PROGRAMACIÓN DIDÁCTICA

CIBERDEFENSA

(CYBER DEFENSE)

Máster Universitario en Formación del Profesorado

Presentado por:

D. CARLOS BAYÓN ARNANZ

Dirigido por:

D. ROBERTO NÚÑEZ PEQUE (EMCE)

Dra. Dª. TERESA I. DÍEZ FOLLEDO (UAH)

Alcalá de Henares, a 20 de mayo de 2021

ÍNDICE

Contenido

1. JUSTIFICACIÓN

Esta Programación Didáctica se refiere al módulo de Ciberdefensa (ESFCYB13), desarrollado durante el tercer trimestre del curso de primero para el acceso a la Escala de Suboficiales del Cuerpo General del Ejército del Aire de la especialidad de Sistemas de Información, Comunicaciones y Ciberdefensa, mediante la forma de ingreso con exigencia de titulación previa. **El módulo se desarrolla durante 15 horas y se dirige a Sargentos Alumnos de formación.**

La condición exigida para acceder con estas condiciones y a esta especialidad es estar en posesión, o en condiciones de obtener, antes del inicio de la primera prueba, de uno de los siguientes tres Títulos de Técnico Superior (TTS):

- Sistemas de Telecomunicaciones e Informáticos.
- Administración de Sistemas Informáticos en Red.
- Desarrollo de Aplicaciones Multiplataforma.

En aras de planificar un curso de manera adecuada, se establecen tres niveles de concreción y, dentro del más bajo, se incluye esta programación didáctica, en la que el docente, además, incluye las unidades didácticas, en las que se declaran los detalles del proceso de enseñanza-aprendizaje que se va a desarrollar durante el proceso educativo, dentro de una estructura marcada por el currículo.

Las líneas maestras de las vías educativas se encuentran en el currículo, pero se requiere de un profundo trabajo de desarrollo doctrinal para transformar esas decisiones de carácter general en una propuesta lógica de actividades en el aula, organizadas en torno a las unidades didácticas del aula. La unidad didáctica es un paraguas bajo el que se desarrolla el trabajo diario en el aula, de forma que establece con todo detalle la evolución que va a sufrir el proceso de enseñanza-aprendizaje en el medio educativo.

Hay diferentes niveles de currículo que tienen que ver con el nivel de toma de decisiones y su concreción.

Partiendo de esta base, la planificación curricular y organizativa se va a realizar a través de tres niveles de concreción como son:

- Primer nivel: aquí encontramos los diferentes documentos legales que marcan las directrices en cuanto a normas de evaluación, de progreso y de permanencia en los centros docentes y el régimen del alumnado de la enseñanza de formación, regulado todo ello mediante Leyes (como la de la Carrera Militar), Reales Decretos y Órdenes Ministeriales, tanto del Ministerio de Defensa como del de Educación. Por último, el currículo, los planes de estudio y las memorias justificativas se extienden, como el conjunto de perfiles profesionales, objetivos, competencias generales y específicas, contenidos, metodologías, resultados de aprendizaje y criterios de evaluación de cada una de las enseñanzas regulada por la ley. En todos estos documentos legales se encuentran una serie de "directrices" sobre lo que se va a enseñar y evaluar y de qué modo se hará.
- Segundo nivel: es un nivel de concreción en el que encajamos los diferentes documentos aprobados por la Dirección de Enseñanza del Ejército del Aire o por la propia Unidad en la que se imparte la materia y que son elaborados por los Equipos Docentes que participan en el proyecto educativo. Este nivel se concreta en las Normas de Régimen Interior, el Plan anual de centro, las Guías Docentes y el Programa del Curso. La concreción se produce por la secuenciación de Objetivos y Contenidos del primer nivel.
- Tercer nivel: cada profesor de módulo o asignatura elabora su Programación Didáctica de aula, donde se concretará el proceso de Enseñanza-Aprendizaje para un grupo de alumnos. Es en definitiva el punto final o la culminación de un proceso de planificación de la intervención educativa en su conjunto.

El artículo 45 de la **Ley 39/2007, de 19 de noviembre, de la carrera militar**, dispone que "*la formación de suboficiales tiene como finalidad la preparación y capacitación para el ejercicio profesional y la obtención de las especialidades fundamentales que sean necesarias. Comprenderá la formación general y la formación específica y la formación técnica correspondiente a un título de formación profesional de grado superior"*.

El artículo 58 de esa misma Ley prevé el ingreso en los centros docentes de formación para el acceso a las escalas de suboficiales, con las titulaciones de formación profesional que reglamentariamente se establezcan.

Por otra parte, el artículo 65.1 de la citada Ley establece que *"los planes de estudios de la formación militar general y específica y, en su caso, técnica, se ajustarán a la definición de capacidades y diseño de perfiles para el ejercicio profesional establecidos por los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire".*

Respecto a la duración y estructura de la enseñanza de formación, en el artículo 11 del **Reglamento de ordenación de la enseñanza de formación en las Fuerzas Armadas, aprobado por Real Decreto 1051/2020**, de 1 de diciembre, se establece que, *"para las Escalas de Suboficiales, en el caso de que se haya ingresado con el requisito de titulación de Técnico Superior, sólo se requerirá la superación de los planes de estudios de la formación militar general, específica y para la adquisición de la especialidad fundamental que, en función de la procedencia y teniendo en cuenta las titulaciones y convalidaciones que sean de aplicación, se integrarán en un currículo único y se distribuirá a lo largo de un solo curso académico".*

