Universidad Zaragoza

Trabajo Fin de Grado

ESTADO DE LA CIBERSEGURIDAD EN LOS MEDIOS CIS TÁCTICOS DE UNA BOP

Autor

CABALLERO ALFÉREZ CADETE DE TRANSMISIONES JUAN IGNACIO OLIVARES GONZÁLEZ

Directores

Dr. D. Ricardo J. Rodríguez

TCol. D. Fernando Gordo García

Centro Universitario de la Defensa-Academia General Militar

2018

-PÁGINA INTENCIONADAMENTE EN BLANCO-

Resumen

Gracias a los avances tecnológicos actuales, la ciberseguridad es un pilar fundamental en cualquier ámbito de la sociedad. Evitar intrusiones o pérdida de información en los sistemas de información es uno de los objetivos principales de cualquier empresa u organización que se precie. También lo es, por tanto, en las Fuerzas Armadas debido a la gran cantidad de información sensible con la que se trabaja.

A partir de este objetivo nace este trabajo, que pretende definir las posibles vulnerabilidades del sistema de información más susceptible de ser dañado del Ejército de Tierra (en adelante ET), que es SIMACET, así como proponer soluciones. Con este objetivo, la metodología utilizada es la siguiente: En un primer lugar se analiza el estado del arte del citado sistema para conocer las actuales vulnerabilidades por medio de entrevistas a personal cualificado de la Compañía de Transmisiones de la Bandera de Cuartel General de la Brigada II de La Legión “Rey Alfonso XIII” y con la búsqueda y posterior filtrado de información proporcionada por ese mismo personal. Más tarde, se utiliza el método científico Delphi distribuyendo dos encuestas a diferente personal del acuartelamiento involucrado en los sistemas. Estas encuestas se entregarán en dos momentos diferentes y servirán para obtener información esencialmente cualitativa y precisa acerca del actual uso y futuro de estos sistemas. Por último, se realiza una práctica en un laboratorio simulando este sistema y monitorizando a tiempo real ciertas amenazas que pueda sufrir con el fin de observar la respuesta dada ante estas situaciones, buscando posibles soluciones de mejora.

Algunas de estas propuestas de mejora son realizar actividades de instrucción y adiestramiento para el personal encargado del Sistema de Información, acudir a charlas coloquios y cursos de familiarización con el Sistema, o aprovechar los recursos disponibles en materia de seguridad. Estas soluciones darán un enfoque diferente a la hora de implementar nuevos sistemas de información o mejorar los actuales.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

Abstract

Thanks to current technological advances, cybersecurity is a fundamental pillar in any area of society. To avoid the trespassing or data breaches in information systems is one of the main objectives of any company or organization. This is also the case in the Armed Forces, due to the large amount of sensitive information they work with.

This project aims to define the possible vulnerabilities of the most susceptible information system susceptible to be compromised on the Army (hereinafter ET), which is SIMACET, and propose solutions against those attacks. Taking this into consideration, the methodology used in this work is as follows: First, the state-of-the-art of SIMACET is analyzed, as a mechanism to know the current vulnerabilities. This analysis is performed through interviews with qualified personnel of the Compañía de Transmisiones de la Bandera de Cuartel General de la Brigada de La Legión "Rey Alfonso XIII", and with the searching and subsequent filtering of information provided by that same personnel. Then, the Delphi scientific method is used, distributing two surveys to different personnel of the quartering involved in the use of SIMACET. These surveys are delivered at two different times and enable us to essentially obtain qualitative and accurate information about the future of SIMACET. Finally, a laboratory session is carried out simulating SIMACET and monitoring in real time a pair of particular threats that it may suffer, in order to find solutions.

Some of these proposals to improve the system are aimed at carrying out instruction and training activities for the staff in charge of the Information System; at attending talks and colloquia, and familiarization courses with the System; and at taking advantage of available resources in security terms. Those solutions will give a different approach when implementing new information systems or improving current ones in the near future.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

Agradecimientos

Con la entrega de este trabajo de fin de grado termina una etapa muy importante en mi vida, la cual no podría haber culminado sin la ayuda y apoyo de mucha gente. De ese modo quisiera agradecer en primer lugar a mi familia y amigos que siempre estuvieron ahí cuando lo necesité. A los profesores civiles y militares que me han enseñado todo lo que sé y me han sabido trasmitir los valores y conocimientos que debe poseer un Oficial del Ejército de Tierra. De igual manera querría agradecer al profesor Ricardo J. Rodríguez todo el tiempo invertido estos últimos meses en mí, sin quien la entrega de este proyecto hubiera sido imposible. Y por último pero no menos importante querría agradecer a mi Director Militar el Teniente Coronel Fernando Gordo García que me abriera las puertas de La Bandera de Cuartel General de La Legión y su apoyo permanente el tiempo que duró mi estancia en Almería, a mi Tutor Militar el Teniente José Javier Belda Morante por su apoyo permanente, y al Capitán Francisco Meneses Cuadrado por la ayuda y tiempo que me brindó las semanas que estuve en la Compañía de Transmisiones.

Hoyo de Manzanares a 14 de marzo de 2018

El CAC. TRA. D. Juan Ignacio Olivares González

-PÁGINA INTENCIONADAMENTE EN BLANCO-

Índice

Índice de Tablas

Índice de Imágenes

Lista de acrónimos

Acrónimo	Inglés	Español
ACIBE		Adiestramiento en Ciberdefensa
BOP		Brigada Orgánica Polivalente
CCN		Centro Criptológico Nacional
CIS		Sistemas de Información y Telecomunicaciones
CNI		Centro Nacional de Información
CONCIBE		Concienciación en Ciberdefensa
DoS	Denial of Service	Denegación de Servicio
ET		Ejército de Tierra
FAS		Fuerzas Armadas
FDM		Fichero de Misión
FORCIBE		Formación en Ciberdefensa
GRECO		Grupo de Reconocimiento
HPS		Habilitación Personal de Seguridad
http	Hipertext Transfer protocol	Protocolo de Transferencia Hipertextual
I3D		Infraestructura Integral de Información para la Defensa
MCCD		Mando Conjunto de Ciberdefensa
MySQL	My Structured Query Languaje	Mi Lenguaje de Consulta Estructurado
NetBios	Network Basic Input/Output System	
Nmap	Network Mapper	Rastreador de Redes
OSSIM	Open Source Security Information Management System	Sistema de gestión de la información de seguridad de fuente abierta
PKI	Public Key Infraestructure	Infraestructura de Clave Pública
RSA		Responsable de seguridad de Área
SAI		Sistema de Alimentación Ininterrumpida
SEGINFOPER		Seguridad de la Información Personal
SIEM	Security Incident and Event Management	
SIMACET		Sistema de Mando y Control del ET
SSL	Secure Sockets Layer	Capa de Puertos Seguros
TASO	Terminal Area Security Officer	Oficial de Seguridad de Área

Tabla 1: Lista de Acrónimos

-PÁGINA INTENCIONADAMENTE EN BLANCO-

1. Introducción

Con carácter previo al análisis de este trabajo es apropiado aportar una definición de los términos relativos a este TFG (ciberseguridad, medios CIS y BOP) para clarificar estos conceptos.

Se entiende por ciberseguridad al conjunto de actividades, herramientas y procedimientos que se realizan para garantizar la protección de los sistemas de información en el ciberespacio, permitiendo de igual modo el uso del mismo y garantizando la disponibilidad, confidencialidad e integridad de la información manejada [1].

Los medios CIS son los Sistemas de Información y Telecomunicaciones que dan apoyo al mando en la estructura operativa de las FAS [2]. Respecto al acrónimo BOP, "Brigada Orgánica Polivalente", se refiere a las unidades del Ejército de Tierra Español de reciente creación cuyo objetivo es optimizar las capacidades operativas en todo el espectro del conflicto, organizadas para tal fin en pequeñas unidades tácticas y logísticas especializadas en diversas funciones operativas [3].

Este trabajo se centra principalmente en SIMACET, debido a que es el sistema más susceptible de ser vulnerado en el nivel táctico en el que tiene lugar este estudio. SIMACET es el Sistema de Información para el Mando y Control de Ejército de Tierra, que permite a las grandes y pequeñas unidades planear, gestionar, controlar y dirigir las operaciones, así como obtener una visión coherente y homogénea del campo de batalla en todos los Puestos de Mando en tiempo operativo [4]. Esto se consigue gracias a que el sistema provee una visión común del espacio de batalla y un sistema de mensajería que facilita el planeamiento compartido mediante el intercambio de información entre los distintos niveles de mando. Todo ello se realiza gracias a la instalación de un sistema en red, lo cual convierte a SIMACET en el núcleo central de la arquitectura de red, dentro de la cadena de mando de una BOP. En cualquier caso, los parámetros globales de seguridad de la denominada I3D (Infraestructura Integral de Información para la Defensa), donde también se incluyen los CIS tácticos de una BOP, debe estar en línea con lo establecido la citada Política de Seguridad de la Información del Ministerio de Defensa y con los criterios que establezca el Mando Conjunto de Ciberdefensa (MCCD) en cada caso [5].

Debido al gran avance tecnológico de los últimos años, el ciberespacio se ha convertido en nuevo medio de actuación, y ha demostrado ser clave para el rendimiento y eficacia de cualquier empresa, incluida. las Fuerzas Armadas. La Doctrina de empleo de las Fuerzas Terrestres subraya al ciberespacio como un dominio común y global en el que las operaciones militares se verán condicionadas por la necesidad de asegurar los flujos de información con el resto de actores que comparten el entorno operativo de actuación, frente a las acciones que intenten paralizarlos, degradarlos o destruirlos. Un dominio de actuación que se une a los clásicos de tierra, mar, aire y espacio, de tecnologías y redes en imparable progresión que sirven de soporte a la información para facilitar las misiones de inteligencia, el mando y control, y muchas otras actividades militares y civiles relacionadas con la seguridad y la defensa [6]. Por ello, el ciberespacio debe contar con todas las medidas de seguridad posibles para garantizar la obtención, tratamiento, presentación y almacenamiento de la información (es decir, garantizar los tres atributos clásicos de seguridad: disponibilidad, confidencialidad e integridad) [7]. La ausencia de medidas de seguridad conlleva que un sistema pueda ser vulnerable a intrusiones o ataques por terceras personas con intenciones maliciosas.

En cuanto a las intrusiones, se materializan básicamente en dos tipos de amenazas factibles en cualquier sistema en red: amenazas externas e internas. Para hacer frente a las amenazas externas en SIMACET, se requiere de los principios de defensa en profundidad y diversidad de defensa. La defensa en profundidad se caracteriza por utilizar varias líneas de defensa consecutivas en vez de una sola muy fuerte, debilitando de esa manera la fuerza del atacante; mientras que la diversidad garantiza que en cada una de esas líneas defensivas exista una manera diferente de protección. Respecto a las amenazas internas, su protección es más compleja y exige de personal cualificado y la aplicación adecuada de las medidas de seguridad de la información [8].

Por todo ello, en este trabajo se han realizado diversos estudios acerca del estado de la ciberseguridad actual. En un primer lugar, gracias a la ayuda de personal cualificado se han determinado cuáles son las medidas que actualmente se toman en "La Legión" para disminuir las vulnerabilidades existentes en el ciberespacio. En segundo lugar, y apoyado por el método científico Delphi, se ha establecido cuál es la visión que tienen los usuarios y especialistas acerca de estas medidas. Por último, y gracias a una práctica en laboratorio, se ha demostrado cómo se actúa ante ciertas eventualidades susceptibles de ocurrir. Con el motivo intencionado de no desvelar todas y cada una de las posibles vulnerabilidades de SIMACET, se mostrarán dos únicos casos prácticos sin tratar en ningún momento información de carácter clasificado.

El primer caso práctico consiste en un ataque de denegación de servicio desde un ordenador de la propia red. Con este caso práctico se pretende determinar la respuesta ante un ataque interno que trata de consumir de manera exhaustiva los recursos del sistema (afectando entonces a la disponibilidad de éste, recuérdense los tres principios de seguridad: confidencialidad, integridad y disponibilidad [8]). El segundo caso práctico consiste en otro ordenador de la propia red que se dedica a buscar información sobre la red a la que está conectado (consultando por ejemplo qué otros equipos hay conectados, qué sistemas están ejecutando, qué servicios ofrecen a los usuarios, etc.). En este segundo caso práctico se pretende determinar la respuesta ante un ataque interno de un usuario que pretende conocer la red en que se mueve (conocido como hacer *fingerprinting* de la red). Este tipo de ataque es habitualmente la primera fase de otros ataques más avanzados, ya que permiten localizar dónde pueden estar eslabones más débiles a atacar o los lugares que pueden almacenar la información sensible que el atacante desea conseguir.

Cabe destacar de igual modo que este proyecto ha sido elaborado, en parte, de conformidad con diversas publicaciones doctrinales derivadas de órganos de decisión como, entre otros, el Ministerio de Defensa. Por último, este trabajo propone algunas medidas que se proponen adoptar en SIMACET para crear un sistema lo más robusto y seguro posible. Cabe comentar que este análisis es el primero que se realiza en esta línea, con lo que no es posible la comparación con ningún otro estudio.

Este trabajo se organiza como sigue: En el Capítulo 2 se introduce la metodología que se llevará a cabo durante el proyecto para ayudar a su comprensión. En el Capítulo 3 se explica el estado actual de la ciberseguridad en SIMACET. El Capítulo 4 titulado "Método científico" explica con más detenimiento el método empleado (Método Delphi). En el Capítulo 5 se analizan los resultados recogidos, y en el Capítulo 6 se realizan dos prácticas de laboratorio. Por último, en el Capítulo 7 se exponen las conclusiones reunidas de todo el Trabajo de Fin de Grado. Respecto a los anexos, en el Anexo A se muestra la primera encuesta realizada a los expertos (Encuesta 1), del mismo modo el Anexo B muestra la Encuesta 2, y en el Anexo C se puede ver el informe realizado tras recoger los datos de la primera encuesta.

