

3.1.4.1.1 Gestión de eventos

Antes de nada hay que definir lo que es un evento según ITIL [9]:

«Cualquier cambio de estado que tiene importancia para la gestión de un elemento de configuración (CI)[8] o servicio de TI. Los eventos son típicamente reconocido a través de notificaciones creadas por un servicio de TI, CI o herramienta de monitoreo.»

Actualmente el nivel de ambición del SAU-AR no contempla la gestión de eventos ya que a día de hoy esto excede las responsabilidades de los CESIN, Además de esto la última versión de GLPI, la versión 10, aún no implementa nativamente esta funcionalidad supliéndola con un *plug-in* (tambien conocido como desarrollo).

3.1.4.1.2 Gestión de incidentes

A igual que en el punto anterior es necesario definir que es un incidente, según ITIL [9]:

«*Interrupción no planificada de un servicio de TI o reducción en la calidad de un servicio de TI o un fallo de un CI que aún no ha impactado un servicio de TI (por ejemplo el fallo de un disco de un conjunto espejo).»*

En la ilustración 13 podemos ver el proceso y subprocesos de gestión de incidentes. Este proceso se desarrolla en los siguientes párrafos:

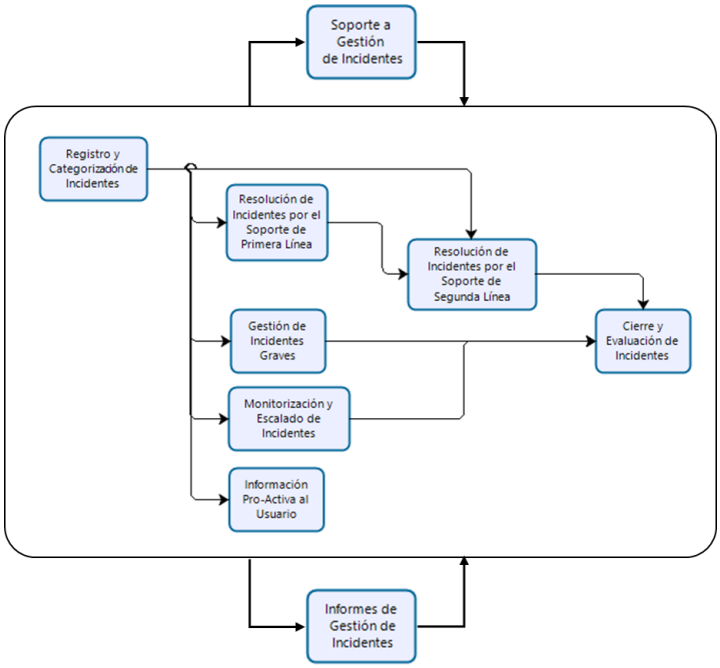


Ilustración 13.- Proceso de gestión de incidentes (Fuente: propia)

[8] Elemento de configuración según ITIL *Service Transition* [9]: *« Cualquier componente u otro activo de servicio que necesita ser administrado para entregar un servicio de TI. Por lo general, incluyen servicios, hardware, software, edificios, personas y documentación formal como proceso documentación y acuerdos de nivel de servicio.»*

- Soporte a Gestión de Incidentes:

  Se definen los siguientes niveles de apoyo al usuario:

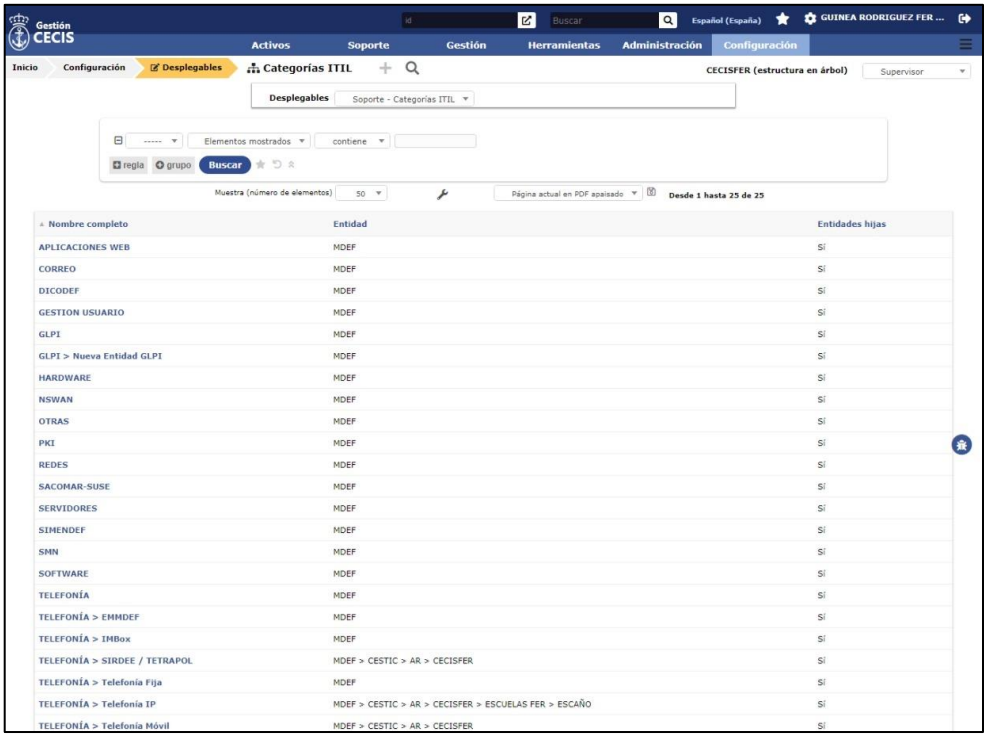
  - Nivel 1: Grupo de técnicos con conocimientos avanzados para resolver incidencias que permitan restablecer de manera temprana del servicio de TI, con alguna solución temporal de ser necesaria. Actualmente ubicados en los CECIS de apoyo (p.ej.: CECISFER). Una vez se confirme que el soporte de Nivel 1 no puede resolver el incidente o cuando se exceda SLA para dicho nivel, el Incidente es transferido a un grupo superior en el Nivel 2.
  - Nivel 2: Grupo de técnicos con conocimientos expertos o con mayor disponibilidad para resolver incidencias que permitan restablecer de manera temprana del servicio de TI, con alguna solución temporal de ser necesaria. Actualmente ubicados en GRUCECIS (p.ej: CECISMAD). En caso necesario, podrán involucrarse otros grupos de soporte o proveedores externos (Nivel 3). Si no se puede corregir la raíz del problema, se crea un Registro de Problema y se transfiere el caso a la Gestión de Problemas.

  Se definen diferentes reglas para poder gestionar los incidentes de manera efectiva y eficiente. Estas reglas distribuyen las incidencias entre los técnicos o incluso, si es posible por privilegios, facilitan la posibilidad al usuario de resolver la incidencia de manera autónoma.

En lo que a los procesos de resolución de incidentes se refiere se usan los definidos en los procedimientos internos de la Armada que a su vez están basado en la normativa del Ministerio de Defensa.

- Registro y Categorización de Incidentes

  La categorización de los incidentes se realiza en base en las lecciones aprendidas con el uso de la aplicación GESCAI así como otras usadas en otros CECIS. En GESCAI se identificaron hasta 140 tipos de incidentes que tras un análisis de las incidencias creadas y eliminando aquellas con menos de 5 solicitudes en los últimos 5 años, se redujeron a las indicadas en la ilustración 14:



Nombre completo	Entidad	Entidades hijas
APLICACIONES WEB	MDEF	Sí
CORREO	MDEF	Sí
DICODEF	MDEF	Sí
GESTION USUARIO	MDEF	Sí
GLPI	MDEF	Sí
GLPI > Nueva Entidad GLPI	MDEF	Sí
HARDWARE	MDEF	Sí
NSWAN	MDEF	Sí
OTRAS	MDEF	Sí
PKI	MDEF	Sí
REDES	MDEF	Sí
SACOMAR-SUSE	MDEF	Sí
SERVIDORES	MDEF	Sí
SIMENDEF	MDEF	Sí
SMN	MDEF	Sí
SOFTWARE	MDEF	Sí
TELEFONÍA	MDEF	Sí
TELEFONÍA > EMMDEF	MDEF	Sí
TELEFONÍA > IMBox	MDEF	Sí
TELEFONÍA > SIRDEE / TETRAPOL	MDEF > CESTIC > AR > CECISFER	Sí
TELEFONÍA > Telefonía Fija	MDEF	Sí
TELEFONÍA > Telefonía IP	MDEF > CESTIC > AR > CECISFER > ESCUELAS FER > ESCAÑO	Sí
TELEFONÍA > Telefonía Móvil	MDEF > CESTIC > AR > CECISFER	Sí

Ilustración 14.- Categorías en GLPI (Fuente: propia)

En lo que al registro de incidentes se refiere el GLPI lo tiene de forma nativa lo que permite asignar prioridades a los incidentes, de manera que las soluciones sean efectivas e inmediatas.

- Resolución de Incidentes por el soporte de primera línea

  El soporte de primera línea es un grupo de técnicos con conocimientos avanzados para resolver incidencias que permitan restablecer de manera temprana del servicio de TI, con alguna solución temporal en caso necesario. Actualmente ubicados en los CECIS de apoyo (p.ej.: CECISFER) Una vez se constate que el soporte de Nivel 1 no puede resolver el Incidente o cuando se exceda el periodo límite propuesto para dicho nivel, el Incidente es transferido a un grupo adecuado en el Soporte de Nivel 2.

- Resolución de incidentes por el soporte de segunda línea

  El soporte de segunda línea Son un grupo de técnicos con conocimientos expertos o con mayor disponibilidad para resolver incidencias que permitan restablecer de manera temprana del servicio de TI, con alguna Solución Temporal de ser necesaria. Actualmente ubicados en GRUCECIS (p.ej: CECISMAD) En caso de que se requiera, podrán involucrarse otros grupos de soporte o proveedores externos (Soporte de Nivel 3). Si no es posible corregir la raíz del problema, se crea un Registro de Problema y se transfiere el caso a la Gestión de Problemas.

- Gestión de Incidentes Graves

  Estos tipos de eventos causan una interrupción significativa y deben resolverse más rápidamente. El objetivo es restaurar los servicios rápidamente, incluso si tenemos que usar soluciones temporales. Si es necesario, pueden participar grupos de apoyo dedicados o proveedores de servicios externos (soporte de tercera línea). Si no se puede solucionar la causa raíz del problema, se crea un registro de problema y se envía a la gestión de problemas, que se abordará más adelante.

- Monitorización e Escalado de Incidentes

  La monitorización de incidentes utiliza un tablero nativo de GLPI que se puede usar para monitorizar continuamente el estado de procesamiento de los casos pendientes y, por lo tanto, tomar medidas para contrarrestar los efectos adversos cuando los niveles de servicio se ven comprometidos.

  Las reglas de escalado se definen en base a los procedimientos existentes y la experiencia adquirida a lo largo de los años.

- Cierre y Evaluación de Incidentes

  El cierre del incidente lo realiza el usuario que lo generó así se asegura que el caso se ha resuelva. Toda la información requerida para describir el ciclo de vida del incidente ha sido registrada con suficientes detalles mediante el GLPI. Además, la resolución se registrará para referencias futura, permitiendo un análisis de SLA, satisfacción del usuario, etc.

- Información Pro-Activa a Usuarios

  El GLPI permite informar a los usuarios de fallos en el servicio tan pronto como se conozcan mediante mensajes en la pantalla de inicio al GLPI ayudando a reducir las solicitudes de los usuarios.

- Informes de Gestión de Incidentes

  El GLPI permite proporcionar información relacionada con los incidentes para uso en otros procesos de Gestión de Servicios, y para asegurar que los incidentes previos sirvan para potenciar las mejoras.

3.1.4.1.2.1 CSF Y KPI de Gestión de Incidentes.

En la tabla 4 se incluyen CSF y KPI alineados inicialmente con el Ministerio de Defensa y en base a las solicitudes de información por parte del CCEA:

CSF ***(Critical Success Factors)***	**KPI** ***(Key Performance Indicators)***	**Descripción**
Resolver incidencias lo más rápido posible y minimizar los impactos en el negocio	Tiempo de resolución del incidente	Tiempo medio para resolver un incidente (agrupados por categorías)
	Desglose de incidente	Desglose de incidentes en cada etapa (por ejemplo, registrado, trabajo en curso, cerrado, etc.)
	Incidentes resueltos a distancia	Cantidad de incidentes resueltos a distancia por el *Service desk* (p.ej. sin acudir al puesto del usuario)
	Tasa de Resolución de Primera Llamada	Porcentaje de incidentes resueltos en el *Service desk* durante la primera llamada (agrupados por categorías)
Mantener la satisfacción del usuario	Puntuación media encuesta calidad	Puntuación promedio de la encuesta de usuario/cliente (total y por categoría de pregunta)
	Porcentaje encuestas calidad realizadas	Porcentaje de encuestas de satisfacción respondido versus número total de satisfacción encuestas enviadas
Alinear las actividades de gestión de incidentes y prioridades con las del negocio	Resolución dentro del SLA	Porcentaje de incidentes resueltos durante el tiempo acordado en el SLA (agrupados por categorías)
	Cantidad de escalados	Cantidad de escalados de incidentes no resueltos en el tiempo acordado
Asegurar que los métodos estandarizados y procedimientos se usan para una gestión eficiente y rápida, respuesta, análisis, documentación, en curso gestión y reporte de incidentes a mantener la confianza organizacional en las capacidades de TI	Esfuerzo de resolución de incidente	Promedio de esfuerzo de trabajo para resolver Incidentes (agrupados por categorías)
	Número de incidentes repetidos	Cantidad de incidentes repetidos (con métodos para su resolución ya conocidos)
	Incidentes incorrectamente asignados	Número y porcentaje de incidentes asignado incorrectamente
	Incidentes incorrectamente categorizado	Número y porcentaje de incidentes categorizado incorrectamente
	Incidentes en la mesa	Número y porcentaje de incidentes procesado directamente por personal del CESIN

Tabla 4.- CSF y KPI Gestión de Incidentes

3.1.4.1.3 Gestión de problemas

A igual que en el punto anterior es necesario definir que es un problema, según ITIL [9]: «*La causa subyacente de uno o más incidentes*».

La gestión de problemas implica el análisis de la causa raíz para determinar y resolver las causas subyacentes de incidentes. Esto también incluye la creación de registros de errores conocidos para documentar las causas raíz y las soluciones alternativas para permitir un diagnóstico.