En desarrollo de lo anterior, la **Orden DEF/1626/2015, de 29 de julio, por la que se aprueban las directrices generales para la elaboración de los currículos de la enseñanza de formación para el acceso a las diferentes escalas de suboficiales de los cuerpos de las Fuerzas Armadas**, modificada por la Orden DEF/368/2017, de 4 de abril, introduce como principal novedad *"la integración en un único currículo de los planes de estudios correspondientes a la formación militar general y específica, la formación para la adquisición de una especialidad fundamental y, en su caso, la formación técnica correspondiente a un título de formación profesional de grado superior",* y establece, en su artículo 6.2, que *"cuando para el ingreso se haya exigido un título de Técnico Superior, la enseñanza de formación excluirá de los planes de estudios los contenidos conducentes a la obtención de un título de Técnico Superior del sistema educativo general. Por otra parte, en su artículo 14, desarrolla nuevos criterios acerca del diseño y contenido de los currículos, en base a los cuales se elabora esta orden ministerial".*

El Real Decreto 595/2016, de 2 de diciembre, en su artículo único, modifica el reglamento de Especialidades Fundamentales de las Fuerzas Armadas, aprobado por Real Decreto 711/2010, de 28 de mayo, estableciendo que *"en la*

escala de suboficiales del Cuerpo General del Ejército del Aire existirán las siguientes especialidades fundamentales:

- *Protección de la Fuerza y Apoyo a las Operaciones.*
- *Mantenimiento Aeronáutico.*
- ***Sistemas de Información, Comunicaciones y Ciberdefensa.***
- *Mantenimiento de Electrónica.*
- *Control Aéreo.*
- *Administración."*

2. CONTEXTUALIZACIÓN

2.1 Localización.

La Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT) se encuentra sita en la Comunidad de Madrid, a la altura del Km. 10,600 de la Carretera A-V (de Extremadura), en la zona sur de la Base Aérea de Cuatro Vientos.

Se ubica junto al Museo del Aire y el Club Deportivo Barberán, dentro del término municipal de Alcorcón (Madrid).

2.2 Historia.

Fecha de creación: 1946

La Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT) es una Unidad histórica que, con la denominación de Escuela de Transmisiones del Ejército del Aire, fue creada por el ministro del Aire, Eduardo González Gallarza, como uno de los componentes del "Servicio de Transmisiones del Ejército del Aire" para el perfeccionamiento teórico y práctico del personal que prestase su servicio en transmisiones.

En 1949 comenzó a impartirse el primer curso de Transmisiones en el Acuartelamiento del primer Regimiento de Transmisiones, en la madrileña colonia de El Viso.

Por Orden Ministerial de 25 de enero de 1950 se reorganizó el "Servicio de Transmisiones del Ejército del Aire", suprimiéndose la Jefatura de Instrucción de dicho Servicio y como consecuencia, la Escuela de Transmisiones asumió directamente las misiones de formación de especialistas de esta materia. El día 2 de septiembre del mismo año tomó posesión el coronel Fernando Alfaro y del Puedo, su primer jefe y organizador.

Tras diversas vicisitudes, en 1951, fue cuando la Escuela de Transmisiones se trasladó al lugar donde actualmente radica, al sur de la Base Aérea de Cuatro Vientos, principalmente dentro del término municipal de Alcorcón, ciudad con la que le unen especiales vínculos de relación.

En febrero de 1952 se incorporaron a la Escuela de Transmisiones los soldados alumnos aspirantes a Ayudantes de Especialistas: Radiotelegrafistas, Mecánicos de Transmisiones y Mecánicos de Radio, procedentes de la Escuela de Especialistas de Málaga que se trasladó como tal a su nueva sede en León, iniciándose con ellos las actividades de formación de tropa especialista, que era el nombre que recibían los soldados cuyos cometidos eran más técnicos. En marzo de 1953, la Escuela consolidó sus actividades de formación, iniciándose en sus instalaciones, el primer curso completo de especialistas.

Por otro lado, en 1958 inició sus actividades como Escuela de Controladores de Interceptación, con la instalación del simulador de una sala de operaciones del Sistema de Defensa Aérea que había recibido España como parte de la ayuda americana tras la II GM, en el histórico edificio de Jefatura de Estudios de la Escuela.

Merece especial mención que la Escuela, desde su traslado a Cuatro Vientos y hasta 1972 contó con una Unidad de Vuelo para las prácticas de alumnos y entrenamiento del profesorado, ubicada en el hangar principal y la plataforma del actual Museo del Aire que, a partir de 1965 se denominó 755 Escuadrón y que en 1970 pasó a ser la 515 Escuadrilla, utilizando principalmente el T-2B Júnker el Ju-52, la E-3B Bucker BU-131, el Huarte Mendicoa HM-1 y el Hispano Suiza HS-42.

En 1966, se crea la Escuela de Formación Profesional Industrial (de Primer Grado) del Ejército del Aire en la Escuela de Transmisiones. Dicha Escuela desarrolló su labor docente en las ramas Eléctrica (Instalador-montador) y Electrónica, hasta septiembre del año 1986, formando hasta veinte promociones. También un año antes concluía la Instrucción Técnica Especial (ITE) que se venía impartiendo en la Escuela a personal de Tropa en materias técnicas, habiéndose formado quince promociones de alumnos.

El 12 de julio de 1978 se inauguró, por Su Majestad El Rey Don Juan Carlos I, la Plaza de Armas de la Escuela, que actualmente lleva su nombre, coincidiendo con la entrega de despachos a todos los sargentos especialistas del Ejército del Aire promocionados ese año.