2. Conocimientos previos

En este capítulo se tratan aspectos necesarios para comprender el resto del trabajo. En particular, primero se presenta el método Delphi, procedimiento científico mediante el cual se puede prever el comportamiento y adecuar el comportamiento futuro de un grupo concreto de personas. Después, se introduce una aplicación informática tipo SIEM (*Security Information and Event Management*) de la empresa *Alien Vault*, que permite observar de una manera visual la estructura y el tráfico de una red, gestionar eventos y obtener información de ciberseguridad.

2.1. Método Delphi

Con el objetivo de analizar el nivel de conocimiento sobre ciberseguridad del personal que forma la Brigada "Alfonso XIII", II de La Legión, se ha usado el método científico Delphi. Se ha escogido este método prospectivo dado que con él se pueden valorar y cuantificar las opiniones de expertos acerca de un tema en concreto y, en última instancia, poder mejorar positivamente esos conocimientos.

La finalidad fundamental de este proceso es medir la diversidad de opiniones acerca de un tema en particular, y guiarlos hacia el acuerdo. Esto se consigue llevando a cabo el siguiente proceso: En un primer momento, se reparte a todo el grupo de expertos una encuesta que debe ser respondida de manera anónima, evitando así posibles influencias en las respuestas. Como segunda fase, se realiza un estudio estadístico de las respuestas contestadas por los seleccionados. Este estudio, además, se hace llegar a los interesados con el fin de poder contrastar sus contestaciones con las del resto de participantes de manera global. Después, con los resultados de esta doble actuación, se dirige una segunda encuesta (ligeramente modificada respecto a la primera) con el fin de cuantificar estadísticamente cuál ha sido la diferencia entre el primer y el segundo sondeo. Esta cuantificación garantiza de ese modo la efectividad del procedimiento y permite medir la mejoría de los conocimientos acerca del tema en concreto. En el supuesto caso de no lograr los objetivos previstos con las dos encuestas, sería necesario realizar más cuestionarios hasta conseguirlos. Todo este proceso se ha reflejado en la Imagen 1.

2.2. SIEM de *Alien Vault*

En este apartado se introduce el programa informático utilizado para la realización de la práctica en laboratorio virtualizado, con el SIEM de *Alien Vault* [9], denominado OSSIM *(Open Source Security Information Management)*.

OSSIM de *Alien Vault* es un programa de reciente implementación en la Brigada "Alfonso XIII", II de La Legión [9]. Esta implantación surge de la necesidad de llevar un control sobre los sistemas conectados en red. En concreto, OSSIM de *Alien Vault* es una aplicación fruto de la combinación de productos de gestión relacionados con la seguridad informática. Estos productos son, en concreto, los siguientes:

- Recolección de datos.
- Correlación.
- Alertas.
- Cuadros de mando.
- Cumplimiento.
- Almacenamiento.

OSSIM de *Alien Vault* trabaja monitorizando una red, buscando vulnerabilidades y mostrándoselas al personal encargado de la seguridad de la red. Este personal crea los llamados "*tickets*", que son documentos basados en la información recogida y remitidos al personal más cualificado para resolver la incidencia. Lo más destacable del programa es que realiza una correlación de los datos, es decir, junta todos los datos recibidos y trata de relacionarlos de manera causal (esto es, intenta inferir posibles relaciones entre ellos) con el objetivo de detectar los posibles problemas de la red.

Cabe destacar que el programa detecta todo lo que ocurre en la red, sin discriminación alguna. Por tanto, es muy importante la formación del personal encargado de este sistema ya que debe saber qué alertas son importantes y cuáles son falsos positivos. Recuérdese que un falso positivo es un evento que ha generado una alerta, cuando en realidad no se trata de un evento problemático.

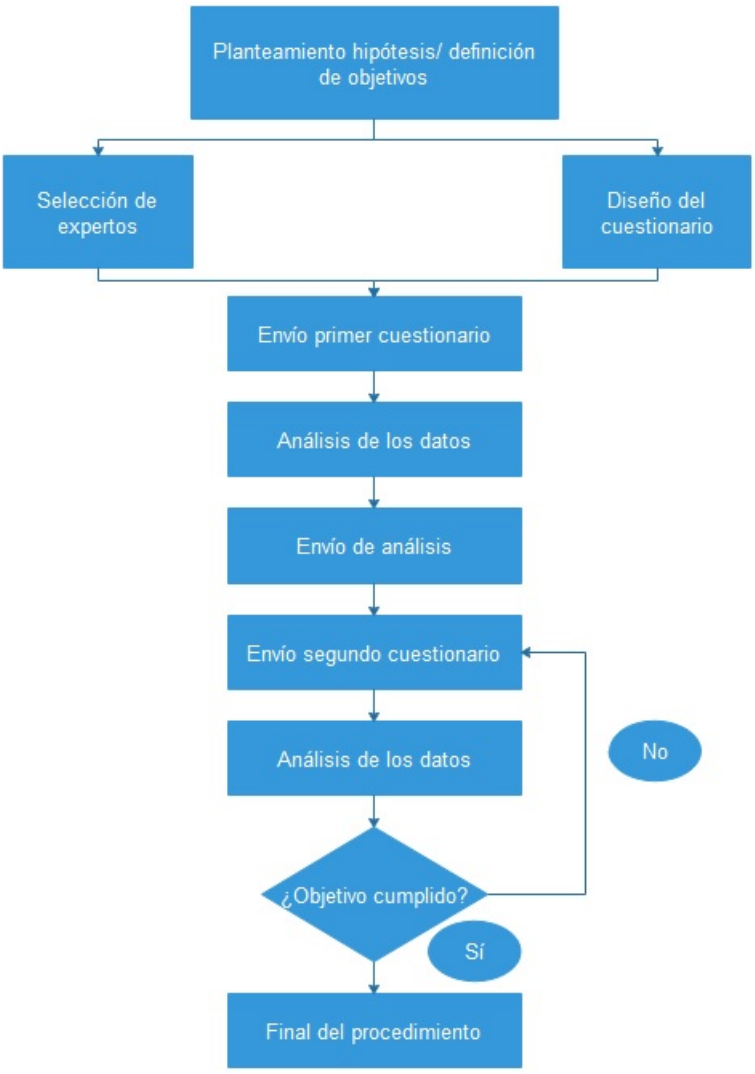

Imagen 1: Mapa conceptual Método Delphi

3. El estudio actual de la ciberseguridad en SIMACET

Gracias a los avances tecnológicos desarrollados en los últimos años, el ciberespacio se ha convertido en el nuevo campo de batalla [10]. Este entorno virtual goza de la gran ventaja de la ausencia de límites geográficos, por lo que cualquier actor puede intervenir en una red remotamente sin el mayor inconveniente que las medidas de seguridad adoptadas por los administradores de dicha red. De igual manera, debido a que todos los componentes informáticos se proyectaron inicialmente con la intención de ser rápidos, que no seguros, se requiere ser muy escrupuloso a la hora de establecer una red lo suficientemente protegida.

Para proteger estas redes es necesaria la seguridad informática, definida como el conjunto de procedimientos de seguridad que se crean e implementan para proteger los datos de los sistemas de información y telecomunicaciones contra su pérdida, ya sea ésta intencionada o accidental [11].

A colación de la definición anterior y, con el fin de securizar las redes, se implementaron ciertas capacidades defensivas en todos los sistemas de información, las cuales están de igual modo presentes en SIMACET. De manera global, se pueden diferenciar tres tipos de medidas: *preventivas*, *proactivas* y *reactivas*.

Las medidas preventivas se pueden a su vez clasificar en tres grupos diferentes: seguridad física, seguridad lógica y seguridad humana. Estas medidas se amplían en más detalle a continuación. Del mismo modo, las medidas de seguridad proactivas se definen como aquellas normas y herramientas que se adoptan con la intención de detectar una irrupción en el sistema antes de que sea fatal. Por último, las medidas reactivas determinan cómo realizar las gestiones de incidentes ante un caso flagrante de ingreso sin consentimiento en la red. Es decir, las medidas proactivas se toman antes de que exista la amenaza, mientras que las medidas reactivas se toman en respuesta a dicha amenaza. Con el objetivo de no profundizar más sobre las medidas reactivas actuales a adoptar en caso de intrusión o intromisión en el sistema de información referido, esta última definición se ha explicado de manera más somera [12].

3.1. Seguridad física

De manera sucinta se puede definir la seguridad física como el conjunto de medidas de protección en edificios, instalaciones y material para impedir el acceso a personal no autorizado de manera física [13]. Esta medida de protección es una de las medidas más importantes y olvidadas por los usuarios, ya que por norma general sólo se piensa en seguridad informática a partir de los elementos de software.

En este primer punto se tratan varios factores que son fundamentales para la seguridad de los sistemas de información. La ausencia de estos factores podría por tanto desencadenar que todos los equipos sufrieran daños, con la consecuente pérdida de información (afectando entonces a la disponibilidad de los datos, recuérdense los tres atributos de seguridad). Así, pueden indicarse los siguientes factores:

- En primer lugar, se pueden citar los **grupos electrógenos**, que son máquinas que generan electricidad a través de combustión de gasoil. Estos equipos son fundamentales debido a la ausencia de corriente eléctrica en los asentamientos militares, la cual es necesaria para alimentar los componentes informáticos.

- En segundo lugar, los **sistemas de refrigeración** (como, por ejemplo, el aire acondicionado). Debido al calor que emanan los equipos militares en uso, es muy probable que se deteriore algún elemento interno o externo de los equipos y se cause el corte total o parcial de flujo de información. Puede suceder que algún componente se llegue a quemar o simplemente deje de funcionar (como ha ocurrido en alguna ocasión).
- En último lugar, **los sistemas de alimentación ininterrumpida (SAI).** Estos sistemas de alimentación funcionan gracias unas baterías internas que proporcionan corriente eléctrica a los sistemas conectados durante un apagón eléctrico. Se trata de un aspecto importante dado que si los equipos no están conectados a un SAI durante un período de corte eléctrico se podría perder la información que se estuviera procesando. Por este motivo, la Brigada "Rey Alfonso XII", II de La Legión lleva a cabo una política de concienciación para que los equipos estén siempre disponibles, esto es, en correcto funcionamiento y dispuestos para cualquier movimiento en el campo.

A continuación, se aborda la relación entre la seguridad física y el acceso físico. En este sentido, se reduce el riesgo a la intrusión en un sistema dado que físicamente no se puede acceder a él. Así pues, los **centinelas** tienen por misión no permitir a ningún intruso (o más formalmente, al personal no acreditado) el acceso al ordenador o el sistema de información en particular. Para estar acreditado es necesario tener la autorización para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad [14]. De igual modo, se emplea una **infraestructura de clave pública o PKI**, que dispone de mecanismos de control y autenticación para el acceso de los usuarios al sistema. Este sistema de acceso proporciona, a su vez, el servicio de integridad y no repudio incorporando la firma digital. Estos dos aspectos también son dos atributos importantes de la definición de seguridad. Con ello, las medidas de seguridad de acreditación se ven duplicadas, lo que dificulta en cierto modo que se pueda acceder por error [14].

Otra de las medidas que la Brigada de La Legión toma es el lugar físico en el que son guardados las **copias de seguridad** (o *backups*). Los *backups*, por definición, se realizan de manera manual o automática con toda la información residente en un sistema y deben almacenarse de manera temporal en lugares con ciertas condiciones de luz y humedad, alejados (geográficamente) entre ellos para garantizar que si hubiera una catástrofe o robo, no se pierda la totalidad de la información. Estas copias de seguridad deben ser borradas cada cierto tiempo por cuestión de optimización del espacio físico y digital.

Por último, dado que los puertos USB están deshabilitados en todos los ordenadores de SIMACET (se describe más en detalle en la siguiente sección), se tiene que **contactar con el TASO** (de sus siglas en inglés: *Terminal Area Security Officer*) **de la unidad** para poder introducir o sacar información de los ordenadores [4]. Esta figura es la responsable de Seguridad de un Área. El TASO es, por tanto, el encargado de supervisar el control de acceso físico del área, asegurar el cumplimiento de los procedimientos diarios establecidos, verificar que todo el hardware de su área está perfectamente etiquetado de acuerdo con la máxima clasificación de la información que soporta, y están únicamente autorizados a almacenar y extraer información del sistema a través de periféricos.

3.2. Seguridad lógica

La seguridad lógica se define como las medidas tomadas en el uso del software y en los sistemas de protección de datos. A continuación, se señalan las medidas de protección más extendida en todos los sistemas de información. En concreto, estas medidas son los antivirus y el bloqueo de puertos lógicos.

Los **programas de antivirus** (o anti-malware, por ser un término más genérico), son programas software que previenen y detectan anomalías o *malware* (software malicioso) en los ordenadores. Como resulta lógico, este tipo de software antivirus es necesario, pero en efecto, no debe residir toda la seguridad en esta única pieza de software, dado que no son 100% eficaces (es decir, existen amenazas software que no van a detectar). Los antivirus actuales

suelen basarse en detecciones basadas en firmas de software malicioso, lo que permite que pequeñas modificaciones en el software malicioso provoquen un falso negativo por parte del antivirus (es decir, el software malicioso se detecta como benigno, con el subsiguiente riesgo que esto implica para el sistema).

Respecto a los puertos lógicos, son los puntos de acceso que permiten el intercambio de información entre dos equipos, es decir, son los lugares por donde las aplicaciones salen al exterior del equipo, o por donde la información entra al mismo. Por ejemplo: el protocolo http usa el puerto 80, o la aplicación eMule usa el 4662. Existen ciertos puertos que son usados siempre por la misma aplicación o protocolo, y otros que se van abriendo o cerrando en función de la necesidad del sistema. Del mismo modo que los puertos físicos, **los puertos lógicos han de tener su propia seguridad para evitar el acceso a posibles irrupciones al sistema**. Debido a que actúan como elementos de entrada/salida al sistema, es importante conocer por cuáles circula información y por cuáles no, teniendo estos últimos cerrados (o, al menos, controlados).

3.3. Seguridad humana

La seguridad humana es una parte fundamental dentro de los sistemas de información, y también es la parte más difícil de conseguir, debido a la alta especialización y acreditaciones que deben poseer los gestores, administradores y usuarios de una red. Para ello, existe la cadena de SEGINFOPER (Seguridad de la Información en las Personas), encargada de acreditar con la Habilitación Personal de Seguridad (HPS) [15] que corresponda al personal, relativa al máximo nivel de clasificación de la información en el sistema a usar.

