Universidad Zaragoza
1542

Trabajo Fin de Grado

Integración de diferentes dominios de seguridad: aplicación en sistemas militares

Autor

CAC. Eloy Fernández Rodríguez

Directores

Director académico: Dra. Dña. Lacramioara Dranca
Director militar: Cap. D. Javier Fernández González

Centro Universitario de la Defensa-Academia General Militar

2020

-Página intencionadamente en blanco-

Agradecimientos

Quisiera agradecer, en primer lugar, a los directores de mi trabajo, la Doctora Lacramioara Dranca y el Capitán Javier Fernández González, por el tiempo que me han dedicado, por su paciencia, y por su ayuda inestimable durante toda la realización del trabajo, sin la cual finalizar esta memoria no habría sido posible.

En segundo lugar, a los distintos entrevistados que colaboraron para que la realización de este trabajo fuera más fácil y a todos los miembros de la Compañía de Transmisiones nº7 por su apoyo incondicional desde mi llegada a la unidad para realizar las prácticas, especialmente al Sargento Jaime Domínguez Muñoz, el cual de forma desinteresada me ayudó con el trabajo siempre que lo necesité.

Por último, quería dar las gracias a mi familia y a mis compañeros y amigos por su apoyo constante durante estos cinco años, apoyo sin el cual me hubiera sido imposible superar todos los obstáculos que surgieron en el camino. Agradecer especialmente a mi madre, donde sea que esté, ya que ha sido la motivación permanente que me ha impulsado a intentar ser mejor cada día, y a mi padre, el mejor ejemplo de superación y entereza que he podido tener.

-Página intencionadamente en blanco-

Resumen

En la sociedad contemporánea en la que vivimos se hace impensable prescindir de las tecnologías de la información y la comunicación. Entre otras muchas utilidades, destaca la capacidad de comunicarse con cualquier persona en cualquier lugar del mundo en tiempo real y la posibilidad de transmitir información (noticias, contenido audiovisual, redes sociales…) de forma instantánea. Sin embargo, no todo son ventajas en la era digital, ya que toda esta gran red que ofrece casi infinitas capacidades también posee vulnerabilidades. Debido a ello en los últimos años se ha tornado fundamental la protección de datos tanto personales, como gubernamentales o empresariales.

En el ámbito de las Fuerzas Armadas y concretamente en el Ejército de Tierra, esta protección es vital, debido a la sensibilidad de algunos de los datos que se manejan en los sistemas de información militares. El extravío de estos datos podría poner en peligro la seguridad de las unidades, de las instalaciones o incluso, la seguridad nacional. Fruto de los rápidos cambios tecnológicos de los últimos años y de la necesidad de proteger la información, el Ejército desarrolló en 2015 (y actualizó en 2017) un plan de modernización de los sistemas de mando, control y comunicaciones. Mediante este plan pretende, entre otras medidas, que los sistemas de información para el mando y control trabajen en dominios de seguridad distintos, es decir, que un sistema no reciba información de otro que se encuentre en un dominio con información más sensible, sino que reciba únicamente la que le corresponde a su nivel.

Los sistemas de información de mando y control no funcionan de forma aislada, sino que intercambian información entre ellos. Debido a ello, si se acreditan con una clasificación de seguridad (RESERVADO, DIFUSIÓN LIMITADA, etc.), para permitir ese intercambio se requiere una solución para integrar los dominios de seguridad y garantizar así la seguridad de esas transmisiones. Esto es así porque las pasarelas que se emplean actualmente en los sistemas de información militares no cumplen con los estándares del Centro Criptológico Nacional (CCN), recogidos en las guías de seguridad de las tecnologías de la información y las comunicaciones (STIC).

Los sistemas de información de mando y control principales que se utilizan en el Ejército de Tierra son: el Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET), que se opera en los puestos de mandos de brigada, y el Battlefield Management System (BMS), que se utiliza en los batallones, estos sistemas intercambian información a través de dos pasarelas, las cuales, no permiten integrar los dominios de seguridad en caso de que se acrediten los sistemas.

Este trabajo, por lo tanto, se ha enfocado en encontrar una solución que permita la integración de los dominios de seguridad de los dos sistemas anteriormente mencionados, motivado por el plan de modernización, por la arquitectura de referencia de seguridad de los CIS (sistemas de información y telecomunicaciones) desplegables, así como por las guías del CCN. El objetivo principal es por tanto encontrar la mejor alternativa posible, pero también que la solución sea acreditable por el Centro Criptológico Nacional, así

como que el trabajo sea de utilidad para una posible adquisición por parte del Ejército de Tierra.

Para poner en práctica estos objetivos, se ha seguido una metodología de búsqueda de información por diversos medios: inicialmente se adquirió una base teórica a través de manuales y documentación relacionada con el trabajo, posteriormente se realizaron búsquedas específicas en bases de datos y motores de búsqueda (tanto civiles como militares), tras ello se realizaron diversas entrevistas tanto a personal civil como militar y se contactó con empresas del sector (por correo electrónico y por videoconferencias) para obtener información más concreta.

Según se iba recopilando toda la información se iba analizando y extrayendo aquella que era interesante para la resolución del problema planteado. Tras este proceso se encontraron diversas soluciones que podrían ser de utilidad para la integración de dominios de seguridad entre BMS y SIMACET (otras soluciones se descartaron durante el proceso), que fueron: diodos de datos, security guards, transporte físico de la información y pasarelas de intercambio seguro. Posteriormente se realizó una comparativa entre las tres primeras soluciones, ya que en el escenario que se planteó, que era un dominio con SIMACET RESERVADO y otro con BMS SIN CLASIFICAR (escenario prioritario según la arquitectura de referencia de seguridad de las CIS), las pasarelas no eran válidas.

De la comparativa se concluyó que la mejor solución era implementar un diodo de datos, se comparó entre dos modelos: el PSTdiode de la empresa Autek Ingeniería y el ELIPS-SD de Thales, de los cuales el primero se impuso como mejor opción, debido, entre otras razones, a que se trata de una empresa española (fomenta la industria de defensa), se ha probado con éxito en ejercicios y experimentos y está acreditado por el CCN. Una vez encontrada la solución, se propone un método para implementar el PSTdiode en el puesto de mando de una brigada. En esta propuesta se especifican cómo se solucionarían los distintos requerimientos que tiene la instalación segura del diodo, para que este pueda transmitir datos tácticos (unidades, líneas tácticas, instalaciones y obstáculos) entre BMS y SIMACET.

Finalmente, se exponen las conclusiones y se proponen dos posibles líneas de trabajo futuras que se detectaron durante la realización del trabajo: búsqueda de una solución para un escenario con dominios de SIMACET RESERVADO y BMS DIFUSIÓN LIMITADA y otra línea de adquisición/desarrollo de firewall seguros para el Ejército de Tierra.

Con la realización de este trabajo se proporciona una solución certificada y viable para integrar los dominios de seguridad entre SIMACET y BMS en el escenario planteado, además de un método para implementar esta solución en las unidades. La resolución de este hito para el Ejército de Tierra es primordial, para que las brigadas dispongan de unos medios adecuados con los que prepararse en territorio nacional, pero que también puedan cumplir las misiones internacionales que se les encomienden con las garantías de seguridad de la información necesarias en el siglo XXI.

Abstract

In today's society, it is unthinkable to dispense with information and communication technologies. Some of the biggest advantages are the ability to communicate with anyone anywhere in the world in real time and the possibility of transmitting information (news, audio-visual content, social networks...) instantly. However, not all are advantages in the digital age, since all this great network that offers almost infinite capacities also has vulnerabilities. Due to this, in recent years the protection of personal, government or business data has become essential.

In the Armed Forces and specifically in the Army, this protection is vital, due to the sensitivity of some of the data handled in military information systems. The loss of this data could endanger the security of the units, as well as the military bases or even the national security. As a result of the rapid technological changes in recent years and the need to protect information, the Army developed in 2015 (and updated in 2017) a plan to update the command, control, and communications systems. Through this plan, the intent, among other measures, is for the information systems for command and control to work in different security domains, that is, that a system does not receive information from another that is in a domain with more sensitive information, but rather receive only the one that corresponds to its level.

Command and control information systems do not operate in isolation, but rather exchange information between them. Because of this, if they are accredited with a security classification (NATO SECRET, NATO RESTRICTED, etc.), to allow this exchange a solution is required to integrate the security domains and thus guarantee the security of those transmissions. This is due to the gateways that are currently used in military information systems not complying with the standards of the "Centro Criptológico Nacional" (CCN), collected in the information and communications technology security guides (STIC).

The main command and control information systems used in the Army are: the "Sistema de Información para el Mando y Control del Ejército de Tierra" (SIMACET), which is operated at the brigade command posts, and the Battlefield Management System (BMS), which is used in the battalions. These systems exchange information through two gateways, which do not allow the integration of security domains in case the systems are accredited.

This work has focused on finding a solution that allows the integration of the security domains of the two aforementioned systems, motivated by the modernization plan, by the security reference architecture of the CIS (communication and information systems), as well as the CCN guides. The main objective is therefore to find the best possible alternative, but also that the solution is creditable by the CCN, as well as that the work is useful for a possible acquisition project by the Army.

To put these objectives into practice, a methodology of searching for information by various means has been followed: initially a theoretical base was acquired through manuals and documentation related to the work, later specific searches were carried out in databases and search engines (both civilian and military), after which various interviews were conducted with both civilian and military personnel and companies in the sector were contacted (by email and videoconferences) to obtain more specific information.

While collecting the information, the most interesting for solving the problem was being analysed and extracted. After this process, various solutions were found that could be useful for the integration of security domains between BMS and SIMACET (other solutions were discarded during the process), which were: data diodes, security guards, physical transport of information and gateways of secure exchange. Subsequently, a comparison was made between the first three solutions, since in the scenario that was proposed, which was a domain with NATO SECRET SIMACET and another with NATO UNCLASSIFIED BMS (priority scenario according to the security reference architecture of the CIS), the gateways they were not valid.

From the comparison, it was concluded that the best solution was to implement a data diode, it was compared between two models: the PSTdiode from the company Autek Ingeniería and the ELIPS-SD from Thales, of which the first was imposed as the best option, due to, among other reasons, it is a Spanish company (it promotes the defense industry), it has been successfully tested in exercises and experiments and it is accredited by the CCN. Once the solution is found, a method is proposed to implement the PSTdiode at the command post of a brigade. This proposal specifies how the different requirements of the safe installation of the diode would be solved, so that it can transmit tactical data (units, tactical lines, facilities, and obstacles) between BMS and SIMACET.

Finally, the conclusions are presented and two possible future lines of work that were detected during the work are proposed: search for a solution for a scenario with NATO SECRET SIMACET domains and NATO RESTRICTED BMS and another line of a make or buy project of secure firewalls for the Army.

With the completion of this work, a certified and viable solution is provided to integrate the security domains between SIMACET and BMS in the proposed scenario, as well as a method of implementing this solution in the units. The resolution of this milestone for the Army is essential, so that the brigades have adequate means with which to prepare in national territory, but also that they can fulfil the international missions that are entrusted to them with the guarantees of information security necessary in the 21st century.

Índice

Índice de Figuras

Índice de Tablas

-Página intencionadamente en blanco-

Lista de abreviaturas, siglas y acrónimos

Se han elaborado dos columnas, una en español y otra en inglés. Hay abreviaturas que aparecen en ambas columnas, esto es debido a que se pueden encontrar en los libros o en la documentación tanto de una forma como de otra.

Siglas	**Español**	**Inglés**
BDT	Base de Datos Táctica	
BMS		Battlefield Management System
C2IS	Sistemas de información para el mando y control	Command Control and Information System
CCEAL		Common Criteria Evaluation Assurance Level
CCN	Centro Criptológico Nacional	
CENTAUR		Cross-domain Enterprise All-source User Repository
CIS	Sistemas de información y telecomunicaciones	Communications and Information Systems
COE	Entorno Operativo Común	Common Operating Environment
DMZ	Zona desmilitarizada	Demilitarized Zone
DPP	Dispositivo de Protección de Perímetro	
EDT	Estructura de Desglose de Trabajos	
EEUU/US	Estados Unidos	United States
ET	Ejército de Tierra	Army
FTP		File Transport Protocol
FTPS		File Transport Protocol Secure
GPS		Global Positioning System
GU	Gran Unidad	
GUL	Gran Unidad Ligero	
HF		High Frequency
IDT	Interfaz de Datos Táctica	
IFTS		ISAF Force Tracking System
IP		Internet Protocol
ISAF	Fuerza Internacional de Asistencia para la Seguridad	International Security Assistance Force
ISR		Intelligence, Surveillance, and Reconnaissance

JCISAT	Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica	
MAC		Media Access Control
MALE	Mando de Apoyo Logístico del Ejército	
NFFI	Información Fuerza Amiga OTAN	NATO Friendly Force Information
OSI		Open System Interconnection
OTAN/NATO	Organización del Tratado del Atlántico Norte	North Atlantic Treaty Organization
PMBOK		Project Management Body of Knowledge
PMI		Project Management Institute
PU	Pequeña Unidad	
PUT	Pequeña Unidad Táctica	
RSA	Responsable de Seguridad de Área	
SC2NET	Sistema de Mando y Control Nacional del Ejército de Tierra	
SECARQINT	Sección de Arquitectura e Interoperabilidad	
SEGINFOSIT	Seguridad de la Información en los Sistemas de Información y Telecomunicaciones	
SFTP		Secure File Transfer Protocol
SI/IS	Sistema de Información	Information System
SIMACET	Sistema de Información para el Mando y Control del Ejército de Tierra	
SMB		Server Message Block
SMTP		Simple Mail Transfer Protocol
SPP	Sistema de Protección de Perímetro	
STIC	Seguridad de las Tecnologías de la Información y la Comunicación	
TASO		Terminal Area Security Officer
TCP		Transmission Control Protocol
TI/IT	Tecnologías de la Información	Information Technology
TIC	Tecnologías de la Información y las Comunicaciones	
UDP		User Datagram Protocol
UE/EU	Unión Europea	European Union
VHF		Very High Frequency

Capítulo 1. Introducción

1.1 Antecedentes y motivación

De unos años a esta parte, las Fuerzas Armadas de la mayoría de los países han ido evolucionando para aprovechar las ventajas de los nuevos sistemas de telecomunicaciones y los sistemas de información, con el objetivo de hacer más eficiente el mando y control de las operaciones militares. En este sentido el Ejército de Tierra (ET) desarrolló el Plan de Modernización de los Sistemas de Mando, Control y Comunicaciones del ET (Plan MC3 [18]). En este plan, el cual abarca numerosas medidas, se da especial importancia a los sistemas de información y a la seguridad de éstos. Los dos sistemas de información para el mando y control principales en el Ejército de Tierra son: BMS (Battlefield Management System) y SIMACET (Sistema de Información para el Mando y Control del Ejército de Tierra), son los sistemas en los que se enfocará este trabajo de fin de grado.