En 1996, la Escuela de Transmisiones ha pasado a denominarse Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT), integrándose más tarde en la Base Aérea de Cuatro Vientos con carácter de unidad independiente.

A partir del año 2000, una vez decidida la integración en una única área doctrinal C2/CIS de las materias: Mando y Control, Telecomunicaciones y Sistemas de Información y Seguridad de la Información Electrónica, la Escuela ha preparado y realizado una serie de cursos, nuevos o modificados, para la dirección, el planeamiento, la operación y el mantenimiento de estos Sistemas CIS.

En el verano de 2002, entró en funcionamiento el nuevo Simulador de Defensa Aérea, de tecnología análoga al nuevo sistema de mando y control implantado en los centros operativos de Grupo Central de Mando y Control (Madrid), Grupo Norte de Mando y Control (Zaragoza) y Grupo de Alerta y Control (Gran Canaria) y que fue desarrollado íntegramente por INDRA.

En la primavera del año 2003 se celebró, con un solemne acto militar, los cincuenta años del ingreso en la Escuela de su 1ª Promoción de Soldados Ayudantes de Especialistas (Radiotelegrafistas, Mecánicos de Radio y Mecánicos de Transmisiones).

En los últimos años, la EMACOT sigue ejerciendo funciones de Centro de Formación Militar para Personal de Tropa, de acuerdo a lo previsto en la Ley 17/99 y en virtud de esta función se han realizado en la plaza de armas de la misma, actos solemnes de Juramento o Promesa de fidelidad ante la Bandera de España, de alumnos de tropa, de ciclos formativos, de diferentes especialidades.

El 24 de noviembre de 2003 se celebró en el salón de actos de la EMACOT el 75 aniversario de la creación de la Escuela Superior de Aerotecnia, con un solemne acto académico presidido por Su Majestad el Rey y que contó con destacadas autoridades civiles y militares. Los edificios principales de la Escuela se construyeron para ubicar en 1930 la entonces Escuela Superior de Aerotecnia, que impartió enseñanzas de ingeniería aeronáutica por primera vez en España.

La Escuela muestra con orgullo su historia y su personal es consciente de la responsabilidad que tiene de conservar sus tradiciones y, al mismo tiempo, innovar en las materias de su competencia, sujetas a una continua evolución tecnológica.

2.3 Misión.

La misión de la Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT) consiste en impartir enseñanza de formación y perfeccionamiento para capacitar al personal del Ejército del Aire en las especialidades de "Mando y Control", "Telecomunicaciones y Electrónica" y “Ciberdefensa”, lo cual agrupa las áreas de conocimiento de mando y control, sistemas de información y comunicaciones (CIS), guerra electrónica, electrónica en general e informática y ciberdefensa. Desde el año 2000, los cursos que se imparten se ampliaron a los Sistemas de Información y a la Seguridad de la Información Electrónica (INFOSEC), dentro del concepto CIS.

Más recientemente, por acuerdo firmado entre el Ejército del Aire y la Dirección General de la Guardia Civil, se ha asignado a la Escuela la responsabilidad de formar como operadores de radar a miembros de la Guardia Civil para desempeñar funciones en sus nuevas aeronaves de ala fija en dotación orgánica.

Dentro de estas materias, se instruye en las actividades de planeamiento, dirección, operación y mantenimiento de estos sistemas. La enseñanza impartida está estructurada en enseñanza de formación y enseñanza de perfeccionamiento para profesionales del Ejército del Aire que deban adquirir una especialidad o adiestramiento complementario.

La enseñanza de formación se estructura en los siguientes niveles:

- Escala Superior de Oficiales (Alféreces Alumnos), del Cuerpo General con formación de Mando y Control y de Sistemas de Información y Comunicaciones.
- Escala de Suboficiales (Sargentos Alumnos), del Cuerpo General con las especialidades “Control Aéreo”, “Sistemas de Información, Comunicaciones y Ciberdefensa” y “Mantenimiento de Electrónica”.
- Militares Profesionales de Tropa (Soldados Alumnos), de las especialidades de Mando y Control (ACO) y Auxiliar de electrónica Telecomunicaciones y Electrónica (AEL).

Los alféreces y los sargentos alumnos realizan la formación general militar en las Academias respectivas; Academia General del Aire (San Javier) y Academia Básica del Aire (León). La posterior formación de especialización se les imparte en la Escuela.

Los soldados alumnos inician, en la Escuela de Técnicas de Seguridad, Defensa y Apoyo (Zaragoza) la fase de su formación general militar junto al resto de especialidades; y la de especialización, en la EMACOT.

Anualmente se imparten unos veintidós cursos de perfeccionamiento para personal del Ejército del Aire, a los que también asisten alumnos de otros ejércitos e, incluso, de otras naciones, en los empleos de oficiales, suboficiales y tropa.

Los Cursos de Perfeccionamiento para oficiales y suboficiales del Ejército del Aire que se realizan actualmente son, entre otros:

- Controlador de Interceptación (CI).
- Avanzados y reentrenamiento de Operadores de Alerta y Control (OAC).
- Seguridad de la Información Electrónica (INFOSEC).
- Cripto-Custodio
- Guerra Electrónica.
- Redes Radio con propagación en diferentes bandas del espectro.
- Comunicaciones tácticas por radio.
- Ciclo de comunicaciones digitales con cuatro tipos de curso.
- Monográficos de equipos, como el de Centrales telefónicas MD-110 (BC-10)

En la Escuela también se imparten los cursos de Sistemas de Información y Comunicaciones (CIS) Conjunto de las Fuerzas Armadas y de Gestión de Frecuencias por la Dirección de Sistemas de Información y Comunicaciones del Estado Mayor Conjunto.