La HPS se consigue después de que el órgano competente (en el caso del Gobierno de España, esta tarea está encomendada al Centro Nacional de Inteligencia) determine que el titular carece de vulnerabilidades o amenazas que puedan poner en riesgo el sistema de información. Del mismo modo, el usuario debe estar amparado por “la necesidad de conocer”, definido como el motivo que le lleva a tener acceso a la información.

Por lo tanto, no sólo teniendo la HPS acorde al nivel de clasificación de la información a la que se va a acceder es razón suficiente para acceder a ella, ya que además se necesita una causa fundada para hacerlo. Además de esta certificación, todo personal que trabaje con sistemas de información debe asistir a cursos y conferencias de concienciación sobre ciberdefensa para afianzar conocimientos adquiridos y, sobre todo, para minimizar las posibilidades de cometer un error [16].

Para terminar con el epígrafe del estado actual de la ciberseguridad, es de obligado cumplimiento hablar de las contraseñas debido a que forman parte de todos los tipos de seguridad mencionados anteriormente.

Es una práctica muy extendida no cambiar las contraseñas proporcionadas por simple comodidad del usuario. Sin embargo, debe existir un balance entre seguridad y usabilidad; esto es, no existe un sistema totalmente seguro debido a la pérdida de usabilidad que generaría. Por lo tanto, es recomendable cambiar las contraseñas cada vez que el administrador de SIMACET lo proponga. Además, el cambio de contraseña debe realizarse de una manera efectiva, es decir, usando letras mayúsculas, minúsculas, números y caracteres especiales, entre otros símbolos posibles, y con una longitud de clave considerable. En definitiva, lo que se busca con estas medidas sobre las contraseñas es incrementar su complejidad y por tanto, reducir de ese modo la posibilidad de que un ataque por fuerza bruta sea realmente efectivo en el sistema.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

4. Método científico: Método Delphi

En esta sección, se definirá de manera más precisa la metodología empleada, en concreto, el método Delphi. Este método se define como una técnica prospectiva, que pretende influir en los conocimientos de una serie de expertos, utilizando para ello la iteración de encuestas. En el caso preciso de este trabajo, la técnica se descompone en cuatro fases claramente diferenciadas:

1. Definición de objetivos: En este momento se concretó cuál es el fin último en la realización del método. En este caso, el objetivo era en primer lugar estudiar el estado de la ciberseguridad y saber cuáles son las líneas futuras en los medios CIS tácticos de la Brigada "Alfonso XIII", II de La Legión para mejorar SIMACET.

2. Selección de expertos: En esta fase, se eligieron quiénes iban a ser los expertos a los cuales se les enviarían las encuestas una vez elaboradas. El grupo de expertos que formaban parte de esta evaluación estuvo integrado por quince especialistas pertenecientes a las diferentes Banderas de la Brigada (en concreto, a la Bandera de Cuartel General, la Bandera de Zapadores, las VII, VIII y X Banderas de Infantería y el GRECO de Caballería).

3. Elaboración y lanzamiento de los cuestionarios: Para la elaboración de las encuestas se tomó como premisa fundamental que todas las preguntas pertenecientes a un mismo campo fueran lineales, es decir, que las respuestas positivas tendieran hacia 5 y las negativas hacia 1 o viceversa. De este modo se podría realizar el análisis posterior de manera más correcta y precisa. La primera encuesta se repartió el día 2 de octubre de 2017, y la segunda fue repartida el día 10 de octubre de 2017.

4. Análisis de los resultados: Después de recoger los resultados de la primera encuesta, se analizaron para elaborar la segunda encuesta de una manera más focalizada. Por último, una vez obtenidos los resultados de los dos cuestionarios se realizó otro análisis que será el análisis definitivo para lograr el objetivo definido en el primer punto.

Los tipos de cuestionarios fueron de diversa índole debido a diversos motivos. Debido a las casuísticas del personal del Ejército, al personal que no se encontraba físicamente en la misma plaza de Almería (como es el caso de los pertenecientes a la X Bandera y al GRECO de Caballería), el cuestionario se envió por correo electrónico. De igual manera, a los participantes que por diversos motivos no se encontraban en la base en el momento de su reparto se utilizó el mismo medio. A los expertos que se pudieron localizar personalmente, se entregó la encuesta en mano y fue devuelta en un plazo acordado de dos días. Por último, el personal que fue localizado y quiso, se le hizo la encuesta *in situ*. En cualquiera de los casos, se garantizó naturalmente el anonimato del encuestado.

4.1. Definición de la primera encuesta

El objetivo fundamental de la primera encuesta es recoger las opiniones, juicios y conocimientos de los expertos acerca de quince preguntas. Las catorce primeras preguntas están recogidas por similitud en siete bloques bien diferenciados. Para su valoración se utiliza la escala Likert, modelo de más amplio uso en encuestas y en el cual se especifica de manera clara el nivel de acuerdo o desacuerdo del encuestado con una declaración [17]. En ese caso, se utilizan valores del 1 al 5, donde el valor de 1 corresponde con las valoraciones negativas o menos probables, y el valor de 5 con las más positivas o usuales (exceptuando el campo usabilidad, en el cual las preguntas están diseñadas de manera negativa; por lo que el valor de 5 corresponde a una respuesta negativa y viceversa). De igual modo, se añade otra opción de "No sabe, no contesta" ("ns/nc") con el fin de no desvirtuar el análisis en caso de que algún seleccionado no sepa o no quiera contestar alguna pregunta. La última pregunta de la encuesta es una pregunta abierta en la cual se propone a los encuestados que aporten observaciones o sugerencias para la mejora del sistema de información SIMACET.

De este modo la primera encuesta lanzada quedó conformada de la siguiente manera:

4.1.1. Preguntas sobre COMPLEJIDAD

1. *¿Cree que es complicada la creación de un fichero de misión de SIMACET?*
2. *¿Cree que es sencilla la utilización de los programas que usa?*
3. *¿Cree que está cualificado para usar correctamente los programas?*

Las tres preguntas realizadas se centran en la dificultad que puede encontrar un usuario y su capacidad resolutiva a la hora de utilizar ciertas aplicaciones pertenecientes al sistema de información SIMACET.

4.1.2. Preguntas sobre CONTRASEÑAS

4. *¿Cree que son robustas las contraseñas que le asignan?*
5. *¿Cambia la contraseña de los equipos con la asiduidad requerida?*

Estas cuestiones hacen referencia en un primer lugar a la opinión de los encuestados acerca de la robustez que a su juicio tienen las contraseñas proporcionadas. También recogen si actúan de acorde a las normas marcadas por los administradores de la red al cambiar las contraseñas (cuando deben hacerlo).

4.1.3. Preguntas sobre PERSONAL

6. *¿Tiene identificado a su TASO y sabe cómo usarlo?*
7. *¿Tiene identificado a su RSA?*

Las preguntas realizadas en este bloque hacen referencia al conocimiento de los encuestados acerca del personal que tienen a su disposición para resolver cualquier incidencia en el sistema o para ayudarles en caso de duda.

4.1.4. Preguntas sobre INCIDENTES

8. *¿Sabe a quién avisar si ocurre algo extraño en el ordenador que utiliza?*
9. *¿Sabe cuál es el método de actuación ante un incidente informático?*

Este bloque de preguntas se diseñó con el propósito de averiguar el nivel de conocimientos de los usuarios ante incidentes eventuales y su capacidad de actuación.

4.1.5. Preguntas sobre USABILIDAD

10. *¿Redirige automáticamente mensajes recibidos a otra cuenta de correo?*
11. *¿Envía sin comprimir los archivos anexados a los mensajes?*

Las preguntas anteriores miden la capacidad de los usuarios de optimizar los recursos en red, de manera que buscan conocer si se puede evitar cierto tráfico de datos redundante o reducirlo.

4.1.6. Preguntas sobre AUTOPROTECCIÓN

12. *¿Borra periódicamente mensajes de las carpetas y de la papelera de reciclaje?*
13. *Si envía un mensaje a múltiples destinatarios ¿hace que las direcciones permanezcan ocultas para el resto de destinatarios?*

Estas cuestiones anteriores pretenden comprobar si los expertos utilizan medidas de autoprotección básicas como borrar mensajes u ocultar direcciones de correo a destinatarios que no tienen la necesidad de conocerlas.

4.1.7. Preguntas sobre INFORMACIÓN

14. *¿Cree que cuenta con la información suficiente sobre ciberdefensa?*

Esta última pregunta va a servir para tener un conocimiento global acerca de la precepción que tienen los encuestados sobre su nivel de formación en ciberdefensa.

Por último, la pregunta de respuesta abierta planteada en la primera encuesta es:

15. Observaciones o sugerencias para una posible mejora del sistema

4.2. Definición de la segunda encuesta

Tras la respuesta por todos los elegidos y la recogida de esta primera encuesta, se realiza un análisis de las respuestas dadas, que se les envía para su conocimiento. En el Anexo C se proporcionan todos los datos relativos a esta primera encuesta. Este análisis es fundamental para la elaboración del segundo cuestionario.

Para que el método sea efectivo, las preguntas de la segunda encuesta deben ser iguales o similares a las de la primera, ya que de ese modo se puede comprobar la utilidad del análisis enviado a los participantes. En base a esta premisa, el diseño usado es el siguiente: Se sustituye las preguntas sobre el campo de complejidad por el campo *"Preguntas de interés estadístico"*, debido a que las primeras no dan información relevante a la hora de crear una segunda encuesta: la mayoría de las respuestas coinciden con los valores 5 y "no sabe/no contesta". El resto de preguntas (de la 4 a la 15) permanecen idénticas en el segundo cuestionario. De este modo, las nuevas cuestiones que se plantean son:

4.2.1. Preguntas sobre INTERÉS ESTADÍSTICO

1. ¿Ha leído el informe enviado por parte del alumno?
2. ¿Le ha servido de ayuda el informe?
3. ¿Ha buscado información sobre las preguntas que desconocía?

Las respuestas de los encuestados a estas preguntas guían al analista de las encuestas a hacerse una idea de hacia dónde se van a dirigir las respuestas posteriores, es decir, permiten conocer si el participante ha buscado información sobre lo que desconocía o no. De esta manera, el método científico utilizado actuará de manera correcta.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

5. Análisis de resultados

A continuación, se procede al análisis de los datos obtenidos a través de las encuestas. Las preguntas de cada una de las partes de la encuesta se han detallado y razonado en el capítulo anterior. En este capítulo se analizan los resultados obtenidos.

Para el análisis estadístico de los datos recogidos en las encuestas se van a usar los datos estadísticos de media y moda. Considérese un conjunto de datos. La media se define como el valor resultante al sumar todos los datos y dividir el resultado entre el número total de datos en el conjunto; mientras que la moda se define como el valor que tiene más frecuencia absoluta, es decir, el valor que se repite más veces en el conjunto de datos.

El estudio siguiente se fundamenta en primer lugar en la interpretación de los datos recogidos de manera global, y más tarde se realiza el análisis diferenciando pregunta a pregunta en algunos casos de interés. Además, se muestran los resultados de cada una de las encuestas realizadas para poder también analizar las diferencias. Por último, se mostrarán gráficas para visualizar el comportamiento de los expertos con relación a las respuestas contestadas. Todo el proceso citado anteriormente se ha iterado además 7 veces, una por cada campo.

5.1. Preguntas sobre complejidad

Recuérdese que este apartado de la encuesta hace referencia a preguntas acerca de los programas que se utilizan en SIMACET (véase la Sección 4.1.1). Son preguntas sencillas de responder que introducen al encuestado hacia las preguntas más interesantes y relevantes. De este modo, al comprobar las respuestas se puede ver la distribución que se muestra en la Tabla 2.

Las respuestas que corresponden con la respuesta 5 son aquellas procedentes de las preguntas 2 y 3, relacionadas con la dificultad que encuentran los usuarios con los programas del sistema y su uso correcto. Este dato es algo que se podía prever debido a que los usuarios de SIMACET saben utilizar todos los programas que se les proporciona y por ello tienen conocimientos para usarlos. Las respuestas que corresponden en su gran mayoría a "ns/nc" se refieren a la pregunta número 1, sobre la creación de los ficheros de misión (FDM). De igual modo, este dato era suponible ya que los FDM no son creados ni gestionados por los usuarios de SIMACET.

Respuestas sobre COMPLEJIDAD (Sección 4.1.1)	
	ENCUESTA 1
1	0
2	2
3	0
4	2
5	28
ns/nc	13
MEDIA	3,37
MODA	5

Tabla 2: Respuestas sobre COMPLEJIDAD

Gracias al análisis y a las premisas con las que se contaba (y como ya se adelantó anteriormente), en la segunda encuesta no aparece este apartado debido a que no da información acerca de los objetivos que se buscan.

5.2. Preguntas sobre CONTRASEÑAS

En el siguiente apartado se analizará el campo "Contraseñas", cuyas preguntas se muestran en la Sección 4.1.2. Antes de ello es conveniente explicar cuál es el modo de operar en SIMACET con las contraseñas para poder entender de una mejor manera el análisis posterior.

Las contraseñas del sistema son proporcionadas a los usuarios por parte de los gestores encargados de generarlas. Una vez proporcionada, se calcula cuál es el tiempo óptimo de existencia de las credenciales. Este tiempo puede variar desde unas horas a semanas, dependiendo del tiempo o la relevancia de la maniobra en la que estén involucrados los usuarios. Por lo tanto, en la pregunta de esta parte del cuestionario relativa a la percepción que tiene el usuario acerca de la complejidad de éstas, una respuesta 5 significa que cree que sí son robustas, mientras que la respuesta 1 significa que cree que no lo son. De igual modo, una persona que conteste con un valor de 5 cuando se pregunta si cambia la contraseña cuando debe, quiere decir que la cambia siempre que la tiene que cambiar. De la misma manera, una persona que conteste con un valor de 1 da a entender que nunca cambia las contraseñas, aunque sepa que ha de hacerlo.