El plan MC3 anteriormente mencionado tenía como horizonte temporal el año 2021. Sin embargo, debido principalmente a problemas presupuestarios [17], en el año 2017 se redactó el Plan de Transición al MC3 del ET, el cual prevé realizar una serie de medidas temporales antes de alcanzar la situación prevista en el plan MC3 inicial.

En el punto 6.3 de ese plan de transición, se abarca el apartado de la seguridad. En ese apartado se plantean tres[1] dominios de seguridad (se profundizará en el capítulo de conceptos previos) distintos:

- Sin Clasificar: para el acceso a redes civiles y militares, nacionales y OTAN (Organización del Tratado del Atlántico Norte).
- Difusión Limitada de Misión: en pequeñas unidades (batallón e inferiores), donde se emplean medios radio y sistemas C2IS (Command Control and Information System). Sería el caso de BMS.
- Reservado Nacional de Misión: para puestos de mando de gran unidad (brigada y superiores) que disponen de SIMACET y medios de telecomunicaciones de mayor ancho de banda.

En este sentido, según la Entrevista 3, pregunta {6}, la cual se encuentra en el Anexo A, SIMACET tiene que acreditarse como RESERVADO y BMS como DIFUSIÓN LIMITADA. Sin embargo, la interconexión entre estos dominios no es posible actualmente, debido a que no se dispone de los dispositivos necesarios (según recoge el Plan de Transición al MC3), problema que debe solucionarse mediante la instalación de dispositivos de interconexión certificados. Ese objetivo se establece

[1] Aclarar que existen cinco niveles de clasificación distintos, tal y como se explicará en el capítulo de conceptos previos. Sin embargo, en el plan MC3 el ET solo contempla utilizar tres dominios de seguridad en sus sistemas.

también en la Arquitectura de Referencia de Seguridad de los CIS[2] (Communications and Information Systems) Desplegables [20].

Por otro lado, con Conceptos para el combate 2035 [22] (planeamiento a largo plazo para el ET) se refuerza la idea del plan MC3 con el siguiente párrafo:

> *En un escenario de alta intensidad lo importante es obtener la superioridad de la información gracias a nuestros CIS y particularmente a nuestros sistemas de información (BMS y SIMACET principalmente), con las correspondientes acreditaciones de seguridad.*

Desde un punto de vista más genérico, la Estrategia Nacional de Ciberseguridad 2019 [39] recoge como medida en su segunda línea de acción:

> *Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.*

La realización de este trabajo tiene otra razón fundamental que lo motiva, que es garantizar la seguridad de la información en los sistemas de mando y control militares y, por lo tanto, garantizar así mismo la seguridad de todos los españoles, misión fundamental de las Fuerzas Armadas Españolas.

1.2 Objeto

La finalidad de este trabajo sobre integración de dominios de seguridad es encontrar posibles soluciones que permitan un flujo de información seguro entre dos sistemas con distintas acreditaciones de seguridad, es decir, en dominios de seguridad distintos. Además, la solución definitiva deber ser acreditable por el Centro Criptológico Nacional (CCN).

El caso de uso es resolver este problema en los sistemas BMS y SIMACET, debido a que se escapa del alcance de este proyecto el encontrar una solución global para todos los sistemas existentes. Este trabajo también tiene como objetivo servir de orientación al Ejército de Tierra para la posible adquisición de dispositivos o servicios que permitan esa integración.

1.3 Alcance y ámbito de aplicación

Este trabajo pretende ser una guía para la integración de dominios de seguridad en sistemas que manejan información sensible, en concreto de BMS y SIMACET, para los cuales se propone una solución. Por ello no trata sobre un proyecto completo de obtención con sus cuatro fases (Figura 1). Sin embargo, pese a que no se profundizará en la gestión de adquisiciones al escaparse del alcance del trabajo, sí que se abordarán parte de las

[2] Es el conjunto de equipos, métodos, procedimientos y personal basados en las Tecnologías de la Información y las Telecomunicaciones (TIC) que se encargan de procesar y transportar información [9].

fases, como la definición de necesidad operativa o la determinación de la alternativa de obtención.

Este proceso se encuadra dentro del siguiente marco legal:

- Instrucción 67/2011, de 15 de septiembre, del Secretario de Estado de Defensa, por la que se regula el Proceso de Obtención de Recursos Materiales [46].
- Instrucción 72/2012, de 2 de octubre, del Secretario de Estado de Defensa, por la que se regula el proceso de obtención del armamento y material y la gestión de sus programas [45].

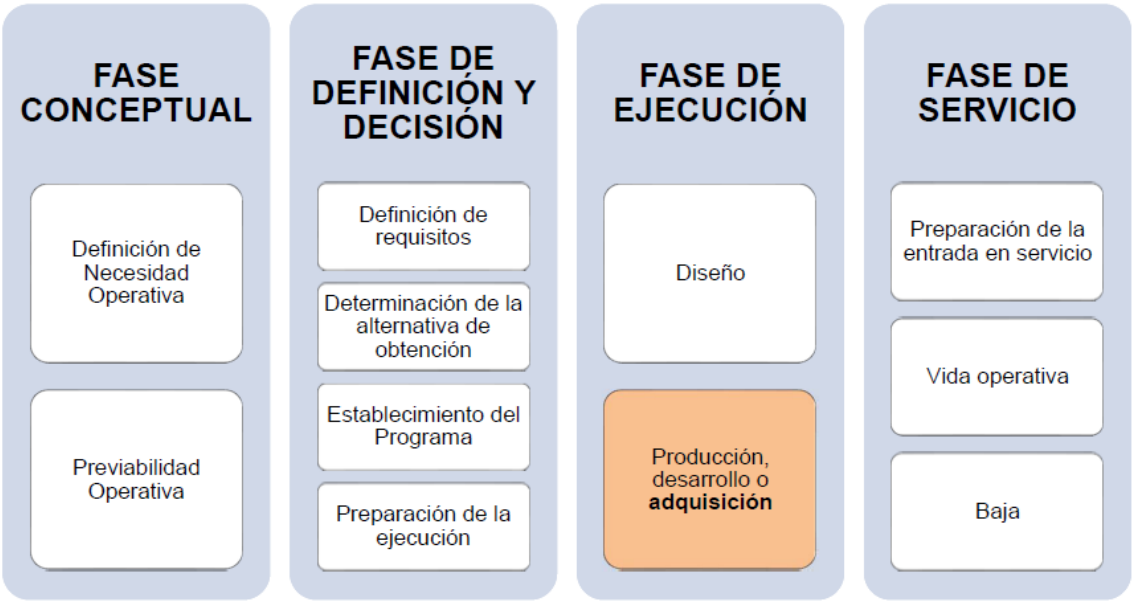

Figura 1: Fases de un proceso de obtención del Ministerio de Defensa. Fuente: Oficina de Proyectos [11].

En los sucesivos capítulos de esta memoria, se irán relacionando algunos apartados con la fase o hito correspondiente del proceso de adquisición de la Figura 1.

Para llegar al objetivo de encontrar una solución adecuada, al principio del proyecto se elaboró una Estructura de Desglose de Trabajo (EDT), en la que se establecieron tareas menores (recopilación de información, definición de la problemática, análisis de alternativas, conclusiones y redacción de la memoria) con sus objetivos de tiempo. En los anexos se encuentran tanto la EDT (Anexo B) como un diagrama de Gantt (Anexo C) en el que se puede ver de forma más gráfica la disposición temporal de las tareas.

En el ámbito del Ejército de Tierra, son varios los puntos en los que se haría necesaria una integración entre dos dominios de seguridad distintos, uno de ellos es entre el sistema BMS que opera a nivel batallón/grupo táctico y SIMACET que se encuentra a nivel brigada. Pero no es el único caso, también sería necesario garantizar la interoperabilidad de los sistemas militares de mando y control del Ejército con otros externos (OTAN, Unión Europea, etc) que puedan encontrarse en dominios de seguridad

distintos, como por ejemplo IFTS [3] (ISAF Force Tracking System). Debido a la imposibilidad de abarcar todos los escenarios posibles, este trabajo se va a centrar en la integración de dominios entre BMS y SIMACET, cuyo ámbito de aplicación es el de las brigadas del Ejército de Tierra (los batallones son los que operan el BMS, pero estos forman parte de las brigadas).

1.4 Estructura de la memoria y metodología

La memoria de este trabajo de fin de grado se trata de la expresión escrita de un trabajo de investigación. Durante las prácticas externas no hubo posibilidad de realizar experimentos, ya que no se disponía de los equipos necesarios, por lo que se ha enfocado el trabajo de forma teórica, aunque proporcionando una solución práctica y funcional.

Para completar el conocimiento sobre la materia tratada, en el Capítulo 6 se encuentra la bibliografía con todo el material que ha sido utilizado durante el trabajo, la cual se ha dividido en bloques según el tipo de fuente. Además, en la memoria también se pueden encontrar citas del tipo {X}, las cuales hacen referencia a informaciones que se han obtenido mediante entrevistas a personal experto (Anexo A).

La memoria comienza con una introducción, la cual se ha realizado ayudándose en la metodología de gestión de proyectos del Project Management Institute (PMI) llamada Project Management Body of Knowledge (PMBOK) [32], estudiada en la asignatura de oficina de proyectos. En esta parte se definen los antecedentes, la motivación, los objetivos, el alcance y el ámbito de aplicación, así como la estructura de la memoria y la metodología.

A continuación, debido al carácter técnico del trabajo, se definen una serie de conceptos que es fundamental comprender antes de continuar con el cuerpo de la memoria, como son: sistemas de información, niveles de clasificación, acreditaciones y dominios de seguridad.

Posteriormente se describirá el estado del arte, explicando la situación de los sistemas de información militares que se van a estudiar, las pasarelas que existen actualmente para que intercambien información y se definirá la problemática de la integración de sus dominios de seguridad. Todo ello ayudándose de toda la información recogida mediante entrevistas, búsquedas en bases de datos, contactos con empresas, etc.

Tras definir el problema, en el siguiente punto se exponen las diferentes alternativas encontradas para integrar los dominios de seguridad de BMS y SIMACET, se realiza una comparativa y se propone una posible solución y la forma de implementarla. Finalmente, se exponen las conclusiones del trabajo y se proponen dos líneas de trabajo futuras.

[3] Sistema de información utilizado en Afganistán [26] por tropas de ISAF (International Security Assistance Force), incluidas tropas españolas, que permitía localización y mensajería instantánea a las unidades, servicios similares a los que proporciona BMS.

La metodología empleada para recopilar toda la información del trabajo ha sido la siguiente:

1) Lectura de manuales militares y repaso de asignaturas del Centro Universitario de la Defensa relacionadas con el ámbito del Trabajo de Fin de Grado.
2) Búsquedas en diversas fuentes:
    - ✓ ZAGUAN: Repositorio institucional de documentos.
    - ✓ Alcorze.
    - ✓ Biblioteca virtual de la Defensa.
    - ✓ Puerta del conocimiento[4].
3) Entrevistas a expertos, en el Anexo A se encuentra una recopilación de las preguntas realizadas. Se realizaron a los siguientes expertos:
    - ✓ Sargento de la sección de explotación de la Compañía de Transmisiones nº7.
    - ✓ Profesor Contratado Doctor del Departamento de Informática e Ingeniería de sistemas de la Universidad de Zaragoza.
    - ✓ Teniente coronel de SECARQINT (Sección de Arquitectura e Interoperabilidad) de la JCISAT (Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica).
    - ✓ Teniente coronel jefe del Centro de Acreditación de Sistemas de la JCISAT.
    - ✓ Comandante de la Sección de Ingeniería de Tecnologías de la Información, Telecomunicaciones y Simulación de la Jefatura de Ingeniería del MALE (Mando de Apoyo Logístico del Ejército).
4) Contacto con empresas mediante videoconferencias y correos electrónicos:
    - ✓ Support and Strategy Spanish Programmes Technician de Thales.
    - ✓ Equipment Engineering Manager de Thales.
    - ✓ Responsable comercial de Autek Ingeniería.

En primer lugar, se obtuvo toda la información posible por medios propios, tras ello se comenzó a realizar entrevistas a personal que fuera experto en la materia (sistemas de información militares, acreditaciones, integración de sistemas, etc.).

Posteriormente, conociendo ya cuales eran las empresas del sector que podían ser más interesantes de cara a adquirir una solución a la integración de dominios de seguridad, se contactó por correo electrónico con las empresas Autek Ingeniería y Thales. Además, se programaron dos videoconferencias (la primera el lunes 21 de septiembre y la segunda el lunes 28 de septiembre), tanto los correos como las videoconferencias fueron de utilidad para conocer en profundidad las soluciones que ofrecía cada empresa.

[4] Es un motor de búsqueda accesible desde la intranet del Ejército de Tierra, en la que se encuentran documentos de numerosas fuentes.

-Página intencionadamente en blanco-

Capítulo 2. Conceptos previos

Antes de profundizar en el trabajo, es conveniente explicar una serie de conceptos clave, como son: sistemas de información, niveles de clasificación, acreditaciones y dominios de seguridad.

2.1 Sistemas de Información

La transformación de datos, que pueden carecer de sentido de forma aislada, en información útil, lo realizan los Sistemas de Información (SI). El siguiente nivel es el conocimiento, el cual se da cuando una persona es capaz de interpretar esa información y tomar una decisión en base a ella.

Según el libro de la asignatura Sistemas de Información para la Dirección [10], editado por el Centro Universitario de la Defensa, un SI basado en ordenadores[5] tiene dos objetivos principales:

- Proveer información útil para los procesos de toma de decisiones.
- Proporcionar información que facilite el control de una organización.

Dentro del concepto de sistema queda englobado hardware, software, personal y procedimientos. Estos sistemas que manejan información electrónica se denominan [8] indistintamente "Tecnologías de la Información y las Comunicaciones", "Tecnologías de la Información (TI)", "Sistemas de Información" o, en terminología inglesa, "Communications and Information Systems".