La Escuela se ha convertido en un centro de excelencia en materia del mando, control, comunicaciones y ciberseguridad, de reconocido prestigio en los ámbitos profesionales específicos del Ejército del Aire y conjuntos de las Fuerzas Armadas.

2.4 Curiosidades

El edificio de la Jefatura de Estudios de la Escuela fue diseñado en 1928 por el entonces teniente coronel Emilio Herrera Linares con motivo de la creación de la Escuela Superior de Aerotecnia, donde en 1930 se empezaron a formar Ingenieros Aeronáuticos en España. A vista de pájaro se distingue la **planta de los edificios principales en forma de "E" e "I" que se corresponden con las iniciales de Escuela de Ingenieros.**

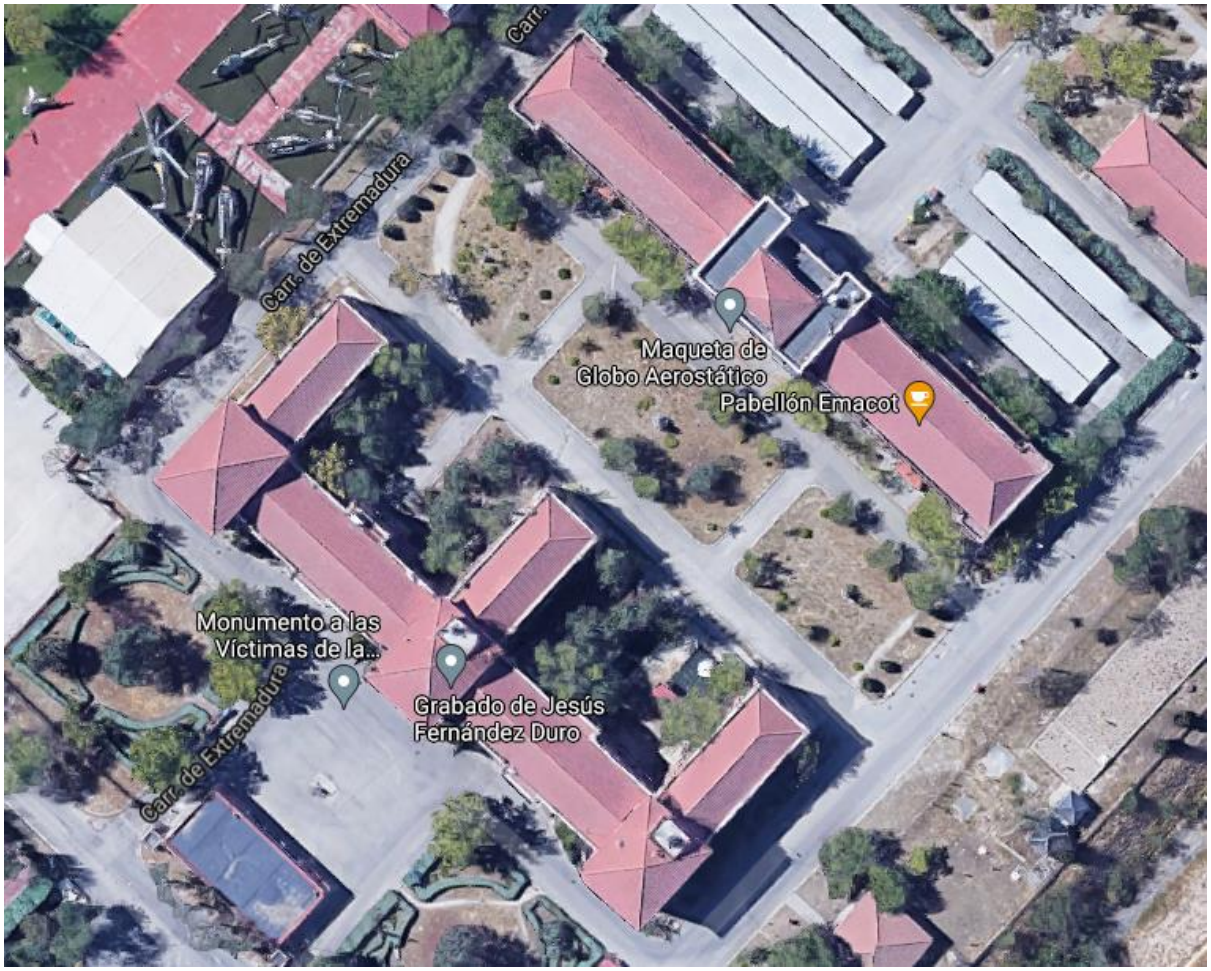

Ilustración 1 obtenida con Google Maps.

La Escuela contó con una Unidad de Vuelo hasta 1972 para las prácticas de alumnos y entrenamiento del profesorado, ubicada en el hangar principal y la plataforma del actual Museo del Aire. El 29 de mayo de 1957 fallecieron en acto de servicio, como consecuencia de accidente aéreo, el director de la Escuela, Coronel Fernando Alfaro y del Pueyo, el Alférez de Complemento José Luis Manzano Marroquí, el Brigada

Radiotelegrafista Serafín Márquez Gómez, y los Cabos Primeros Dionisio Estévez de Pablo y Francisco Alonso Sánchez.

Las relaciones de la Escuela con la ciudad de Alcorcón son estrechas. El 7 de julio de 1989 se celebró la entrega e imposición de una corbata honorífica al Estandarte y, recientemente, el 16 de junio de 2009 tuvo lugar el acto de entrega del Guion de Unidad por parte del Ayuntamiento de Alcorcón.