Las respuestas proporcionadas en este campo son las siguientes:

Respuestas sobre CONTRASEÑAS (Sección 4.1.2)		
	ENCUESTA 1	ENCUESTA 2
1	0	0
2	1	0
3	9	7
4	6	5
5	14	18
ns/nc	0	0
MEDIA	4,1	4,36
MODA	5	5

Tabla 3: Respuestas sobre CONTRASEÑAS

De una manera general, se aprecia que los valores son altos, observando que la media es de 4.1 y 4.36 en la primera y segunda encuesta, respectivamente. Esto quiere decir que se tiende de una manera directa a los resultados que se esperaba encontrar: los usuarios dan más importancia por norma general a la seguridad en el sistema de información que a la usabilidad del mismo. La moda es 5 en ambas encuestas, lo cual coincide con las expectativas.

		Respuestas sobre CONTRASEÑAS						
PREGUNTA 4		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	13%	13%	73%	0%	15
	ENCUESTA 2	0%	0%	7%	7%	87%	0%	15

Tabla 4: Respuestas sobre PREGUNTA 4

Hablando de la robustez de las contraseñas (pregunta 4, véase la Sección 4.1.2) existe una tendencia a pensar por parte de los expertos que las contraseñas proporcionadas por los gestores de SIMACET son fuertes. Los resultados concretos de esta pregunta se muestran en la Tabla 4. Este hecho está motivado en primer lugar por la combinación de letras y números que la conforman, y en segundo lugar por la propensión que hay a definirlas de una manera automática para evitar posibles intrusiones.

Cabe destacar que se comprueba cómo en la segunda encuesta la tendencia es pensar que las contraseñas son más robustas, aumentando el número de respuestas hacia el valor 5. Por lo tanto, se concluye que los usuarios están satisfechos con el nivel de seguridad que proporcionan las contraseñas recibidas por los gestores.

		Respuestas sobre CONTRASEÑAS						
PREGUNTA 5		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	7%	47%	27%	20%	0%	15
	ENCUESTA 2	0%	0%	40%	27%	33%	0%	15

Tabla 5: Respuestas sobre PREGUNTA 5

En cuanto a la cuestión número 5, que pregunta por la asiduidad en que los usuarios cambian las contraseñas proporcionadas, se observa que el 93% ha contestado con un valor de 3, 4 ó 5 en la primera encuesta (resultados mostrados en la Tabla 5). Este dato significa que casi todos los usuarios la cambian en algún momento dado. Este hecho también ayuda a pensar que hay bastante concienciación entre el personal del ET acerca de la necesidad de renovar las contraseñas, lo cual es francamente positivo. En contra, cabe destacar también que sólo un 20% lo hace siempre que lo tiene que hacer, lo cual no resulta tan positivo.

En la segunda encuesta se puede observar que las respuestas 1 y 2 no las ha respondido nadie. Esto significa que el informe proporcionado a los expertos tras el primer cuestionario ha conseguido concienciar al personal de la importancia de la cuestión tratada.

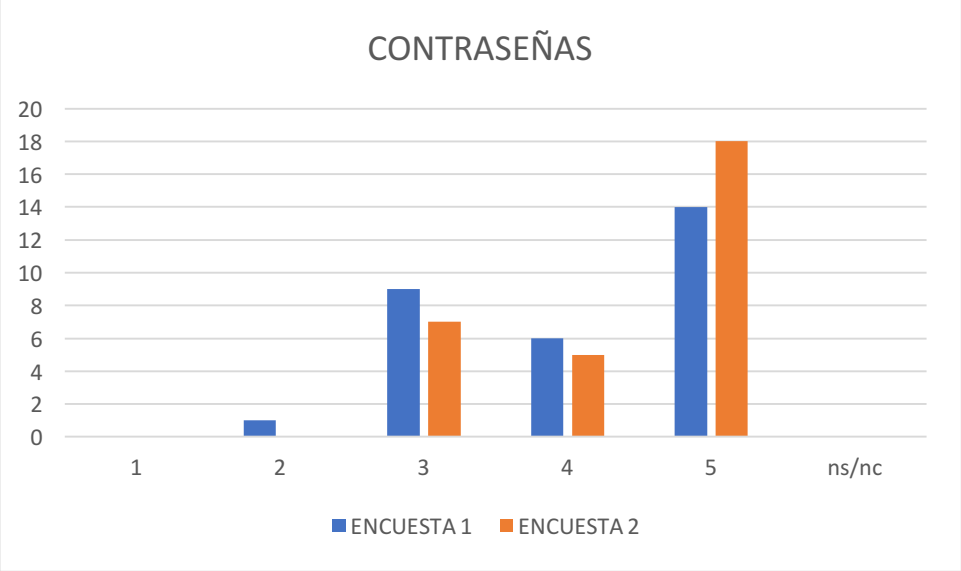

Imagen 2: Respuestas sobre CONTRASEÑAS

La imagen 2, muestra visualmente cómo en términos generales la gente da más importancia a las contraseñas como medida de protección. Este razonamiento viene sustentado al comprobar que ha subido el número de respuestas contestadas del valor 5, consiguiendo así que el resto de posibles contestaciones bajen su número de respuestas en la segunda encuesta.

5.3. Preguntas sobre PERSONAL

En estas preguntas se tratará el conocimiento que tienen los usuarios de SIMACET acerca del personal que tienen a su disposición (*Personal Helpdesk*) para cualquier duda o problema que surja. Las preguntas concretas realizadas se pueden consultar en la Sección 4.1.3.

En la Tabla 6 se observa cuáles han sido las respuestas de los encuestados en global en el apartado "Personal":

Respuestas sobre PERSONAL (Sección 4.1.3)		
	ENCUESTA 1	ENCUESTA 2
1	2	1
2	2	2
3	8	10
4	6	7
5	9	10
ns/nc	3	0
MEDIA	3,3	3,76
MODA	5	5

Tabla 6: Respuestas sobre PERSONAL

Se puede apreciar, observando la moda, que el valor que más se repite en ambas encuestas es la respuesta 5. Sin embargo, en el segundo cuestionario la moda de la respuesta 5 coincide con la respuesta 3. Esto significa que hay más gente que conoce a su TASO y su RSA (Responsable de Seguridad de Área) sabiendo usarlo siempre, aunque hay otros que no tienen tan claro su utilización.

En cuanto a la media, lo más significativo es que aumenta de una encuesta a otra gracias al informe enviado a los encuestados antes de realizar el segundo cuestionario. Esto quiere decir que los expertos que no estaban seguros de tener identificado a ese personal en cuestión se han informado acerca de este tema.

		Respuestas sobre PERSONAL						
PREGUNTA 6		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	13%	27%	13%	20%	20%	15
	ENCUESTA 2	7%	13%	33%	20%	27%	0%	15

Tabla 7: Respuestas sobre PREGUNTA 6

Más específicamente, en cuanto a la pregunta 6 que investigaba si tienen identificado a su TASO y saben cómo usarlo, los expertos contestaron lo que refleja en la Tabla 7. Lo más característico de los resultados es comprobar cómo en la primera encuesta un 20% de los encuestados no sabían quién era su TASO ("ns/nc"), y tras el informe, estas respuestas han desaparecido (es decir, localizaron a su TASO).

		Respuestas sobre PERSONAL						
PREGUNTA 7		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	0%	27%	27%	40%	0%	15
	ENCUESTA 2	0%	0%	33%	27%	40%	0%	15

Tabla 8: Respuestas sobre PREGUNTA 7

La pregunta 7 en general no proporciona mucha información acerca del RSA. Esta afirmación se corrobora al ver los resultados de la Tabla 8. El único dato que cambia es que en la primera encuesta un 7% (corresponde con una persona de los encuestados, al tratarse de 15 expertos) de los expertos no localizaba físicamente su Responsable de Seguridad de Área, y tras el informe, lograron saber en cierta medida quién es.

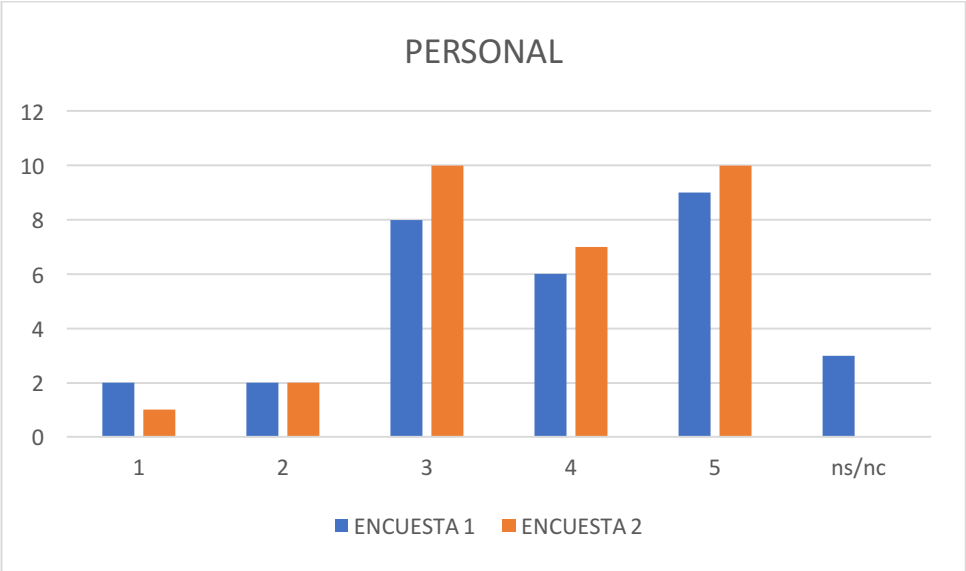

Imagen 3: Respuestas sobre PERSONAL

La Imagen 3 muestra, como se puede observar, que en la segunda encuesta se ha logrado eliminar las respuestas 1 y "ns/nc", lo que denota un mayor conocimiento de los expertos acerca del personal que tienen disponible para solucionar diferentes fallos o incidencias en SIMACET.

5.4. Preguntas sobre INCIDENTES

En el siguiente apartado se valoran las respuestas de los encuestados en función del método de actuación ante incidentes dentro del sistema SIMACET (preguntas 8 y 9, véase la Sección 4.1.4). Dichos métodos comprenden el conocimiento de protocolos de actuación ante determinadas incidencias que pudieran ocurrir en el mismo.

Respuestas sobre INCIDENTES (Sección 4.1.4)		
	ENCUESTA 1	ENCUESTA 2
1	0	0
2	0	0
3	7	5
4	11	12
5	12	13
ns/nc	0	0
MEDIA	4,16	4,26
MODA	5	5

Tabla 9: Respuestas sobre INCIDENTES

Tal y como se puede observar en la Tabla 9, tanto la media como la moda toman valores bastante altos. Este hecho muestra que hay un fuerte conocimiento por parte de los usuarios acerca de los diferentes protocolos de actuación ante determinadas incidencias en el sistema.

		Respuestas sobre INCIDENTES						
PREGUNTA 8		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	20%	47%	33%	0%	15
	ENCUESTA 2	0%	0%	20%	53%	27%	0%	15

Tabla 10: Respuestas sobre PREGUNTA 8

Como se puede contemplar en la Tabla 10, las respuestas tanto de la primera encuesta como de la segunda son bastante similares, es decir, los usuarios no han cambiado mucho su conocimiento acerca de a quién avisar en caso de que ocurra algo extraño en su ordenador. De igual manera, se observa que los valores de las respuestas son bastante elevados. De nuevo, esto denota que los usuarios tienen un alto conocimiento acerca de a quién avisar en caso de un incidente informático, lo cual es positivo pues demuestra el alto nivel de formación que los usuarios poseen acerca del protocolo de actuación ante casos de incidentes.

		Respuestas sobre INCIDENTES						
PREGUNTA 9		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	27%	27%	47%	0%	15
	ENCUESTA 2	0%	0%	13%	27%	60%	0%	15

Tabla 11: Respuestas sobre PREGUNTA 9

En cuanto a la pregunta 9, cuyos resultados de las encuestas se muestran en la Tabla 11, se puede deducir que los expertos poseen un alto conocimiento concerniente al método de actuación ante incidencias en el sistema. Lo más característico es que la segunda encuesta experimenta un aumento de respuestas con valor 5 y una reducción significativa en la repuesta 3, lo que representa un aumento en los conocimientos del personal encuestado tras el informe.

La Imagen 4 muestra todo lo anteriormente explicado de manera más visual.

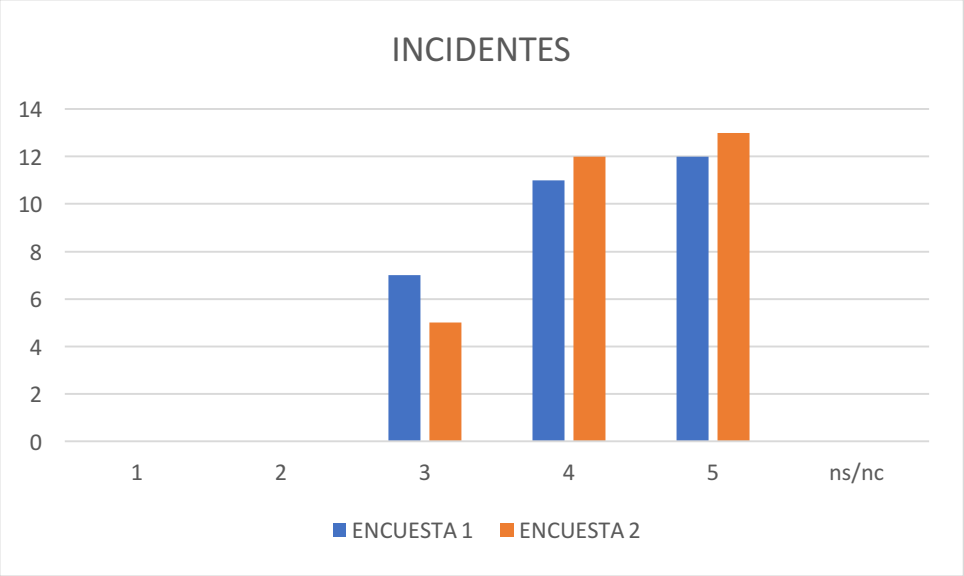

Imagen 4: Respuestas sobre INCIDENTES

5.5. Respuestas sobre USABILIDAD

En el siguiente apartado se analizarán las preguntas correspondientes al campo “Usabilidad” (preguntas 10 y 11, véase la Sección 4.1.5).

