

Análisis de Riesgos de la Red de Asistencia al Personal (RAP) del Ministerio de Defensa

Autor: Alvarez Lanzarote, David

Director/es: López Román, Iago y Nocelo López, Rubén.

Contacto: dalvalan@hotmail.com, lanzarote@et.mde.es

Resumen:

El proyecto de Red de Asistencia al Personal comienza en el año 2018 con el fin de proporcionar un acceso a Internet de calidad y protegido al personal de nuestras Fuerzas Armadas tanto en instalaciones militares en territorio nacional, como cuando está participando en las distintas misiones en el exterior.

Estos servicios de Internet seguro se proporcionan principalmente en emplazamientos donde existen dificultades para acceder por otros medios, o las situación de seguridad de la zona así lo aconseja. Por ello, una de sus premisas de diseño inicial es la seguridad y protección de los servicios proporcionados. De este modo, se contribuye a la propia seguridad de las operaciones y del personal militar desplegado en el exterior. Para conseguirlo, todo el tráfico de navegación y servicios de valor añadido pasan primero por una infraestructura central de gestión y supervisión centralizada del sistema ubicada en CESTIC (Madrid) antes de conectarse a Internet a través de una serie de dispositivos y mecanismos de seguridad.

En la actualidad, esta infraestructura de comunicaciones se extiende desde el Nodo Central de Gestión en el CESTIC hasta las principales misiones de las Fuerzas Armadas españolas en el exterior, buques de la Armada, y cerca de 250 bases, acuartelamientos y arsenales militares dentro del Territorio Nacional con el fin principal de mejorar la calidad de vida del personal alojado en los mismos.

Si bien, como se ha dicho, una de las premisas de diseño de toda las TIC de este sistema es la de la seguridad, todavía no se ha realizado un análisis de riesgos de este, ni dispone de un plan de tratamiento de riesgos, ni una declaración de aplicabilidad (SOA). Sin embargo, por la complejidad y extensión de esta red, el presente documento se ceñirá en el análisis de riesgos.

Es por ello por lo que el trabajo, además de su utilidad académica, se considera de utilidad práctica de cara a la evolución y mejora del sistema.

Palabras clave: RAP, ENS, MAGUERIT, PILAR, SEGURIDAD

1. Introducción

Una de las premisas principales del diseño de la Red de Asistencia al Personal del Ministerio de Defensa, es precisamente la garantizar unas condiciones de seguridad en el uso de Internet por el personal militar que está desempeñando sus cometidos en las distintas misiones de las Fuerzas Armadas en el exterior. Así pues, la seguridad es un aspecto que se ha tenido en cuenta de forma constante desde su concepción. Sin embargo, esta red es un tanto peculiar en el sentido de que, tratándose de una red corporativa de Ministerio de Defensa, por su naturaleza, función y tipo de interconexión con Internet, puede procesar información sin clasificar de USO PÚBLICO exclusivamente.

No obstante, y de acuerdo con lo especificado en el artículo 2 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad [1], se trata de un sistema de información del Ministerio de Defensa, por lo que se considera que se aplica a pesar de que no trata información clasificada, pero que precisa adoptar medidas complementarias de seguridad, específicas para dicho sistema.

Dado el interés que despertó en mí la materia de “Gestión de la seguridad y análisis de riesgos” del presente Máster, la consideré de mucha utilidad para los cometidos que estaba desempeñando por entonces en el CESTIC como responsable del contrato por el que se había iniciado en 2018 el Proyecto de la Red de Asistencia al Personal Militar en Zona de Operaciones (SAPZO), una de las dos partes principales de la infraestructura que pasó a denominarse Red de Asistencia al Personal (RAP) del Ministerio de Defensa.