3. OBJETIVOS, RESULTADOS DE APRENDIZAJE Y CONTENIDOS.

3.1 Objetivos

Capacitar al Sargento de la Escala de Suboficiales del Cuerpo General del Ejército del Aire, Especialidad Fundamental Sistemas de Información, Comunicaciones y Ciberdefensa para actuar con disciplina, asumiendo los principios de jerarquía y unidad de acción, con sujeción a la Constitución, a las Reales Ordenanzas, al derecho de los conflictos armados y al resto del ordenamiento jurídico, utilizando las formas propias de acción del Ejército del Aire.

Proporcionar la capacitación y especialización requeridas para ejercer las funciones operativas, técnicas, logísticas, administrativas y docentes que le corresponden de acuerdo con su empleo, en el desempeño de las actividades relacionadas con el diseño, desarrollo, instalación, configuración, administración y mantenimiento de los sistemas de información y de los equipos y redes que los soportan, así como la implantación y gestión de medidas de seguridad TIC («Tecnologías de la información y la comunicación») y operaciones de ciberdefensa en dichos sistemas, equipos y redes.

Componer un esquema mental que le permita adecuar sus acciones a las circunstancias, mediante la evaluación de riesgos y la deducción de opciones oportunas y adecuadas.

Facilitar la interpretación, transmisión y ejecución de órdenes e ideas en castellano o inglés, para desarrollar su actividad integrado en organizaciones militares multinacionales.

3.2 Competencias generales.

Se señalan todas las que corresponden al currículo y en negrita las que afectan al módulo.

- CG.1 Adquirir los principios y valores constitucionales para enmarcar su actuación en las reglas de comportamiento militar y en el código de conducta de los empleados públicos.

- CG.2 Ejercer, potenciando aquellas cualidades que contribuyen a motivar a sus subordinados, el liderazgo para ejercer el mando a su nivel.
- **CG.3 Potenciar adecuadamente la capacidad de aprendizaje, análisis y síntesis para construir conocimiento.**
- **CG.4 Aplicar con precisión los conocimientos a la práctica para tomar decisiones oportunas, concretas y acertadas en el cumplimiento de las órdenes recibidas.**
- CG.5 Organizar, planificar y trabajar conjuntos de personas de entidad pelotón, con diferentes habilidades y aptitudes para lograr objetivos claramente definidos.
- CG.6 Afrontar con habilidad las modificaciones de conductas impuestas por las circunstancias para adelantarlas a nuestras necesidades.
- CG.7 Potenciar mediante el ejercicio de la habilidad para la expresión oral y escrita en castellano y en inglés la capacidad de comunicación que posibilite la comprensión y transmisión de órdenes, ideas y conceptos.
- CG.8 Identificar adecuadamente la normativa marco de ámbito internacional relacionándola con los conflictos armados y el derecho internacional humanitario.
- CG.9 Aplicar adecuadamente las medidas medioambientales necesarias para preservar las instalaciones y zonas de operación.
- **CG.10 Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo.**
- CG.11 Adquirir las normas de conducta y virtudes militares para adecuar su actuación a las disposiciones en vigor.
- **CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular.**
- CG.13 Adquirir los fundamentos de primeros auxilios y soporte vital básico.
- CG.14 Identificar las organizaciones internacionales de Seguridad y Defensa y los Tratados suscritos por España para poder integrarse en dichas organizaciones
- **CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional.**

- CG.16 Adquirir los fundamentos socio-humanísticos necesarios para el ejercicio profesional.
- CG.17 Adquirir los fundamentos teóricos sobre riesgos laborales necesarios para el ejercicio profesional.
- CG.18 Adquirir los fundamentos teóricos básicos de seguridad y defensa necesarios para el ejercicio profesional.
- CG.19 Aplicar el mando y preparación de la unidad militar de su nivel y el marco general de las superiores en las que se encuentra.
- CG.20 Alcanzar y mantener mediante la práctica deportiva la preparación psicofísica, para soportar las situaciones de esfuerzo físico y psíquico a que estuviese sometido.
- CG.21 Detectar con rapidez situaciones de peligro, potencialmente peligrosas o que puedan afectar a la seguridad para reaccionar ante ellas con oportunidad y acierto.
- **CG.22 Interpretar adecuadamente documentos profesionales operativos, para ordenar con claridad y precisión y ejecutar las órdenes que reciba con prontitud y habilidad.**

3.3 Competencias específicas.

Se señalan todas las que corresponden a la especialidad fundamental Sistemas de Información, Comunicaciones y Ciberdefensa y en negrita las que afectan al módulo.

- CE.1 Manejar y aplicar la normativa de los sistemas CIS/TIC en el ámbito del E.A., Conjunto, Nacional e Internacional, así como la normativa de seguridad de estos sistemas.
- CE.2 Instalar, configurar, operar y mantener equipos de radiocomunicaciones (bandas HF, VHF, UHF y Microondas).
- CE.3 Instalar, configurar, operar y mantener tanto los equipos de comunicaciones satélite como las centrales telefónicas y equipos asociados.
- CE.4 Configurar y explotar sistemas informáticos, aplicando los conocimientos en Bases de Datos y Sistemas Operativos; desarrollando aplicaciones informáticas de acuerdo con las diferentes metodologías y entornos de programación.

- CE.5 Instalar, configurar, mantener y gestionar redes de datos (LAN/WAN).
- **CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo con la normativa de Ciberdefensa.**

3.4 Resultados de aprendizaje.

Conoce el concepto de Ciberdefensa, su organización y fundamentos de la seguridad en la información.