2.2 Niveles de clasificación

La especial sensibilidad de algunos de los datos que se transmiten a través de los sistemas de información, hace que surja la necesidad de proteger estos sistemas frente a posibles ataques o fallos que pusieran en riesgo esa información. Debido a ello nació la Ley 9/1968, de 5 de abril, sobre secretos oficiales, en la que se establecen [41] los grados de clasificación de la información de SECRETO y RESERVADO, añadiéndose posteriormente y debido a la adhesión de España a la OTAN, los grados de CONFIDENCIAL y DIFUSIÓN LIMITADA.

La información que se protege con cada nivel de clasificación está recogida en la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa [43]:

- SECRETO: proporciona el más alto grado de protección, su revelación no autorizada podría dar lugar a riesgos o perjuicios de la seguridad y defensa del Estado.

[5] Existen distintos tipos de sistemas de información, ya que un informe escrito o una conversación también puede considerarse como tal.

- RESERVADO: información de menor importancia que la anterior, cuya divulgación podría afectar a la seguridad y defensa del Estado.
- CONFIDENCIAL: la revelación no autorizada de la información podría dañar a la seguridad del Ministerio de Defensa, perjudicar a sus intereses o dificultar el cumplimiento de la misión.
- DIFUSIÓN LIMITADA: informaciones no comprendidas en los niveles anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

En la Figura 1 se pueden ver los distintos grados ordenados de mayor a menor sensibilidad de la información y sus grados equivalentes en la Unión Europea (UE) y en la OTAN.

Nacional	UNIÓN EUROPEA	OTAN
SECRETO	TRES SECRET UE /UE TOP SECRET	COSMIC TOP SECRET (CTS)
RESERVADO	SECRET UE / UE SECRET	NATO SECRET (NS)
CONFIDENCIAL	CONFIDENTIEL UE / EU CONFIDENTIAL	NATO CONFIDENTIAL (NC)
DIFUSIÓN LIMITADA	RESTREINT EU / EU RESTRICTED	NATO RESTRICTED (NR)
SIN CLASIFICAR USO OFICIAL USO PÚBLICO	EU SENSITIVE INFORMATION (EUSI) LIMITE PUBLIC	NATO UNCLASSIFIED (UN) COMMERCIAL-MEDIAL-PERSONAL-PUBLIC- OPEN SOURCE

Figura 2: Guía de equivalencias entre grados de clasificación de la información. Fuente: CCN-STIC 001 [8].

Toda aquella información que no pueda ser clasificada con uno de los grados que se recogen en la citada Orden Ministerial, será información SIN CLASIFICAR, pudiendo marcarse como USO OFICIAL o USO PÚBLICO, según el Ministerio de Defensa determine [44] si es de un tipo o de otro. Esta información puede manejarse sin aplicar medidas de protección, aunque para los documentos de USO OFICIAL se debe evitar que puedan ser accesibles por personal no autorizado, debiendo de existir una persona u organismo que se encargue de custodiarlos.

2.3 Acreditaciones

Para que un sistema de información adquiera uno de los grados de clasificación anteriores, es necesario que sea sometido una acreditación que lo certifique. La entidad que la realiza es la Autoridad de Acreditación de Seguridad [1].

En la guía CCN-STIC 001[6] [8] especifica que antes de interconectar dos sistemas (en nuestro caso, BMS y SIMACET), primero se deberá acreditar cada sistema por

[6] Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. El Real

separado y posteriormente acreditar la interconexión entre ellos. Este proceso se escapa el alcance del presente trabajo, por lo que no se profundizará más en él.

2.4 Dominios de Seguridad

Según la Unión Internacional de Telecomunicaciones, dominio de seguridad se define [40] como:

> *Un conjunto de elementos, una política de seguridad, una autoridad responsable de la seguridad y un conjunto de actividades relacionadas con la seguridad cuyos elementos se gestionan de conformidad con la política de seguridad.*

También puede referirse a redes con distintos niveles de clasificación, o redes con distintas autoridades operativas o incluso redes sin clasificar pero que se mantengan aisladas por razones de seguridad [4].

En el caso de estudio concreto que compete a este trabajo, podrían definirse dos dominios de seguridad diferentes, uno en la red creada por el sistema BMS (de menor seguridad) y otro en la red del sistema SIMACET (de mayor seguridad).

En la Figura 3, extraída de la Arquitectura de Referencia de Seguridad de los CIS Desplegables [20], pueden verse los distintos dominios de seguridad que se pretenden implementar en el ET. Por un lado, puede verse que, desde los batallones hasta el último soldado desembarcado, se establece un dominio de seguridad de DIFUSIÓN LIMITADA (las circunferencias amarillas) o NATO (North Atlantic Treaty Organization)/EU (European Union) RESTRICTED (equivalentes de la OTAN y de la Unión Europea). En este dominio es en el que se encuentra el sistema BMS.

Por otro lado, al nivel de la brigada se establece otro dominio de seguridad RESERVADO NACIONAL (cruz azul) o NATO/EU SECRET (equivalentes de la OTAN y de la Unión Europea).

Decreto 3/2010 de 8 de Enero [42], actualizado por el Real Decreto 951/2015, de 23 de octubre, promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC).

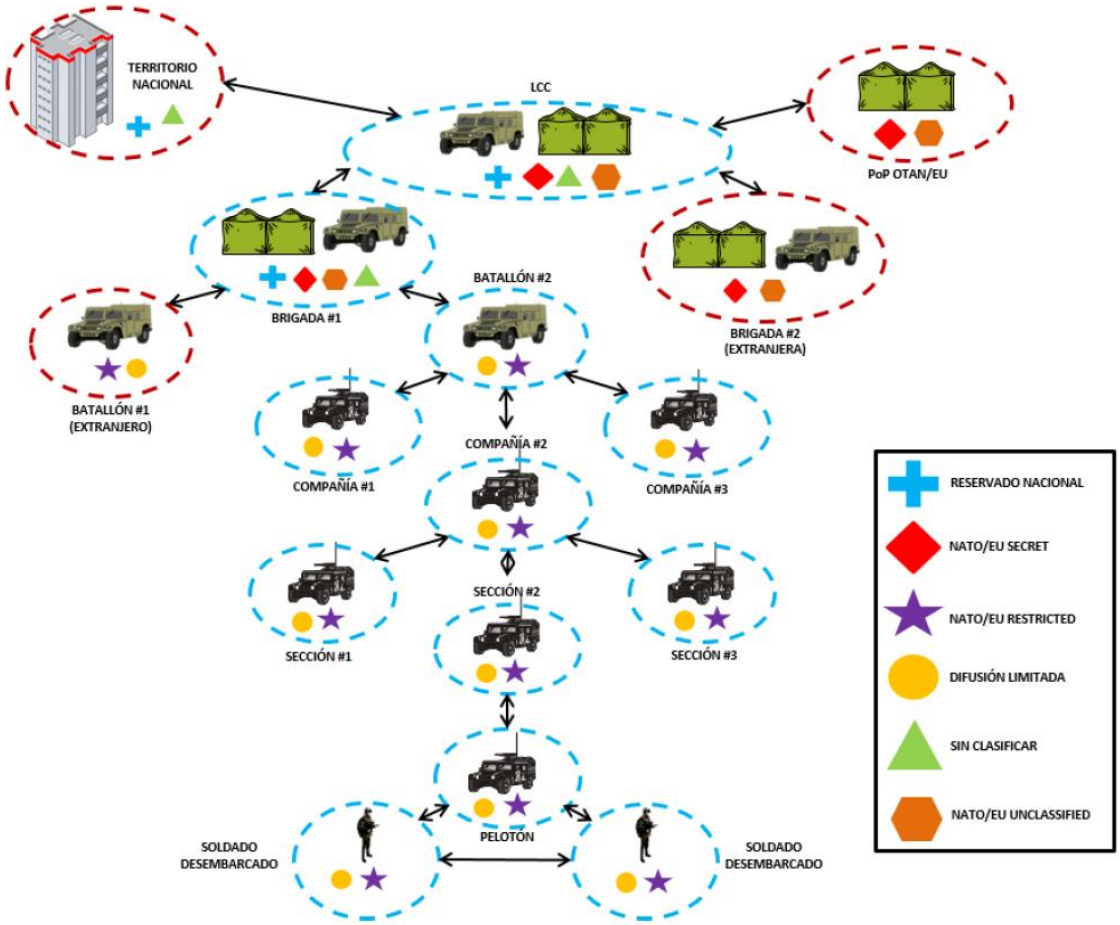

Figura 3: Dominios de seguridad en el sistema CIS desplegable. Fuente: Arquitectura de Referencia de Seguridad de los CIS Desplegables [20].

Capítulo 3. Estado del arte

Una vez definidos los conceptos clave de forma teórica, en este punto se explicará en qué situación se encuentran actualmente los dos sistemas del estudio, para poder definir posteriormente el problema en profundidad.

3.1 Situación actual de los sistemas de información militares

En el ámbito militar, se consideran dos tipos genéricos de sistemas de información:

- Sistemas de información para el mando y control (C2IS).
- Sistemas de información de propósito general.

Los sistemas de información para el mando y control permiten una conducción en vivo de las operaciones y facilitan la toma de decisiones a los escalones superiores. También sirven de apoyo en actividades de planeamiento, dirección, coordinación y control del empleo de las fuerzas y los medios en las operaciones militares.

En el Ejército de Tierra, los dos sistemas de información principales para el mando y control son SIMACET y BMS, los cuales se explicarán a continuación.

3.1.1 Sistema de Información para el Mando y Control del Ejército de Tierra

Se trata de una herramienta que permite al jefe la dirección, planeamiento y conducción de las operaciones militares, así como obtener una visión coherente y homogénea del escenario terrestre [24], facilitando así mismo el intercambio de información entre distintos escalones.

El núcleo principal de SIMACET es la Base de Datos Táctica[7] (BDT), en la cual se guardan datos como iconografía, plantillas, grupos y perfiles de usuario, entre otros. Estos datos, según van siendo modificados en las operaciones, se modifican en todos los nodos mediante un mecanismo de réplica.

Un nodo se trata de un conjunto de hardware y software que contiene la BDT y la intercambia con otros nodos. Hay distintos tipos según el tamaño de la unidad a la que da servicio, normalmente: nodo de Pequeña Unidad (PU) para un puesto de mando de batallón[8] y nodo de Gran Unidad (GU) para puestos de mando de brigadas o unidades superiores. Los nodos GU son capaces de dar servicio a más clientes (es decir, instalar en el puesto de mando más portátiles para que el cuartel general pueda trabajar con ellos)

[7] Se trata de una base de datos en base al software Oracle.

[8] Actualmente no se emplea SIMACET en los puestos de mando de batallón, aunque las brigadas siguen disponiendo de estos nodos PU.

que los nodos PU. Estos nodos intercambian la información por medio de sistemas de telecomunicaciones, inalámbricos o guiados, generalmente mediante satélite.

Los servicios principales que ofrece SIMACET a los usuarios son información táctica (mapa de situación con la ubicación de las unidades), mensajería oficial y mensajería interpersonal, aunque hay más aplicaciones a parte de estas.

El sistema comenzó a implementarse en las unidades de transmisiones en el año 2001 y actualmente, las versiones que se están utilizando son:

- SIMACET v4.2: en esta versión, los nodos están compuestos por una serie de servidores físicos (controlador de dominio, SIMACET, exchange y share point).
- SIMACET v5: el software es esencialmente el mismo que en la versión 4.2. Sin embargo, hay cambios en el hardware ya que existen únicamente dos servidores físicos, en los cuales se encuentran virtualizados[9] todos los servidores. Ambos servidores son redundantes, para poder garantizar el servicio en caso de que uno de ellos falle.
- SIMACET v6 "PROMETEO": aún no se ha implementado en las unidades, en esta versión se modifican las aplicaciones del sistema para adecuarse al modelo de datos de OTAN [18]. El hardware es similar al de la versión 5.

Recientemente, la denominación de SIMACET ha cambiado (aunque se utilizan ambas siglas indistintamente) a SC2NET (Sistema de Mando y Control Nacional del Ejército de Tierra) y además se distinguen dos partes: SC2NET-D (Desplegable) y SC2NET-CGP (Cuarteles Generales Permanentes). La red permanente sí que está acreditada a reservado. Sin embargo, debido a que únicamente se intercambia información entre sus 12 nodos, no requiere de una solución que integre dominios de seguridad (Anexo A, entrevista 4, pregunta {8}). En cambio, SC2NET-D sí que requiere una solución para poder integrar distintos dominios de seguridad, ya que es el sistema que se utiliza en las brigadas e interopera con BMS.

3.1.2 Battlefield Management System

BMS es un software creado por Thales e Indra que nació originalmente como un sistema de información para el mando y control de pequeñas unidades de carros de combate (BMS-LINCE en el año 2017), pero actualmente se ha generalizado también a unidades ligeras (BMS-ET) [28]. Además del software, el sistema también está

[9] Virtualizar consiste en abstraer los recursos de un computador, proporcionando acceso lógico a recursos físicos [13]. En este caso es una virtualización unhosted, ya que las máquinas virtuales (en nuestro caso: SIMACET, exchange, etc.) acceden directamente al servidor físico.

compuesto por hardware, en forma de tablets GETAC[10], desde las cuales el cliente puede utilizar los diferentes servicios que proporciona el dispositivo.

El sistema es escalable ya que en un mismo fichero de misión[11] se pueden introducir tantos nodos como se quiera siempre y cuando se respeten las restricciones propias del medio de comunicación (por ejemplo, las radios PR4G permiten un máximo de 32 nodos en una red) y también es compatible con otros sistemas, bien por pasarelas o bien por protocolos que implementa BMS, como NFFI[12], que es el NATO Friendly Force Information.

El sistema proporciona diversas herramientas, siendo las más utilizadas la mensajería con archivos adjuntos y el mapa táctico en el que pueden dibujarse unidades (amigas, enemigas y neutrales) y líneas tácticas.

Para poder intercambiar información, el sistema utiliza los medios de comunicación de las unidades del Ejército de Tierra, como por ejemplo radios PR4G V3 que van instaladas en los vehículos. BMS permite el posicionamiento a través de los medios de comunicación conectados a la tablet (como las PR4G, las cuales proporcionan posicionamiento), pero también se pueden conectar elementos GPS (Global Positioning System) externos a la tablet.