En la Ilustración 15 podemos ver el proceso y subprocesos de la gestión de problemas:

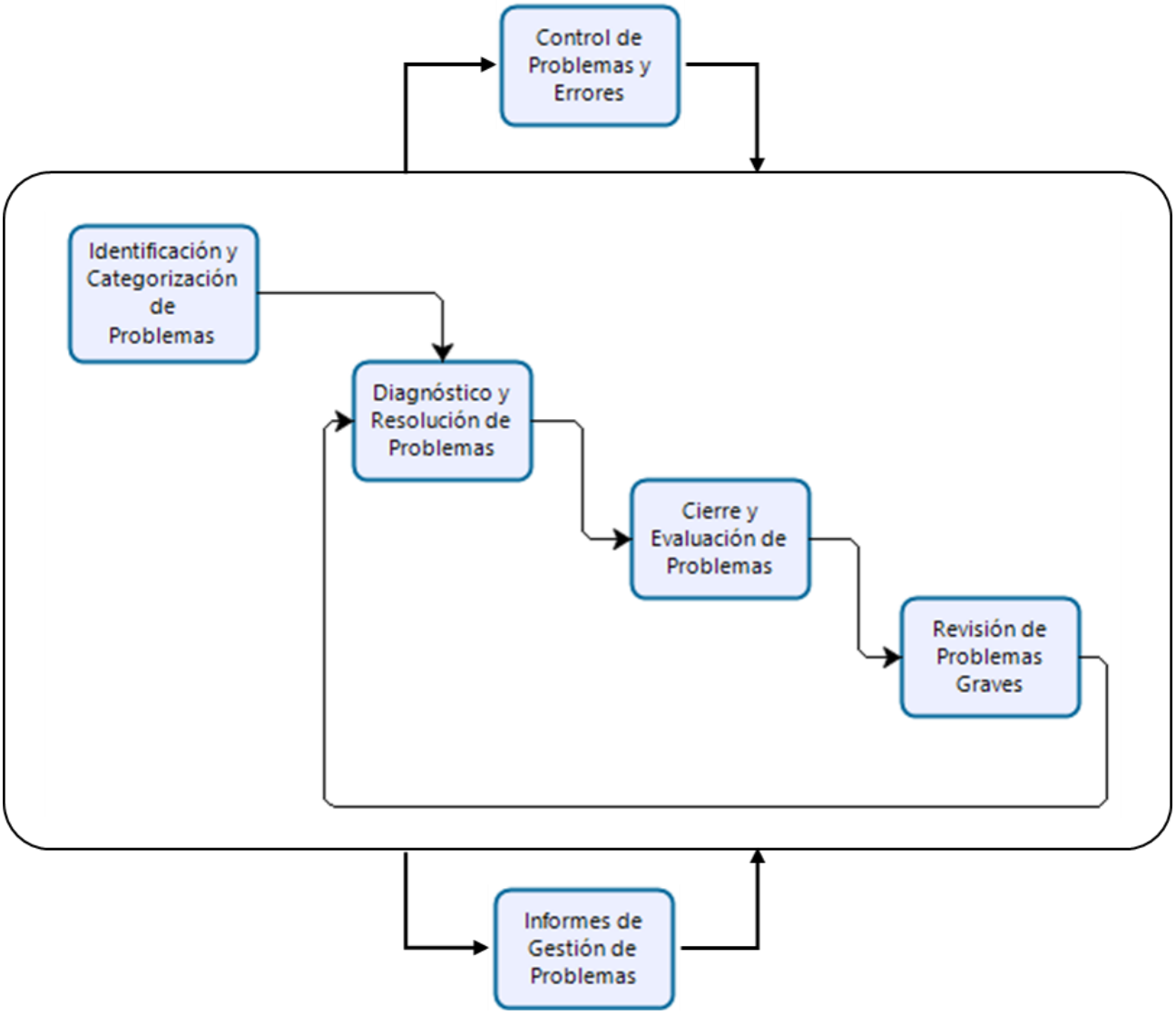


Ilustración 15.- Gestión de problemas (Fuente: propia)

Analizando uno por uno los subprocesos vemos que esta gestión es similar a la de gestión de incidentes. La principal diferencia es que los problemas son el resultado de muchos incidentes por lo que en el SAU-AR es el Nivel 2 el responsable de la gestión de problemas ya que es el que tiene visibilidad de todas las incidencias de la Armada.

3.1.4.1.3.1 CSF Y KPI de Gestión de Problemas

En la tabla 5 se incluyen CSF y KPI alineados inicialmente con el Ministerio de Defensa y en base a las solicitudes de información por parte del CCEA:

CSF *(Critical Success Factors)*	**KPI** *(Key Performance Indicators)*	**Descripción**
Mantener la calidad de los servicios de TI mediante eliminación de incidentes recurrentes	Número de problemas	Cantidad de problemas registrados por la Gestión de Problemas (agrupados por categorías)
	Tiempo hasta la identificación del problema	Tiempo medio transcurrido entre la primera aparición de un incidente y la identificación de la raíz del problema
	Tiempo de resolución de problemas	Tiempo medio para resolver problemas (agrupados por categorías)
Mantener la calidad de los servicios de TI mediante eliminación de incidentes recurrentes	Número de incidentes por problema	Cantidad media de incidentes vinculados al mismo problema antes de identificar el problema
Proporcionar calidad general y profesionalismo de las actividades de manejo de problemas para mantener la confianza organizativa en capacidades TI	Número de incidentes por problema conocido	Cantidad media de incidentes vinculados al mismo problema después de identificar el problema
	Esfuerzo de resolución de problemas	Tiempo medio de esfuerzo de trabajo para resolver problemas,(agrupados por categorías)

Tabla 5.- CSF y KPI Gestión de Problemas

3.1.4.1.4 Cumplimiento de la solicitud

El cumplimiento de la solicitud es el proceso para gestionar el ciclo de vida de todas las solicitudes. Para el cumplimiento de la solicitud se define el ciclo de vida de una solicitud que podemos ver en la Ilustración 16:

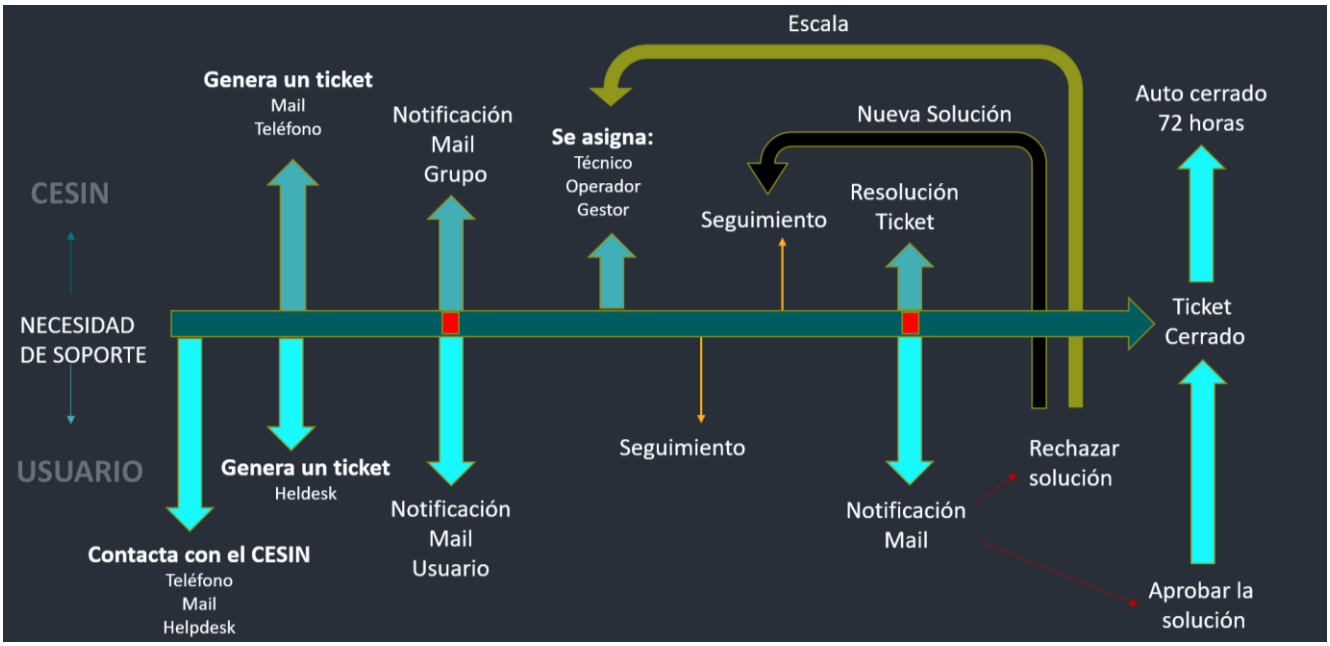


Ilustración 16.- Ciclo de vida de una petición (Fuente: propia)

En la Ilustración 16 podemos ver que las acciones indicadas en la parte inferior son acciones del o hacia el usuario mientras que las superiores corresponden al CESIN de Apoyo.

3.1.4.1.5 Gestión de Acceso

La gestión de acceso se ha solucionado mediante el acceso LDAP corporativo del Ministerio de Defensa lo que permite conceder a los usuarios autorizados los derechos de uso del servicio dependiendo del rol asignado. Esto nos permite identificar con precisión usuarios autorizados y luego administrar su capacidad para acceder a los servicios según lo requieran las necesidades específicas.

Los roles que se han definido para los usuarios son:

- Usuario MDEF: este perfil está dedicado a la presentación de solicitudes de asistencia mediante la creación de solicitudes. Responsable en Armada: Todos los miembros de la Armada.

- Operador: este perfil permite introducir incidencias y tener acceso a su seguimiento. En cambio, este perfil no permite hacerse cargo de ellas. Aún no definido en la Armada.

- Técnico: este perfil corresponde a la función de técnico del departamento de informática. Permite acceder a las funciones de gestión del parque en modo lectura e intervenir en el tratamiento de las incidencias del centro de soporte.
  - Técnico N2: personal administrador a nivel CESIN Central
  - Técnico N1: personal administrador a nivel unidad CESIN
  - CIS-POC: personal sin capacidad de administración CIS pero puede tener conocimientos para resolver incidencias orientando al usuario o resolviéndolas él mismo sin necesidad de ser administrador (p.ej.: reseteo portal personal, “conectar una impresora”)

- Supervisor: este perfil posee permisos similares a los del técnico y además posee permisos para gestionar la organización de un equipo (asignación de incidencias). (Jefe CESIN, OF CESIN…)

3.1.4.2 Funciones dentro del Servicio de Operación

Los procesos por sí solos no darán como resultado la operación de servicio. Es necesaria una infraestructura estable y también se necesitan personas debidamente capacitadas. Para lograr esto, la operación del servicio se basa en varias funciones para ejecutar tareas operativas. Las funciones incluyen grupos de personas capacitadas que llevan a cabo una o más procesos y actividades del ciclo de vida del servicio. Dentro de la operación del servicio, hay cuatro funciones principales:

3.1.4.2.1 Service Desk

La s*ervice desk* debe ser una unidad funcional siendo el punto de contacto físico con el usuario principalmente por vía telefónica, esto puede suceder, por ejemplo, porque el usuario no tiene acceso a la plataforma para cargar una incidencia. Una *service desk* es una unidad funcional compuesta por un número dedicado de personas, en el caso de los CESIN de apoyo esta unidad no existe como tal asumiendo sus funciones el personal de taller. Estas funciones son:

- Registro de todos los incidentes/solicitudes de servicio relevantes y sus detalles, asignación de categorización y códigos de priorización.
- Proporcionar investigación y diagnóstico de primera línea.
- Resolver incidencias/solicitudes de servicio siempre que sea posible.
- Mantener informados a los usuarios sobre el progreso de sus incidencias.
- Llevar a cabo devoluciones de llamada de satisfacción del cliente/usuario/ encuestas según lo acordado.
- Comunicación con los usuarios: mantenerlos informados del progreso del incidente, notificándoles de cambios inminentes o interrupciones acordadas, etc.

Actualmente el servicio que proporciona la *service desk* se circunscribe a las áreas geográficas por lo que se podría considerar que cada CESIN tiene una s*ervice desk* Local.

3.1.4.2.2 Gestión de instalaciones TI

Esta función apoya el proceso de operación de los servicios de TI y la gestión de la infraestructura de TI. Además tienen un papel importante en el diseño, pruebas, liberación y mejora de los servicios de TI.

Para esta función se definen los siguientes roles:

- Super-Admin: este perfil posee todos los permisos con función de gestionar las reglas y las entidades. El número de usuarios con este perfil debe ser restringido. Responsable en la Armada: GRUCECIS
- Admin: este perfil administra los derechos de acceso para todo el GLPI. Sin embargo, no tiene acceso a todos los atributos de definición de reglas, entidades y otros temas confidenciales que pueden degradar la funcionalidad de GLPI. Responsable en la Armada: Un técnico por CECIS de apoyo.

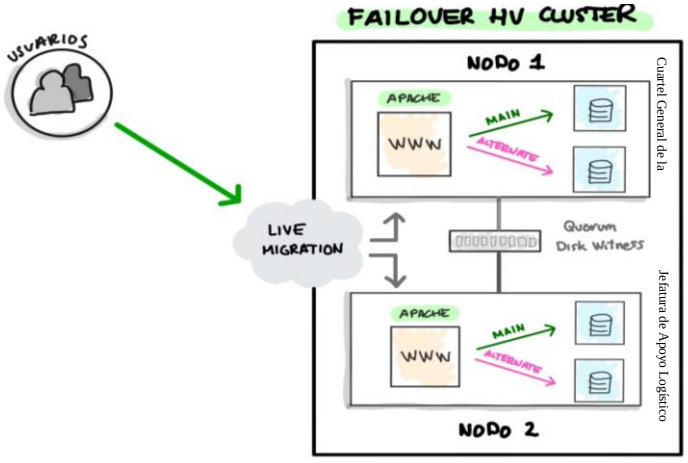


Ilustración 17.-Alta Disponibilidad GLPI en Armada (Fuente: Carlos Delgado Huertas)

En la Ilustración 17 vemos el *cluster* que soporta el GLPI, la arquitectura se definió en base a los usuario potenciales de la Armada, aproximadamente 20.000 así como la prioridad de disponibilidad para los usuarios ya que estos podrían estar en la mar trabajando 24/7 los 365 días del año. Por todo por esto que se definió un *cluster* de alta disponibilidad ubicando dos nodos en Madrid, uno en el Cuartel General y otro en la Jefatura de Apoyo logístico de la Armada (JAL)

3.1.4.2.3 Gestión de operaciones de TI

La función de la gestión de operaciones de TI es ejecutar las actividades y procedimientos continuos necesarios para gestionar y mantener la infraestructura de TI para prestar y mantener los servicios de TI en los niveles acordados.

A día de hoy esta función la realiza una única persona a tiempo parcial y bajo demanda ya que la carga actual del sistema se suple con la automatización programando las copias de seguridad, solo comprobando si en las tareas programadas que producen algún problema, etc.

3.1.4.2.4 Gestión de la aplicación

En este caso, y como hemos visto anteriormente la decisión de si diseñábamos o adquiríamos una aplicación fue sencilla gracias a la normativa del Ministerio de Defensa. Se decidió que GLPI sería la aplicación. Pero debido a las limitaciones de personal dedicado se optó por buscar apoyo en una empresa externa con experiencia tanto en la propia aplicación como en nuevos desarrollos (también llamados *plug-in*). Por lo tanto la gestión de la aplicación se realiza mediante la contratación de la empresa externa, TIC.GAL [23] .

3.1.5 Mejora Continua

Por último, y si como podemos ver en la ilustración 18, vemos que el servicio de mejora continuo es permanente. Para el Servicio de Atención al Usuario de la Armada es fundamental la mejora continua ya que si un usuario no consigue cerrar su incidencia sin un motivo aparente, la aplicación no funciona, el interfaz es complicado…y el usuario deja de utilizar la aplicación porque esta no le aporta valor. Es por esto que es necesario evaluar la calidad del servicio regularmente. Esto incluye la identificación de donde no se cumplen los niveles de servicio propuestos. Esto lo conseguimos, entre otras opciones que permite el GLPI, mediante las encuestas de satisfacción.