3.5 Criterios de evaluación.

1. Se conocen los principales conceptos que definen que es la ciberdefensa. Conoce las principales recomendaciones defensivas de seguridad.
2. Se conocen los fundamentos de seguridad de la información.
3. Se conocen los principales procedimientos para una inspección de seguridad TIC.
4. Se conocen los pasos para la acreditación de seguridad de un sistema informático.

Resultados de Aprendizaje	**CE**	**Criterios de Evaluación**
Conoce el concepto de ciberdefensa, su organización y fundamentos de la seguridad en la información.	1	Se conocen los principales conceptos que definen que es la ciberdefensa. Conoce las principales recomendaciones defensivas de seguridad.
	2	Se conocen los fundamentos de seguridad de la información.
	3	Se conocen los principales procedimientos para una inspección de seguridad TIC.
	4	Se conocen los pasos para la acreditación de seguridad de un sistema informático.

3.6 Contenidos.

Los contenidos señalados en el currículo para este módulo son los siguientes:

- U.D.1: Introducción a la ciberdefensa.
- U.D.2: Organización y Gestión de Seguridad.
- U.D.3: Acreditación de sistemas.
- U.D.4: Procedimiento de Inspección STIC.
- U.D.5: Fundamentos de Seguridad de la información: Control de accesos y mecanismos de autenticación.
- U.D.6: Gestión de incidentes de seguridad.

4. DISTRIBUCIÓN TEMPORAL DE LOS ELEMENTOS CURRICULARES.

4.1 Distribución temporal.

El módulo se distribuye en 15 horas, de la siguiente manera:

(1 hora)	**Día 1**	Presentación.	Introducción a la asignatura y distribución de los trabajos a los equipos.
U.D.1 (4 horas)	**Día 2**	**Tema 1** Análisis de la situación actual.	Los ataques más dañinos. Fake videos y audios. Donde informarnos.
	Día 3	**Tema 2** Vulnerabilidades, amenazas y ataques.	Tipos de malware (código dañino). Salvaguardas.
	Día 4	**Tema 3** Organismos oficiales de seguridad.	INCIBE, CCN, CNPIC, MCCD, EC3, NSA
	Día 5	**Tema 4** Legislación relativa y estrategia nacional en ciberdefensa	Los mapas de las Ciberleyes. Normativa Ciberdefensa. Normativa Ciberseguridad. La estrategia nacional de ciberseguridad.
U.D.2 (1 hora)	**Día 6**	**Tema 5** Recomendaciones de Seguridad Informática	Plantillas de seguridad del CCN-CERT. Equipo frontera y equipo aduana. IP 40-11. Sanitización de soportes de almacenamiento. Copias de seguridad y respaldo.

U.D.3 (2 horas)	**Día 7**	**Tema 6** Emanaciones electromagnéticas	Ciberataques a partir de las emanaciones electromagnéticas. Arquitectura Red/Black. Evaluación Zoning. Certificación TEMPEST.
	Día 8	**Tema 7** Acreditación de Sistemas. Autoridades CIS	Condiciones para la acreditación. Interconexión de sistemas acreditados. Situaciones posibles de la acreditación. Autoridades CIS. Gestión de riesgos (CCN-SITC 410 y herramienta PILAR)
U.D.4 (2 horas)	**Día 9**	**Tema 8** Inspecciones de seguridad TIC.	Procedimiento de seguridad de las TIC CCN-STIC-120. Competencia técnica.
	Día 10	**Tema 9** Contramedidas vigilancia electrónica. TSCM	Detección de micrófonos. Barrido radioeléctrico.
U.D. 5 (1 hora)	**Día 11**	**Tema 10** Control de accesos y mecanismos de autenticación.	Controles físicos. Seguridad del S.O. Seguridad de la red
U.D.6 (1 hora)	**Día 12**	**Tema 11** Acciones a tomar ante una infección por Ransomware.	Gestión de incidentes de seguridad informáticos (CCN-STIC 403).
(1 hora)	**Día 13**	Exposiciones	Equipo 1
(1 hora)	**Día 14**	Exposiciones	Equipo 2
(1 hora)	**Día 15**	Exposiciones	Equipo 3

4.2 Ficha resumen de cada Unidad Didáctica

Título de la UD	U.D.1: Introducción a la ciberdefensa
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de describir los principales conceptos que definen qué es la ciberdefensa, así como los fundamentos de seguridad en la información.
Contenidos	Tema 1. Análisis de la situación actual. Los ataques más dañinos. Fake videos y audios. Donde informarnos. Tema 2. Vulnerabilidades, amenazas y ataques. Tipos de malware (código dañino). Salvaguardas. Tema 3. Organismos oficiales de seguridad. INCIBE, CCN, CNPIC, MCCD, EC3, NSA Tema 4. Legislación relativa y estrategia nacional en ciberdefensa. Los mapas de las Ciberleyes. Normativa Ciberdefensa. Normativa Ciberseguridad. La estrategia nacional de ciberseguridad.
Criterios de evaluación	Se conocen los principales conceptos que definen que es la ciberdefensa y las principales recomendaciones de seguridad.
Actividades Formativas (las obligatorias del PLAEST)	Clases teóricas.

Título de la UD	U.D.2: Organización y gestión de la seguridad
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de los mismos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de describir los fundamentos de Seguridad en la Información.
Contenidos	Tema 5. Recomendaciones de Seguridad Informática. Plantillas de seguridad del CCN-CERT. Equipo frontera y equipo aduana. IP 40-11. Sanitización de soportes de almacenamiento. Copias de seguridad y respaldo.
Criterios de evaluación	Se conocen los fundamentos de seguridad de la información.
Actividades Formativas (las obligatorias que aparecen en el PLAEST)	Clases teóricas.