3.1.3 Pasarelas

Una pasarela se trata de un conjunto de software y hardware que actúa como traductor entre los protocolos que usan dos sistemas de información interconectados, de tal manera que los datos puedan pasar de un sistema a otro. En cuanto a los sistemas de estudio en el presente trabajo, SIMACET y BMS, las pasarelas que se utilizan son las siguientes:

- IDT (Interfaz de Datos Táctica): permite el intercambio de correo electrónico entre los clientes de ambos sistemas. El software va instalado sobre un portátil. Traduce el protocolo IDT[13] de BMS al protocolo de mensajería Simple Mail Transfer Protocol (SMTP) [21].
- COE (Common Operating Environment) o Entorno Operativo Común: esta pasarela permite la transferencia de los datos tácticos (unidades, líneas tácticas,

[10] En la última versión el software está diseñado para funcionar con cualquier dispositivo con Windows 10, por lo que podría instalarse también en un portátil para dar servicio en un puesto de mando (hay licencias sobrantes).

[11] Es un archivo que se crea antes de cada maniobra, en él se configuran los distintos nodos (tablets), los medios de comunicación de cada nodo y las redes a las que va a pertenecer.

[12] Estándar de la OTAN que permite intercambiar información (unidades y alarmas) con fuerzas amigas [19].

[13] BMS puede trabajar con dos protocolos: NFFI para sistemas OTAN e IDT para sistemas nacionales, la pasarela de mensajería se llama de la misma manera, lo que puede dar lugar a confusión.

instalaciones y obstáculos) creados en los nodos BMS a los nodos de SIMACET. De manera similar a IDT, COE se instala en un portátil (pueden instalarse ambas pasarelas en el mismo). Funciona como traductor entre el protocolo IDT y File Transport Protocol (FTP) [27].

En la Entrevista 1 (Anexo A) se dedujo que el funcionamiento de estas pasarelas no es del todo óptimo {3}. Sin embargo, se espera que con la futura llegada de la versión 6 de SIMACET (llamada PROMETEO) se solucione este problema, ya que SIMACET utilizaría el mismo protocolo IDT que usa BMS, prescindiendo del uso de pasarelas para interconectar ambos sistemas.

3.2 Definición de la problemática

Actualmente, en las unidades del Ejército de Tierra se utilizan los sistemas de mando y control SIMACET (o SC2NET-D) en los puestos de mando de brigada y superiores y BMS en las unidades de maniobra (batallones, compañías, secciones, etc.).

Las pasarelas IDT y COE, disponen de una serie de filtros (por ejemplo en COE se puede limitar que la unidad mínima que pueda verse en SIMACET sea de tipo compañía, no mostrando unidades de tipo sección e inferiores), pero no son suficientes para acreditar la interconexión según los estándares del Centro Criptológico Nacional, por lo que se hace necesario buscar una solución que permita interconectar ambos sistemas con seguridad ya que actualmente, tal y como confirmaron en la Entrevista 1 (Anexo A), en las unidades se utiliza tanto SIMACET {1} como BMS {2} sin ninguna clasificación de seguridad (SIN CLASIFICAR) y además, tampoco están preparados para la acreditación. Sin embargo, como ya se explicó, los nodos permanentes de SIMACET sí que se han acreditado a nivel RESERVADO (Anexo A, Entrevista 3, pregunta {7}).

Para comprender la problemática actual, es interesante saber que el CCN dispone de una instrucción técnica [7] que regula la interconexión de sistemas de las TIC que manejan información nacional clasificada, la CCN-STIC 302. En este documento se recoge que para interconectar dos sistemas se requiere de un sistema de protección perimetral:

> *La interconexión de dos Sistemas se realizará mediante un Sistema de Protección de Perímetro (SPP). Este SPP consiste en una combinación de recursos hardware y/o software, denominados Dispositivos de Protección de Perímetro (DPP), cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los Sistemas.*

Estos dispositivos de protección de perímetro se clasifican según el nivel de seguridad que proporcionan y van desde un DPP-0 hasta un DPP-6. Los menos seguros

únicamente actúan en los niveles más bajos (físico y enlace) del modelo OSI[14] (Open System Interconnection), mientras que en los más seguros los dispositivos rompen la continuidad de los protocolos de comunicaciones, denegando el flujo de información en uno de los sentidos, generalmente desde el sistema más sensible al menos sensible. La clasificación es la siguiente:

- DPP-0. Conexión directa: interconexión a nivel físico (dispositivos tipo hub[15]) o de enlace (dispositivos tipo switch[16]), permite restricciones mínimas.
- DPP-1. Filtro de paquetes: permite filtrar paquetes IP (Internet Protocol) entre dos sistemas, trabaja a nivel de red (dispositivos tipo router[17]).
- DPP-2. Cortafuegos/Firewall: nivel de red, transporte y/o sesión. Permite filtrados más avanzados y más opciones de gestión.
- DPP-3. Proxy: permite controlar el tráfico a nivel de aplicación (correo electrónico, transferencia de ficheros, etc.).
- DPP-4. Pasarela: es un conversor de protocolos, permiten mecanismos de seguridad complejos.
- DPP-5. Dispositivo de sentido único: rompen la continuidad de los protocolos de comunicaciones, obligando a un flujo de datos de sentido único.
- DPP-6. Otros tipos de dispositivo: los diseñados específicamente para una interconexión, siempre que no se contemplen en los apartados anteriores.

En el Anexo D se ha incluido una tabla de equivalencias para profundizar en los modelos de interconexión de redes y los dispositivos asociados a cada nivel.

En ese mismo documento, la CCN-STIC 302, se recogen dos escenarios de interconexión que se pueden extrapolar a los sistemas sobre los que se centra este trabajo:

(1) SIMACET RESERVADO – BMS SIN CLASIFICAR → Es necesario un dispositivo de sentido único (DPP-5) en DMZ[18] (Desmilitarized Zone).

[14] OSI es el modelo básico de referencia [14] para la interconexión de sistemas abiertos, se publicó en 1988 y define un marco para facilitar el diseño de los estándares en las comunicaciones de datos.

[15] Es un dispositivo de interconexión que trabaja a nivel físico, no lee las tramas de datos (bits), únicamente las recibe por un puerto y las retransmite por los demás.

[16] El switch/bridge funciona a nivel de enlace, trabaja con una tabla de conmutación en la cual guarda direcciones MAC (Media Access Control), que son identificadores únicos de cada dispositivo, con las cuales puede decidir a dónde enviar las tramas (bloque de información de nivel de enlace) que le llegan. Conecta equipos de una misma red.

[17] Equipo de interconexión de nivel de red que conecta dos o más redes, para ello dispone de una tabla de encaminamiento o enrutamiento en la cual almacena las direcciones IP de otras redes a las que puede enviar paquetes (bloque de información de nivel de red).

[18] Una DMZ se establece interponiendo entre la red interior y la exterior uno o más equipos protegidos por uno o dos cortafuegos, con la finalidad de proteger la red interior de intrusiones indeseadas.

(2) SIMACET RESERVADO – BMS DIFUSIÓN LIMITADA → Es necesaria una pasarela (DPP-4) en DMZ.

Actualmente, en el Ejército de Tierra la prioridad es resolver el escenario (1), tal y como se recoge en el documento de Arquitectura de Referencia de Seguridad de los CIS Desplegables [20]:

> *Hito 0 (Situación actual): Disponer de una solución que permita el despliegue en el PC Brigada de dos dominios de seguridad con niveles de clasificación ("SINCLAS" y "RESERVADO NACIONAL").*

Por otro lado, para resolver el escenario (2), en el mismo documento se define un Hito 1, para el cual se establece un plazo de dos años a partir de la resolución del Hito 0.

En cuanto a la gestión de adquisiciones, con la información contenida en este apartado, se podría elaborar la definición de necesidad operativa, la cual tiene como objeto identificar la carencia que se pretende solventar (solución para integrar los dominios de seguridad de BMS y SIMACET) y su justificación (CCN-STIC 302, Arquitectura de Referencia de Seguridad, Plan MC3, etc.).

Para solventar esta cuestión, se han identificado diversas soluciones, las cuales han sido recopiladas mediante este trabajo de investigación en el Capítulo 4 de la memoria.

Capítulo 4. Soluciones de integración de dominios de seguridad

Para la elaboración de este punto, se analizó previamente toda la información obtenida por las distintas fuentes que se explicaron en la metodología, obteniendo así los requisitos necesarios para la solución del problema planteado.

Una vez planteado el problema y los requisitos para resolverlo, se realizó una búsqueda de diversas alternativas que podrían ser útiles para lograr la integración entre los dominios de seguridad de SIMACET y BMS. En este capítulo no aparecen todas las que se habían planteado inicialmente, ya que algunas de ellas se descartaron por no cumplir los requerimientos de seguridad, como por ejemplo la implementación de una solución exclusivamente mediante software, que se descartó tras la realización de la Entrevista 2, pregunta {5} (Anexo A).

Con las soluciones expuestas en este capítulo, se completaría el hito de previabilidad operativa en el proceso de obtención, hito que tiene como objetivo identificar las posibles alternativas para cubrir la carencia descrita en la definición de necesidad operativa.

A continuación, van a exponerse las soluciones encontradas:

4.1 Diodos de datos

Antes de hablar de modelos específicos de diodos, se va a hacer una introducción genérica sobre ellos. Los diodos de datos son los dispositivos de protección de perímetro (DDP-5) que aportan una mayor seguridad frente a la fuga de información sensible [6], dado que garantizan el flujo unidireccional de la información mediante hardware, al no existir un canal de retorno físico, tal y como se puede ver en la Figura 4. En el caso de los sistemas de este trabajo, el componente de transmisión (Tx) sería un nodo BMS ubicado en la red externa y el de recepción (Rx) un nodo de SIMACET en la red interna.

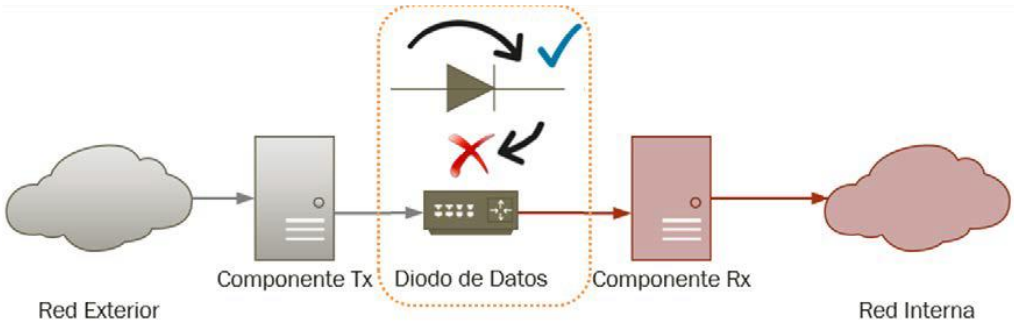

Figura 4: Flujo de datos en un diodo. Fuente: CCN-STIC 140 [3].

La clave de estos dispositivos es que son capaces de interpretar protocolos bidireccionales (como por ejemplo Transmission Control Protocol o TCP[19]), "romperlos" y transformarlos en unidireccionales (entre los servidores proxy[20] y el hardware del diodo) para luego enviarlos de nuevo a la otra red como bidireccionales.

Debido a que son dispositivos de sentido único, estos dispositivos serían apropiados para resolver el escenario (1) descrito anteriormente.

Existen diversos fabricantes de este tipo de dispositivos, entre los que se encuentran Autek Ingeniería y Thales. En este trabajo se ha profundizado en las soluciones de estas dos empresas ya que el Ejército de Tierra ha realizado pruebas con ellas.

4.1.1 Diodo PSTdiode de Autek Ingeniería

Este diodo ha sido desarrollado por Autek Ingeniería, una empresa española de desarrollo de productos de seguridad de la información y comunicaciones IP fundada en 1998, la cual realiza proyectos de desarrollo a medida.

Especificaciones de seguridad (extraídas a través de contactos con la propia empresa):

- CCEAL4+[21] [35].
- Incluido en el Catálogo de Productos de Seguridad TIC del CCN [2]:
  - Producto Cualificado para el manejo de información sensible.
  - Producto Aprobado para el manejo de información clasificada.
- Incluido en el NATO Information Assurance Product Catalogue [37].

El diodo [5], está formado por dos appliances[22], uno que se conecta al domino de seguridad origen y otro al dominio destino. Ambos appliances están conectados por una única fibra óptica. Este dispositivo permite transferencia de ficheros mediante los protocolos FTP, FTPS (File Transport Protocol Secure), SMB (Server Message Block) y SFTP (Secure File Transfer Protocol) y de paquetes UDP (User Datagram Protocol).

Este diodo sería útil por tanto para la transferencia de datos tácticos entre BMS y SIMACET mediante el protocolo FTP, así como mediante el protocolo NFFI (el cual

[19] TCP es un protocolo del nivel de transporte que realiza conexiones seguras en tres vías, por lo que a priori sería imposible utilizarlo entre dos sistemas con un flujo unidireccional de datos, problema que solventa el diodo de datos.

[20] En el modelo de cliente-servidor, un servidor proxy es un equipo que recibe solicitudes del cliente, las analiza y decide el servidor al que debe enviarlas [15].

[21] Common Criteria Evaluation Assurance Level (CCEAL) es un estándar que verifica el cumplimiento de los requisitos de seguridad de un producto de acuerdo con un nivel de garantía de evaluación. Esta certificación tiene validez internacional.

[22] El appliance es el conjunto del hardware de comunicación unidireccional y el software necesario que va instalado (firmware).

utiliza paquetes UDP). Sin embargo, no permite envío de correos al no trabajar con ningún protocolo de mensajería.

El sistema se integra con la infraestructura existente y no es necesario instalar proxies, ni servidores dedicados adicionales. Sin embargo, de forma opcional dispone de un software de administración, otro de registro de transferencias y de un registro de información de funcionamiento y seguridad.

En el Anexo E se encuentra la ficha técnica del diodo donde se pueden consultar todas las características del equipo.

4.1.2 Diodo ELIPS-SD de Thales

Se trata de otro diodo de datos, fabricado en este caso por la empresa francesa Thales. Especificaciones de seguridad:

- Equivalente[23] a CCEAL7+.
- Recomendado por la Agencia de Seguridad de la Información de Francia, en sus directrices de seguridad cibernética para los sistemas industriales [38].
- Certificado equivalente a RESERVADO en Francia (NATO SECRET/EU SECRET) [36].
- Incluido en el NATO Information Assurance Product Catalogue [36].