Al contrario que en los análisis previos, al realizar el estudio correspondiente a esta característica se considera óptima una puntuación de 1, al estar confeccionado dicho campo en sentido negativo. En cuanto a la pregunta 10, relativa a si se redirigen los mensajes recibidos de manera automática, es importante saber que no es conveniente hacerlo debido a que puede haber saturación en el canal de información. Del mismo modo la pregunta 11 cuestiona sobre si los usuarios comprimen los mensajes antes de enviarlos. Conviene realizar siempre esa acción para que los archivos ocupen menos, consiguiendo de ese modo una mayor velocidad en el envío y optimizando así los recursos.

Respuestas sobre USABILIDAD (Sección 4.1.5)		
	ENCUESTA 1	ENCUESTA 2
1	12	16
2	0	2
3	11	7
4	0	1
5	7	4
ns/nc	0	0
MEDIA	2,66	2,16
MODA	1	1

Tabla 12: Respuestas sobre USABILIDAD

Tal y como se puede constatar en la Tabla 12, la media constituye un valor relativamente bajo. Es decir, de manera general se aprecia que los expertos saben cómo usar los sistemas de los que disponen para que sean óptimos. Del mismo modo, la moda es 1, por lo que se puede comprobar que los encuestados conocen el modo en el cual han de trabajar para mejorar la eficiencia de los recursos disponibles al máximo posible.

		Respuestas sobre USABILIDAD						
PREGUNTA 10		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	47%	0%	27%	0%	27%	0%	15
	ENCUESTA 2	53%	7%	20%	7%	13%	0%	15

Tabla 13: Respuestas sobre PREGUNTA 10

En cuanto a la pregunta 10, que hace referencia al reenvío automático de correos, lo más significativo que se observa es que en la segunda encuesta han disminuido las respuestas número 5 (véase el estudio pormenorizado en la Tabla 13). Este hecho recalca que, tras el informe distribuido después del primer cuestionario, los expertos han tomado conciencia y ya no reenvían tantos correos de manera automática. Se puede apreciar también en el hecho de que las respuestas número 1 han aumentado el porcentaje en la segunda encuesta de manera considerable.

		Respuestas sobre USABILIDAD						
PREGUNTA 11		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	33%	0%	47%	0%	20%	0%	15
	ENCUESTA 2	53%	7%	27%	0%	13%	0%	15

Tabla 14: Respuestas sobre PREGUNTA 11

De forma análoga, en la pregunta 11 relativa a la compresión de archivos, se observa algo parecido que en la pregunta 10: se han reducido el número de respuestas 5 y han aumentado las respuestas 1 (resultados mostrados en la Tabla 14). De nuevo, estos resultados indican que los encuestados son más eficientes, y por lo tanto el sistema de información también lo es, a raíz del método usado en este Trabajo Fin de Grado.

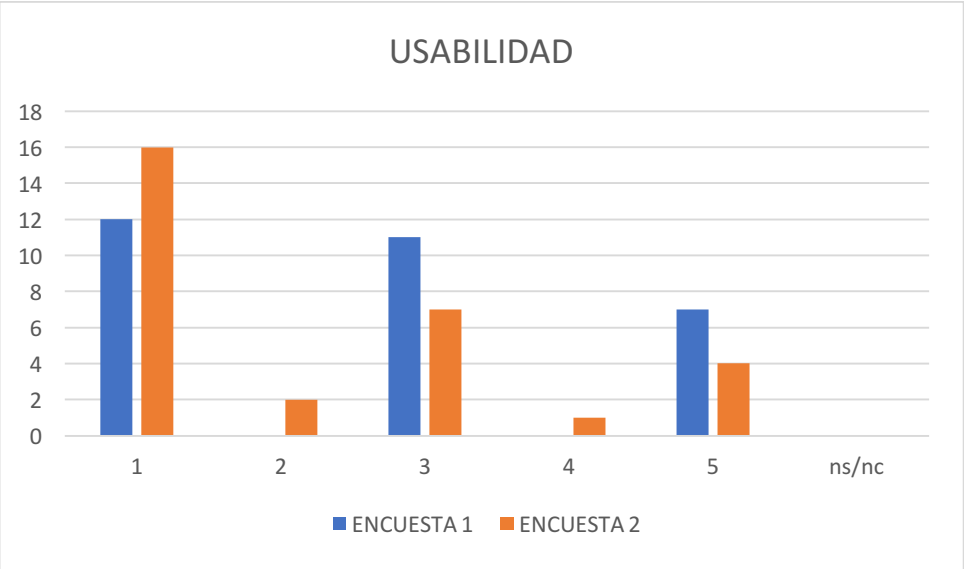

Imagen 5: Respuestas sobre USABILIDAD

Por último, y tal y como se comprueba en la Imagen 5, todas las respuestas excepto la 1 han disminuido el número de veces que aparecen en la encuesta 2. Consecuentemente, las respuestas número 1 han aumentado, dirigiendo el conocimiento de los expertos hacia un sistema más eficiente.

5.6. Preguntas sobre AUTOPROTECCIÓN

En el siguiente apartado se analiza el campo “Autoprotección”. Las preguntas de la encuesta a primera vista pueden resultar triviales, pero tienen mucha importancia debido a la confidencialidad de la información con la que se trabaja.

Respuestas sobre AUTOPROTECCIÓN (Sección 4.1.6)		
	ENCUESTA 1	ENCUESTA 2
1	2	1
2	4	3
3	7	8
4	8	9
5	9	9
ns/nc	0	0
MEDIA	3,6	3,73
MODA	5	5

Tabla 15: Respuestas sobre AUTOPROTECCIÓN

En la Tabla 16 y 17 pueden observarse los resultados de ambas encuestas sobre las preguntas 12 y 13, respectivamente (véase Sección 4.1.6): borrado de mensajes y carpetas, y ocultación de destinatarios en los mensajes. Como se constata, la media es un valor relativamente alto, lo cual indica que los usuarios encuestados denotan un alto grado de conocimientos acerca de la protección propia.

También se aprecia el hecho de que nadie ha contestado la respuesta "ns/nc", por lo que todos los encuestados saben qué es lo que se está preguntado, reforzando de esa manera la hipótesis anterior relativa a la importancia de las cuestiones (a pesar de parecer triviales).

		Respuestas sobre AUTOPROTECCIÓN						
		1	2	3	4	5	ns/nc	SUMA
PREGUNTA 12	ENCUESTA 1	7%	7%	20%	33%	33%	0%	15
	ENCUESTA 2	0%	7%	27%	33%	33%	0%	15

Tabla 16: Respuestas sobre PREGUNTA 12

La pregunta 12 hace referencia al borrado de documentos de las carpetas y papelera. Es importante la supresión de los archivos cada cierto tiempo para liberar espacio en los sistemas. Del mismo modo, esta práctica recomendada puede evitar fugas de información en el caso de intrusión en el sistema de información. Lo más relevante en la Tabla 16 es que, tras el informe dado a los expertos tras la primera encuesta, el personal que nunca borraba los archivos comenzó a hacerlo de manera más periódica.

		Respuestas sobre AUTOPROTECCIÓN						
		1	2	3	4	5	ns/nc	SUMA
PREGUNTA 13	ENCUESTA 1	7%	20%	27%	20%	27%	0%	15
	ENCUESTA 2	7%	13%	27%	27%	27%	0%	15

Tabla 17: Respuestas sobre PREGUNTA 13

La pregunta número 13 corresponde a la cuestión sobre el envío de correos a múltiples destinatarios en copia oculta. Recuérdese que uno de los principios básicos en seguridad informática hace referencia a la necesidad de conocer. Bajo esta premisa, ningún usuario debe dar a conocer la identidad de todos los destinatarios de sus correos al resto de destinatarios. Por lo tanto, debe ser una práctica común el ocultar las direcciones a la hora de mandar un correo a varios destinatarios.

Observando la Tabla 17, que resume las respuestas a la pregunta 13, no se puede garantizar con certeza el efecto del informe posterior a la primera encuesta dado que todos los valores son muy similares. Lo más importante es que en mayor o menor medida todos los usuarios son conocedores de este hábito, ya que nadie ha contestado "ns/nc".

Por último, todo lo mencionado con anterioridad en este apartado de “Autoprotección” se analiza visualmente en la Imagen 6, que muestra todos los datos.

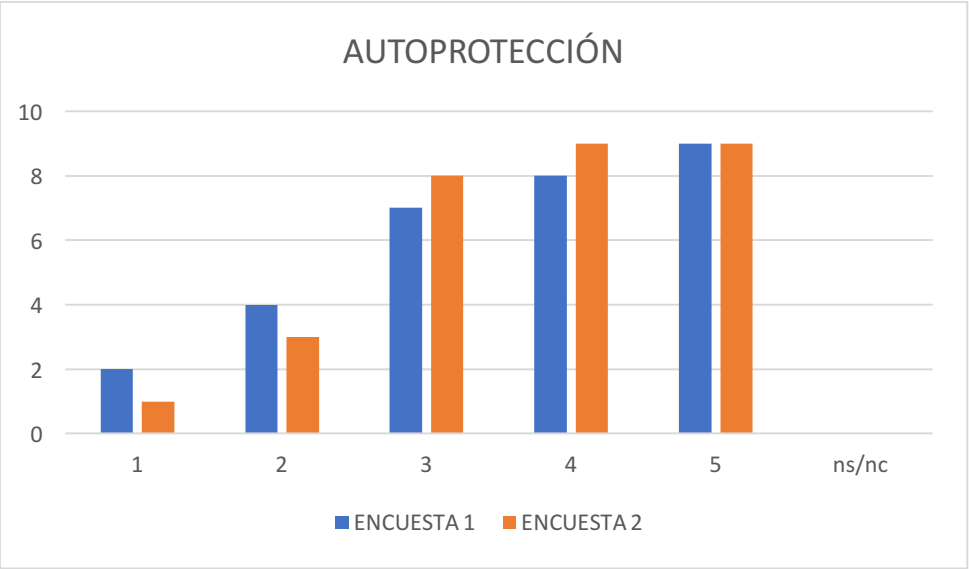

Imagen 6: Respuestas sobre AUTOPROTECCIÓN

5.7. Pregunta sobre INFORMACIÓN

En último lugar, pero no menos importante, se encuentra el campo de "Información". Este apartado solamente se fundamenta de una pregunta relativa a la percepción de los expertos acerca de sus conocimientos de ciberseguridad y ciberdefensa. Es una cuestión de gran importancia debido a que los usuarios de los sistemas de información deben estar cualificados y capacitados para poder usarlos. Las respuestas negativas denotarían ciertas carencias en el uso de SIMACET.

Respuesta sobre INFORMACIÓN (Sección 4.1.7)		
	ENCUESTA 1	ENCUESTA 2
1	0	0
2	0	0
3	5	3
4	8	8
5	2	4
ns/nc	0	0
MEDIA	3,8	4,06
MODA	4	4

Tabla 18: Respuestas sobre INFORMACIÓN

		Pregunta sobre INFORMACIÓN						
		1	2	3	4	5	ns/nc	SUMA
PREGUNTA 14	ENCUESTA 1	0%	0%	33%	53%	13%	0%	15
	ENCUESTA 2	0%	0%	20%	53%	27%	0%	15

Tabla 19: Respuestas sobre PREGUNTA 14

Al tratarse de una única pregunta, las dos tablas anteriores están directamente conectadas. Se puede apreciar que ningún usuario ha contestado las respuestas 1 ó 2, lo cual es satisfactorio dado que indican que los expertos encuestados tienen conocimientos sobre ciberseguridad.

En general, se percibe que el conocimiento por parte de los usuarios es alto (la media y la moda son valores cercanos a 4). Sin embargo, dada la criticidad del sistema y la confidencialidad de la información con la que se trabaja, sería conveniente que los valores moda y media estuvieran más cercanas a 5.

5.8. Conclusiones de las ENCUESTAS

De manera general y para finalizar este apartado, se tratarán ciertos aspectos derivados de los datos. De manera amplia se puede observar que la preparación y conocimientos del personal de la "Brigada Alfonso XIII, II de La Legión" acerca de la Ciberseguridad es elevado, y más aún después de realizar el Método Delphi empleado, ya que los encuestados han sido capaces de informarse y aumentar sus conocimientos. De todas maneras, se plantean varias actividades que serían beneficiosas para el personal y el futuro de la Unidad. La primera de ellas sería seguir realizando actividades de Instrucción y Adiestramiento para lograr de ese modo mejorar e impulsar la concienciación y el adiestramiento del personal en materia de ciberdefensa, integrándola con el resto de actividades y ejercicios. Para ello se propone de igual modo la involucración del personal en los planes de Ejército de Adiestramiento en Ciberdefensa (Plan ACIBE), Formación (Plan FORCIBE), y Concienciación (Plan CONCIBE). Por último, se sugiere participar de manera activa en charlas, reuniones y coloquios acerca de la Ciberseguridad que se realizan desde el Mando Conjunto de Ciberdefensa del Ejército (MCCD). De este modo se mejorarán y ampliarán los conocimientos acerca de este tema dado que es un campo en constante evolución.

6. Prácticas de laboratorio de SIMACET

En este Capítulo se explican las prácticas de laboratorio llevadas a cabo, con la intención de mostrar una de las capacidades más importantes con las que cuenta "La Legión" en cuanto a Ciberdefensa (subcapacidad de defensa): la aplicación OSSIM de *Alien Vault*. Como ya se explicó en la Sección 2.2, se trata de un programa encargado de encontrar anomalías o vulnerabilidades en la red, y de esta manera preservar la integridad y seguridad de los sistemas. El objetivo de estas prácticas es observar esta capacidad.

En primer lugar, es importante introducir el concepto de **virtualización** [18]: la virtualización es la creación, a través de un software tercero, de una versión virtual de un recurso tecnológico de tal forma que se simula el hardware original. Es decir, este método permite disponer de un entorno de simulación sobre un hardware real. Mediante la virtualización se reparten los recursos hardware del equipo físico (también llamado anfitrión o *host)* entre los distintos sistemas virtuales que alberga. En el caso concreto de este trabajo, se ha creado una máquina virtual que imita el comportamiento real de una red de datos del entorno de SIMACET.