Título de la UD	U.D.3: Acreditación de sistemas.
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de los mismos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de seguir los pasos para la acreditación de seguridad de un sistema informático.
Contenidos	Tema 6. Emanaciones electromagnéticas. Ciberataques a partir de las emanaciones electromagnéticas. Arquitectura Red/Black. Evaluación Zoning. Certificación TEMPEST. Tema 7. Acreditación de Sistemas. Autoridades CIS. Condiciones para la acreditación. Interconexión de sistemas acreditados. Situaciones posibles de la acreditación. Autoridades CIS. Gestión de riesgos (CCN-SITC 410 y herramienta PILAR)
Criterios de evaluación	Se conocen los pasos para la acreditación de seguridad de un sistema informático.
Actividades Formativas (las obligatorias que aparecen en el PLAEST)	Clases teóricas.

Título de la UD	U.D.4: Procedimiento de Inspección STIC.
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de aplicar los principales procedimientos para una inspección de seguridad TIC.
Contenidos	Tema 8. Inspecciones de seguridad TIC. Procedimiento de seguridad de las TIC (CCN-STIC-120). Competencia técnica. Tema 9. Contramedidas vigilancia electrónica. TSCM. Detección de micrófonos. Barrido radioeléctrico.
Criterios de evaluación	Se conocen los principales procedimientos para una inspección de seguridad TIC.
Actividades Formativas (las obligatorias que aparecen en el PLAEST)	Clases teóricas.

Título de la UD	U.D.5: Fundamentos de Seguridad en la Información: control de accesos y mecanismos de autenticación.
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de aplicar los fundamentos de Seguridad en la Información.
Contenidos	Tema 10. Control de accesos y mecanismos de autenticación. Controles físicos. Seguridad del S.O. Seguridad de la red
Criterios de evaluación	Se conocen los fundamentos de seguridad de la información.
Actividades Formativas (las obligatorias que aparecen en el PLAEST)	Clases teóricas.

Título de la UD	U.D.6: Gestión de incidentes de seguridad.
Competencias a las que contribuye	CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo. CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular. CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional. CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo a la normativa de Ciberdefensa.
Objetivos didácticos (obtenidos de los criterios de evaluación)	Al finalizar esta Unidad Didáctica, el alumno debe ser capaz de aplicar los fundamentos de Seguridad en la Información.
Contenidos	Tema 11. Acciones a tomar ante una infección por Ransomware. Gestión de incidentes de seguridad informáticos (CCN-STIC 403).
Criterios de evaluación	Se conocen los fundamentos de seguridad de la información.
Actividades Formativas (las obligatorias que aparecen en el PLAEST)	Clases teóricas.

5. METODOLOGÍA DIDÁCTICA.

5.1 Metodologías de enseñanza-aprendizaje.

El conocimiento previo de la experiencia y los estudios previos del estudiante, así como de cuál es la motivación que lleva al alumno al estudio del módulo, son imprescindibles para promover una metodología activa y participativa enfocada en el sentido de perseguir el fin último y primordial de que al finalizar cada parte de las que componen el módulo, se cumplan los siguientes objetivos:

- El alumno deberá saber algo que antes no sabía.
- Deberá ser capaz de entender algo que antes no entendía.
- Deberá ser capaz de plantear dudas sobre el mundo real que nos hagan reflexionar sobre las aplicaciones de lo estudiado.

Del mismo modo, es muy importante conocer las necesidades reales de los alumnos, puesto que a partir de estas se pueden organizar los contenidos y actividades.

La metodología utilizada en la impartición de este módulo reúne los siguientes aspectos:

- Trabajo en equipo:
    - Las presentaciones realizadas en los últimos días, realizadas en grupo, tienen como una de sus finalidades el desarrollo de estrategias sociales.
    - La combinación de múltiples perfiles hace que la presentación final cuente con múltiples perspectivas y puntos de vista, siendo el contenido así de mayor calidad, con mejores resultados y co propuestas más exactas, creativas y fiables.
    - Además, fomenta la interacción, la cooperación y la coordinación, fortaleciendo las interacciones sociales.
- Auto-evaluación:
    - El profesor debe de hacer el esfuerzo de aprenderse el nombre de todos los alumnos y mantener en clase una actitud constantemente inquisitiva hacia ellos, de forma que los alumnos menos predispuestos mantengan una actitud de alerta permanente y sean

conscientes, a través de las respuestas que ellos mismos den al profesor, de su verdadero nivel de conocimiento de la materia tratada.

  - La auto-evaluación es la estrategia por excelencia para educar en la responsabilidad y para aprender a valorar, criticar y reflexionar sobre el proceso de enseñanza y aprendizaje realizado por el estudiante.