El sistema está compuesto por el diodo de datos en sí y por dos servidores: Low Network Server (para el dominio menos seguro) y High Network Server (en el dominio de mayor seguridad). El dispositivo permite la transferencia de ficheros mediante el protocolo FTP y de mensajería mediante el protocolo SMTP.

Por lo tanto, este diodo permitiría el traspaso de datos tácticos y de mensajería (siempre de manera unidireccional, debido a la limitación física del diodo) entre BMS y SIMACET.

4.2 Pasarelas de intercambio seguro

Las pasarelas de intercambio seguro [24] de información son dispositivos de protección de perímetro (DPP-4) más avanzados que un cortafuegos/firewall o un proxy. Al igual que los diodos, están orientadas a la protección de interconexiones entre redes

[23] En el documento de presentación del producto, obtenido a través de una videoconferencia con ingenieros de Thales, la empresa declara esta característica. Sin embargo, en el listado de productos certificados por common criteria (https://www.commoncriteriaportal.org/products/) no aparece. Debido a ello no se ha considerado esta especificación en la comparativa del apartado 4.7.

[24] No confundir con las pasarelas COE e IDT descritas en el estado del arte, las cuales no son dispositivos de protección de perímetro, sino que se emplean para permitir el intercambio de ficheros y mensajería entre BMS y SIMACET.

que manejan información con diferentes categorías o políticas de seguridad [3], con el fin de evitar la entrada o salida de información no autorizada. Sin embargo, las pasarelas de intercambio seguro, a diferencia de los diodos, no limitan el flujo de información en un único sentido.

De la misma manera que lo diodos, estas pasarelas rompen la continuidad de los protocolos de comunicaciones en todas las capas del modelo OSI. La pasarela está formada por dos dispositivos (uno en cada uno de los sistemas a los que interconecta) y ambos dispositivos se comunican mediante un protocolo desarrollado ad-hoc. De esta manera se impiden conexiones TCP/IP[25] entre origen y destino, impidiendo la salida de información sensible desde la red interna (más segura) hacia la red externa (menos segura). Para ello realiza un filtrado, analizando el contenido de cada paquete y permitiendo el paso solamente cuando el paquete cumpla las reglas de entrada o de salida.

La empresa Autek Ingeniería dispone de una pasarela de intercambio seguro acreditada por el CCN [2]. Así mismo, en las conversaciones establecidas con la empresa Thales confirmaron que también disponen de equipos de pasarelas de seguridad.

Estos dispositivos podrían ser utilizados para integrar los dominios de seguridad de SIMACET y BMS en el escenario (2) expuesto anteriormente, en el cual se podría transferir tanto datos tácticos como mensajería en ambos sentidos [27].

4.3 Security Guard

Otra solución encontrada, es el security guard, se trata de un dispositivo que podría servir para interconectar los dominios de seguridad de SIMACET y BMS. Según el informe “Strategies for transporting data between classified and unclassified networks” [30] del US (United States) Army armament research, development and engineering center, se puede definir como:

> *In information security, a guard is a combination of hardware and software used to provide secure data transfer between two information domains. There are many different types of guards with different functionalities, but each guard implements essentially the same basic function: to protect networks at their boundaries and secure data transfer between those networks.*

Este tipo de dispositivo lo utilizan entidades tales como el US Navy, el Department of Defense o la comunidad de inteligencia estadounidense. Del informe se puede extraer que, los Security Guard podrían servir para interconectar SIMACET y BMS tanto en el escenario (1) como en el escenario (2), dependiendo de la configuración del dispositivo:

[25] TCP/IP es un modelo que, a diferencia del modelo OSI, define varios protocolos y constituye la arquitectura actual de Internet [12]. Tiene sus orígenes en investigaciones del Departamento de Defensa de los Estados Unidos. En el Anexo D se puede encontrar una tabla con las equivalencias entre los niveles de ambos modelos.

> *Several types of guards exist, including multiple single levels of security, multilevel security, low to high, high to low, and bidirectional.*

Por ejemplo, el Security Guard CENTAUR (Cross-domain Enterprise All-source User Repository) sería empleable en el escenario (1):

> *The CENTAUR automates the process of pushing data between classified and unclassified systems and enables web-based queries to electronically transfer information. The high-speed guard component validates security, ISR (intelligence, surveillance, and reconnaissance) information markings, and data structure prior to transferring the information between security domains.*

4.4 Transporte físico

Otra alternativa, es la transferencia manual de los datos, alternativa que también se recoge en el informe anteriormente mencionado del US Army.

Para materializar esta solución de forma única, se propone lo siguiente: se dispondría en el puesto de mando de dos nodos, uno de BMS (red menos segura) y otro de SIMACET (red más segura), los cuales no estarían conectados de ninguna manera. El posicionamiento de las unidades de BMS podría proyectarse en una pantalla y de ahí ir moviendo las unidades en el mapa de situación de SIMACET de forma manual. De igual manera, los archivos que se quisieran traspasar de un sistema a otro tendrían que transportarse de forma manual, tarea que realizaría el elemento que se describe en el siguiente párrafo.

En la doctrina del Ejército de Tierra, se contempla la figura del RSA (Responsable de Seguridad de Área), también llamado TASO (Terminal Area Security Officer) según la terminología OTAN. Dentro de un puesto de mando, el RSA dispone de un dispositivo de almacenamiento portátil seguro y es la única persona que puede extraer o introducir ficheros en los sistemas de información, para lo cual sigue un procedimiento que garantice la seguridad de los sistemas. Esta responsabilidad viene recogida en el manual de procedimientos operativos CIS [25]:

> *Como norma general serán los únicos autorizados a introducir y extraer información del sistema a través de sus periféricos, de acuerdo a las normas que se especifiquen en la documentación de seguridad del sistema.*

Este podría ser el elemento responsable de transferir manualmente la información que fuera necesaria entre ambos sistemas.

4.5 Comparativa entre soluciones

Debido a que la prioridad actual del Ejército de Tierra es resolver el escenario (1), tal y como se explicó en la definición de la problemática, la comparativa se va a realizar buscando resolver este escenario. Para ello, y antes de proponer una solución óptima, se

van a analizar las ventajas e inconvenientes de cada una de las alternativas encontradas que podrían servir para integrar los dominios de seguridad de SIMACET RESERVADO y BMS SIN CLASIFICAR. Por lo tanto, se ha descartado incluir la solución de pasarelas de seguridad en la comparativa, ya que no serían útiles para este escenario.

Para la comparativa se ha elaborado la siguiente tabla, en la que se han ordenado las distintas alternativas según su adecuación:

<table>
<tr><td colspan="2">1. Diodo PSTdiode (Autek Ingeniería)</td></tr>
<tr><td>Ventajas</td><td>Inconvenientes</td></tr>
<tr><td>• Garantía física de flujo unidireccional de información.
• Certificado por el CCN [2].
• Empresa nacional[26].
• Probado con éxito [29][27].</td><td>• Coste elevado[27] [33].
• No permite envío de correo, ya que no soporta ningún protocolo de mensajería.</td></tr>
<tr><td colspan="2">2. Diodo ELIPS-SD (Thales)</td></tr>
<tr><td>Ventajas</td><td>Inconvenientes</td></tr>
<tr><td>• Garantía física de flujo unidireccional de información.
• Trayectoria de contratos entre el ET y la empresa Thales (como los de las radios PR4G o el sistema BMS).
• Probado con éxito en maniobras (TIWAR 17) [21].
• Permite envío de correos (en un único sentido) a través del protocolo SMTP.</td><td>• Coste elevado[28].
• Empresa extranjera[29].
• No está certificado por el CCN.</td></tr>
</table>

[26] Fomentar la base tecnológica e industrial de defensa para tener una sólida industria de defensa nacional, es una de las principales estrategias que las potencias emplean para obtener superioridad militar y competitividad en el mercado [16].

[27] En las entrevistas realizadas, se obtuvo un coste unitario del diodo de alrededor de 20.000 €, el cual puede considerarse elevado teniendo en cuenta que se podría fabricar un diodo por 1.000 € con tecnología de código abierto [31], lo cual podría ser interesante, pero el desarrollo de un diodo desde cero y su correspondiente acreditación alargaría la búsqueda de una solución para la integración de dominios.

[28] En las videoconferencias realizadas con los ingenieros de Thales, el departamento comercial de la empresa proporcionó un precio unitario de entre 15.000 y 20.000 € por diodo, el cual también podría considerarse elevado debido a la misma razón expuesta en la nota a pie de página 27, aunque similar al coste del PSTdiode.

[29] Ante un hipotético conflicto con el país donde reside la matriz de la empresa fabricante del dispositivo (Francia), la empresa podría dejar de suministrar asistencia y actualizaciones, llegando a dejar inoperativos los sistemas.

3. Security Guard	
Ventajas	**Inconvenientes**
• Mayor flexibilidad que un diodo, ya que, según su configuración, se podría emplear como dispositivo de sentido único o de doble sentido (en los dos escenarios contemplados). • Utilizado por las Fuerzas Armadas estadounidenses y por agencias de inteligencia, lo que es una garantía de su utilización en situaciones reales.	• Imposibilidad de comprar el sistema al encontrarse en uso por parte de los Estados Unidos. Sería necesario un proyecto de I+D (Investigación y Desarrollo), con lo cual la solución se retrasaría en el tiempo.
4. Transporte físico	
Ventajas	**Inconvenientes**
• Figura del RSA/TASO contemplada en la doctrina del ET. • Facilidad de implementación, ya que no requeriría instalar dispositivos nuevos ni cambiar la configuración del puesto de mando. • Coste casi nulo, al no requerir adquisición de hardware ni software nuevo.	• Posibilidad de fallo humano, con el consiguiente problema de seguridad. • Baja velocidad de traspaso de la información, ya que el RSA tendría que ir transportando los archivos en su dispositivo portátil siguiendo sus procedimientos de seguridad.

Tabla 1: Comparativa entre las soluciones encontradas. Fuente: Elaboración propia (Word).

De la anterior comparativa se puede extraer que, por un lado, la implementación de un Security Guard similar al estadounidense podría ser una buena solución, pero la adquisición de un diodo actualmente parece mucho más al alcance del Ejército de Tierra. Por otro lado, la utilización de transporte físico de información como solución única es muy poco flexible, lo que restaría operatividad a las brigadas, serviría como solución temporal en el caso de que se acreditara SC2NET-D a RESERVADO, utilizando la figura del RSA de la manera que se expuso en el punto 4.4.

Se deduce, por tanto, que actualmente la solución más viable se presenta en forma de diodo, con lo cual la cuestión estaría en decidir entre el diodo de Autek y el diodo de Thales, la cual se resuelve en el apartado siguiente.

4.6 Propuesta de solución

Basándose en el análisis de toda la información obtenida, y en la comparativa anterior, la mejor alternativa actualmente para resolver el escenario (1) es la de Autek Ingeniería. Además de tratarse de una empresa española y de que el diodo haya sido probado con éxito[30], el hecho de que este dispositivo se encuentre ya acreditado por el CCN es casi decisivo, debido por un lado a la premura[31] de la solución para el Ejército de Tierra y por otro lado debido al alto coste de certificación que supondría la adquisición del diodo ELIPS-SD, tal y como se recoge en un artículo del Hague Security Delta [31]:

> *An additional cost is certification. The certification of a cybersecurity product by the French Cybersecurity Agency can cost anywhere from twenty to thirty thousand euros. At current demand levels, certification is a significant factor that drives up prices.*

Para solventar el problema de que este diodo no permite enviar mensajería entre los sistemas, se podría optar también por una solución híbrida: utilizar el diodo de Autek y también la figura del RSA/TASO, esta solución se explicará con más detalle en el punto 4.7. Igualmente, entre el puesto de mando de la brigada y los batallones, existen otras alternativas para enviar mensajería, como por ejemplo el Tactical Chat de las radios HF (High Frequency) Harris RF-5800-H [23].

Por lo tanto, se recomendaría la adquisición de diodos PSTdiode por parte del Ministerio de Defensa para dotar a las brigadas de ellos. En relación con el proceso de obtención, con esta propuesta se determinaría la alternativa de obtención en la fase de definición y decisión, para posteriormente ejecutar los contratos en la fase de ejecución y finalizar con la fase de servicio de los diodos adquiridos.

4.7 Implementación en la brigada

A continuación, se va a proponer un método para poder implementar el diodo PSTdiode en una brigada.

En el diagrama de la Figura 5, está representado el puesto de mando de la brigada con un rectángulo verde, dentro del cual se encuentra un nodo de SIMACET (con sus servidores) y un nodo de BMS. Además, existen dos dominios de seguridad distintos, un dominio RESERVADO (círculo azul) en el que se encuentra el nodo de SIMACET y otro dominio SIN CLASIFICAR (círculo rojo) en el que se encuentra el sistema BMS. Ambos

[30] Se han obtenido resultados satisfactorios con el PSTdiode en un experimento de interconexión segura entre SIMACET (GU) Reservado y BMS (PU) SIN Clasificar [27] y también en pruebas transmisión de vídeo desde una aeronave no tripulada hacia una red segura [29].

[31] Como ya se explicó en el apartado 3.2, este escenario (1) se ampara por el hito 0 de la Arquitectura de Referencia de Seguridad, el cual debe resolverse cuanto antes para poder continuar con los siguientes hitos.

dominios se encuentran interconectados a través del PSTdiode[32], que se encontraría dentro del puesto de mando de la brigada.