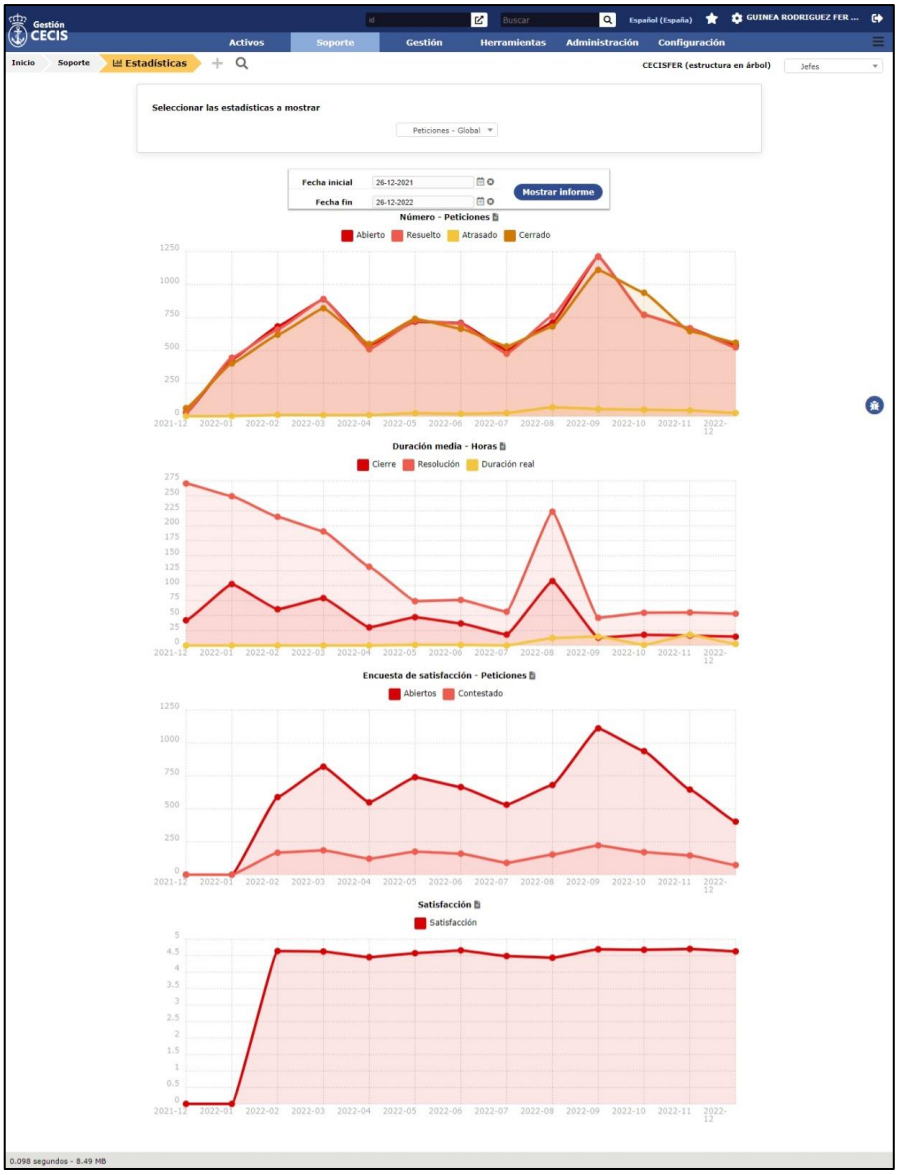


Ilustración 18.- Estadísticas de encuestas de calidad en GLPI (Fuente: propia)

Mediante estas encuestas se gestionan las quejas y satisfacción de los clientes y se revisan los servicios regularmente. El objetivo es mejorar la calidad de los servicios, si es necesario, y encontrar formas más eficientes de prestarlos.

3.2 Aplicación ITSM

Teniendo en cuenta la normativa en vigor [22] se define que:

«Los sistemas de información del Ministerio de Defensa tendrán en cuenta, con carácter preferente, las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados. Al efecto deberán consultarse, entre otros, directorio de aplicaciones reutilizables el CTT - Centro de Transferencia de Tecnología [21], *con carácter previo, a la adquisición, al desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación informática».*

Con estas premisas, teniendo cuenta la metodología ITIL, y tras buscar en el CTT identificamos al GLPI, y a su agente (GLPI *Agent*[9]), como la ITSM que se adapta a las necesidades de la Armada.

Para poder utilizar la aplicación es necesario previamente que sea auditada y para ello se define un servidor de pruebas en el CECISFER. Una vez que supere la auditoria del CESTIC y el servicio empiece a estar disponible se prevé una concurrencia potencial de 20.000 usuarios que pueden acceder al SAU-AR. Tras analizar estas necesidades se determina que es necesario tener un servicio de alta disponibilidad. Para esto se dimensiona la arquitectura y este se ubica en el Cuartel General de la Armada[10], más adelante se tratará este tema.

3.3 Implantación del servicio

Hasta ahora hemos visto que tenemos todos los elementos para establecer el servicio pero partimos de un servicio previo, el GESCAI. Hay que definir una metodología para esta transición e implantación. Como hemos visto en el estado del arte existen varias metodologías que se pueden emplear. Analizando los elementos a nuestra disposición, definidos en los apartados anteriores, se define que las metodologías a emplear sean agiles ya que nos permite:

- Enfoque en la entrega continua de valor al cliente: entregar software funcional de manera incremental y en colaboración con el usuario.
- Flexibilidad para adaptarse a los cambios: se adaptan fácilmente a los cambios en los requisitos del cliente.
- Trabajo en equipo: promueven el trabajo colaborativo y la comunicación constante entre los miembros del equipo.
- Iteraciones cortas: los proyectos se dividen en ciclos cortos de trabajo, conocidos como *sprints*, para permitir una entrega rápida de software funcional.
- Retroalimentación constante: estas metodologías promueven la retroalimentación constante del cliente para asegurar que el software cumpla con sus necesidades.
- Documentación minimalista: esta metodología se enfocan en la entrega de software funcional en lugar de documentación extensa.

Una vez definida que tipo de metodología utilizar debemos ser más específicos y es por ello que nos decantamos por SCRUM y KANBAN.

3.3.1 SCRUM

Como expuse en el Estado del Arte de esta memoria SCRUM se basa en el desarrollo incremental de los requisitos del proyecto en bloques temporales cortos y fijos, priorización los requisitos por valor para el cliente y coste de desarrollo en cada iteración.

[9] GLPI Agent es un programa utilizado para ejecutar un inventario automático y funciona con la herramienta de software GLPI ITSM. También admite la ejecución de algunas otras tareas, como la implementación de paquetes, la recopilación de información, el descubrimiento e inventario de dispositivos de red o el inventario remoto.
[10] Esta ubicación es la única que cuenta con guardia 24/7 de mantenimiento de redes.

Se definen los siguientes roles:

- Cliente: se define a los Centros de Sistemas de Información de la Armada (CECIS), definidos en el punto 1.5.2 de la presente memoria. Son los CIS-POC de todos los usuarios de las respectivas zonas y tienen el *know how* así como una extensa base de datos de todos los incidentes/peticiones TI..
- Dueño del producto (PO): Se define PO al JEGRUCECIS ya que es el interesado en que el SAU-AR sea una herramienta centralizada de uso nacional. Esta labor la delega en el Jefe del Centro de Sistemas de Información de Ferrol (CESINFER).
- Equipo de desarrollo (DT): este rol se asigna los siguiente miembros:
  - Tres miembros de la Armada destinados en el CESINFER, dos programadores con amplia experiencia en herramientas ITSM y un Coordinador del equipo.
  - Un ingeniero informático, formado en metodologías ágiles y herramientas ITSM, destinado en Madrid.
  - TICGAL [23]: Empresa civil ubicada en Pontevedra con amplia experiencia en GLPI
- SCRUM Máster (SM): se define al Jefe del Centro de Sistemas de Información de Ferrol (CESINFER).

Tras definir los roles se deberían definir los eventos pero debido a que los integrantes de los diferentes roles no tienen exclusividad con este proyecto es necesario realizar ciertas modificaciones a SCRUM en el siguiente sentido:

- Planificación diaria (*Daily SCRUM*): no se realiza de manera estricta, con el objeto de facilitar la transferencia de información y colaboración se define un servidor de pruebas sobre el que se puede hacer seguimiento. Esto se favorece debido a que GLPI integra una funcionalidad de historial sobre todos los elementos.
- Planificación de la iteración (*Sprint planning*): esta reunión se realiza mensualmente alineando necesidades de los CECIS y equipo de desarrollo.
- Revisión de los requisitos completados (*Sprint review*): a mitad de mes, y tras la reunión anterior, se realiza está exponiendo las nuevas funcionalidades para que el cliente y usuarios las utilicen.
- Retrospectiva del sprint (*Sprint retrospective*): aproximadamente 5 días después de la reunión anterior se realiza esta para obtener *feedback* y alimentar la planificación de la iteración.

Por definición los artefactos para la metodología SCRUM serían: la lista de objetivos y la lista de tareas. La primera lista está perfectamente definida e interiorizado por todos los CESIN (véase en [6]) Si bien la lista de tareas no se definen inicialmente estas salen como resultado de las reuniones planificación de la iteración, como podemos ver en la Ilustración 19:

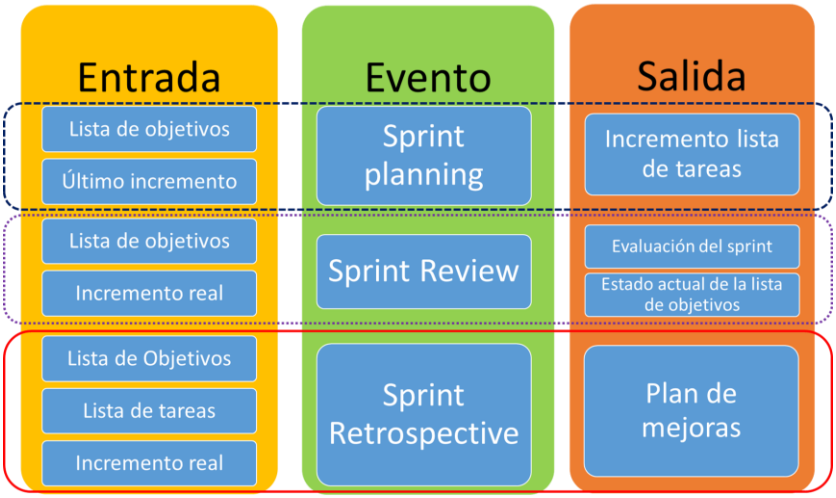


Ilustración 19.- Relación Eventos, entrada y salida (Fuente: propia)

En la ilustración 20 podemos ver el ciclo de SCRUM que se ha seguido para implementar las diferentes iteraciones en GLPI.

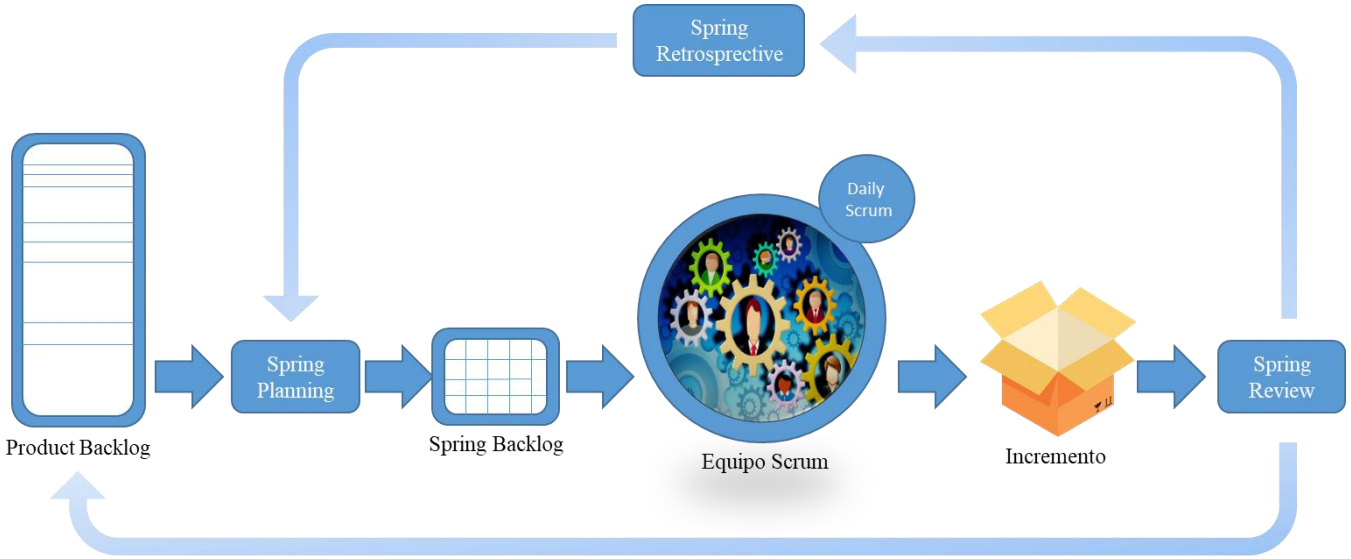


Ilustración 20.- SCRUM (Fuente: propia)

3.3.2 KANBAN

Debido a la deslocalización de los integrantes del Grupo de Trabajo de GLPI era necesario utilizar un método visual para la gestión del proyecto. Para ello decidimos usar la metodología KANBAN que nos permitió:

- Enfocar en el flujo de trabajo: permite visualizar el flujo de trabajo, limitar el trabajo en progreso y mejorar continuamente el proceso de producción.
- Trabajar con un tablero único: utilizar un tablero Kanban permitió visualizar el estado del proyecto y el flujo de trabajo.
- Mejorar continuamente: mediante la retroalimentación y el análisis de datos para optimizar el proceso de producción.
- No definir roles fijos: cualquier miembro del equipo puede trabajar en cualquier tarea.

Para poder utilizar este método utilizamos la plataforma TRELLO [24] pero principalmente en la parte visual, véase tablero de la Ilustración 21 y tarjeta de la Ilustración 22, ya que permite hacer seguimiento de la lista de tareas del punto anterior. Para esto se definieron los siguientes roles:

- *Service Request Manager* (SRM): Es responsable de la gestión de la demanda y los requisitos y gestiona las relaciones con los clientes y el resto de grupo de trabajo. Promueve la transparencia sistemática en la priorización del trabajo. Este rol lo asumió el Jefe del CESINFER.