2. Desarrollo

El trabajo se ha desarrollado siguiendo la siguiente secuencia:

- (a) Recopilación de información referente a la RAP: para ello ha sido necesario estudiar todos los detalles de diseño y arquitectura de este sistema de información. Asimismo, se ha entrevistado a personal responsable de su gestión y administración de seguridad con la finalidad de conocer detalles de su evolución, estado actual para valorar la madurez de la seguridad de este, y planificar si futuro desde el prisma de la seguridad.
- (b) Estudio de la normativa en vigor, empezando por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad [1], y documentación referente a MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [2]. También las principales guías CCN-STIC relacionadas con la aplicación del ENS.
- (c) Obtención, instalación y estudio del manejo de la aplicación PILAR del CCN, destinada a llevar a cabo todo el proceso de análisis y gestión de riesgos que permite dicha herramienta. También fue preciso mantener una reunión con personal conocedor de la herramienta para recibir consejos prácticos sobre su uso.
- (d) Carga de información en el sistema siguiendo el proceso lógico de un análisis de riesgos.
- (e) Analizar los resultados obtenidos tras completar este proceso de análisis y gestión de riesgos.
- (f) Extraer todas las conclusiones como consecuencia del trabajo realizado identificando aquellos aspectos en los que se podría seguir trabajando para mejorar y ampliar el TFM.

2.1 Descripción de la Red de Asistencia al Personal del Ministerio de Defensa

Los servicios de asistencia al personal tienen por finalidad mejorar la conectividad a Internet del personal en las zonas de vida de las Bases, Acuartelamientos y Establecimientos militares (BAE) del Ministerio de Defensa.

En ningún caso se trata del acceso mediante tecnología WiFi a una red corporativa. De hecho, de acuerdo con la arquitectura prevista, la infraestructura está caracterizada por la separación física (air gap) de esta infraestructura de cualquier otra infraestructura de red del emplazamiento.

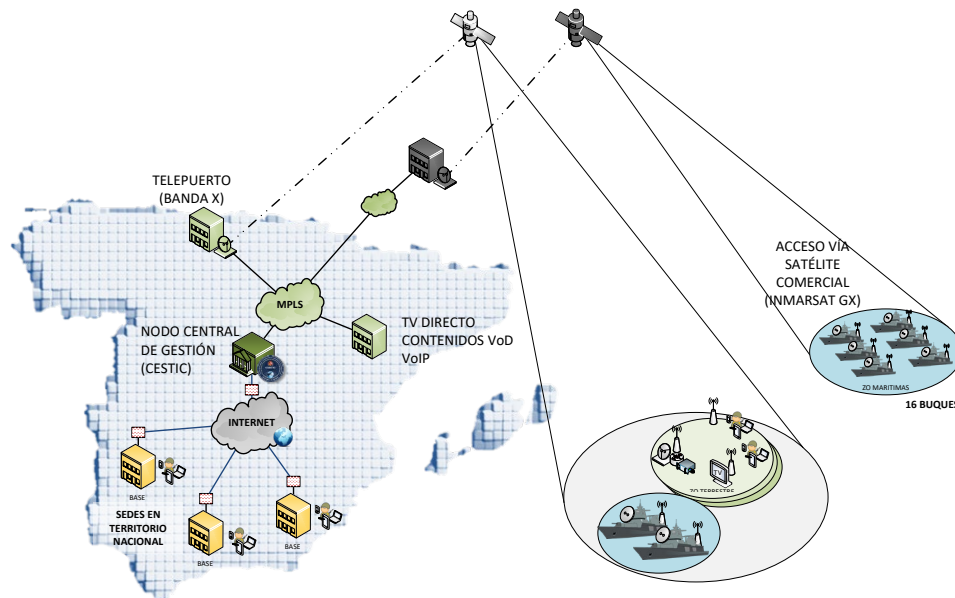


Figura 1: alcance de la Red de Asistencia al Personal del MDEF

Dichos servicios se proporcionan sobre la infraestructura hardware y software de la Red de Asistencia al Personal (RAP). La misma aúna dos infraestructuras distintas como consecuencia de los dos entornos operativos en los que se despliega que llevan asociados unos requisitos de seguridad diferentes.

- (a) El **Sistema de Asistencia al Personal Militar desplegado en Zona de Operaciones (SAPZO)**. Abarca bases terrestres en operaciones en el exterior, y buques de la Armada que participan en distintas misiones internacionales.

Por la naturaleza de estos escenarios, es muy probable sea difícil disponer de un acceso a Internet de calidad y que garantice unas condiciones mínimas de seguridad teniendo en cuenta el riesgo que puede suponer el uso de infraestructura de telecomunicaciones locales. Además del acceso protegido a Internet, se proporcionan otros servicios de valor añadido con el fin de mejorar las condiciones de vida del personal desplegado:

- Una serie de canales de TV en directo con una parrilla de contenidos exclusiva para el Ministerio de Defensa.
- Unos contenidos de entretenimiento, principalmente películas y series de actualidad, así como cursos de idiomas, a los que se puede acceder bajo demanda.
- Un servicio de telefonía IP con numeración geográfica española, con la finalidad de facilitar el contacto con familiares y facilitar la realización de gestiones administrativas privadas desde la distancia.