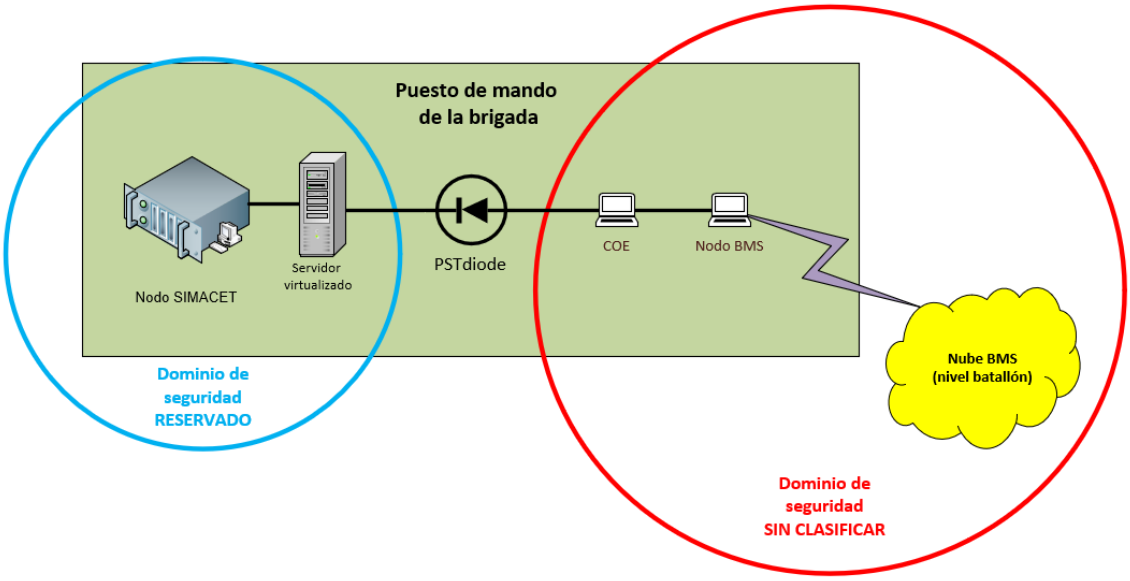

Figura 5: Diagrama de interconexión del PSTdiode en la brigada. Fuente: Elaboración propia (Visio).

La implementación se ejecutaría de la siguiente manera:

- Dentro del puesto de mando de la brigada, se desplegaría un nodo de SIMACET (preferiblemente versión 5), el cual daría servicio a los distintos clientes del cuartel general.
- A parte del nodo SIMACET, se instalaría un nodo BMS (que podría ir instalado en un portátil con Windows 10), el cual sería operado por el capitán de batalla[33].
- BMS se integraría con SIMACET mediante la pasarela COE, la cual enviaría los datos tácticos de un sistema a otro, pasando por el diodo, que integra ambos dominios de seguridad. En este escenario no se utilizaría la pasarela IDT ya que el PSTdiode no permite el envío de mensajería.
- BMS podría comunicarse con los batallones mediante distintos medios, entre ellos mediante radios VHF[34] (Very High Frequency).
- El PSTdiode está formado por dos appliances [5], el PSTs que se conectaría al dominio sin clasificar y el PSTd que se conectaría al dominio reservado, la

[32] Se optó por colocar el diodo entre COE y SIMACET ya que de esa manera está demostrado que los datos tácticos se transfieren correctamente [27].

[33] Es uno de los usuarios del puesto de mando, tanto en las maniobras CREVAL 20, realizadas durante las prácticas externas entre el 13 y el 22 de septiembre de 2020, como en las maniobras TORO 20, entre el 14 de octubre y el 28 de octubre de 2020, el capitán de batalla dispuso de un nodo BMS en el puesto de mando.

[34] Con el modo SUPERMUX de las radios PR4G V3 S se consiguen alcances de hasta 30 kilómetros, lo cual se pudo probar con éxito en las maniobras CREVAL 20.

conexión entre ambos se realizaría mediante fibra óptica, según se recoge en el documento de especificaciones técnicas del propio fabricante [34].

- El sistema del diodo puede incluir además servidores SYSLOG y de registro de transferencias[35], estos podrían ir virtualizados dentro del servidor de SIMACET v5 (el que aparece en la Figura 5 conectado al nodo SIMACET), los cuales tienen ya varias máquinas virtuales. Esto sería viable ya que, por un lado, en las especificaciones del PSTdiode se recoge que no hace falta utilizar servidores dedicados y por otro lado en la Entrevista 1 (Anexo A), pregunta {4}, se confirmó que los servidores HP ProLiant de SIMACET v5 tienen capacidad para instalar más máquinas virtuales de las que tienen actualmente.
- En la CCN-STIC 302 se recoge que, para interconectar dos sistemas, uno RESERVADO y otro SIN CLASIFICAR, se requiere un diodo en DMZ (zona desmilitarizada), para lo cual habría que instalar un cortafuegos a cada lado del diodo. Estos cortafuegos podrían ir virtualizados[36], uno en el servidor de SIMACET y otro en el portátil donde va instalada la pasarela COE (representados a ambos lados del diodo en la Figura 5). Esto sería viable ya que se podría usar cualquier tipo de firewall, según se extrajo en la pregunta {10} de la Entrevista 5 (Anexo A).
- Por último, en el sistema PSTdiode puede instalarse un software de administración (PSTadm), el cual funciona en ordenadores de propósito general, podría instalarse en un cliente de SIMACET (portátil) en el dominio RESERVADO y por otro lado en el portátil del COE[37] en el lado SIN CLASIFICAR. Los sistemas operativos de los portátiles estarían securizados según las guías correspondientes, las CCN-STIC serie 500 para entornos Windows o la serie 600 para otros entornos (LINUX, Solaris, etc.).

En la Figura 6 se puede ver en detalle cómo se implementarían todos los posibles servidores adicionales y equipos de administración. Dentro de los cuadros de texto de color rojo se especifica la ubicación, física o virtual, en la que se propone que se instale cada elemento. Los equipos en blanco pertenecen al dominio destino (SIMACET RESERVADO), mientras los equipos en negro compondrían el dominio origen (BMS SIN CLASIFICAR).

---

[35] El servidor SYSLOG recibiría del sistema información de funcionamiento (estado del sistema y notificaciones de errores) y de seguridad. Mientras que el de transferencia registraría la información de las transferencias de ficheros realizadas [34].

[36] Existen firewall/cortafuegos tanto hardware como software. Aprovechando tanto el servidor virtualizado de SIMACET v5 como el portátil de la pasarela COE, se podrían utilizar firewall en máquinas virtuales, como por ejemplo pfSense, que es una solución open source (https://www.pfsense.org/).

[37] En las maniobras TORO 20 mencionadas anteriormente, las cuales discurrieron durante las prácticas externas, se virtualizaron las pasarelas COE, IDT y el sistema BMS en un mismo equipo, con lo cual sería viable virtualizar en un mismo equipo la pasarela COE, el PSTadm y un firewall open source.

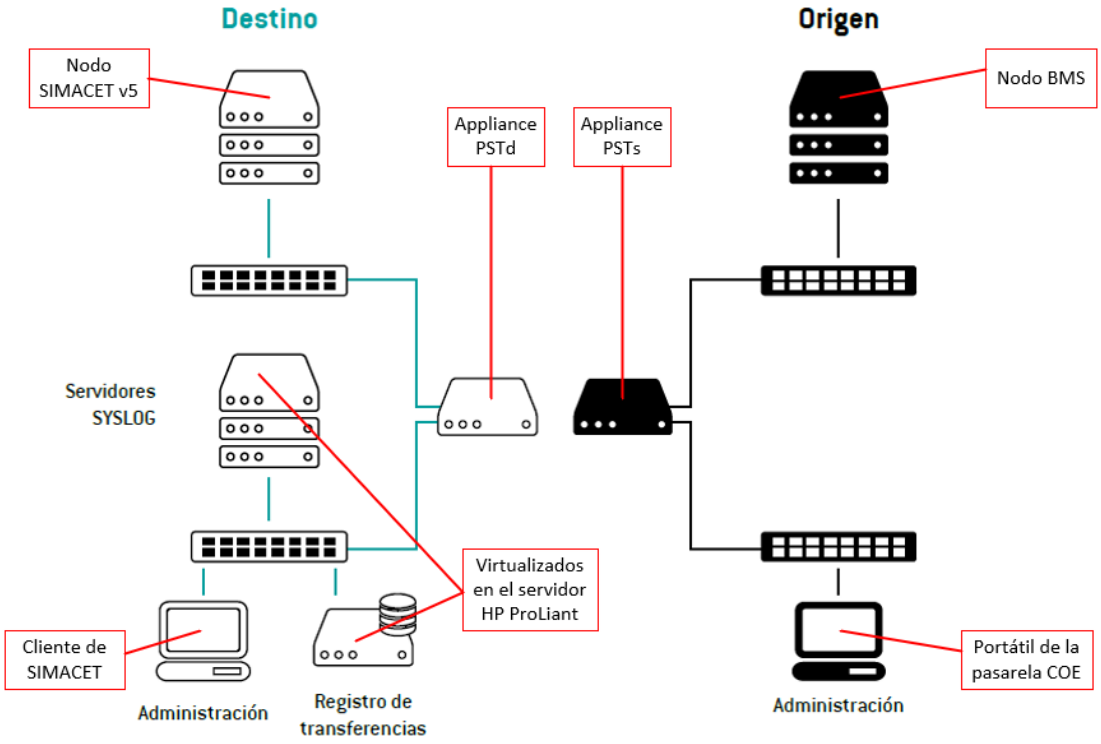

Figura 6: Diagrama detallado de los elementos del PSTdiode. Fuente: Especificaciones técnicas del PSTdiode [34] y elaboración propia (Visio).

De esta manera tendríamos integrados los dos dominios de seguridad. Por un lado, estaría el dominio de seguridad de la red de BMS SIN CLASIFICAR, que enviaría los datos tácticos hacia SIMACET y, por otro lado, el dominio RESERVADO conectado mediante el PSTdiode, el cual garantiza que no hay transferencia de información hacia el dominio menos seguro.

Se propone la solución híbrida[38] que se mencionó anteriormente para el caso en el que se requiera enviar mensajería entre ambos sistemas. Se explicará mediante un ejemplo: un comandante de cuartel general (con su puesto de trabajo en el puesto de mando de la brigada) quiere enviar un mensaje/archivo por BMS[39] con destino al batallón 1. El comandante se lo comunicaría al RSA, el cual lo introduciría en su dispositivo de almacenamiento portátil seguro y lo introduciría en el nodo de BMS que se encuentra en el puesto de mando, donde posteriormente el operador de ese nodo enviaría el archivo a su destinatario. Del mismo modo, si se quisiera enviar un archivo de BMS a SIMACET, como por ejemplo un informe de situación que provenga de un batallón, se realizaría el procedimiento inverso.

[38] Esta solución híbrida que se propone es distinta a la que se propuso en el apartado 4.6, en el cual se contemplaba utilizar transporte físico como solución única (sin utilizar diodo).

[39] Con la precaución de que, en el caso de enviar un mensaje desde un sistema RESERVADO hacia otro SIN CLASIFICAR, el mensaje no podría ser de otro nivel que no fuera SIN CLASIFICAR, ya que es el máximo nivel de clasificación que se permite manejar en ese sistema (Anexo A, Entrevista 3, pregunta {9}).

Como se mencionó anteriormente, también estaría la posibilidad de utilizar el Tactical Chat a través de los equipos HF de Harris. Tanto el sistema de mensajería de BMS como el de Tactical Chat permiten enviar mensajes de texto y archivos.

Capítulo 5. Conclusiones y líneas de trabajo futuras

5.1 Conclusiones

Enlazando con los objetivos que se establecieron al inicio del presente trabajo, y tras la aplicación de la metodología descrita en la introducción, se concluye lo siguiente:

- Se han encontrado cuatro posibles soluciones (diodos, pasarelas de intercambio seguro, security guard y transporte físico) para la integración de dominios de seguridad entre BMS y SIMACET, de las cuales, para el escenario (1) que se propuso resolver (dominios SIMACET RESERVADO y BMS SIN CLASIFICAR), únicamente se determinó viable la alternativa de los diodos de datos después de la comparativa y el análisis realizado.
- La solución definitiva propuesta es el diodo PSTdiode desarrollado por la empresa Autek Ingeniería, debido a que se trata de una empresa española, se ha comprobado el funcionamiento del diodo de forma satisfactoria y además se encuentra acreditado por el Centro Criptológico Nacional.
- Esta solución se ha buscado para lograr la integración de los dominios de BMS y SIMACET (lo cual no quiere decir que el diodo no fuera útil para otros sistemas), para la cual se ha propuesto un método para implementarla en las brigadas del ET sin tener que adquirir nada más que el PSTdiode.
- El presente trabajo de fin de grado podría servir para orientar un posible proyecto de adquisición de diodos para lograr la buscada integración de dominios de seguridad, para lo cual se han abordado fases del proceso de adquisición del Ministerio de Defensa, como la definición de la necesidad operativa con la definición de la problemática y la determinación de la alternativa de obtención en la parte de propuesta de solución.

Cabe remarcar que la integración de dominios de seguridad en general, y en particular entre BMS y SIMACET, no tiene una solución estática en el tiempo ni única, ya que como hemos visto con los distintos escenarios, puede ir variando, dependiendo de la clasificación de seguridad que se pretenda establecer en cada sistema y de la normativa vigente.

Como conclusión final, para que la integración de dominios de seguridad no fuera un impedimento burocrático ni una merma en la operatividad de las brigadas del Ejército de Tierra, sería interesante que se agilizaran los procesos de acreditación de los sistemas de información de mando y control y que las unidades dispusieran de los dispositivos de protección de perímetro adecuados a cada situación. Todo ello para que las compañías de transmisiones puedan desempeñar su trabajo en condiciones reales en los ejercicios en territorio nacional, mejorando su preparación de cara a desplegar en teatro de operaciones. Siempre con el foco en la seguridad de la información, para que las brigadas del Ejército de Tierra puedan cumplir las misiones que les sean encomendadas con las garantías necesarias.

5.2 Líneas de trabajo futuras

Durante la realización de este trabajo de fin de grado, se detectaron posibles proyectos, los cuales no se encontraban dentro del alcance de este trabajo. Sin embargo, se proponen dos líneas de trabajo que podrían ser interesantes:

1) Como ya se explicó, tras la resolución del Hito 0 (en el cual se focaliza este trabajo), se establece un plazo de dos años para resolver el Hito 1 [20]:

   > *Disponer de una solución que permita el despliegue en el PC Brigada de dos dominios de seguridad que manejen información con niveles de clasificación "DIFUSIÓN LIMITADA" y "RESERVADO NACIONAL".*

   En este caso nos encontraríamos en el escenario (2) que se propuso anteriormente, para el cual sería necesario buscar una pasarela de intercambio seguro que completara este hito.
2) En este trabajo se ha propuesto la instalación de dos firewalls virtualizados para crear la DMZ como solución temporal, ya que se escapaba del ámbito de este trabajo la determinación de un firewall óptimo. Sin embargo, en un proyecto "make or buy" podría abordarse el desarrollo de un firewall propio para el ET o la compra de firewalls disponibles en el mercado.

Capítulo 6. Bibliografía

La bibliografía se ha clasificado según el tipo de publicación y dentro de cada grupo, por orden alfabético. La normativa, al final de la bibliografía, se ha ordenado según la jerarquía normativa en España, y las del mismo nivel, en orden cronológico descendente.