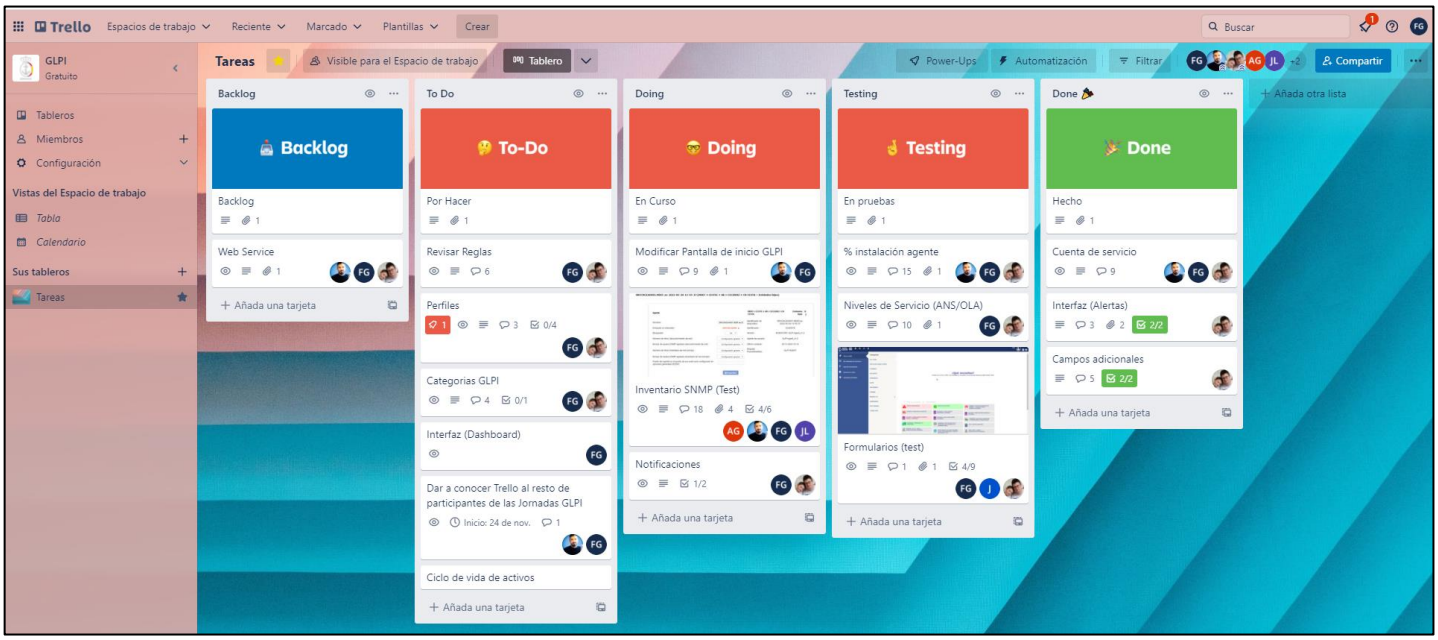


Ilustración 21.- Tablero KANBAN para GLPI (Fuente: propia)

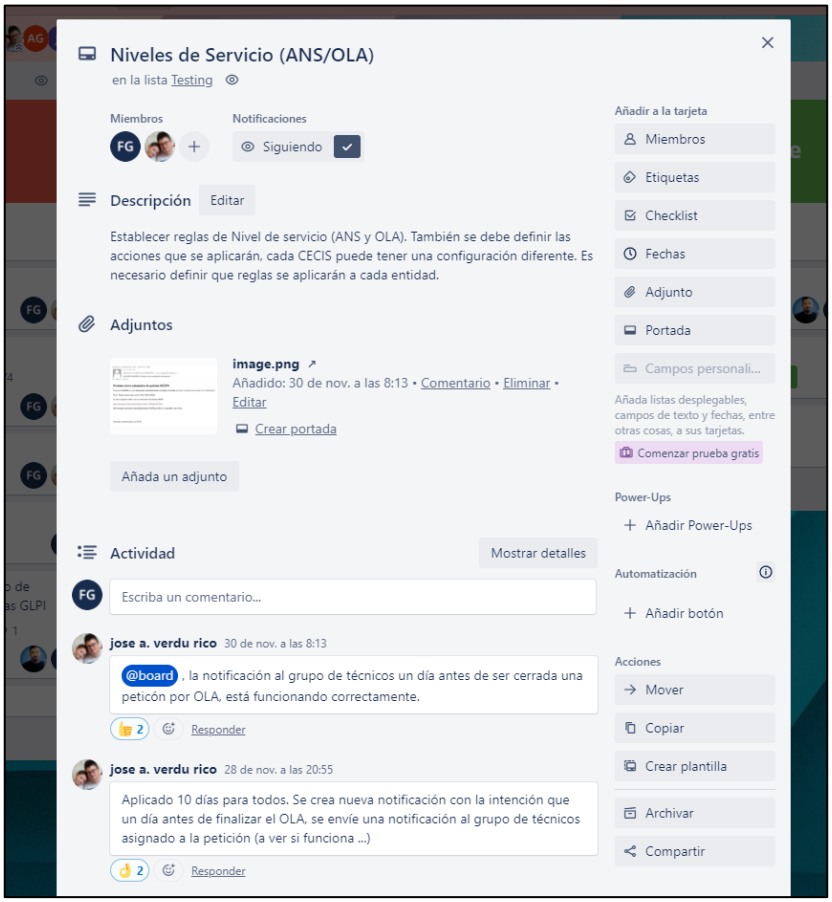


Ilustración 22.- Ejemplo de tarjeta tablero KANBAN GLPI (Fuente: propia)

4 RESULTADOS

Tras conseguir la autorización del CESTIC para el uso de GLPI en la red de propósito general del Ministerio de Defensa la implantación inicial se realizó en el Centro de Sistemas de Información de la Jefatura de Apoyo Logístico de la Armada (CECISJAL) y el Centro de Sistemas de Información de Ferrol (CECISFER) en mayo del 2022 extendiendo su uso al resto de CECIS de la Armada el 4 de julio de 2022. A día de hoy están implementados en la Armada los módulos de gestión de peticiones (Eventos e Incidentes) y gestión de activos.

En la Ilustración 23 se puede ver el *dashboard* de GLPI donde se muestran los usuarios registrados (24,9K), los activos (hardware y software) y desde donde se pueden extraer los KPI de ejemplo que se pueden muestran en el Gráfico 1.

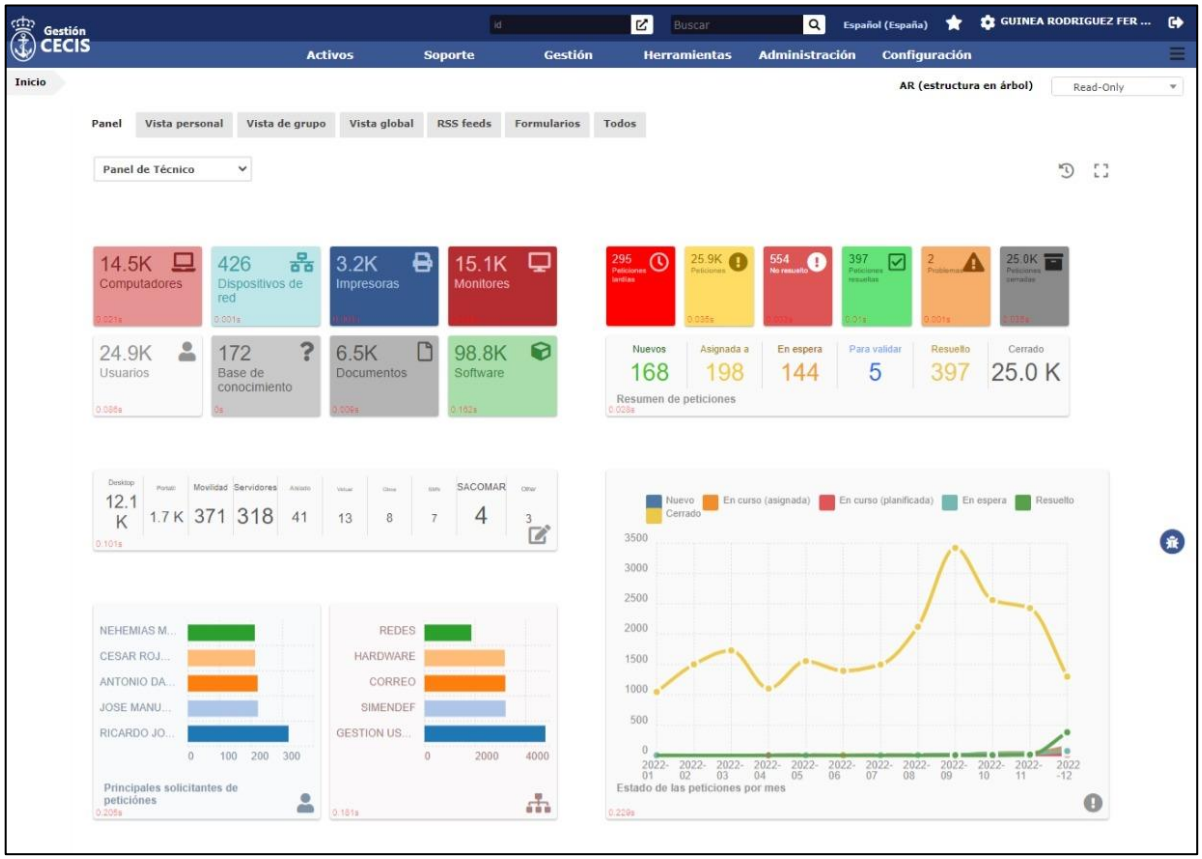


Ilustración 23.- Dashboard GLPI (Fuente: propia)

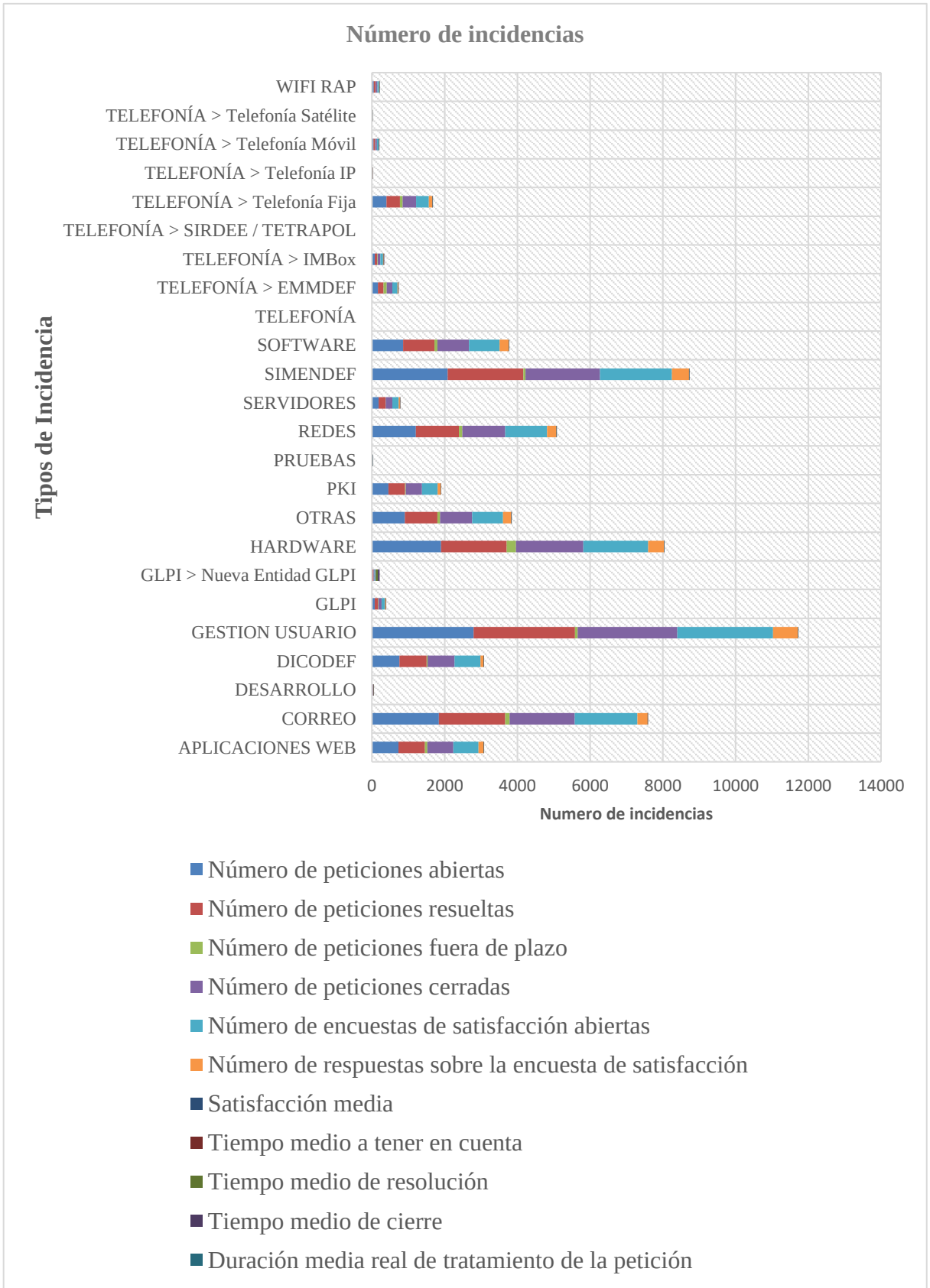


Gráfico 1.- KPI Incidencias (fuente: Propia)

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones.

Es necesario implementar en la Armada un servicio de atención al usuario ya que actualmente los medios que proporciona, así como los que está previsto que proporcione, el Ministerio de Defensa no llegan al elemento más importante el usuario como dice ITIL [25]:

«Independientemente de cómo se gestionan los servicios, procesos y la tecnología, todo está relacionado con las personas. Son las personas las que impulsan la demanda de los servicios de la organización y sus productos y son las personas las que deciden cómo se harán las cosas. En última instancia, son las personas las que gestionan la tecnología, procesos y servicios. El no reconocer esto resultará (y ha resultado) en el fallo de la gestión del servicio.»

Ya se han definido las líneas futuras que guiarán la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa así como los medios que nos permitirán alcanzarlas. Estas líneas futuras incluyen nuevos procedimientos para proporcionar nuevos servicios que están a disposición de los usuarios. Estos nuevos procedimientos convivirán con los anteriores, pero esto no es un impedimento, ya que gracias a la metodología ITIL esta transición debe ser natural.

Se está avanzando en definir las herramientas que nos permitirán alcanzar los objetivos mediante la definición de un Pliego de Prescripciones Técnicas (PPT) que ha de regir el establecimiento de un acuerdo marco para la contratación de Servicios e Infraestructuras de Telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D). Si bien es verdad que hay margen para mejorar en la atención al usuario.

Existe la tecnología para poder hacer que las buenas practicas ITIL alcancen todos los estamentos de las Fuerzas Armadas y principalmente al soldado/marinero. En esta memoria se ha propuesto una solución que actualmente está en funcionamiento en la Armada, el GLPI con un coste tanto económico como humano razonable. La implementación del GLPI ha supuesto una inversión de 50.000€ que ha permitido implementar el GLPI de una manera más ágil así como la programación de ciertos *plug-in* personalizados. En lo que al recurso humano para la implantación del GLPI se refiere en la Armada se ha creado un Grupo de Trabajo formado por 44 personas, donde 40 eran clientes y 4 el Equipo de Desarrollo. Se han realizado un total de 16 reuniones formales y 776 horas de videoconferencias informales.

La implementación se pudo realizar porque tanto la organización de los 7 CECIS de apoyo como los procesos definidos actualmente en el GLPI son similares. La organización, en lo que a personal y roles se refiere es la definida por el CCEA y los procesos, a excepción de los que afectan a las unidades

en la mar, no deben diferir mucho por lo que en el resto de ámbitos también debe ser posible implantar una ITSM.

Y lo más importante, el recurso humano que hay detrás del usuario, sin un técnico que resuelva las incidencias lo anteriormente definido no tendría ningún sentido. El personal destinado en los CECIS de Apoyo de la Armada tiene la capacidad para satisfacer las necesidades mínimas un SAU-AR.