Todos estos servicios se proporcionan sobre una infraestructura de telecomunicaciones exclusiva para este sistema para así maximizar la confidencialidad y disponibilidad de las comunicaciones privadas. El enlace entre sedes remotas y el CESTIC se hace vía satélite gubernamental en banda X, lo que permite una mejor conectividad en los principales buques de la Armada al aprovechar el excedente de capacidad que tienen los terminales navales de mayor tamaño. En el caso de que el terminal en banda X embarcado tenga menos prestaciones, se recurre a un acceso a vía satélite comercial de alta velocidad en banda Ka civil Inmarsat Global Express (IGX).

- (b) La **Red WiFi de Asistencia al Personal Militar en Territorio Nacional (RAPNA)**. En este caso, sin dejar de lado el aspecto de seguridad, el objetivo es básicamente el de poder proporcionar un acceso a Internet al personal en las zonas de descanso y vida de las bases, acuartelamientos y arsenales. La complejidad en este caso se encuentra en el número de usuarios, actualmente cerca de 50.000, lo que requiere una alta exigencia en términos de disponibilidad del sistema].

Aunque en el momento de creación de las dos redes en 2018, estas se concibieron como dos dominios diferenciados en cuanto a arquitectura de red y servicios proporcionados, enseguida se interconectaron sus infraestructuras en un único nodo central de gestión, ubicado en las instalaciones del CESTIC, en Arturo Soria, donde se lleva a cabo una gestión integral de todo el sistema.

Tras más de tres años en funcionamiento y constante evolución y mejora de su arquitectura, antes de acometer el análisis de riesgos del sistema, ya se intuía que había un alto grado de madurez en la seguridad del sistema como consecuencia de que en este tiempo se ha puesto en funcionamiento:

- Un equipo de personas responsables de la gestión y administración del sistema.
- Un centro de atención al usuario incluyendo una Instrucción Operativa para Gestión de Incidencias y Peticiones de la RAP (IOP) [3] a través del Sistema de Gestión de Peticiones e Incidencias (SCANS) ya implantado en CESTIC para abordar todos los aspectos de atención de los usuarios de los distintos sistemas de su responsabilidad.
- Una normativa detallada de gestión de todo el sistema en todos los aspectos: operativos, logísticos, de formación. [4]
- Se han realizado varias auditorías de seguridad en distintas sedes tanto en la geografía española, como en bases en zona de operaciones y buques. Las vulnerabilidades observadas se han ido corrigiendo de forma progresiva.
- Se dispone de la financiación necesaria para contratar todos los servicios de soporte necesarios, así como para incorporar personal externo para reforzar al equipo responsable de la administración del sistema.
- Periódicamente se imparten cursos de formación y actualización de conocimientos adaptados a las particularidades del personal que ocupa puestos relacionados con la administración, gestión y supervisión del sistema de distintas partes de la infraestructura de la RAP.

2.2 El proceso de análisis de riesgos

Este proceso comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del

riesgo. De este modo, nos permitirá determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema de información analizado, e implantar sus salvaguardas o contramedidas.

La RAP es un sistema de información del MDEF, y como tal se le debe aplicar el Marco Operacional del ENS, constituido por las medidas a tomar para proteger la operación de dicho sistema como conjunto integral de componentes con la finalidad de facilitar un acceso a Internet al personal del Ministerio dentro de sus instalaciones, tanto en TN como en ZO.

Para poder medir el nivel de cumplimiento del ENS, como se ha expresado anteriormente, se hará uso de la aplicación PILAR del CCN, que siguiendo la metodología Magerit [2], nos ayuda a la adecuación de dicho nivel de cumplimiento. Una vez que se analizan las dimensiones de seguridad de la RAP, en el siguiente paso se abordará una Evaluación de Riesgos, una Declaración de Aplicabilidad (las medidas que se deberán tener en cuenta) y el Perfil de Cumplimiento que especificará la configuración de seguridad de las medidas incluidas en la Declaración de Aplicabilidad.