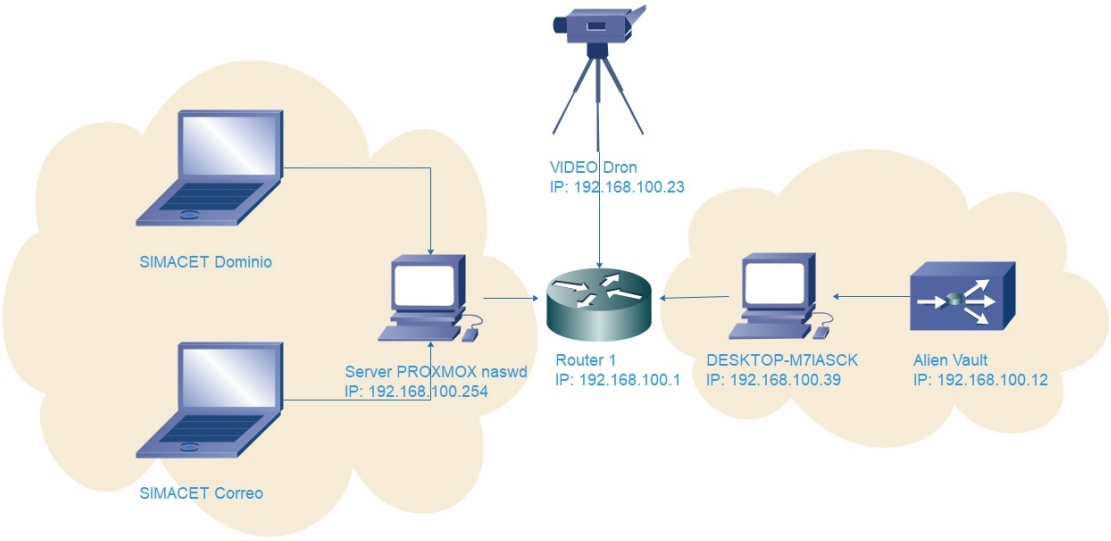

Imagen 7: Esquema laboratorio SIMACET. Elaboración propia.

El sistema básico de la disposición de los ordenadores y servidores del laboratorio sigue el esquema mostrado en la Imagen 7 y explicado a continuación.

Los dos primeros dispositivos (a mano izquierda en la imagen) son dos máquinas virtualizadas que simulan el dominio de SIMACET y su correo. Estas dos máquinas están albergadas en el host "*Server PROXMOX naswd*" cuya dirección IP es 192.168.100.254.

El siguiente dispositivo en la red llamado "*Vídeo DRON*" (parte superior de la Imagen 7) sirve para mostrar que SIMACET puede interoperar con otros muchos sistemas en red. Este dispositivo no afecta al desarrollo de la práctica y únicamente se ha colocado en el esquema de manera informativa.

Seguidamente, y tal y como se puede observar en el esquema, se encuentra "*DESKTOP-M7IASCK*" con dirección IP: 192.168.100.39, que es el ordenador anfitrión que alberga el programa OSSIM de Alien Vault, el cual se encuentra virtualizado dentro con su dirección IP: 192.168.100.12

Para finalizar, todo ello está físicamente conectado al "*Router 1*" cuya dirección IP es 192.168.100.1.

6.1. Práctica de denegación de servicio

En esta práctica se evalúa la capacidad del sistema SIMACET frente a los ataques de denegación de servicio (o ataques DoS por sus siglas en inglés, *Denial-of-Service*). Este tipo de ataques buscan inhabilitar un servicio para que sea inaccesible por sus usuarios legítimos, atentando contra la legítima disponibilidad del servicio (recuérdese la tríada de la seguridad: confidencialidad, integridad y disponibilidad). El funcionamiento básico de estos ataques se basa en enviar numerosas peticiones de servicio a un servidor para saturarlo y que deje de funcionar. En este caso, el ataque se realiza desde un ordenador del mismo laboratorio (es decir, desde la red interna). En un entorno real, el atacante puede realizar el ataque desde una red externa de manera remota.

La Imagen 8 muestra la monitorización realizada por el programa OSSIM de *Alien Vault*. Se puede observar que exceptuando ciertos servicios (motivado por las limitaciones del laboratorio), el host "*naswd*" tiene cuatro servicios en estado "OK" (es decir, funcionando correctamente). Se han destacado estos servicios en la imagen. Estos cuatro servicios son los que el ataque simulado va a tratar de inhabilitar.

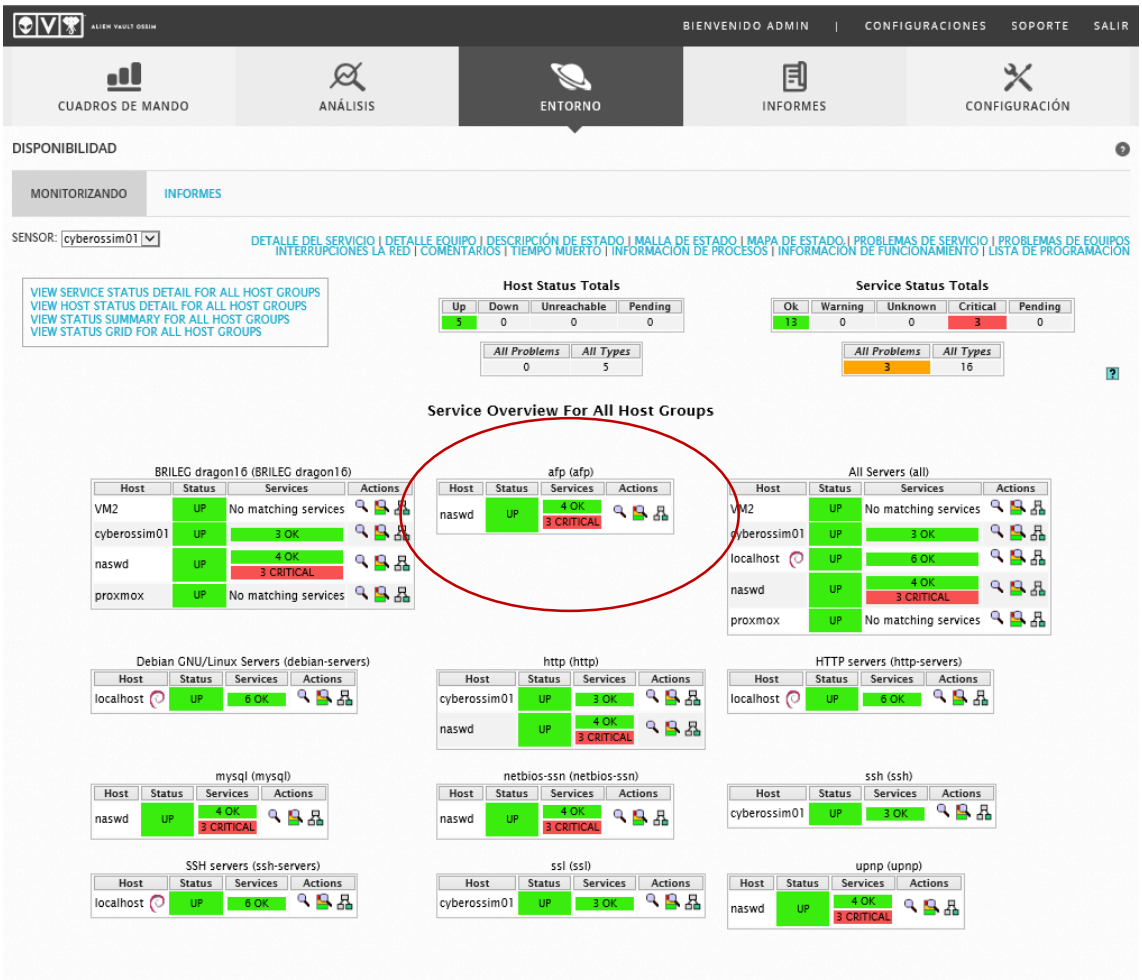

Imagen 8: Entorno OSSIM de Alien Vault. Fuente: Elaboración propia

La Imagen 8 muestra mediante un escaneo de red cuáles son los servicios que el equipo naswd tiene habilitados. Estos servicios son, en concreto, los servicios HTTP, NetBios-ssn, http-SSL y MySQL. El primero de ellos, HTTP, es el protocolo de comunicación, a través del cual se permiten los intercambios de información con la red internet. NetBios hace referencia a una capa de software desarrollada para enlazar un Sistema Operativo (SO) con un hardware determinado. El siguiente servicio es http-SSL, el cual es igual que HTTP descrito con anterioridad, pero con la diferencia que utiliza un cifrado seguro, útil para el intercambio de información seguro. Y por último MySQL, encargado de gestionar las bases de datos.

En la Imagen 9 se ven de igual modo los servicios activos tras el escaneo.

Imagen 9: Resultado del escaneo. Fuente: Elaboración propia

Se procede a realizar el ataque simulado. Para ello, se ha hecho uso de la herramienta Evil FOCA, la cual permite realizar entre otros, ataques DoS como el efectuado a continuación a determinadas direcciones IP.

En la Imagen 10 se muestra la herramienta Evil FOCA siendo usada para el ataque de denegación de servicio entre las direcciones IP 192.168.100.1 y 192.168.100.12 con la dirección IP 192.168.100.254, que es el servidor de archivos (servidor *naswd*).

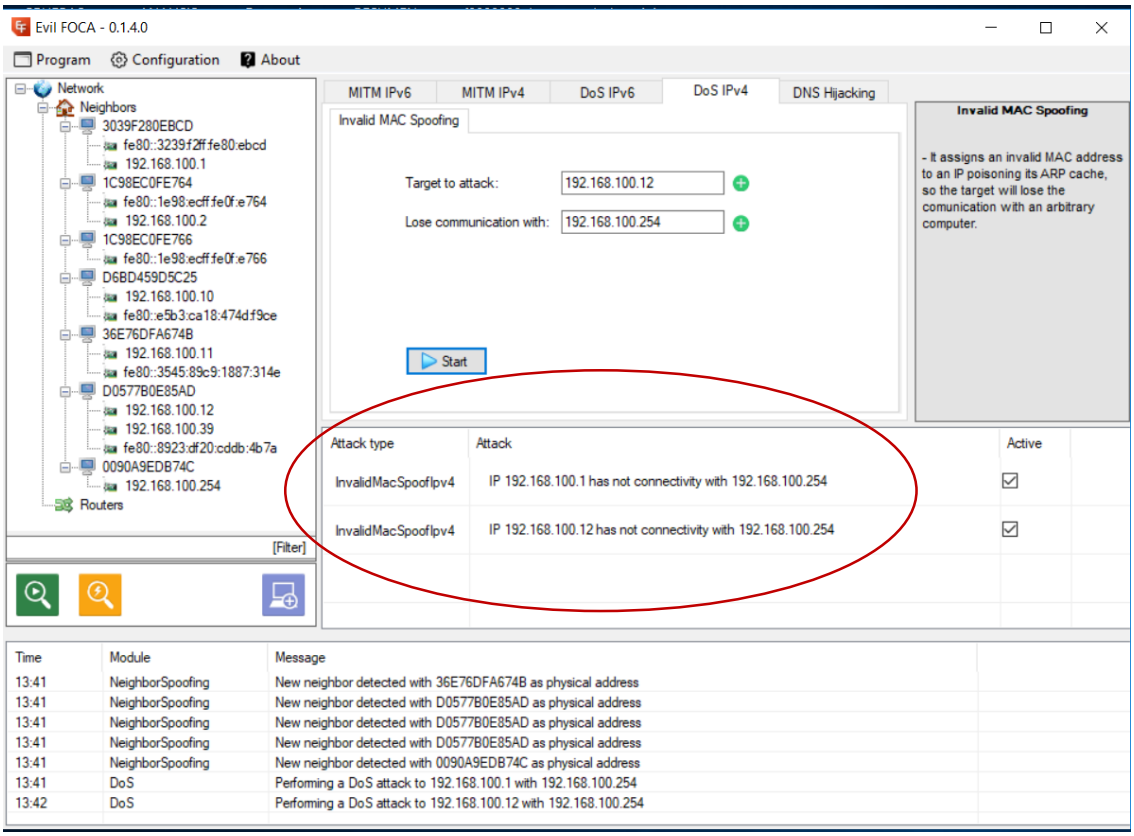

Imagen 10: Ataque DoS. Fuente: Elaboración propia.

Transcurridos unos segundos, el servicio ofrecido por el servidor naswd deja de estar disponible. La Imagen 11 muestra que los servicios http, NetBios-SSN, http-SSL y MySQL están inhabilitados, ya que aparecen reflejados en la interfaz del programa OSSIM de *AlienVault* con color rojo. Existen también otros servicios que siguen en buen estado. Esto es debido a que el programa refresca la información cada cierto tiempo y todavía no ha detectado que estos servicios no están disponibles debido al ataque DoS.

Por todo ello se puede comprobar la efectividad del programa OSSIM de *Alien Vault* y la recomendación de explotarlo en las Unidades de Ciberdefensa como una de sus herramientas fundamentales.