Como conclusión final, el GLPI es la solución que satisface las necesidades expuestas y se alinea con la normativa del Ministerio de Defensa permitiendo a la Armada dar un salto de calidad y ofrecer valor al usuario.

5.2 Líneas Futuras

Hemos visto que la solución planteada permite tener una s*ervice desk* local. Pero con esta solución podemos dar servicio de manera parcial ya que, como vimos en la introducción, la Armada cuenta con unidades desplegadas en todo el mundo. Además de esto hemos visto que los 7 CECIS de Apoyo tienen la misma organización esto quiere decir que si un técnico de redes CECISFER no tiene incidencias que resolver en Ferrol estaría de brazos cruzados. En los tiempos que corren esto es un lujo que la Armada no se puede permitir. Por esto la Armada debe aspirar a tener una *service desk* Virtual que permita, como dice [9]: *«Mediante el uso de la tecnología, en particular de Internet, y el uso de herramientas corporativas de apoyo, es posible dar la impresión de un único, centralizado, cuando en realidad el personal puede estar diseminado o ubicado en cualquier tipo de ubicaciones geográficas u organizativas. Esto permite el trabajo en casa, grupos de apoyo secundarios, deslocalización o externalización, o cualquier combinación necesaria para satisfacer la demanda de los usuarios.»*

Como hemos visto en las conclusiones el personal actual destinado en los CECIS de Apoyo es el mínimo y hay ciertos roles de la metodología ITIL que actualmente o no están cubiertos o están cubiertos a tiempo parcial. Si se marca como horizonte el SAU-AR virtual el personal destinado en los diferentes CECIS de Apoyo se consideraría un todo por lo que se podrían repartir los roles de manera nacional siendo transparente para el usuario. Por hacer un símil, el usuario sólo vería el escaparate (*service desk*) donde elegiría su producto (servicio) y lo obtendría sin saber que hay detrás de él.

6 BIBLIOGRAFÍA

[1] Ministerio de Defensa, *Pliego de Prescripciones Técnicas que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la infraestructura integral de información para la defensa (I3D),* Madrid, 2022.

[2] Ministerio de Defensa, «Instrucción número 236/2002, de 7 de noviembre, del Secretario de Estado de Defensa por la que se crea el Centro Corporativo de Explotación y Apoyo para los Sistemas de Información y Telecomunicaciones del Ministerio de Defensa.,» de *BOD 222*, España, 2002, p. 11312.

[3] Ministerio de Defensa - Comisionado CIS, *Creación del Centro Corporativo de Explotación y Apoyo CIS. Programa de Detalle*, Madrid, 2003.

[4] Ministerio de Defensa -Comisionado CIS, *Definición del sistema SCANS-DEF (Sistema de Control de Acuerdos del Nivel de Servicio),* Madrid, 2003.

[5] Armada - Seccion CIS de la Secretaria General del Estado Mayor de la Armada, Organizacion de las Comunicaciones Navales, Madrid, 2020.

[6] Almirante Jefe de Sistemas De Información y Telecomunicaciones (AJECIS), Norma Permanente de Organización (NPOR) 1/2022 donde se desarrolla la estructura de la JECIS, Madrid, 2022.

[7] Centro de Apoyo Informático de Ferrol, *CAI (PROYECTO- PMS-ESTRUCTURADO),* Ferrol, 2016.

[8] «Portal de Administracion electronica,» Ministerio de Asuntos Económicos y Transformación Digital Secretaría General de Administración Digital, [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.Y6anZn3MLt4. [Último acceso: 10 octubre 2022].

[9] AXELOS, ITIL Foundation: ITIL 4 Edition, 2019.

[10] Centro Universitario de la Defensa (CUD)., *ITIL. Apuntes y clases magistrales de la asignatura COM3 del Máster DIRETIC 2020-2021 del Centro Universitario de la Defensa (CUD).*, Pontevedra, 2022.

[11] Axelos, Managing Successful Projects with PRINCE2, Stationery Office Books, 2009.

[12] ISO, Norma ISO/IEC 20000-1 Tecnologías de la información. Gestión de Servicios, 2018.

[13] Centro Universitario de la Defensa (CUD)., DevOPS. Apuntes y clases magistrales de la asignatura COM3 del Máster DIRETIC 2021-2023, Marin, 2022.

[14] Attribution-NonCommercial-ShareAlike 4.0 International., «PRINCE2 wiki,» [En línea]. Available: https://prince2.wiki/es/principios/adaptacion-al-entorno-del-proyecto/. [Último acceso: 15 11 2022].

[15] UNE-ISO, UNE-ISO 21500 Gestión de proyectos, 2013.

[16] Ministerio de Defensa, *Orden de Defensa 2639/2015, que establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, define a la Infraestructura Integral de Información para la Defensa (I3D),* Madrid, 2015.

[17] NATO, NATO C3 CLASSIFICATION TAXONOMY, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/10/pdf/210830-C3-taxonomy-baseline.pdf, 2021.

[18] Ministerio de Defensa, Ley Orgánica 5/2005 de la Defensa Nacional, Madrid, 2005.

[19] Ministerio de Defensa, (PECIS) Instrucción 33/2018, de 6 de junio,del Secretario de Estado de Defensa, aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, Madrid, 2018.

[20] Ministerio de Defensa, *Orden DEF/2639/2015, de 3 de diciembre,Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.*, Madrid, 2015.

[21] Ministerio de Asuntos Económicos y Transformación Digital Secretaría General de Administración Digital, «GLPI -CTT,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/inventarioseap#.Y6aton3MLt4. [Último acceso: 15 11 2022].

[22] *Instruccion Tecnica 01/07 sobre Arquitectura Técnica Unificada del Ministerio de Defensa,* Madrid, 2010.

[23] TICGAL, «TICGAL,» TICGAL, [En línea]. Available: https://tic.gal/es/.

[24] Atlassian, «TRELLO,» 13 09 2021. [En línea]. Available: https://trello.com/es.

[25] TSO- The Stationery Office, ITIL Service Operation, Norwich: TSO Ireland, 2011, p. 4.

[26] O. Masana, «Sistema pull y tarjetas kanban como pilares del JIT,» [En línea]. Available: https://www.leankaizen.es/sistema-pull-y-tarjetas-kanban/. [Último acceso: 12 10 2022].

7 ANEXO I: SEVERIDAD

Tablas obtenidas de la referencia [1]:
«*La severidad de una incidencia viene dada por la siguiente tabla:*

SEVERIDAD INCIDENCIA	
ALTA	- *Pérdida total de algún servicio o de conectividad total de datos o voz en la sede.* - *Incumplimiento continuado de especificaciones de indicadores de red en un enlace determinado implicando la degradación alta de servicios dependientes de latencia, pérdida de paquetes o jitter afectando a más del 50% de usuarios o extensiones de la ubicación.* - *Comunicación por parte de personal autorizado del MINISDEF de la imposibilidad o seria dificultad para mantener comunicaciones de voz por parte de gran cantidad de usuarios de una ubicación, o bien comunicación masiva de incidencias por parte de los usuarios de una ubicación.* - *Repetición de una misma incidencia de severidad media en un plazo de 48 h (naturales).* - *Acceso no autorizado, modificación o destrucción de las claves de cifrado, LOGs o del contenido de las comunicaciones del MINISDEF.* - *Cuando el MINISDEF así lo indique.*
MEDIA	- *Degradación media del servicio superior al 51% de su capacidad/funcionalidad nominal.* - *Comunicación de imposibilidad o seria dificultad para mantener comunicaciones de voz por parte de 5 o más usuarios de una ubicación en el mismo día en la misma ubicación.* - *Incumplimiento de especificaciones de indicadores de red en un enlace proporcionado por el adjudicatario de este Lote, como por ejemplo los enlaces a red NGN (latencia, pérdida de paquetes o jitter) por periodos de varios minutos seguidos.* - *Incumplimiento de especificaciones de indicadores de red en un enlace determinado (latencia, pérdida de paquetes o jitter) que provoca la queja de más de cinco usuarios de una misma sede.* - *Repetición de incidencia de severidad baja en un plazo de 48 h (naturales)* - *Desaparición de la configuración de Alta Disponibilidad de un enlace por caída de un alguno de sus elementos o por otra causa* - *Acceso no autorizado, modificación o destrucción de los Datos de Incidencias y Peticiones.* - *Cuando el MINISDEF así lo indique.*
BAJA	- *Degradación leve (menor o igual del 51%) del servicio permanentemente o de forma esporádica.* - *Comunicación de imposibilidad o seria dificultad para mantener comunicaciones de voz por parte de un usuario de una ubicación.* - *Incumplimiento de especificaciones de indicadores de red en un enlace proporcionado por el adjudicatario de este Lote, como por ejemplo los enlaces a red NGN (latencia, pérdida de paquetes o jitter) que provoca la queja de un usuario del MINISDEF.*

	- *Incumplimiento esporádico y por periodos de menos de 1 minuto de especificaciones de indicadores de red en un enlace (latencia, pérdida de paquetes o jitter), con baja repercusión en los servicios soportados en la red de datos, repetido más de 10 veces a lo largo de 5 días.* - *Incumplimiento de especificaciones de indicadores de red en un enlace que provoca la queja de un usuario del MINISDEF.* - *Desaparición o minoración de la configuración de Alta Disponibilidad de un servicio por caída de un alguno de sus elementos o por otra causa, sin impacto en los servicios.*

En el caso de incidencias de seguridad, se definen las siguientes severidades

SEVERIDAD	***INCIDENCIA DE SEGURIDAD***
ALTA	- *Acceso no autorizado, modificación o destrucción intencional de los activos.* - *No recogida en la herramienta de gestión de incidencias de cualquier incidente de severidad alta o media.* - *No puesta a disposición del MINISDEF de los logs que éste le requiera del equipamiento objeto de este contrato, incluyendo los logs de las herramientas de gestión.* - *Violación de la confidencialidad o integridad de los datos transportados por el tramo de red o activos que opere el adjudicatario.* - *Cuando el MINISDEF así lo indique.*
MEDIA	- *No recogida en la herramienta de gestión de incidencias de cualquier incidente de severidad baja.* - *Cambios sin autorización del MINISDEF sobre el listado de personal autorizado para la administración de equipos.* - *Modificación o destrucción accidental de los activos de gestión o de los datos.* - *Acceso, alteración o destrucción no autorizada de datos personales asociados al contrato.* - *Cuando el MINISDEF así lo indique.*
BAJA	- *Incumplimiento de las políticas de seguridad del MINISDEF en cualquier otro aspecto recogido en este pliego, la oferta del adjudicatario, política de seguridad del adjudicatario o política de seguridad del MINISDEF. »*

8 ANEXO II: PLAZOS, DISPONIBILIDAD Y COMPROMISOS

Los siguientes apartados y tablas están obtenidos de la referencia [1]:

1. Plazos aplicables en la gestión de incidencias y peticiones

«*Se definen los siguientes tiempos para todos los lotes:*

- *Tiempo de Solicitud (T0 = H0) (notificación) de incidencias o peticiones. Momento que o bien se notifica fehacientemente una incidencia o petición por parte del MINISDEF o bien se genera una alarma de monitorización indicando degradación o caída del servicio o activo.*
- *Tiempo de Registro (TR= HR). Momento en que una petición o incidencia se registra en el Sistema de Gestión de Peticiones e Incidencias. Deberá cumplirse que:*

$$TR - T0 \leq 5\,minutos$$

- *Tiempo de acuse de recibo (TACK): Tiempo transcurrido desde T0 (por la vía establecida) y el momento de envío por parte del adjudicatario del ticket correspondiente de registro de la incidencia o petición (HACK).*

$$TACK = HACK - T0$$

- *Tiempo de Respuesta, (TRSP): Tiempo transcurrido entre la notificación de una petición o incidencia por parte del MINISDEF (T0) y el envío por parte del adjudicatario de la Respuesta (HRSP) con la lista de acciones y plazos de aplicación de las mismas.*

$$TRSP = HRSP - T0$$

- *Tiempo de Parada (TP): suma de los períodos de tiempo en los que una incidencia está paralizada debido a:*
  - *Paradas del servicio programadas para mantenimiento y convenientemente notificadas con antelación de al menos cinco días laborables y aceptados previamente por el MINISDEF. La indisponibilidad de los servicios fuera de este horario de corte sí computará como período no disponible.*
  - *Tiempos de indisponibilidad debidos a la imposibilidad de restablecimiento del servicio por motivos imputables al MINISDEF (por ejemplo inaccesibilidad a las instalaciones).*
  - *Pérdidas de servicio debidas a causas de fuerza mayor (incendios, inundaciones, etc.). La prioridad de la incidencia vendrá determinado por el tipo de sede, activo o servicio afectado.*
  - *Altas en accesos de nueva construcción: aquéllas para las que el adjudicatario no dispone de infraestructura previa para dar el servicio, lo que implica que ha de crear la nueva infraestructura. Para este tipo de actuaciones no computarán para el cálculo de Tiempo de Resolución los siguientes casos:*
    - *Retardos debidos a la imposibilidad de obtener permisos de obra de administraciones ajenas al adjudicatario (municipales por ejemplo).*
    - *Retardos en accesos que requieran obra civil con plazos difíciles de establecer a priori (p.e. accesos vía fibra óptica), siempre y cuando estos retrasos sean debidamente justificados y comunicados en fecha.*
  - *Tiempo de Recuperación del Servicio, (TRS) como el tiempo transcurrido entre T0 y el momento de notificación al MINISDEF de la restauración de servicio (HRS) en caso de incidencia (solución temporal o definitiva). La recuperación sólo aplica al caso de incidencias, y se debe realizar en el menor tiempo posible sin poner en riesgo otros activos o servicios objeto del contrato, siendo posible que no todos los atributos del servicio estén disponibles. Se descontarán los tiempos de parada (TP).*

$$TRS = HRS - T0 - TP$$

- *Tiempo de Cierre (TCPI) de Peticiones o Incidencias: Tiempo transcurrido entre el envío de solicitud/notificación de incidencia o petición (T0) y el momento de notificación al MINISDEF del cierre de Petición o Incidencia (HCPI). El cierre de una incidencia o petición se realizará cuando se haya restaurado el servicio con plena capacidad y disponibilidad de todos los atributos previstos del servicio. Se descontarán los tiempos de parada (TP).*

$$TCPI = HCPI - T0 - TP$$

- *Tiempo de Entrega de Informe de Resolución de Incidencia Crítica (TICI). En caso de incidencias con prioridad 0 o 1, se deberá entregar al MINISDEF el Informe de Resolución de Incidencia Crítica donde se deberá detallar al menos la siguiente información:*
  - *Descripción de la incidencia.*
  - *Elementos y servicios afectados por la avería.*
  - *Causa de la incidencia.*
  - *Duración de la incidencia.*
  - *Acciones realizadas para el restablecimiento del servicio.*
  - *Fecha y hora de apertura y cierre de la incidencia.*
  - *Conclusiones y posibles acciones de mejora.*

  Se define Tiempo de Entrega de Informe de Resolución de Incidencia Crítica (TICI) como el tiempo que transcurre desde que se cierra la incidencia hasta que el adjudicatario realiza la entrega del informe al MINISDEF (HICI). $TICI = Horaentregainforme - TCPI$
- *Tiempo de Notificación proactiva de Incidencia (TNOT): Se define como el tiempo transcurrido desde que se produce la incidencia o se detectan sus primeros síntomas por parte del MINISDEF hasta su registro por parte del adjudicatario en el Sistema de Gestión de Peticiones e Incidencias.*

Los tiempos anteriormente definidos se medirán teniendo en cuenta el horario de atención del adjudicatario del servicio para las peticiones de provisión y de administración.