Publicaciones del Centro Criptológico Nacional:

[1] Centro Criptológico Nacional. *CCN-STIC 101: Acreditación de sistemas de las TIC que manejan información clasificada* [en línea]. 2016 [consulta: 10 septiembre 2020]. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/8-ccn-stic-101-procedimiento-de-acreditacion-nacional/file.html

[2] Centro Criptológico Nacional. *CCN-STIC 105: Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación* [en línea]. 2020 [consulta: 1 septiembre 2020]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

[3] Centro Criptológico Nacional. *CCN-STIC 140: Taxonomía de referencia para productos de seguridad TIC - Anexo D.6: Pasarelas para intercambio de datos* [en línea]. 2017 [consulta: 25 septiembre 2020]. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3941-guia-140-anexo-d-6-pasarelas-seguras-de-intercambio-de-datos/file.html

[4] Centro Criptológico Nacional. *CCN-STIC 1401: Configuración segura de pasarelas de Autek Ingeniería* [en línea]. 2018 [consulta: 9 septiembre 2020]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2916-ccn-stic-1401-configuracion-segura-de-pasarelas-de-autek-ingenieria/file.html

[5] Centro Criptológico Nacional. *CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería* [en línea]. 2019 [consulta: 1 septiembre 2020]. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/3656-ccn-stic-1408-procedimiento-de-empleo-seguro-diodo-autek-ingenieria/file.html

[6] Centro Criptológico Nacional. *CCN-STIC 811: Interconexión en el ENS* [en línea]. 2017 [consulta: 4 octubre 2020]. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/521-ccn-stic-811-interconexion-en-el-ens/file.html

[7] Centro Criptológico Nacional. *CCN-STIC-302: Interconexión de sistemas de las tecnologías de la información y las comunicaciones que manejan información nacional clasificada en la administración*. 2012.

[8] Centro Criptológico Nacional. *Política de Seguridad de las TIC (CCN-STIC 001)* [en línea]. 2016 [consulta: 28 septiembre 2020]. Disponible en: https://www.ccn-

cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1579-ccn-stic-001-informacion-clasificada-en-la-administracion/file.html

Publicaciones del Centro Universitario de la Defensa/Academia General Militar:

[9] Área de Transmisiones. *Introducción a los CIS*. 2019.

[10] BERNARDI, Simona y DRANCA, Lacramioara. *Sistemas de Información para la Dirección: Un enfoque guiado por un caso de estudio*. Zaragoza: Centro Universitario de la Defensa, 2016. ISBN 978-84-942315-0-6.

[11] Centro Universitario de la Defensa. *Oficina de Proyectos. Tema 6: Gestión de adquisiciones*. 2019.

[12] Centro Universitario de la Defensa. *Redes y Servicios de Comunicaciones. Tema 1: Introducción a las redes de comunicaciones*. 2019.

[13] Departamento de Técnica Militar. *AGM-TM-406 Fundamentos de los ordenadores*. 2017.

[14] Departamento de Técnica Militar. *AGM-TM-408 Transmisión de datos. Volumen I: Redes de datos y comunicaciones inalámbricas*. 2017.

[15] Departamento de Técnica Militar. *AGM-TM-409 Transmisión de datos. Volumen II: Transmisión multimedia*. 2017.

[16] Silvia VICENTE, Jorge GONZÁLEZ y Pedro José MARTÍNEZ. *Gestión de la Innovación y Política Tecnológica (Perfil Defensa)*. 1ª edición. Zaragoza: Centro Universitario de la Defensa, 2019. ISBN 978-84-942315-7-5.

Manuales/documentos doctrinales del Ejército de Tierra:

[17] Estado Mayor del Ejército. *Plan de transición al MC3 del ET*. 2017.

[18] Estado Mayor del Ejército. *Plan MC3 "Plan de modernización de los sistemas de mando, control y comunicaciones del Ejército de Tierra"*. 2015.

[19] Indra Sistemas, S.A., Thales Programas, S.A.U. y Ministerio de Defensa. *Manual de Planificación, Parametrización y Administración del sistema BMS-ET-XP*. 2017.

[20] Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica. *Arquitectura de Referencia de Seguridad de los CIS Desplegables*. 2017.

[21] Mando de Adiestramiento y Doctrina. *Apoyo a la preparación: Experiencias y Lecciones 2016-2017*. Granada: 2018.

[22] Mando de Adiestramiento y Doctrina. *Conceptos para el combate 2035*. 2019.

[23] Mando de Adiestramiento y Doctrina. *MI-506 Radio HF Harris RF-5800-H*. Granada: 2018.

[24] Mando de Adiestramiento y Doctrina. *PD3-602 Establecimiento y empleo de SIMACET*. Granada: 2009.

[25] Mando de Adiestramiento y Doctrina. *PD4-500 Procedimientos operativos CIS*. 2ª edición. Granada: 2013.

Revistas:

[26] HERRERA CRUZ, Sebastián Pedro. Los CIS para el mando y control en Afganistán. *Revista Ejército: Operación Romeo Alfa: Balance de las Operaciones en Afganistán* [en línea]. 2014, nº 878 [consulta: 20 septiembre 2020]. ISSN 1696-7178. Disponible en: https://ejercito.defensa.gob.es/Galerias/multimedia/revista-ejercito/2014/Revista_Ejercito_878_Extra_Mayo_2014.pdf

Trabajos académicos/artículos/informes:

[27] Cuartel General de la Fuerza Terrestre. *Plan de experimentación mando y control: Ficha de experimento Nº 8*. 2020.

[28] GARCÍA SOBRIDO, Juan Manuel. *Trabajo de Fin de Grado: Capacidades y limitaciones del sistema BMS*. 2017.

[29] Regimiento de Transmisiones Nº 21. *Informe sobre el intercambio de información clasificada de la aeronave no tripulada "ScanEagle" para la red SIJE en el ejercicio JFX-19*. 2019.

[30] ROSS, D. Arnold. *Strategies for transporting data between classified and unclassified networks* [en línea]. New Jersey: 2016 [consulta: 16 septiembre 2020]. Disponible en: https://apps.dtic.mil/dtic/tr/fulltext/u2/1005160.pdf

[31] The Hague Security Delta. *Understanding the Strategic and Technical Significance of Technology for Security: The Case of Data Diodes for Cybersecurity*. 2019.

Libros:

[32] Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. Pennsylvania: 2000. ISBN 1-880410-22-2.

Otros:

[33] Adquisición de diodos de intercambio de información clasificada para SIMACET. En: *Plataforma de Contratación del Sector Público* [en línea] [consulta: 3 octubre 2020]. 2018. Disponible en: https://contrataciondelestado.es/wps/wcm/connect/f7baf653-b795-430e-b1df-419904679f9c/DOC_CAN_ADJ2018-566993.html?MOD=AJPERES

[34] Autek Ingeniería. PSTdiode Technical Specifications. En: *NATO Communications and Information Agency* [en línea] [consulta: 11 octubre 2020]. Disponible en: https://www.ia.nato.int/DocumentGenerator/repository/version/ea08f001-6ea0-40fb-b1c3-e719dcd59f10/PSTdiode-Data-Diode-Product%20Sheet

[35] Centro Criptológico Nacional. CCRA Certificate Autek PSTdiode. En: *Common Criteria Portal* [en línea] [consulta: 10 octubre 2020]. Disponible en: https://www.commoncriteriaportal.org/files/epfiles/2017-09-CCRA.pdf

[36] NATO Information Assurance Product Catalogue. ELIPS-SD. En: *NATO Communications and Information Agency* [en línea] [consulta: 12 octubre 2020]. Disponible en: https://www.ia.nato.int/niapc/Product/ELIPS-SD_419

[37] NATO Information Assurance Product Catalogue. PSTdiode Data Diode. En: *NATO Communications and Information Agency* [en línea] [consulta: 11 octubre 2020]. Disponible en: https://www.ia.nato.int/niapc/Product/PSTdiode-Data-Diode_773

[38] New Thales cybersecurity solution for industrial networks. En: *Thales Group* [en línea] [consulta: 13 octubre 2020]. Disponible en: https://www.thalesgroup.com/en/worldwide/security/press-release/new-thales-cybersecurity-solution-industrial-networks

[39] Presidencia del Gobierno. Estrategia Nacional de Ciberseguridad 2019. En: *Agencia Estatal Boletín Oficial del Estado* [en línea] [consulta: 25 septiembre 2020]. Disponible en: https://www.boe.es/eli/es/o/2019/04/26/pci487

[40] Unión Internacional de Telecomunicaciones. *Términos y definiciones de referencia para la gestión de la identidad* [en línea]. 2010 [consulta: 8 septiembre 2020]. Disponible en: https://www.itu.int/rec/T-REC-X.1252-201004-I/es

Normativa:

[41] Ley 9/1968, de 5 de abril, sobre secretos oficiales. (https://www.boe.es/buscar/act.php?id=BOE-A-1968-444).

[42] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. (https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330).

[43] Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa. (https://www.defensa.gob.es/Galerias/portalservicios/seginfoemp/OM_76_06_Politica_Seguridad_Informacion_MINISDEF.pdf).

[44] Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos (SEGINFODOC). (http://www.madrid.org/archivos/images/AREA_PROFESIONAL/Legislacion_archivistica/EST_SED_Instruccion_51-2013.pdf).

[45] Instrucción 72/2012, de 2 de octubre, del Secretario de Estado de Defensa, por la que se regula el proceso de obtención del armamento y material y la gestión de sus programas. (https://www.infodefensa.com/archivo/files/04_INSTRUCCION_72_2012_PROCESO_DE_OBTENCION_DE_ARMAMENTO.pdf).

[46] Instrucción 67/2011, de 15 de septiembre, del Secretario de Estado de Defensa, por la que se regula el Proceso de Obtención de Recursos Materiales. (https://www.infodefensa.com/archivo/files/03__INSTRUCCION_67_2011_PROCESO_DE_OBTENCION_RECURSOS.pdf).

Capítulo 7. Anexos

Anexo A. Entrevistas realizadas a personal experto

Recopilación de las preguntas más relevantes realizadas en las distintas entrevistas a expertos:

Entrevista 1: Sargento de la sección de explotación de la Compañía de Transmisiones nº7.

{1} En cuanto a número de nodos, clientes, versiones, acreditaciones, etc. ¿Cuál es la situación actual de SIMACET en la Brigada "Galicia" 7?

Ahora mismo la Brigada "Galicia" VII cuenta con 3 nodos de SIMACET, uno de ellos en versión 5 (que utiliza máquinas virtuales) y 2 en versión 4.2 sobre servidores físicos. Dependiendo del tipo de nodo los clientes que tenemos son los siguientes:

- *2 nodos GUL (Gran Unidad Ligero): cada uno con 20 clientes (40 en total).*
- *1 nodo PUT (Pequeña Unidad Táctica): con 5 clientes.*

En cuanto a una posible acreditación, ahora mismo no se contempla puesto que aún utilizamos servidores con Windows Server 2008 R2 y clientes con Windows 7. Ambos han perdido recientemente el soporte por parte de la empresa Microsoft, por tanto, no pasarían una acreditación de seguridad del CCN.

{2} ¿Cuál es la situación actual de BMS en la Brigada "Galicia" 7?

En cuanto a acreditaciones ahora mismo con el BMS se trabaja SINCLAS, aunque en un futuro se espera que funcione a nivel Difusión Limitada.

{3} ¿Cómo se realiza la integración de SIMACET con BMS en la brigada? ¿Funciona esa integración de forma satisfactoria?

Si bien en un futuro se espera que tanto SIMACET como BMS trabajen con protocolo IDT y por tanto su conectividad sea directa, ahora mismo la versión que se utiliza en SIMACET utiliza un protocolo diferente y por lo tanto es necesario el uso de pasarelas. La integración de BMS y SIMACET utiliza un cliente especial con base de datos de Oracle que integra la información recibida de BMS y la transforma para que funcione en SIMACET, este cliente especial se conoce como cliente COE.

Esta integración aún debe ser sometida a un proceso de pulido para que proporcione más información que la que actualmente se recibe, pero de momento la información es suficiente para que el mando pueda tomar decisiones en base a lo que se integra en SIMACET.

{4} ¿Sería viable virtualizar tres máquinas virtuales extra (un servidor SYSLOG, un servidor de registro de transferencias y un firewall open source) en los servidores de SIMACET v5?

Los servidores HP ProLiant DL380p Gen8 que actualmente usamos con los nodos de SIMACET v5 tienen capacidad de sobra, actualmente con SIMACET se utiliza

aproximadamente un 20% de la capacidad de almacenamiento de los servidores y también tienen capacidad de memoria RAM sobrante (cada uno de los dos servidores tiene 192 GigaBytes de RAM), por lo que no habría ningún problema en instalar máquinas virtuales extra.

Entrevista 2: Profesor Contratado Doctor del Departamento de Informática e Ingeniería de sistemas de la Universidad de Zaragoza.

{5} ¿Sería viable el desarrollo de un software que funcionara como diodo de datos para lograr la integración de los dominios de seguridad entre SIMACET y BMS?

Desde un punto de vista software se podría implementar algo similar a la solución de diodo planteada por el CCN, aunque existe el riesgo que, si se desconocen los problemas inherentes a la tecnología, puede haber fallos en el diseño del sistema que supongan el compromiso de información sensible.

Entrevista 3: Teniente coronel de la SECARQINT (Sección de Arquitectura e Interoperabilidad) de la JCISAT (Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica).

{6} En cuanto a la acreditación de SIMACET y BMS a los niveles de clasificación que pretende alcanzar el Ejército de Tierra, ¿En qué situación se encuentran?

EL SIMACET (SC2NET) es reservado ya que la información que maneja es de nivel reservado, esto implica que el sistema se tiene que acreditar.

El BMS actualmente es SINCLAS, pero se está trabajando para que sea Difusión Limitada. Lo previsto es que alcance esa situación en 2021 o 2022, dependiendo de la situación presupuestaria.

{7} ¿Por qué hay unidades que utilizan SIMACET SINCLAS?

Las Brigadas, para utilizar SIMACET en ejercicios internacionales u operaciones, necesitan acreditar el sistema a RESERVADO. Mientras no se encuentren en esa situación no necesitan la acreditación.

Hay unidades, que acreditan el sistema todos los años para los ejercicios internacionales en los que participa. Por otro lado, el SC2NET CGP (SIMACET Cuarteles Generales Permanentes) está acreditado a RESREVADO.