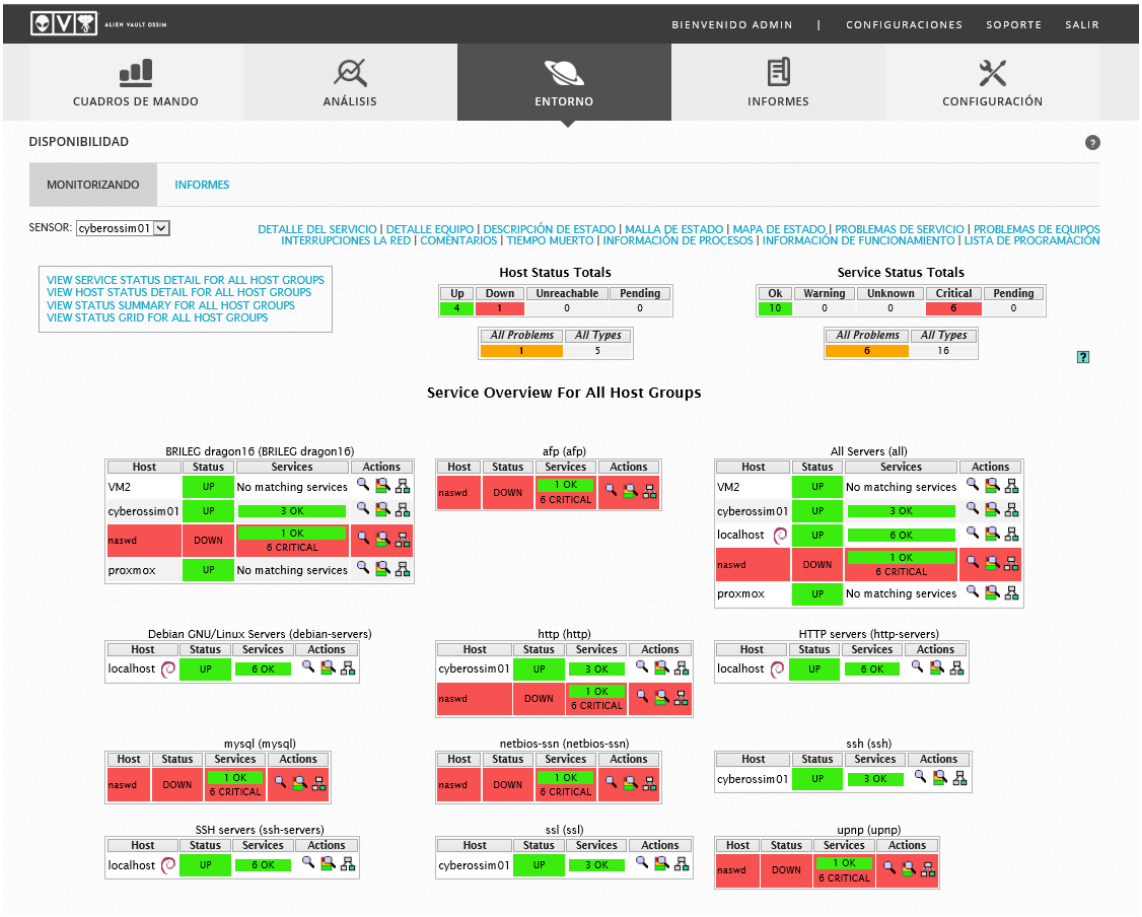

Imagen 11: Entorno OSSIM *Alien Vault* después del ataque.
Fuente: Elaboración propia.

6.2. Práctica de "*Fingerprinting*"

En esta segunda parte de la práctica, se realiza un *fingerprinting* desde un ordenador de la red con el objetivo de buscar información para aprender de la configuración y comportamiento de la misma. Para esta recolecta de información se pueden utilizar varias herramientas. En este caso se ha utilizado la herramienta *nmap*, que sirve para efectuar rastreo de puertos y servicios de un sistema. Esta herramienta se ha ejecutado desde el equipo de nombre *DESKTOP-A7IASCK* y con la dirección IP 192.168.100.39.

En esta primera imagen se puede ver el análisis de vulnerabilidades de los recursos antes del ataque, es decir, qué posibles fallos de seguridad presenta la red antes de de recibir el ataque. Encontramos varias vulnerabilidades que son fruto de las limitaciones del sistema en el laboratorio, y de igual modo, se pueden observar varios falsos positivos, definidos así debido a que al estar en el laboratorio no existe ningún tipo de vulnerabilidad real.

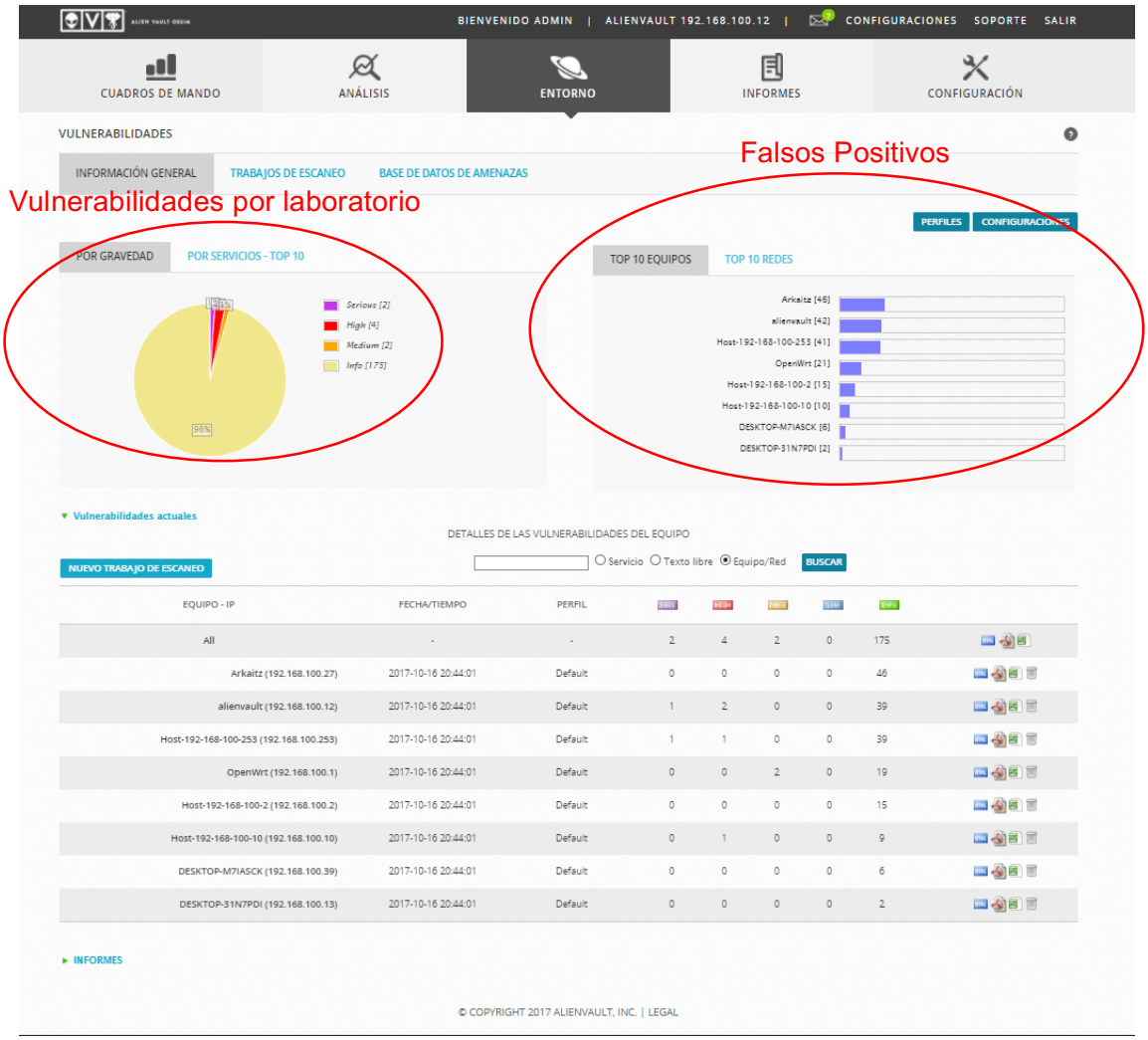

Imagen 12: Análisis anterior al ataque. Fuente: Elaboración propia

En la Imagen 13 se muestran los detalles del tráfico que el programa *Alien Vault* ha detectado debido a los paquetes de tráfico de red generados por el ataque *nmap.* Es decir, que al estar dentro del laboratorio no debería existir gran cantidad de tráfico en la red, y los picos marcados dentro del círculo rojo en la Imagen 13, revelan que sí hay exceso de este tráfico, generado en este caso por el *nmap.*

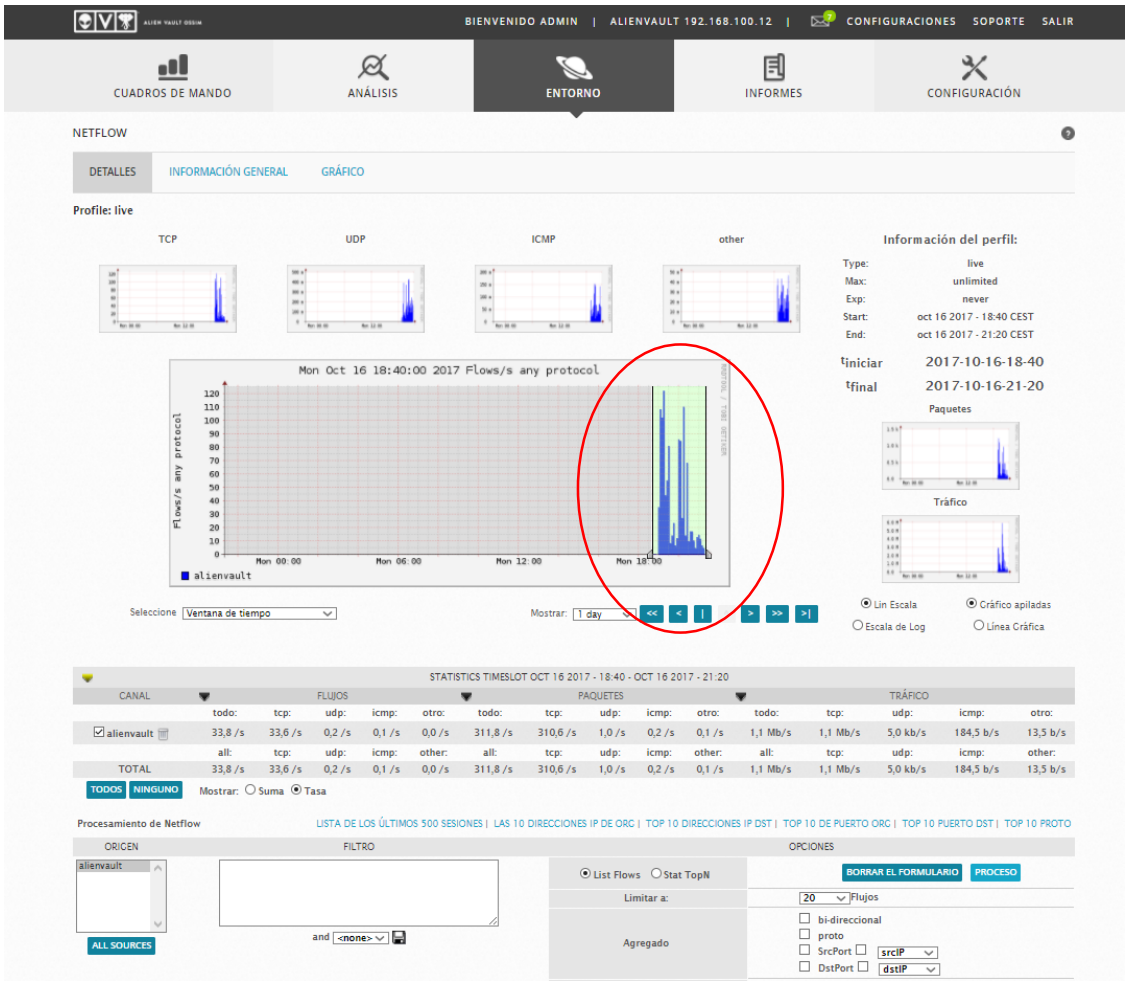

Imagen 13: Tráfico en la red detectado por OSSIM de *Alien Vault*.
Fuente: Elaboración propia

Por último, en la Imagen 14 se muestra en detalle cómo *Alien Vault* ha detectado todos los ataques que ha recibiendo. Los detalla en modo de gráfica (a la izquierda) y en modo de gráfico sectorial a la derecha.

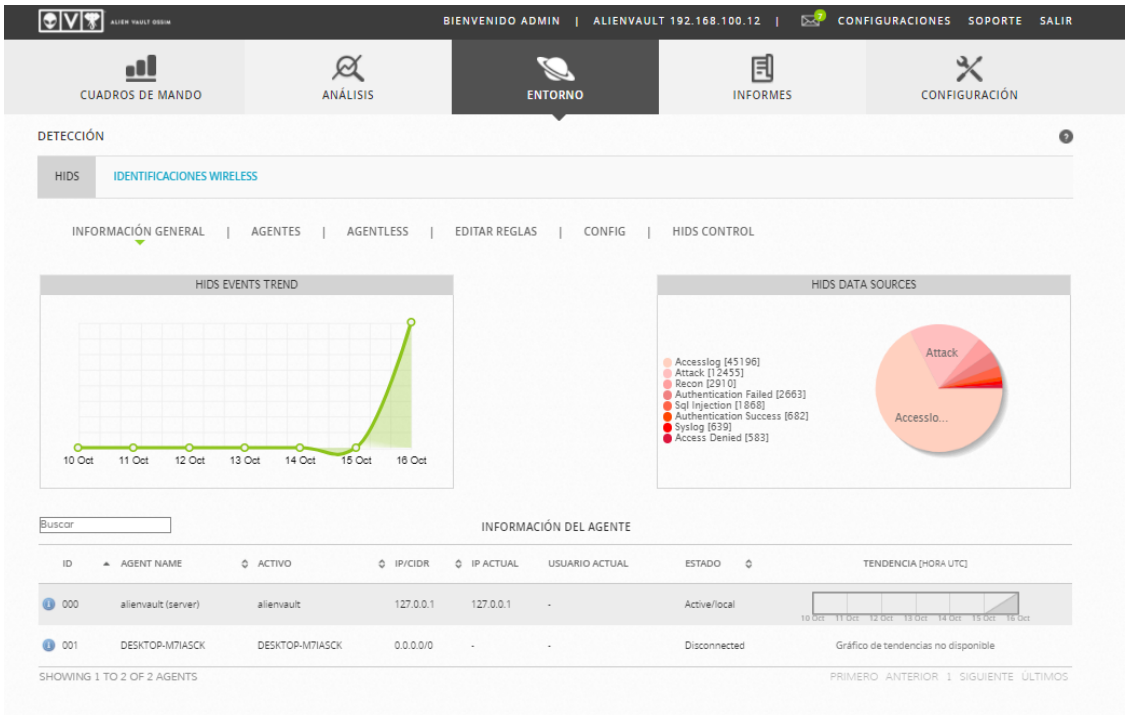

Imagen 14: Ataques recibidos. Fuente: Elaboración propia.