Pero antes que nada es preciso identificar la categoría de la RAP dentro del ENS valorando el impacto que tendría un incidente que afecte a la seguridad de la información y el propio sistema. Para determinarlo, hay que tener en cuenta las dimensiones de la seguridad¹ de sus activos, principalmente los esenciales que suelen ir asociados a la información y servicios del sistema. Tras el proceso que se describe en detalle en el TFM se llega a la conclusión de que la RAP se trata de un sistema de información de categoría MEDIA, lo que, de acuerdo con el anexo II del ENS 2022 [1], nos impone la aplicación de unos controles de seguridad concretos. Entre otros, la necesidad de realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. No obstante, en el TFM se ha realizado un análisis formal con la finalidad principal de conocer mejor las posibilidades que ofrece la herramienta.

Tras seguir una secuencia de carga de información guiados por la herramienta, llegaremos a los primeros resultados que reflejan el índice de madurez del sistema en las distintas fases que hemos marcado en el proyecto (inicial en el momento que se pusieron en servicio las primeras sedes en Octubre de 2019 con una infraestructura precaria, actual, fechado en diciembre de 2022, y objetivo, estableciendo en diciembre de 2025 la fecha tope de duración del contrato en vigor).

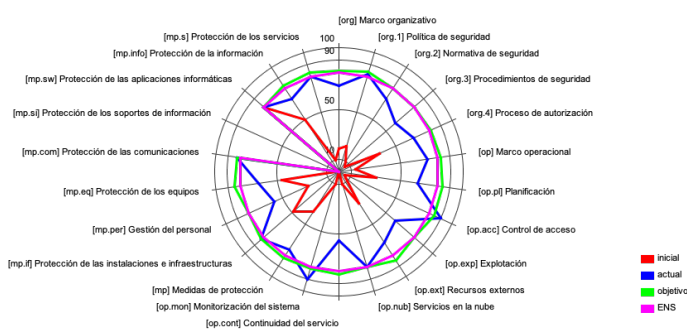


Figura 2: nivel de aplicación de las medidas de seguridad

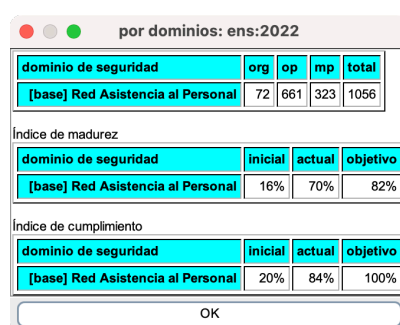


Figura 3: índice de madurez y de cumplimiento del ENS del sistema

En la imagen se aprecia que actualmente, línea azul, hemos aplicado medidas de seguridad incluso por encima del nivel exigido por el propio ENS porque así lo he considerado necesario. Del mismo

¹ Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T], en adelante [DICAT]

modo, ya nos orienta hacia qué controles y tipos de protección debemos dedicar el esfuerzo por incrementar la seguridad del sistema.

3. Resultados y discusión

Llegados al apartado de informes, la herramienta facilita algunos que he encontrado de mucha utilidad como es el de Valoración del cumplimiento del anexo II del ENS en el que se refleja la valoración de cada uno de los controles que son de aplicación de acuerdo con la declaración de Aplicabilidad que hemos obtenido en el paso previo.

Para cada uno de ellos incluye un gráfico de rosa de los vientos que facilita la identificación de las medidas de seguridad que requieren mayor atención para alcanzar el nivel especificado por el ENS para el sistema, además de reflejar la evolución de la seguridad desde las fases previas del proyecto.

Como consecuencia de un análisis detallado del mismo, se llegan a identificar aquellas medidas de seguridad reflejadas en el punto siguiente, las cuales requieren de especial atención para mitigar el impacto y riesgo de las amenazas.

4. Conclusiones

A partir de los resultados obtenidos del análisis de seguridad, se observa que la RAP goza de buena salud desde el punto de vista de la seguridad, teniendo siempre en consideración de que se trata de un sistema ENS Medio como consecuencia de la valoración de sus activos e información a proteger.

Pero este grado de madurez no es fortuito, sino que, de forma indirecta, y gracias a la experiencia previa en el despliegue de sistemas de naturaleza similar, se habían exigido al contratista requisitos de seguridad que precisamente se encuentran recogidos dentro del conjunto de medidas de seguridad exigidas por el ENS 2022.