Por días laborables se entenderán los comprendidos de lunes a viernes, excluyendo los festivos que afecten a la localidad donde se realice la correspondiente actuación.

Las incidencias y peticiones estarán paradas fuera del horario de resolución definido para cada nivel de prioridad. Para reducir al máximo los tiempos de parada en aquellas ubicaciones que no ofrezcan un servicio 24 horas (en las cuales el acceso por parte del personal encargado de las reparaciones resulta complicado fuera de la jornada habitual de trabajo), el adjudicatario del servicio deberá solicitar el apoyo del MINISDEF para conseguir una persona de contacto que facilite el acceso a la sede afectada.

El horario de atención de incidencias varía según la prioridad de las incidencias. Así:

- *Prioridad 0 y 1: de lunes a domingo entre las 0h y las 24h*
- *Prioridad 2 y 3: días laborables de la ubicación entre las 7h y las 19h*

Las consultas al adjudicatario serán consideradas como una petición de servicio de administración más, con la prioridad que le corresponda de acuerdo a su matriz de prioridades.

2. Disponibilidad de activos y servicios

En todos los lotes se calcula la disponibilidad de los activos, en el periodo de tiempo T, según la siguiente expresión:

$$D_{at} = \frac{T_{tot} - T_{NODisp}}{T_{tot}} * 100$$

Donde:

T_{tot}: Tiempo total del periodo considerado (minutos)

T_{NoDisp}: Tiempo de no disponibilidad de alguno de los servicios del activo dentro del intervalo T_{tot} considerado.

Disponibilidad en caso de activos redundados: En el caso de activos redundados (caso de Soluciones Técnicas que utilizan servicios de datos y equipos en alta disponibilidad) no se considera su Disponibilidad individual, sino la de la Solución que proporcionen, considerando una minoración del 40% en caso de caída de alguno de los elementos redundados. Así, en caso de líneas o equipos redundados, la caída de uno de ellos se corresponderá con una degradación del 40% de la Solución Técnica que soportan, mientras que en los no redundados la caída del dispositivo supondrá la caída total de la Solución Técnica.

Disponibilidad para una conexión a Internet en un periodo de tiempo T (DLT): Se calcula como el porcentaje de tiempo mensual en el que está la línea con todos sus activos disponibles. Esta disponibilidad se calculará en el periodo de tiempo T según la siguiente expresión

$$D_{CT} = \frac{T_{tot} - T_{NODisp}}{T_{tot}} * 100$$

Donde:

D_{CT}: Disponibilidad de una conexión en el periodo T.

Disponibilidad Global del MINISDEF en un periodo de tiempo T, para las conexiones a Internet de criticidad C (DGMC): Promedio de Disponibilidad de todas las líneas satelitales del MINISDEF. Esta disponibilidad se calcula de forma separada para cada una de las posibles criticidades de las líneas, lo que resulta en dos valores diferentes de disponibilidad para el MINISDEF.

Esta disponibilidad se calculará en el periodo de tiempo T según la siguiente expresión:

$$D_{GMC} = \frac{T \sum_{i=1}^{N} D_{LiT}}{N} (\%)$$

Donde:

D_{LiT}: Disponibilidad de cada línea de acceso a Internet "i" en el periodo T

D_{MTC}: Disponibilidad Global del MINISDEF en el periodo T, para el valor de criticidad C

C: criticidad de las líneas (Extrema, Alta)

N: Número total de líneas satelitales del MINISDEF

Para el cómputo de la disponibilidad no se tendrán en cuenta las siguientes situaciones:

- *Averías que no supongan una degradación del servicio alta. Únicamente se contabilizarán dentro del tiempo de no disponibilidad las averías que supongan falta de servicio y averías que*

supongan una degradación del servicio alta. Se considera degradación del servicio alta cualquier degradación que suponga la imposibilidad de la provisión del servicio con una calidad óptima.

- *Caídas en la infraestructura que no afecten al servicio gracias a los mecanismos de redundancia y backup.*
- *Cortes debidos a trabajos programados y debidamente notificados al MINISDEF. Siempre y cuando estos trabajos no excedan el tiempo programado de corte. La indisponibilidad de la red fuera de este horario de corte sí computará como período no disponible.*
- *Tiempos de indisponibilidad debidos a la imposibilidad de restablecimiento del servicio por motivos imputables al MINISDEF (p.e. inaccesibilidad de las instalaciones).*
- *Indisponibilidad del servicio por causas de fuerza mayor, tanto naturales (terremotos, inundaciones, etc.), como artificiales (sabotajes, atentados, etc.).*

Los activos sujetos a la disponibilidad anteriormente mencionada, de los diferentes lotes, son:

2.1. LOTE 1: Servicios e infraestructuras de datos, telefonía y localización de la I3D

- *Circuitos de acceso a I3D, incluyendo equipamiento.*
- *Servicio de VPN sobre I3D, según tipo de sede.*
- *Equipamiento de Voz. No computará el cálculo de disponibilidad de terminales telefónicos.*
- *Enlaces de concentración a NGN.*
- *Enlaces de supervivencia.*
- *Otros circuitos, incluyendo equipamiento.*
- *Servicios básicos de red.*
- *Herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

2.2. LOTE 2: Servicios e infraestructuras de comunicaciones móviles de la I3D.

- *Enlaces de concentración a NGN móvil.*
- *Enlaces de supervivencia.*
- *Servicios básicos de red móvil.*
- *Sistema de Gestión de Movilidad.*
- *APNs privados.*
- *Mensajería masiva.*
- *Herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los datos de monitorización, por ejemplo).*

2.3. LOTE 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D

- *Herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los datos de monitorización, por ejemplo).*

2.4.LOTE 4: Servicios e infraestructuras de acceso a Internet de la I3D

- *Servicios básicos de red.*
- *Activos de gestión y herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

2.5.LOTE 5: Servicios e infraestructuras de Telemedicina de la I3D

- *Servicios básicos de telemedicina.*
- *Activos de gestión y herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

2.6.LOTE 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D

- *Servicios básicos de videoconferencia.*
- *Activos de gestión y herramientas de gestión. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

3. No disponibilidad de un activo

Se define que un activo determinado estará NO disponible cuando se encuentre bajo los efectos de una incidencia de severidad alta.

3.1.Lote 2: Servicios e infraestructuras de comunicaciones móviles de la I3D

Herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los datos de monitorización, por ejemplo).

3.2.Lote 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D

- Activos de gestión y herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).

3.3.Lote 4: Servicios e infraestructuras de acceso a Internet de la I3D

- Servicios básicos de red.

- Activos de gestión y herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).

3.4. Lote 5: Servicios e infraestructuras de Telemedicina de la I3D

- *Servicios básicos de telemedicina.*

- *Activos de gestión y herramientas del CGT. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

3.5. Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D

- *Servicios básicos de videoconferencia.*

- *Activos de gestión y herramientas de gestión. En el caso de las herramientas de gestión (herramientas de acceso remoto en general) se considerará indisponibilidad tanto su caída física como la imposibilidad de acceso a los servicios que soportan (como puede ser el acceso a los cuadros de mando o de los datos de monitorización, por ejemplo).*

4. Compromisos

La medida de los parámetros del ANS cuantificables en unidades de tiempo abarcará desde el instante de inicio hasta el de finalización; posteriormente, ya que en los informes que se presentarán al MINISDEF se podrán incluir justificaciones al incumplimiento que, en caso de ser aceptadas por el MINISDEF, deducirán del total las demoras justificadas y cuantificadas. Se deberá por tanto incorporar la hora de inicio y finalización del parámetro medido y de cada una de las demoras justificadas.

Los informes de reporte del ANS se entregarán con la periodicidad que defina el MINISDEF (por defecto, periodicidad mensual). El MINISDEF definirá asimismo el formato y contenido de los informes, pudiendo modificarlos a lo largo del periodo de contratación, para facilitar el seguimiento y el control de los parámetros de calidad. También es posible la petición de informes por periodos específicos, desde una fecha de inicio a una fecha final.

De forma general, y salvo que se indique específicamente lo contrario, los compromisos de cumplimiento del ANS no se cierran al final de cada periodo y se reinicia la cuenta a cero; el periodo indica simplemente la frecuencia de reporte de los mismos. Los registros que permanezcan abiertos al cierre de ciclo de medición de los parámetros de ANS se volverán a reportar en el ciclo siguiente con el mismo identificador, de manera que puedan ser relacionados con el anterior registro pendiente de cierre. Ello no debe ser considerado en ningún caso como doble penalidad.

Dependiendo del lote se define en el PPT los compromisos siguientes compromisos:

4.1.Lote 1: Servicios e infraestructuras de datos, telefonía y localización de la I3D

- *Compromisos relativos a Peticiones de Provisión y Administración*

	TIEMPOS DE ACTUACIÓN					
	Acuse de recibo (TACK)	***Tiempo de respuesta (TRSP)***	***Tiempo de Cierre (TCPI)***			
			Prioridad 0	***Prioridad 1***	***Prioridad 2***	***Prioridad 3***
CONCEPTO PROVISIÓN SOLICITADO						
Servicio de traslado de Sedes	*15m*	*3d*	*15d*	*30d*	*40d*	*60d*
Traslado interno de routers y equipamiento en general que forma parte del servicio	*15m*	*3d*	*5d*	*10d*	*20d*	*30d*
Baja de cualquier servicio o sede	*15m*	*9h*	*2d*	*5d*	*10d*	*15d*
Modificación de caudal de sede, sin cambio de acceso	*15m*	*9h*	*1d*	*3d*	*5d*	*10d*
Modificación de acceso de sede	*15m*	*3d*	*15d*	*30d*	*40d*	*60d*
Provisión de Enlaces de Sedes	*15m*	*1d*	*5 d*	*10 d*	*15 d*	*30 d*
Provisión de nuevo flujo de datos en enlace de F.O. respaldo del STM	*15m*	*1d*	*30 d*	*45 d*	*60 d*	*60 d*
Actualización o sustitución de equipamiento	*15m*	*1d*	*1 d*	*2 d*	*4 d*	*8 d*

Provisión de Líneas especiales	*15m*	*1d*	*5 d*	*10 d*	*15 d*	*30 d*
Provisión de enlaces de dato para interconexión a NGN	*15m*	*1d*	*5 d*	*10 d*	*15 d*	*30 d*
Cambio de tipología de sedes	*15m*	*1d*	*5 d*	*10 d*	*15 d*	*30 d*
Implantación y configuración de VPNs	*15m*	*3d*	*5d*	*10d*	*15d*	*30d*
Provisión instalación y configuración de Equipamiento	*15m*	*3d*	*30 d*	*30 d*	*45 d*	*45 d*
Peticiones de gestión y monitorización de los servicios	*15m*	*1h*	*2h*	*4h*	*6h*	*8h*
Petición de retirada de equipamiento	*15m*	*1d*	*10d*	*15d*	*30d*	*30d*
Petición de diseño técnico	*15m*	*16h*	*5d*	*10d*	*20d*	*30d*
Petición de emisión de informes	*15m*	*1h*	*4h*	*8h*	*2d*	*5d*
Petición de planificación de proyectos	*15m*	*8h*	*5d*	*10d*	*20d*	*30d*
Provisión infraestructuras de obra civil, asociadas a nuevo enlace	*15m*	*5d*	*30 d*	*45 d*	*60 d*	*60 d*
Plazo de provisión de línea (extensión) y traslados externos de voz	*15m*	*3d*	*10d*	*10d*	*20d*	*20d*
Plazo de traslado interno de línea (extensión)	*15m*	*5 h*	*1 d*	*1 d*	*5 d*	*5 d*
Plazo altas en accesos de nueva construcción	*15m*	*3 d*	*10 d*	*10 d*	*20 d*	*20 d*
Plazo de provisión o traslado de acceso	*15m*	*3 d*	*10 d*	*10 d*	*20 d*	*20 d*

Tabla 6.- Tiempos de actuación para las Peticiones de Servicio

- ***Compromisos relativos a Resolución de Incidencias***

CONCEPTO INCIDENCIA (sobre activo, sede o servicio)	***TIEMPOS DE ACTUACIÓN***				
	Tiempo de Recuperación del Servicio, (T_{RS})				***Tiempo de cierre(T_{CPI})***
	Prioridad 0	***Prioridad 1***	***Prioridad 2***	***Prioridad 3***	
Cualquiera por defecto	*4 h*	*6 h*	*10 h*	*16 h*	*48 h*
Equipamiento de datos o voz	*1 h*	*4 h*	*8 h*	*16 h*	*72 h*

Circuitos de acceso a I3D y enlaces de concentración NGN	*1 h*	*2 h*	*3 h*	*6 h*	*18 h*
Enlaces de supervivencia y otros circuitos	*1 h*	*2 h*	*3 h*	*6 h*	*18 h*
Servicio de VPN sobre I3D	*1 h*	*2 h*	*3 h*	*6 h*	*18 h*
Servicios básicos de red	*1 h*	*2 h*	*3 h*	*6 h*	*18 h*
Herramientas del CGT	*8 h*	*16 h*	*24 h*	*36 h*	*108 h*

Tabla 7 Tiempos de actuación para Cierre de incidencias

4.2.Lote 2: Servicios e infraestructuras de comunicaciones móviles de la I3D

Las Peticiones, tanto de Provisión como de Administración, se clasifican según su prioridad de resolución. Tomando como criterio el concepto de petición de provisión o administración solicitado y la prioridad de la petición, derivada de la urgencia asignada por el MINISDEF, el proveedor del servicio se deberá comprometer a ofrecer, al menos, los siguientes tiempos:

Concepto de Provisión Solicitado	***Tiempos de Actuación***			
			Tiempo de cierre (T_{CPI})	
	Acuse Recibo (T_{ACK})	***Tiempo respuesta (T_{RSP})***	***Prioridad 0 y 1***	***Prioridad 2 y 3***
Petición general de provisión. En general, repuestos, accesorios, dispositivos, etc.…	*15m*	*2h*	*1d*	*3d*
Petición general de administración	*15m*	*2h*	*12h*	*1d*
Petición de consultas al adjudicatario	*15m*	*N/A*	*1d*	*5d*
Ampliación de cobertura móvil en el interior de las sedes	*1h*	*1d*	*5d*	*30d*
Provisión o traslado de circuitos de acceso red móvil	*1h*	*1d*	*5d*	*30d*
Plazo de ampliación de ancho de banda en los enlaces de acceso en movilidad	*1h*	*1d*	*10d*	*30d*
Plazo de configuración de la infraestructura de red móvil (casos habituales)	*1h*	*2h*	*1d*	*48h*
Plazo de configuración de la infraestructura de red móvil (casos especiales: enlaces de voz o acceso en movilidad, con el equipamiento de acceso en movilidad o con características del servicio en la red del operador que requieren un estudio o informe de ingeniería)	*1h*	*3h*	*7d*	*15d*
Provisión de circuitos adicionales, líneas o servicios en nuevas sedes	*1h*	*2h*	*15d*	*20d*
Plazo de baja de los servicios	*1h*	*1d*	*10d*	*20d*
Plazo de portabilidad para altas nuevas fuera de la provisión inicial	*1h*	*2h*	*1d*	*2d*
Plazo de cambio de titularidad	*1h*	*2h*	*1d*	*1d*
Plazo de provisión o sustitución de un terminal de telefonía móvil; por robo o avería	*30m*	*1h*	*1d*	*2d*
Plazo de configuraciones especiales o instalaciones determinadas	*1h*	*4h*	*2d*	*7d*
Plazo de bloqueo o borrado remoto del terminal	*10m*	*15m*	*15m*	*4h*
Plazo de inhabilitación de dispositivos	*30m*	*1h*	*12h*	*48h*
Plazo de suspensión o bloqueo de una línea	*30m*	*1h*	*30m*	*2h*
Plazo de activación o desactivación de determinadas restricciones	*10m*	*30m*	*30m*	*2h*

Tabla 8.- Tabla de compromisos de respuesta y resolución de peticiones de administración y provisión del Servicio de Comunicaciones Móviles

Los tiempos de las tablas anteriores están siempre expresados en días u horas laborables. Por días laborables se entenderán los comprendidos de lunes a viernes, excluyendo los festivos que afecten a la localidad donde se realice la correspondiente actuación. El horario laboral se establece en la franja de 07:00 a 19:00 a efectos de peticiones de provisión.