De este modo, y gracias a las prácticas realizadas en el laboratorio de SIMACET, se puede observar de una manera gráfica y tangible cuán efectivo es el programa utilizado OSSIM de *Alien Vault*. Por motivos de seguridad y para no desvelar todas las herramientas que utiliza el programa, se han realizado estas prácticas de una manera muy escueta, pero suficiente para poder comprobar su efectividad.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

7. CONCLUSIONES

El presente trabajo trata de analizar el estado de la ciberseguridad de los medios CIS tácticos de una BOP, más concretamente en el sistema SIMACET. El sistema SIMACET es el Sistema de Mando y Control del Ejército de Tierra mediante el cual, el mando puede ejercer su función de Mando y Control. De igual modo, después de conocer el estado se pretende buscar las posibles recomendaciones de mejora para conseguir un sistema lo más robusto posible ante posibles ataques intencionados.

Para conocer el estado de ciberseguridad actual se ha usado el método científico Delphi. Así, a través de diversas encuestas se han conseguido mejorar ciertos aspectos en los campos de contraseñas, personal, incidentes, usabilidad y autoprotección. Estas mejoras son, en particular, las siguientes: en primer lugar, la concienciación del personal ante la exigencia de cambiar las contraseñas en los periodos marcados por sus responsables. En segundo lugar, el conocimiento por parte de los usuarios del personal encargado de la protección básica de SIMACET. En tercer lugar, la concienciación de los usuarios acerca del borrado de correos, metadatos y demás archivos residentes en los ordenadores. Por último, se ha mejorado el nivel de autoprotección de los expertos bajo la premisa de “necesidad de conocer”. Como se puede observar, todas estas mejoras se encuentran en el ámbito de la concienciación de los usuarios. Ha quedado patente, por tanto, que el usuario sigue siendo el eslabón más débil de la cadena de la seguridad.

De igual modo, se proponen cuatro soluciones para mejorar la seguridad del sistema. La primera de ellas consiste en realizar actividades de Instrucción y Adiestramiento con todo el personal perteneciente a la Compañía de Transmisiones de la Brigada “Alfonso XIII”, II de La Legión. Estas actividades se consideran muy positivas al centrarse en ambientación de ciberdefensa y la capacidad de gestionar incidencias al respecto. La segunda propuesta de mejora consiste en la realización de cursos, charlas y coloquios, al igual que prácticas para el manejo de los programas de familiarización e interpretación de la información obtenida. Con estas actividades se pretende mejorar y aumentar los conocimientos del personal involucrado en materia de Ciberseguridad. En la tercera propuesta, se recomienda el aprovechamiento de los recursos disponibles como son los planes del ET de Concienciación (CONCIBE), Adiestramiento (ACIBE) y Formación (FORCIBE) en Ciberdefensa desarrollados por el MCCD. Por último, pero no menos importante, se propone hacer un uso más exhaustivo del programa OSSIM de *Alien Vault* como herramienta para monitorizar las redes del Ejército de Tierra en busca de posibles vulnerabilidades o ataques.

-PÁGINA INTENCIONADAMENTE EN BLANCO-

ANEXOS

-PÁGINA INTENCIONADAMENTE EN BLANCO-

Anexo A: Encuesta 1

ENCUESTA:

La siguiente encuesta está creada y diseñada por el C.A.C de transmisiones Juan Ignacio Olivares González, cuya finalidad es recoger datos sobre las distintas opiniones de personal especializado acerca de SIMACET. El objetivo final de la encuesta es analizar todas las respuestas y mediante un método científico llegar a conclusiones fiables que se adjuntarán al Trabajo de Fin de Grado.

Se contestarán las preguntas de forma anónima por lo que se ruega máxima seriedad en las respuestas, las cuales varían de 1 a 5, siendo 1 poco, pocas veces, nada, nunca… y 5 siempre, muchas veces, mucho… y otro recuadro a mayores para las preguntas en las que no se sepa la respuesta marcado con ns/nc. La manera de contestarlas será poniendo una X en la casilla correspondiente.

Complejidad:

- 1. ¿Cree que es complicada la creación de un fichero de misión de SIMACET? (G6)

1	2	3	4	5	ns/nc

- 2. ¿Cree que es sencilla la utilización de los programas que usa?

1	2	3	4	5	ns/nc

- 3. ¿Cree que está cualificado para usar correctamente los programas?

1	2	3	4	5	ns/nc

Contraseñas:

- 4. ¿Cree que son robustas las contraseñas que le asignan?

1	2	3	4	5	ns/nc

- 5. ¿Cambia la contraseña de los equipos con la asiduidad requerida?

1	2	3	4	5	ns/nc

Personal:

- 6. ¿Tiene identificado a su TASO y sabe cómo usarlo?

1	2	3	4	5	ns/nc

- 7. ¿Tiene identificado a su RSA?

1	2	3	4	5	ns/nc

Incidentes:

- 8. ¿Sabe a quién avisar si ocurre algo extraño en el ordenador que utiliza?

1	2	3	4	5	ns/nc

- 9. ¿Sabe cuál es el método de actuación ante un incidente informático?

1	2	3	4	5	ns/nc

Usabilidad:

- 10. ¿Redirige automáticamente mensajes recibidos a otra cuenta de correo?

1	2	3	4	5	ns/nc

- 11. ¿Envía sin comprimir los archivos anexados a los mensajes?

1	2	3	4	5	ns/nc

Autoprotección:

- 12. ¿Borra periódicamente mensajes de las carpetas y de la papelera de reciclaje?

1	2	3	4	5	ns/nc

- 13. Si envía un mensaje a múltiples destinatarios ¿hace que las direcciones permanezcan ocultas para el resto de destinatarios?

1	2	3	4	5	ns/nc

Información:

- 14. ¿Cree que cuenta con la información suficiente sobre ciberdefensa?

1	2	3	4	5	ns/nc

- 15. Observaciones o sugerencias para una posible mejora del sistema:

Anexo B. Encuesta 2

ENCUESTA:

La siguiente encuesta está creada y diseñada por el C.A.C de transmisiones Juan Ignacio Olivares González, cuya finalidad es recoger datos sobre las distintas opiniones de personal especializado acerca de SIMACET. A raíz de las preguntas más destacables de la anterior encuesta, se ha elaborado otra similar con el fin último de comparar respuestas, analizarlas y mediante un método científico llegar a conclusiones fiables que se adjuntarán al Trabajo de Fin de Grado.

Se contestarán las preguntas de forma anónima por lo que se ruega máxima seriedad en las respuestas, las cuales varían de 1 a 5, siendo 1 poco, pocas veces, nada, nunca… y 5 siempre, muchas veces, mucho… y otro recuadro a mayores para las preguntas en las que no se sepa la respuesta marcado con ns/nc. La manera de contestarlas será poniendo una X en la casilla correspondiente.

Preguntas de interés estadístico:

- 1. ¿Ha leído el informe enviado por parte del alumno?
- 2. ¿Le ha servido de ayuda el informe?
- 3. ¿Ha buscado información sobre las preguntas que desconocía?

Contraseñas:

- 4. ¿Cree que son robustas las contraseñas que le asignan?

1	2	3	4	5	ns/nc

- 5. ¿Cambia la contraseña de los equipos con la asiduidad requerida?

1	2	3	4	5	ns/nc

Personal:

- 6. ¿Tiene identificado a su TASO (Terminal Area Security Officer) y sabe cómo usarlo?

1	2	3	4	5	ns/nc

- 7. ¿Tiene identificado a su RSA(Responsable de Seguridad de Área)?

1	2	3	4	5	ns/nc

Incidentes:

- 8. ¿Sabe a quién avisar si ocurre algo extraño en el ordenador que utiliza?

1	2	3	4	5	ns/nc

- 9. ¿Sabe cuál es el método de actuación ante un incidente informático?

1	2	3	4	5	ns/nc

Usabilidad:

- 10. ¿Redirige automáticamente mensajes recibidos a otra cuenta de correo?

1	2	3	4	5	ns/nc

- 11. ¿Envía sin comprimir los archivos anexados a los mensajes?

1	2	3	4	5	ns/nc

Autoprotección:

- 12. ¿Borra periódicamente mensajes de las carpetas y de la papelera de reciclaje?

1	2	3	4	5	ns/nc

- 13. Si envía un mensaje a múltiples destinatarios ¿hace que las direcciones permanezcan ocultas para el resto de destinatarios?

1	2	3	4	5	ns/nc

Información:

- 14.¿Cree que cuenta con la información suficiente sobre ciberdefensa?

1	2	3	4	5	ns/nc

15. Observaciones o sugerencias para una posible mejora del sistema:

Anexo C: Informe encuesta 1

INFORME: RESULTADOS DE LA ENCUESTA SOBRE CIBERSEGURIDAD EN SIMACET:

UNIVERSO:

En el conjunto de encuestas que forman parte del método Delphi, se planteó como primer objetivo la elaboración de un estudio para saber cuál es el estado de la ciberseguridad en SIMACET actualmente y cuáles son las líneas futuras que se podrían proponer para así conseguir un sistema lo más robusto y utilizable posible.

LA MUESTRA:

En el desarrollo del objetivo participaron 15 personas, pertenecientes a:

- VII Bandera
- VIII Bandera
- BZAP
- GACA
- GRECO
- X Bandera

Y ocupando los puestos de:

- Jefes de Bandera
- S2/S3 de Bandera
- Equipo CIS de Bandera
- G6 de Brigada

HERRAMIENTA O TÉCNICA DE RECOLECCIÓN DE DATOS:

Para la elaboración del método se realizó una primera encuesta al personal experto que juegan un papel importante en la ciberseguridad de SIMACET. En este primer cuestionario se definieron 15 preguntas, las cuales debían permitir conocer:

1. Si los usuarios están capacitados para usar los servicios que proporciona SIMACET.

2. La opinión sobre las contraseñas proporcionadas.

3. Si se conoce al personal encargado de la seguridad.

4. El grado de conocimiento ante un incidente.

5. El grado en que los usuarios optimizan los servicios.

6. El nivel de autoprotección con el que se cuenta.

7. Percepción de los conocimientos de ciberdefensa por parte de los usuarios.

RESULTADOS:

		COMPLEJIDAD						
PREGUNTA 1		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	0%	0%	13%	87%	15

		COMPLEJIDAD						
PREGUNTA 2		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	7%	0%	7%	87%	0%	15

		COMPLEJIDAD						
PREGUNTA 3		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	7%	0%	7%	87%	0%	15

		CONTRASEÑAS						
PREGUNTA 4		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	13%	13%	73%	0%	15

		CONTRASEÑAS						
PREGUNTA 5		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	7%	47%	27%	20%	0%	15

		PERSONAL						
PREGUNTA 6		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	13%	27%	13%	20%	20%	15

		PERSONAL						
PREGUNTA 7		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	0%	27%	27%	40%	0%	15

		INCIDENTES						
PREGUNTA 8		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	20%	47%	33%	0%	15

		INCIDENTES						
PREGUNTA 9		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	27%	27%	47%	0%	15

		USABILIDAD						
PREGUNTA 10		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	47%	0%	27%	0%	27%	0%	15

		USABILIDAD						
PREGUNTA 11		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	33%	0%	47%	0%	20%	0%	15

		AUTOPROTECCIÓN						
PREGUNTA 12		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	7%	20%	33%	33%	0%	15

		AUTOPROTECCIÓN						
PREGUNTA 13		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	7%	20%	27%	20%	27%	0%	15

		INFORMACIÓN						
PREGUNTA 14		1	2	3	4	5	ns/nc	SUMA
	ENCUESTA 1	0%	0%	33%	53%	13%	0%	15

-PÁGINA INTENCIONADAMENTE EN BLANCO-

BIBLIOGRAFÍA

[1] Orden Ministerial, 76/2002, Madrid: BOD número 83, 2013.

[2] Cuartel General de Fuerza Terrestre, Norma 205/15 Ciberdefensa Táctica en Fuerza Terrestre, Sevilla, 2015.

[3] Ministerio de Defensa, Orden DEF/1265/2015 por la que se desarrolla la organización básica del Ejército de Tierra, Madrid, 2015.

[4] Mando de Adiestramiento y Doctrina, PD3-602 Establecimiento y empleo de SIMACET, Madrid, 2009.

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

[6] S. A. Fernando Gordo, CIBERSEGURIDAD GLOBAL, oportunidades y compromisos en el uso del Ciberespacio, Granada: Universidad de Granada, MADOC, 2013.

[7] J. L. B. R. a. C. L. A. Avizienis, Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing, 2004.

[8] Instrucción General 9/ 89 de Protección de Materias Clasificadas del Ejército de Tierra, 1989.

[9] Alien Vault, «Alien Vault,» [En línea]. Available: https://www.alienvault.com/. [Último acceso: Enero 2018].

[10] J. J. R. Fernández, Visión del JEMAD de la Ciberdefensa Militar, 2011.

[11] Estado Mayor de la Defensa, Norma General 05/ 03 INFOSEC, Madrid, 2003.

[12] M. R. Brey, Estrategia de Ciberseguridad Nacional, Madrid, 2013.

[13] Estado Mayor de la Defensa, Instrucción Técnica 08/ 05 CRIPTOSEC seguridad física y personal de material de Cifra, Madrid, 2005.

[14] Estado Mayor del Ejército, Norma General 01/ 04 EME de Procedimiento de acreditación para sistemas del ET, Madrid, 2004.

[15] JCISAT, Arquitectura de Referencia de Seguridad de los CIS Desplegables, Madrid, 2017.

[16] Mando Conjunto de Ciberdefensa, Plan de Formación en Ciberdefensa del Ministerio de Defensa, Madrid, 2015.

[17] C.-C. H. y. B. A. Sandford, «pareonline,» 2007. [En línea]. Available: http://pareonline.net/pdf/v12n10.pdf. [Último acceso: Enero 2018].

[18] S. H. Lapeña, «Virtualización,» Marines, 2018.