Entrevista 4: Teniente coronel jefe del Centro de Acreditación de Sistemas de la JCISAT.

{8} En cuanto a la acreditación de los sistemas BMS y SIMACET a los niveles de clasificación que pretende alcanzar el Ejército de Tierra, ¿En qué situación se encuentran actualmente?

Un sistema se acredita en unas condiciones y situación determinadas, lo que implica el lugar, las personas y la configuración lógica. Es decir, un conjunto de ordenadores no se acredita para dejarlo almacenado a la espera de ser usado. La acreditación es un proceso largo y complejo. Las normas de la ONS (Oficina Nacional de Seguridad) y la NT 04/11 "Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT) en el ámbito del Ejército de Tierra", explican bien todo el proceso.

Ten en cuenta que: SIMACET como hasta ahora se ha entendido no es un sistema de ordenadores, sino que ha pasado a ser un servicio dentro de sistemas TIC desplegables o permanentes. Es decir, se instala una red o sistema que se denomina SC2NET-D, (Sistema de Mando y Control Nacional del Ejército de Tierra Desplegable) que consiste en un conjunto de servidores, clientes, electrónica de red y equipos de comunicaciones capaces de conectarse a otros sistemas y de servir de "granja de servicios", entre los cuales hay muchas máquinas virtuales que los soportan, entre otros, el SIMACET.

SC2NET-CGP es la red permanente que está acreditada a RESERVADO Nacional, y son 12 nodos actualmente, 12 "granjas" como las que he mencionado. De momento está en estudio su futura posibilidad de interconexión con sistemas tácticos (y por tanto aún no se permite), sea cual sea su nivel de acreditación.

BMS debería ser una red DL o como mucho acreditarse a CONFIDENCIAL, pero ningún BMS actualmente permite ni uno ni lo otro.

{9} ¿Por qué la información que maneja SIMACET es reservada y la que maneja BMS va a ser difusión limitada? ¿Qué tipo de información se "encuadra" dentro de cada nivel de clasificación?

La Política de SEGINFO define perfectamente lo que es información clasificada y las potestades para clasificarla, de acuerdo con la Ley 9/1968, de 5 de abril, sobre secretos oficiales, se establece la SECRETA y la RESERVADA, y por la propia política la CONFIDENCIAL y la DIFUSION LIMITADA.

En cuanto a cómo se clasifica cada una, las guías de clasificación son muy antiguas, provienen de la Instrucción comunicada 1/82, ya derogada y de la IG 9/89 EME (2ª División).

¿Por qué en un sistema la información es RESERVADA y en el otro DIFUSIÓN LIMITADA? Pues depende de la propia información, pero es al revés como hay que mirarlo, en un sistema acreditado a RESERVADO solo se puede manejar información hasta el nivel de RESERVADO y los más bajos, y en un sistema DIFUSIÓN LIMITADA no se puede manejar información CONFIDENCIAL o RESERVADA.

Entrevista 5: Comandante de la Sección de Ingeniería de Tecnologías de la Información, Telecomunicaciones y Simulación de la Jefatura de Ingeniería del MALE (Mando de Apoyo Logístico del Ejército).

{10} En el CCN-STIC 302 especifica que para interconectar dos sistemas uno sin clasificar y otro reservado es necesario un diodo en DMZ, para lo cual serían necesarios dos firewalls, uno a cada lado. ¿Sabe usted si sería viable implementar un firewall de código abierto? ¿O sería necesario instalar dos firewalls hardware?

Lo que indica la guía del CCN 302 es un ejemplo de arquitectura de sistema de protección. El diodo es un dispositivo independiente de los cortafuegos, en caso de que estos sean requeridos/empleados.

Existen cortafuegos de varios tipos y puedes elegir para ilustrar tu ejemplo el que más te interese puesto que, el diodo simplemente transfiere la información de forma unidireccional con seguridad física. Su operativa básica es independiente del tipo de cortafuegos que pueda flanquearlos.

Anexo B. Estructura de Desglose de Trabajo

En la EDT se detallan las distintas tareas que se han acometido para lograr los objetivos del trabajo, con sus hitos temporales asociados.

ID	Nombre tarea	Descripción	Fecha inicio	Fecha fin
1	**Recopilación de información**	En esta primera fase se obtendrá toda la información posible y se hará un estudio detallado de la misma.	01/07/2020	27/09/2020
1.1	Lectura de manuales y documentación disponible previamente	Repaso de asignaturas de cursos previos de la Academia General Militar y consulta de manuales de transmisiones.	01/07/2020	06/09/2020
1.2	Búsqueda en bases de datos civiles y militares	Biblioteca virtual de defensa, ALCORZE y búsqueda de normativas relacionadas con el trabajo.	07/09/2020	20/09/2020
1.3	Entrevistas a personal experto	Realización de entrevistas y consultas a expertos en la materia, tanto civiles como militares.	21/09/2020	27/09/2020
1.4	Contacto con empresas	Búsqueda y contacto con empresas que provean productos o servicios que sean interesantes para el proyecto.	21/09/2020	27/09/2020
1.4	Estudio de toda la documentación	Discriminación de la información relevante para la investigación.	07/09/2020	27/09/2020
2	**Definición de la problemática y posibles soluciones**	En este punto, se explicará detalladamente el problema y las posibles soluciones encontradas.	28/09/2020	04/10/2020
2.1	Recopilación de requisitos	Detallar el problema en base a la información obtenida tanto en bases de datos como en consultas y entrevistas.	28/09/2020	30/09/2020
2.2	Búsqueda de las diferentes soluciones	Enumeración y explicación de las posibles soluciones.	01/10/2020	04/10/2020
3	**Análisis de las distintas alternativas y elección de la más óptima**	Se compararán las soluciones encontradas y se propondrá la más apropiada para las necesidades del Ejército de Tierra.	05/10/2020	11/10/2020
3.1	Comparativa de las soluciones encontradas	Pros y contras de cada alternativa en base a distintos criterios, como por ejemplo criterios de seguridad o de operatividad.	05/10/2020	08/10/2020
3.3	Propuesta de la solución más óptima	Se realizará una propuesta objetiva de una solución en base a los criterios utilizados anteriormente.	09/10/2020	11/10/2020
4	**Conclusiones y gestión de adquisiciones**	Relación del trabajo realizado con un posible proceso de adquisición y se comprobarán los resultados del trabajo en relación con los objetivos iniciales.	12/10/2020	18/10/2020
5	**Elaboración de la memoria**	Realización de un informe de todos los trabajos realizados y redacción de las conclusiones finales.	28/09/2020	25/10/2020

Figura 7: Estructura de Desglose de Trabajo. Fuente: Elaboración propia (Excel).

Anexo C. Diagrama de Gantt

El diagrama de Gantt complementa la EDT, mostrando de una forma más gráfica la distribución temporal de cada una de las cinco tareas más importantes que se realizaron durante el desarrollo del trabajo.

Actividades	Fecha inicio	Duración en días	Fecha fin
Recopilación de información	01-sep	26	27-sep
Definición de la problemática y búsqueda de soluciones	28-sep	6	04-oct
Análisis de alternativas y elección de solución	05-oct	6	11-oct
Conclusiones y gestión de adquisiciones	12-oct	6	18-oct
Elaboración de la memoria	28-sep	27	25-oct

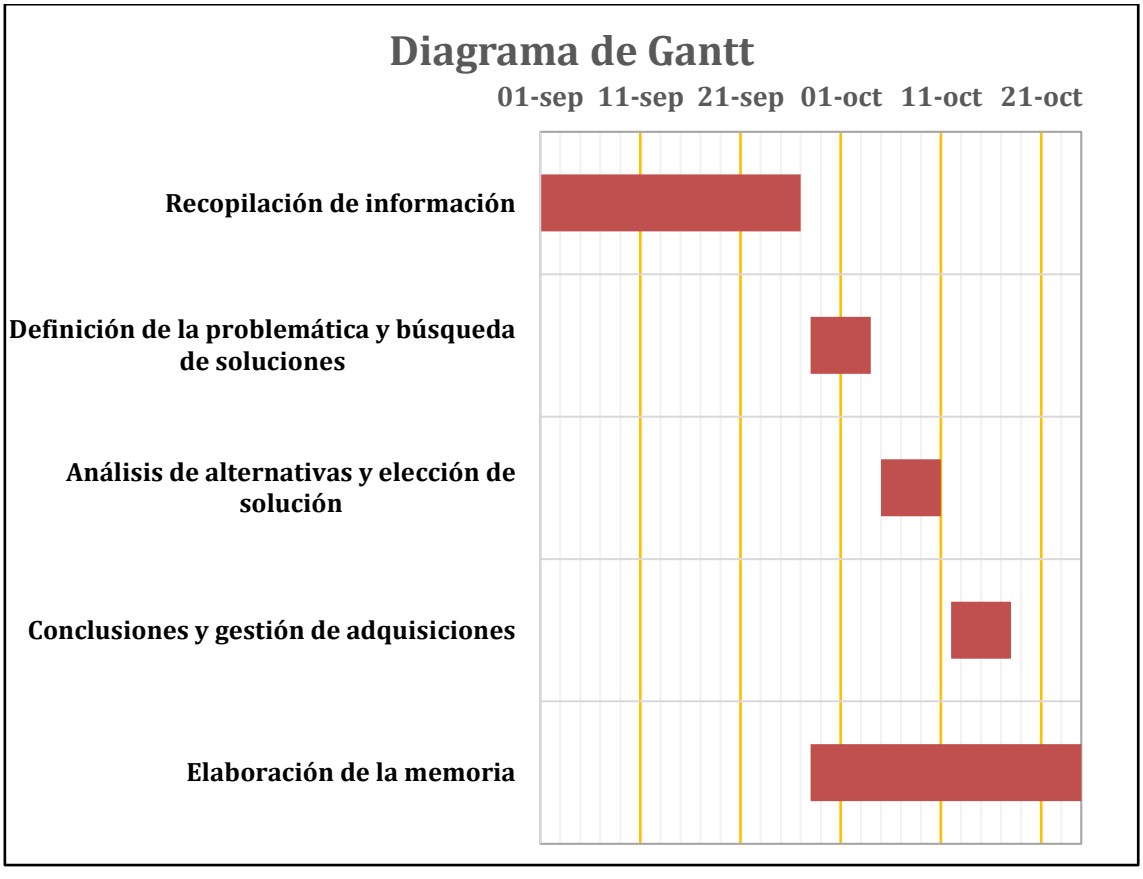

Figura 8: Diagrama de Gantt. Fuente: Elaboración propia (Excel).

Anexo D. Equivalencia entre modelos OSI, TCP/IP, protocolos y dispositivos

En esta tabla se han incluído únicamente los protocolos y los tipos de dispositivos que se mencionan en esta memoria, aunque existen más protocolos y dispositivos de los aquí representados.

CAPAS MODELO OSI	CAPAS MODELO TCP/IP	PROTOCOLOS	DISPOSITIVOS	
Aplicación	Aplicación	FTP, FTPS, SFTP, SMTP, SMB	PCs, portátiles, servidores	
Presentación				
Sesión				
Transporte	Transporte	TCP, UDP		
Red	Internet	IP	Router	
Enlace	Acceso a la red		Switch	
Físico			Hub	

Tabla 2: Equivalencia entre modelos OSI y TCP/IP. Fuente: Elaboración propia (Excel).

Anexo E. Ficha técnica del diodo PSTdiode

CARACTERÍSTICAS GENERALES

Topología	Un *appliance* en cada dominio de seguridad, la comunicación entre ambos se realiza exclusivamente a través de fibra óptica.
Topología de administración	Interfaz de administración separada (opcional) en ambos *appliances*.
Despliegue	*Appliances* listos para usar. El sistema se configura remotamente una vez establecidos, en ambos *appliances*, los parámetros de red y PKI mediante una interfaz local.
Administración	El sistema se monitoriza mediante PSTadm desde el dominio de destino. La administración remota del *appliance* del dominio de origen sólo es necesaria para cambios de configuración y solución de problemas.
Estado y notificaciones de error	El sistema envía eventos de SYSLOG de funcionamiento y seguridad de manera independiente.
Roles de administración	El sistema permite definir 4 roles diferentes de administración: • Administrador raíz • Administrador de seguridad • Administrador de servicios • Administrador de monitorización
Registro de transferencias	Es posible registrar la información de las transferencias realizadas en ficheros o base de datos. Se realiza mediante un componente software separado (PSTaud) que funciona en un ordenador de propósito general ubicado en la red destino.
Tasa de transferencia	La tasa de transferencia del dispositivo PSTdiode ATKDDL es 1 Gbps.

DATOS TÉCNICOS DE LOS *APPLIANCES*

Conexiones

Interfaz de video	VGA 15 pines
Interfaz teclado y ratón	USB tipo A
Interfaz red de datos	RJ45 (Ethenet 10/100/1000 Mbps) o LC duplex 1000 Mbps
Interfaz red de administración	RJ45 (Ethenet 10/100/1000 Mbps) o LC duplex 1000 Mbps

Características físicas

Altura	4.28 cm (1U)
Anchura	48.24 cm (19"rack)
Profundidad	49.7 cm sin frontal
Peso	8.78 kg

Alimentación

Conector	IEC-60320-C14
Potencia	250 W
Disipación de calor	1039 BTU/hr máximo
Tensión	100-240 V AC, autoranging, 50/60 Hz,4.0 A-2.0 A
Corriente de irrupción máxima	55 A
Batería	CR-2032

Temperatura

Funcionamiento	De 10ºC a 35ºC
Almacenamiento	De -40ºC a 65ºC
Gradiente máximo	20º C/h

SEGURIDAD

Topología	Permite separar todo el tráfico de administración del tráfico de datos en ambos *appliances*.
Estado y notificaciones de error	Los eventos de seguridad se pueden tratar de manera separada.
Comunicaciones de administración	Solo los administradores autorizados, mediante certificados digitales, pueden administrar el sistema. Las comunicaciones de los componentes software con los *appliances* están protegidas mediante TLS con autenticación del extremo remoto. Se registran todos los accesos y operaciones realizados por los administradores del sistema.
Garantía de integridad del firmware	Todo el software (incluido el sistema operativo) se ejecuta desde una partición de solo lectura, cuya integridad puede ser verificada en cualquier momento.

Figura 9: Especificaciones técnicas del PSTdiode. Fuente: PSTdiode: Especificaciones técnicas [34].