Compromisos relativos a Resolución de Incidencias

Para todos los servicios, el adjudicatario del Lote se deberá comprometer a los siguientes niveles de calidad para la Recuperación y Cierre de Incidencias.

- *Tiempo máximo de respuesta ante incidencias:*

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo de respuesta (T_{RSP})***	***Tiempo de recuperación del servicio (T_{RS})***	***Tiempos de Cierre (T_{CPI})***
Prioridad 0	*15m*	*30m*	*1h*	*1d*
Prioridad 1	*20m*	*1h*	*4h*	*2d*
Prioridad 2	*30m*	*4h*	*1d*	*3d*
Prioridad 3	*1h*	*9h*	*2d*	*4d*

Tabla 9.- Tabla de compromisos de respuesta y resolución de peticiones de administración y provisión del Servicio de Comunicaciones Móviles

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*
- *Tiempo Máximo de entrega de Informe de Resolución de Incidentes de seguridad:*

Compromisos relativos a Resolución de Incidencias

- *Tiempo máximo de respuesta ante incidencias:*

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo de respuesta (T_{RSP})***	***Tiempo de recuperación del servicio (T_{RS})***	***Tiempos de Cierre (T_{CPI})***
Prioridad 0	*15m*	*30m*	*1h*	*1d*
Prioridad 1	*20m*	*1h*	*4h*	*2d*
Prioridad 2	*30m*	*4h*	*1d*	*3d*
Prioridad 3	*1h*	*9h*	*2d*	*4d*

Tabla 10.- Compromisos de Tiempo máximo de respuesta ante incidencias para el Servicio de Comunicaciones Móviles

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*
- *Tiempo Máximo de entrega de Informe de Resolución de Incidentes de seguridad:*

Tipo de Incidencia	***Tiempo máximo de entrega***
Incidente de seguridad de prioridad 0	*4h*
Incidente de seguridad de prioridad 1	*8h*
Incidente de seguridad de prioridad 2	*2d*
Incidente de seguridad de prioridad 3	*4d*

Tabla 11.- Tiempo Máximo de Entrega de Informes de Resolución de Incidentes de Seguridad

El adjudicatario se comprometerá a mantener en todo momento los requisitos de seguridad expuestos en este pliego, debiendo cumplir al menos los siguientes niveles máximos mensuales:

Parámetro	***Valor Exigido***
Incidencias de seguridad de severidad alta	*0*
Incidencias de seguridad de severidad media	*4*
Incidencias de seguridad de severidad baja	*9*

Tabla 12.- Número máximo de incidencias de seguridad mensuales

Compromisos relativos a la Disponibilidad

Los valores de disponibilidad que se requieren se han calculado en base a los siguientes escenarios modelo:

- *Periodo de tiempo (T) en el que se calcula la disponibilidad. El objetivo de disponibilidad se establece como un valor de periodicidad anual, pero se fijan ANS también a nivel mensual.*
- *Tiempo de Recuperación del Servicio (TRS). Se tiene en cuenta, en cada caso, el correspondiente al caso de incidencia de severidad alta, aplicable a cada activo considerado.*
- *Nº de caídas en el periodo considerado de activos o sedes según el tipo de Disponibilidad (de activos, sedes o global) considerado.*

Se diferencia entre los siguientes activos o grupos de activos a efectos de cálculo de disponibilidad:

- *Activos sujetos a disponibilidad:*
  - *Enlaces de concentración a NGN móvil.*
  - *Enlaces de supervivencia.*
  - *Servicios básicos de red móvil.*
  - *Sistema de Gestión de Movilidad.*
  - *APNs privados.*
  - *Mensajería masiva.*
  - *Mensajería instantánea*
  - *Herramientas del CGT.*

En la siguiente tabla se indican los valores de Disponibilidad mínimos exigidos (se hace notar que la acumulación de muchas caídas con plazo de recuperación muy corto podría dar lugar a incumplimiento de ANS):

Disponibilidad requerida en %, según criticidad de activos afectados.	***Periodo T (días)***	***Criticidad (prioridad en caso de incidencia de severidad alta)***			
		Extrema	***Alta***	***Media***	***Baja***
D. mensual por activo	*30*	*99,84*	*99,42*	*99,42*	*98,86*

Tabla 13.- Compromisos de Disponibilidad en %.

4.3. Lote 3: Servicios e infraestructuras de comunicaciones satelitales civiles de la I3D

Compromisos relativos a Peticiones de Provisión y Administración

Las Peticiones, tanto de Provisión como de Administración, se clasifican según su prioridad de resolución. Tomando como criterio el concepto de petición de provisión o administración solicitado y la prioridad de la petición, derivada de la urgencia asignada por el MINISDEF, el proveedor del servicio se deberá comprometer a ofrecer, al menos, los siguientes tiempos:

	TIEMPOS DE ACTUACIÓN			
			Tiempo de Cierre (T_{CPI})	
	Acuse de recibo (T_{ACK})	***Tiempo de respuesta (T_{RSP})***	***Urgencia alta (días naturales)***	***Urgencia normal (días naturales)***
CONCEPTO PROVISIÓN SOLICITADO				
Alta de servicio	*2h*	*7d*	*30d*	*45d*
Baja de cualquier servicio	*2h*	*9h*	*7d*	*7d*
Reconfiguración de funcionalidades en una línea, mediante reconfiguración en la infraestructura de red del operador o en el terminal satélite.	*2h*	*9h*	*3d*	*5d*
Reconfiguración de funcionalidades en todas las líneas de una constelación satelital, mediante reconfiguración en la infraestructura de red del operador o en el terminal satélite.	*2h*	*3d*	*10d*	*20d*
CONCEPTO ADMINISTRACIÓN SOLICITADO				
Peticiones Administración	*15m*	*2h*	*12 h*	*2d*
Petición de consultas al adjudicatario	*15m*	*N/A*	*1d*	*5d*

Tabla 14.- Tiempos de actuación para las Peticiones de Provisión y Administración

Los tiempos de las tablas anteriores están siempre expresados en días u horas laborables. Por días laborables se entenderán los comprendidos de lunes a viernes, excluyendo los festivos que afecten a la localidad donde se realice la correspondiente actuación. El horario laboral se establece en la franja de 07:00 a 19:00 a efectos de peticiones de provisión.

Compromisos relativos a Resolución de Incidencias

Para todos los servicios, el adjudicatario del servicio se deberá comprometer a los siguientes niveles de calidad para la Recuperación y Cierre de Incidencias.

- *Tiempo máximo de respuesta ante incidencias:*

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo de respuesta (T_{RSP})***	***Tiempo de recuperación del servicio (T_{RS})***	***Tiempos de Cierre (T_{CPI})***
Prioridad 0	*15m*	*30m*	*2h*	*1d*
Prioridad 1	*20m*	*1h*	*4h*	*2d*
Prioridad 2	*30m*	*1h*	*8h*	*3d*
Prioridad 3	*1h*	*24h*	*5d*	*6d*

Tabla 15.- Compromisos de Tiempo máximo de respuesta ante incidencias

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*
- *Tiempo Máximo de entrega de Informe de Resolución de Incidentes de seguridad:*

Tipo de incidencia	***Tiempo máximo de entrega***
Incidente de seguridad de prioridad 0	*4h*
Incidente de seguridad de prioridad 1	*8h*
Incidente de seguridad de prioridad 2	*2d*
Incidente de seguridad de prioridad 3	*4d*

Tabla 16.- Tiempo Máximo de Entrega de Informes de Resolución de Incidentes de Seguridad

- *El adjudicatario se comprometerá a mantener en todo momento los requisitos de seguridad expuestos en este pliego, debiendo cumplir al menos los siguientes niveles máximos mensuales:*

Parámetro	***Valor Exigido***
Incidencias de seguridad de severidad alta	*0*
Incidencias de seguridad de severidad media	*4*
Incidencias de seguridad de severidad baja	*9*

Tabla 17.- Número máximo de incidencias de seguridad mensuales

Los tiempos de las tablas relativas a la resolución de incidencias no se refieren a días u horas laborales, sino a días u horas naturales, al considerarse que la operación del servicio debe ser mantenida en régimen 24x7x365.

Compromisos relativos a la Disponibilidad

Los valores de disponibilidad que se requieren se han calculado en base a los siguientes escenarios modelo:

Periodo de tiempo (T) en el que se calcula la disponibilidad. El objetivo de disponibilidad se establece como un valor de periodicidad anual, pero se fijan ANS también a nivel mensual.

- *Tiempo de Recuperación del Servicio (TRS). Se tiene en cuenta, en cada caso, el correspondiente al caso de incidencia de severidad alta, aplicable a cada activo considerado.*
- *Nº de caídas en el periodo considerado de activos o sedes según el tipo de Disponibilidad (de activos, sedes o global) considerado.*
- *En la siguiente tabla se indican los valores de Disponibilidad mínimos exigidos (se hace notar que la acumulación de muchas caídas con plazo de recuperación muy corto podría dar lugar a incumplimiento de ANS):*

Disponibilidad requerida en %, según criticidad de activos afectados.	***Periodo T (días)***	***Criticidad (prioridad en caso de incidencia de severidad alta)***			
		Extrema (P=0)	***Alta (P=1)***	***Media (P=1)***	***Baja (P=2)***
D. mensual por línea	*30*	*97,00%*	*96,95%*	*96,9%*	*96%*

Tabla 18.- Compromisos de Disponibilidad en %.

4.4.Lote 4: Servicios e infraestructuras de acceso a Internet de la I3D

Compromisos relativos a Peticiones de Provisión y Administración

*Las **Peticiones,** tanto de Provisión como de Administración, se clasifican según su prioridad de resolución. Tomando como criterio el concepto de petición de provisión o administración solicitado y la prioridad de la petición, derivada de la urgencia asignada por el MINISDEF, el proveedor del servicio se deberá comprometer a ofrecer, al menos, los siguientes tiempos:*

	TIEMPOS DE ACTUACIÓN					
	Acuse de recibo (T_{ACK})	***Tiempo de respuesta (T_{RSP})***	***Tiempo de Cierre (T_{CPI})***			
			Prioridad 0	***Prioridad 1***	***Prioridad 2***	***Prioridad 3***
CONCEPTO PROVISIÓN SOLICITADO						
Servicio de traslado de conexión	*15m*	*3d*	*15d*	*30d*	*40d*	*60d*
Baja de conexión a Internet	*15m*	*9h*	*2d*	*5d*	*10d*	*15d*
Provisión de conexión a Internet (incluye equipamiento y línea)	*15m*	*1d*	*5 d*	*10 d*	*15 d*	*30 d*
Actualización o sustitución de equipamiento	*15m*	*1d*	*1 d*	*2 d*	*4 d*	*8 d*
Peticiones de gestión y monitorización de la conexión a Internet	*15m*	*1h*	*2h*	*4h*	*6h*	*8h*
Petición de diseño técnico	*15m*	*16h*	*5d*	*10d*	*20d*	*30d*
Petición de emisión de informes	*15m*	*1h*	*4h*	*8h*	*2d*	*5d*
Petición de planificación de proyectos	*15m*	*8h*	*5d*	*10d*	*20d*	*30d*
Provisión infraestructuras de obra civil, asociadas a nueva conexión a Internet	*15m*	*5d*	*30 d*	*45 d*	*60 d*	*60 d*
Resto de provisiones	*15m*	*3 d*	*10 d*	*10 d*	*20 d*	*20 d*
CONCEPTO ADMINISTRACIÓN SOLICITADO						
Reconfiguración de equipamiento de conexión a Internet, sin sustitución de equipos o accesos	*15m*	*9h*	*1d*	*3d*	*5d*	*10d*
Reconfiguración de equipamiento de conexión a Internet, con sustitución de equipos y/o accesos	*15m*	*3d*	*15d*	*30d*	*40d*	*60d*
Petición de consultas al adjudicatario	*15m*	*N/A*	*1d*	*3d*	*5d*	*10d*

Tabla 19.- Tiempos de actuación para las Peticiones de Servicio

Los tiempos de las tablas anteriores están siempre expresados en días u horas laborables. Por días laborables se entenderán los comprendidos de lunes a viernes, excluyendo los festivos que afecten a la localidad donde se realice la correspondiente actuación. El horario laboral se establece en la franja de 07:00 a 19:00 a efectos de peticiones de provisión.

Compromisos relativos a Resolución de Incidencias
Para todos los servicios, el adjudicatario del lote se deberá comprometer a los siguientes niveles de calidad para la Recuperación y Cierre de Incidencias.

CONCEPTO INCIDENCIA (sobre activo, sede o servicio)	***TIEMPOS DE ACTUACIÓN***			
	Tiempo de Recuperación del Servicio, (T_{RS})			***Tiempo de cierre(T_{CPI})***
	Prioridad 0	***Prioridad 1***	***Prioridad 2***	
Cualquiera por defecto	*4 h*	*6 h*	*10 h*	*48 h*
Circuito de conexión a Internet	*1 h*	*2 h*	*3 h*	*18 h*
Servicios básicos de red	*4 h*	*6 h*	*8 h*	*48 h*
Herramientas del CGT	*8 h*	*16 h*	*24 h*	*108 h*

Tabla 20.- Tiempos de actuación para Cierre de incidencias

Tiempo Máximo de Respuesta ante Incidencias y Tiempo de notificación proactiva de la incidencia, en función de la prioridad de las mismas:

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo máximo de respuesta (T_{RSP})***
Prioridad 0	*15m*	*30m*
Prioridad 1	*20m*	*1h*
Prioridad 2	*30m*	*2h*

Tabla 21.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*

- *Tiempo Máximo de entrega de Informe de Resolución de Incidentes de seguridad:*

Tipo de incidencia	***Tiempo máximo de entrega***
Incidente de seguridad de prioridad 0	*4h*
Incidente de seguridad de prioridad 1	*8h*
Incidente de seguridad de prioridad 2	*2d*

Tabla 22.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad

El adjudicatario se comprometerá a mantener en todo momento los requisitos de seguridad expuestos en este pliego, debiendo cumplir al menos los siguientes niveles máximos mensuales:

Parámetro	***Valor Exigido***
Incidencias de seguridad de severidad alta	*0*
Incidencias de seguridad de severidad media	*4*
Incidencias de seguridad de severidad baja	*9*

Tabla 23.- Número máximo de incidencias de seguridad mensuales

Los tiempos de las tablas relativas a la resolución de incidencias se refieren a días u horas naturales, debiendo tener en cuenta el horario de atención a incidencias para cada una de las prioridades de las mismas.