No obstante, con ocasión del comienzo del nuevo contrato de servicios de la RAP que entró en vigor en diciembre 2022, con una duración máxima de tres años, se deberán aplicar las medidas de seguridad que se han identificado en el apartado 8.1.3 de este TFM.:

- (a) En relación con los Procedimientos de Seguridad, en la Norma de Gestión de la RAP [5] se incluirá un nuevo anexo con este mismo título en el que se refleje:
 - a. Cómo identificar y reportar comportamientos anómalos.
 - b. La forma en que se ha de tratar la información relativa a la gestión de la RAP, precisando cómo efectuar su control de acceso, almacenamiento, la realización de copias, el etiquetado de soportes, su transmisión telemática empleando la herramienta de seguridad EP880 y cualquier otra actividad relacionada con dicha información.
 - c. En la misma Norma de Gestión, se establecerá un proceso formal de autorizaciones que cubra todos los elementos de la RAP abarcando la entrada de equipos, aplicaciones en producción, así como el establecimiento de enlaces de comunicaciones con otros sistemas.
- (b) Sobre la base de la información introducida en la aplicación PILAR para la elaboración del análisis de riesgos objeto de este TFM, se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida.
- (c) Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

- (d) Se contratarán servicios de comunicaciones vía satélite LEO (por ejemplo, Starlink, con la que ya existe contacto) como vía alternativa y de alta capacidad a la comunicación vía satélite que da soporte a la comunicación. Ello mejorará la supervivencia del sistema a la vez que tendrá un impacto muy positivo en la experiencia de uso del sistema.
- (e) Se deberá redactar un documento de descripción de los deberes y responsabilidades en materia de seguridad de cada puesto de trabajo asociado a la RAP.
- (f) Por parte del responsable de seguridad del sistema, periódicamente se impartirán charlas de concienciación al personal administrador del sistema acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.
- (g) Del mismo modo, se distribuirá de forma periódica entre los usuarios de la RAP y se hará difusión formal del tríptico ya existente elaborado para dar a conocer los servicios de la RAP, uso básico, deberes y responsabilidades, así como concienciación sobre buen uso de los servicios de Internet, y en especial de las redes sociales.
- (h) Se potenciará la formación al personal administrador del sistema en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, tales como la configuración de los sistemas que forman parte de la RAP.

4.1 Sobre la aplicación PILAR

Se trata de una aplicación muy potente a la vez que muy compleja que necesita de muchas horas de trabajo y experiencia para maximizar su rendimiento. A pesar de ello, hace mucho más asequible y simplifica la aplicación de la metodología Magerit tal como propugna el ENS 2022.

Considero que se trata de una herramienta fundamental para quién que desempeñe cometidos relacionados con la seguridad de las TIC, si bien requiere de mucha formación previa y conocer consejos y recomendaciones acerca de su uso por parte de personal experto.

Para mantener un proceso continuo de mejora de este sistema de información en cuestión, se deberán hacer revisiones periódicas del análisis de riesgos realizado, verificando que se estén aplicando correctamente las salvaguardas y medidas de seguridad que se habían identificado en fases anteriores.

4.2 Líneas futuras

Además de las medidas de seguridad propuestas en el apartado anterior, al tratarse de un sistema de categoría ENS Media, deberá llevarse a cabo una auditoría para la certificación tal como se expresa en el artículo 38 del ENS 2022 [1].

Además, se deberán programar las auditorías de seguridad previstas en el artículo 31 del ENS 2022, entre las que debe incluirse la del nodo central de gestión, todavía pendiente.

Por parte del autor, y con el fin anterior de elaborar el análisis de riesgos que se ha identificado que es necesario acometer, se cederán a CESTIC/DISEGINFO todos los archivos y documentación empleados para la elaboración de este TFM.

Referencias:

- [1] Ministerio de Asuntos Económicos y Transformación Digital, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 2022.
- [2] Ministerio de Hacienda y Administraciones Públicas, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método,» 2012. [En línea]. Available: <https://pilar.ccn-cert.cni.es/index.php/docman/documentos/1-magerit-v3-libro-i-metodo>. [Último acceso: 09 12 2022].
- [3] CESTIC, Instrucción Operativa para Gestión de Incidencias y Peticiones de la RAP, 2020.
- [4] CESTIC, NORMA 03/21 de Gestión de la Red WIFI de Asistencia al Personal, 2022.