Compromisos relativos a la Disponibilidad

Los valores de disponibilidad que se requieren se han calculado en base a los siguientes escenarios modelo:

- *Periodo de tiempo (T) en el que se calcula la disponibilidad. El objetivo de disponibilidad se establece como un valor de periodicidad anual, pero se fijan ANS también a nivel mensual.*
- *Tiempo de Recuperación del Servicio (TRS). Se tiene en cuenta, en cada caso, el correspondiente al caso de incidencia de severidad alta, aplicable a cada activo considerado.*
- *Nº de caídas en el periodo considerado de activos o sedes según el tipo de Disponibilidad (de activos, sedes…) considerado.*
- *Los activos sujetos a disponibilidad son los siguientes:*
    - *Conexiones a Internet, tanto de caudal garantizado y no garantizado.*
    - *Servicios básicos de red.*
    - *Activos de gestión y herramientas del CGT.*

Se hace notar que la acumulación de muchas caídas con plazo de recuperación muy corto podría dar lugar a incumplimiento de ANS.

En la siguiente tabla se indican los valores de Disponibilidad mínimos exigidos:

Disponibilidad requerida en %, según criticidad de activos afectados.	***Periodo T (días)***	***Criticidad (prioridad en caso de incidencia de severidad alta)***			
		Extrema (P=0)	***Alta (P=1)***	***Media (P=1)***	***Baja (P=2)***
D. mensual por activo	*30*	*98,889*	*97,778*	*97,778*	*96,667*
D. mensual por línea	*30*	*99,861*	*99,444*	*99,444*	*98,889*
D. mensual Global	*30*	*99,999*	*99,994*	*99,994*	*99,989*
D. anual por activo	*365*	*98,909*	*97,808*	*97,808*	*96,697*
D. anual por línea	*365*	*99,989*	*99,954*	*99,954*	*99,909*
D. anual Global	*365*	*99,9995*	*99,9982*	*99,9982*	*99,9963*

Tabla 24.- Compromisos de Disponibilidad en %.

4.5.Lote 5: Servicios e infraestructuras de Telemedicina de la I3D

Compromisos relativos a Peticiones de Provisión y Administración

Las Peticiones, tanto de Provisión como de Administración, se clasifican según su prioridad de resolución. Tomando como criterio el concepto de petición de provisión o administración solicitado y la prioridad de la petición, derivada de la urgencia asignada por el MINISDEF, el proveedor del servicio se deberá comprometer a ofrecer, al menos, los siguientes tiempos:

	TIEMPOS DE ACTUACIÓN				
	Acuse de recibo (TACK)	***Tiempo de respuesta (TRSP)***	***Tiempo de Cierre (TCPI)***		
			Prioridad 0	***Prioridad 1***	*Prioridad 2*
CONCEPTO PROVISIÓN SOLICITADO					
Servicio de traslado de Nodo de Telemedicina en Territorio Nacional	*15m*	*3d*	*15d*	*30d*	*40d*
Traslado interno de routers y equipamiento en general que forma parte del servicio	*15m*	*3d*	*5d*	*10d*	*20d*
Baja de cualquier servicio	*15m*	*9h*	*2d*	*5d*	*10d*
Actualización o sustitución de equipamiento	*15m*	*1d*	*1 d*	*2 d*	*4 d*
Implantación y configuración	*15m*	*3d*	*5d*	*10d*	*15d*
Provisión de nuevo Nodo de Telemedicina	*15m*	*3d*	*30 d*	*30 d*	*45 d*
Peticiones de gestión y monitorización de los servicios de Telemedicina	*15m*	*1h*	*2h*	*4h*	*6h*
Petición de retirada de equipamiento	*15m*	*1d*	*10d*	*15d*	*30d*
Petición de diseño técnico	*15m*	*16h*	*5d*	*10d*	*20d*
Petición de emisión de informes	*15m*	*1h*	*4h*	*8h*	*2d*
Petición de planificación de proyectos	*15m*	*8h*	*5d*	*10d*	*20d*
Provisión infraestructuras de obra civil, asociadas a un nuevo Nodo	*15m*	*5d*	*30 d*	*45 d*	*60 d*
Resto de provisiones	*15m*	*3 d*	*10 d*	*10 d*	*20 d*
CONCEPTO ADMINISTRACIÓN SOLICITADO					
Reconfiguración de funcionalidades en un Nodo, sin sustitución de equipos o accesos	*15m*	*9h*	*1d*	*3d*	*5d*
Reconfiguración de funcionalidades de un Nodo, con sustitución de equipos y/o accesos	*15m*	*3d*	*15d*	*30d*	*40d*
Reconfiguración de funcionalidades en red del Operador, o en equipos de cliente, con alcance a todas las sedes o servicios	*15m*	*3d*	*5d*	*10d*	*20d*
Peticiones Administración de servicios de Telemedicina	*15m*	*2h*	*8 h*	*12 h*	*24 h*
Petición de consultas al adjudicatario	*15m*	*N/A*	*1d*	*3d*	*5d*

Tabla 25.- Tiempos de actuación para las Peticiones de Servicio

Compromisos relativos a Resolución de Incidencias
Para todos los servicios, el adjudicatario del lote se deberá comprometer a los siguientes niveles de calidad para la Recuperación y Cierre de Incidencias.

Concepto Incidencia (sobre activo o nodo)	***TIEMPOS DE ACTUACIÓN***			
	Tiempo de Recuperación del Servicio, (T_{RS})			***Tiempo de cierre(T_{CPI})***
	Prioridad 0	***Prioridad 1***	***Prioridad 2***	
Cualquiera por defecto	*72 h*	*96 h*	*120 h*	*140 h*
Herramientas del CGT	*8 h*	*16 h*	*24 h*	*36 h*

Tabla 26.- Tiempos de actuación para Cierre de incidencias

- *Tiempo Máximo de Respuesta ante Incidencias y Tiempo de notificación proactiva de la incidencia, en función de la prioridad de las mismas:*

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo máximo de respuesta (T_{RSP})***
Prioridad 0	*15m*	*30m*
Prioridad 1	*20m*	*1h*
Prioridad 2	*30m*	*2h*

Tabla 27.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*
- *Tiempo Máximo de entrega de Informe de Resolución de Incidentes de seguridad:*

Tipo de incidencia	***Tiempo máximo de entrega***
Incidente de seguridad de prioridad 0	*24h*
Incidente de seguridad de prioridad 1	*48h*
Incidente de seguridad de prioridad 2	*72h*

Tabla 28.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad

- *El adjudicatario se comprometerá a mantener en todo momento los requisitos de seguridad expuestos en este pliego, debiendo cumplir al menos los siguientes niveles máximos mensuales:*

Parámetro	***Valor Exigido***
Incidencias de seguridad de severidad alta	*0*
Incidencias de seguridad de severidad media	*4*
Incidencias de seguridad de severidad baja	*9*

Tabla 29.- Número máximo de incidencias de seguridad mensuales

Los tiempos de las tablas relativas a la resolución de incidencias se refieren a días u horas naturales, debiendo tener en cuenta el horario de atención a incidencias para cada una de las prioridades de las mismas.

Estos tiempos sólo son aplicables en los casos de nodos que se encuentran en Territorio Nacional. Para el resto de nodos que se encuentran fuera del Territorio Nacional., se exigirán los mismos tiempos de respuesta descontando el tiempo de desplazamiento.

Compromisos relativos a la Disponibilidad

Los valores de disponibilidad que se requieren se han calculado en base a los siguientes escenarios modelo:

- *Periodo de tiempo (T) en el que se calcula la disponibilidad. El objetivo de disponibilidad se establece como un valor de periodicidad anual, pero se fijan ANS también a nivel mensual.*
- *Tiempo de Recuperación del Servicio (TRS). Se tiene en cuenta, en cada caso, el correspondiente al caso de incidencia de severidad alta, aplicable a cada activo considerado.*
- *Nº de caídas en el periodo considerado de activos o nodos según el tipo de Disponibilidad (de activos, nodos…) considerado.*

Se hace notar que la acumulación de muchas caídas con plazo de recuperación muy corto podría dar lugar a incumplimiento de ANS.

En la siguiente tabla se indican los valores de Disponibilidad mínimos exigidos:

Disponibilidad requerida en %, según criticidad de activos afectados.	***Periodo***	***Criticidad (prioridad en caso de incidencia de severidad alta)***		
	T (días)	***Extrema (P=0)***	***Alta (P=1)***	***Media (P=1)***
D. mensual por nodo	*30*	*99.861*	*99.444*	*99.444*

Tabla 30.- Compromisos de Disponibilidad en %.

4.6.Lote 7: Servicios e infraestructuras de Videoconferencia Segura de la I3D

Compromisos relativos a Peticiones de Provisión y Administración

Las Peticiones, tanto de Provisión como de Administración, se clasifican según su prioridad de resolución. Tomando como criterio el concepto de petición de provisión o administración solicitado y la prioridad de la petición, derivada de la urgencia asignada por el MINISDEF, el proveedor del servicio se deberá comprometer a ofrecer, al menos, los siguientes tiempos:

	TIEMPOS DE ACTUACIÓN				
	Acuse de recibo (TACK)	***Tiempo de respuesta (TRSP)***	***Tiempo de Cierre (TCPI)***		
			Prioridad 0	***Prioridad 1***	***Prioridad 2***
CONCEPTO PROVISIÓN SOLICITADO					
Baja de cualquier servicio	*15m*	*9h*	*2d*	*5d*	*10d*
Actualización o sustitución de equipamiento	*15m*	*1d*	*1 d*	*2 d*	*4 d*
Implantación y configuración	*15m*	*3d*	*5d*	*10d*	*15d*
Provisión de nuevo nodo de Videoconferencia	*15m*	*3d*	*30 d*	*30 d*	*45 d*
Peticiones de gestión y monitorización de los servicios de Videoconferencia	*15m*	*1h*	*2h*	*4h*	*6h*
Petición de retirada de equipamiento	*15m*	*1d*	*10d*	*15d*	*30d*
Petición de diseño técnico	*15m*	*16h*	*5d*	*10d*	*20d*
Petición de emisión de informes	*15m*	*1h*	*4h*	*8h*	*2d*
Petición de planificación de proyectos	*15m*	*8h*	*5d*	*10d*	*20d*
Resto de provisiones	*15m*	*3 d*	*10 d*	*10 d*	*20 d*
CONCEPTO ADMINISTRACIÓN SOLICITADO					
Reconfiguración de funcionalidades en un Nodo, sin sustitución de equipos o accesos	*15m*	*9h*	*1d*	*3d*	*5d*
Reconfiguración de funcionalidades de un Nodo, con sustitución de equipos y/o accesos	*15m*	*3d*	*15d*	*30d*	*40d*
Peticiones Administración de servicios de Videoconferencia	*15m*	*2h*	*8 h*	*12 h*	*24 h*
Petición de consultas al adjudicatario	*15m*	*N/A*	*1d*	*3d*	*5d*

Tabla 31 .-Tiempos de actuación para las Peticiones de Servicio

Los tiempos de las tablas anteriores están siempre expresados en días u horas laborables. Por días laborables se entenderán los comprendidos de lunes a viernes, excluyendo los festivos que afecten a la localidad donde se realice la correspondiente actuación. El horario laboral se establece en la franja de 07:00 a 19:00 a efectos de peticiones de provisión.

Compromisos relativos a Resolución de Incidencias
Para todos los servicios, el adjudicatario del lote se deberá comprometer a los siguientes niveles de calidad para la Recuperación y Cierre de Incidencias.

CONCEPTO INCIDENCIA (sobre activo, o nodo)	***TIEMPOS DE ACTUACIÓN***		
	Tiempo de Recuperación del Servicio, (T_{RS})		***Tiempo de cierre(T_{CPI})***
	Prioridad 0	***Prioridad 1***	
Cualquiera por defecto	*72 h*	*96 h*	*140 h*
Herramientas de gestión	*8 h*	*16 h*	*36 h*

Tabla 32 .- Tiempos de actuación para Cierre de incidencias

- *Tiempo Máximo de Respuesta ante Incidencias y Tiempo de notificación proactiva de la incidencia, en función de la prioridad de las mismas:*

Prioridad de la incidencia	***Tiempo de notificación proactiva de la incidencia (T_{NOT})***	***Tiempo máximo de respuesta (T_{RSP})***
Prioridad 0	*15m*	*30m*
Prioridad 1	*20m*	*1h*

Tabla 33.- Compromisos de Tiempo Máximo de Respuesta ante Incidencias

- *Tiempo Máximo de Entrega de Informe de Resolución de Incidencia Crítica (TICI): 2 días laborables.*
- *Tiempo Máximo de Entrega de Informe de Resolución de Incidentes de seguridad:*

Tipo de incidencia	***Tiempo máximo de entrega***
Incidente de seguridad de prioridad 0	*24h*
Incidente de seguridad de prioridad 1	*48h*

Tabla 34.- Compromisos de Tiempo Máximo de Entrega ante Incidencias de Seguridad

- *El adjudicatario se comprometerá a mantener en todo momento los requisitos de seguridad expuestos en este pliego, debiendo cumplir al menos los siguientes niveles máximos mensuales:*

Parámetro	***Valor Exigido***
Incidencias de seguridad de severidad alta	*0*
Incidencias de seguridad de severidad media	*4*
Incidencias de seguridad de severidad baja	*9*

Tabla 35.- Número máximo de incidencias de seguridad mensuales

Los tiempos de las tablas relativas a la resolución de incidencias se refieren a días u horas naturales, debiendo tener en cuenta el horario de atención a incidencias para cada una de las prioridades de las mismas.

Estos tiempos sólo son aplicables en los casos de nodos que se encuentran en Territorio Nacional. Para el resto de nodos que se encuentran fuera del Territorio Nacional., se exigirán los mismos tiempos de respuesta descontando el tiempo de desplazamiento.

Compromisos relativos a la Disponibilidad

Los valores de disponibilidad que se requieren se han calculado en base a los siguientes escenarios modelo:

- *Periodo de tiempo (T) en el que se calcula la disponibilidad. El objetivo de disponibilidad se establece como un valor de periodicidad anual, pero se fijan ANS también a nivel mensual.*
- *Tiempo de Recuperación del Servicio (TRS). Se tiene en cuenta, en cada caso, el correspondiente al caso de incidencia de severidad alta, aplicable a cada activo considerado.*
- *Nº de caídas en el periodo considerado de nodos según el tipo de Disponibilidad considerado.*

Se hace notar que la acumulación de muchas caídas con plazo de recuperación muy corto podría dar lugar a incumplimiento de ANS.

En la siguiente tabla se indican los valores de Disponibilidad mínimos exigidos:

Disponibilidad requerida en %, según criticidad de activos afectados.	***Periodo***	***Criticidad (prioridad en caso de incidencia de severidad alta)***	
	T (días)	***Extrema (P=0)***	***Alta (P=1)***
D. mensual por nodo	*30*	*99.861*	*99.444*

Tabla 36.- Compromiso de Disponibilidad en %»