- Diversidad de actividades y tareas significativas:
  - Con estas metodologías se persigue el ideal de que el alumno mantenga su atención hacia el profesor y que el uso de distintas herramientas permita que las diferentes capacidades de los alumnos sean mostradas a través de distintos ámbitos de actuación durante el proceso de aprendizaje.
  - La intención es salir de la rutina en la que tradicionalmente se han desarrollado las clases en el aula y probar mecanismos innovadores que permitan crear situaciones de aprendizaje que no necesariamente sigan la secuencia: explicación de la teoría, comprensión de la misma y posterior aplicación de lo asimilado.
- Trabajo con casos reales:
  - No todas las materias lo permiten, pero este módulo facilita enormemente al estudio de casos reales, recientes y profusamente tratados, tanto en profundidad con un elevado nivel técnico como de una forma más ligera a nivel periodístico o informativo, de forma que se puede profundizar más o menos dependiendo del interés del caso para el aprendizaje.
  - Los alumnos, en general, si se sienten identificados por la temática y el problema que tienen que solucionar, no dudan en reconocer que es una actividad muy útil, especialmente para ejercitar la producción oral al participar en reuniones de trabajo. Durante el transcurso de las exposiciones, aunque sus intervenciones estén preparadas, el factor de imprevisibilidad les obliga a reaccionar e improvisar ante las propuestas y argumentos de sus compañeros o del profesorado. La interacción natural que llega a producirse en el análisis de casos prácticos les aproxima a la realidad de su entorno laboral y

comprueban que se les prepara realmente para ser capaces de desenvolverse adecuadamente en su ámbito de trabajo

- Así, se propone el estudio de casos, los cuales son situaciones reales en la que o bien se plantea un problema o bien se describe una situación, ambos dentro del dominio profesional. Los estudiantes, estudian el caso, lo analizan, e intentan encontrar soluciones adecuadas.

Se ha pretendido que la metodología usada tenga como elemento central al alumno y de este modo sea una metodología activa, participativa y en la que el alumno se sienta en todo momento responsable de su aprendizaje, además de potenciar las actividades relacionadas con el trabajo en equipo y la interacción.

5.2 Actividades generales de las Unidades Didácticas.

Actividades formativas	N.º de horas	Metodología enseñanza-aprendizaje	Relación con las competencias a adquirir
U.D.1: Introducción a la ciberdefensa.	4	Clase Presencial	CG.10 CG.12 CG.15 CE.6
U.D.2: Organización y gestión de la seguridad.	1	Clase Presencial	CG.10 CG.12 CG.15 CE.6
U.D.3: Acreditación de sistemas.	2	Clase Presencial	CG.10 CG.12 CG.15 CE.6
U.D.4:Procedimiento de Inspección STIC.	2	Clase Presencial	CG.10 CG.12 CG.15 CE.6
U.D.5: Fundamentos de Seguridad de la información.	1	Clase Presencial	CG.10 CG.12 CG.15 CE.6
U.D.6: Gestión de incidentes de seguridad.	1	Clase Presencial	CG.10 CG.12 CG.15 CE.6
Presentaciones de los alumnos	3	Expositiva	CG.3 CG.22

*Total: **11** horas dedicadas a la impartición de las unidades didácticas, **1** hora a la presentación, introducción a cada uno de los posibles trabajos a elegir y distribución de grupos y **3** horas dedicadas a la exposición por parte de los alumnos de los temas elegidos.

6. MATERIALES Y RECURSOS DIDÁCTICOS.

6.1 Espacios formativos, equipamiento y materiales.

Los recursos materiales tales como aulas y su equipamiento se adecúan al número de estudiantes y a las actividades formativas programadas.

La plataforma “Campus Virtual de Defensa” se utiliza para poner a disposición de los alumnos toda la información general del módulo, tanto lo referente a normativa (Currículo, Guías Docentes, etc.) como lo que afecta al desarrollo formal de la asignatura (grupos de trabajo, materias a investigar, calendario de exposiciones, rúbrica con la que se les evaluará e instrucciones para darse de alta en la aplicación ***“Corubrics”***).

No se dispone en la EMACOT de conexión Wifi en todos los espacios dedicados a la docencia, pero sí que todas las aulas están dotadas de cañón de proyección, como complemento al ordenador del profesor y de pizarra digital.

Los recursos didácticos, en cuanto a su concepción, definición e implementación han evolucionado mucho y así, en la EMACOT, como escuela donde se imparte este módulo, se cuenta con varias aulas dotadas de un ordenador por pupitre, no obstante, para la impartición de este módulo no se considera imprescindible.

6.2 Recursos de apoyo a la docencia.

Lo que actualmente consideramos sociedad del conocimiento, la cual viene definida por una evolución producto de la tecnología, ha abarcado distintas áreas, permitiendo también innovar en la educación, estimulando la creación de nuevos espacios y transformando el proceso de enseñanza-aprendizaje.

Los estudiantes actuales, utilizan las herramientas tecnológicas para facilitar el aprendizaje. La evolución ha sido tal que los recursos tecnológicos se han convertido en recursos educativos, donde la búsqueda por mejorar el aprendizaje trae consigo la tarea de involucrar la tecnología con la educación.

Este complemento, acompañado de herramientas tecnológicas ha de generar en la sociedad una realidad y presencia cada vez mayor, de tal forma que su extensión a las aulas, pues todos los alumnos llevan a clase como mínimo un teléfono móvil,

cuando no una tableta o un ordenador, generalizará la optimización de un mejor proceso de enseñanza-aprendizaje.

Para la captación de la atención del alumnado, utilizaremos tres recursos de apoyo a la docencia basados en las tecnologías.

1. Por un lado, durante el transcurso de la clase se intentará una o dos veces, que los alumnos encuentren la respuesta a una pregunta que requiera de cierta "**indagación en la web"**. Para ello se les permitirá usar los móviles o cualquier otro dispositivo que permita realizar búsquedas en la web, en cuantos de tiempo, no de manera permanente durante la clase.
2. Una segunda opción que usaremos como recurso de apoyo a la docencia es el uso de una aplicación que permite que un taller sea divertido, colaborativo e interactivo. Se trata de la aplicación ***"Mentimeter"*,** la cual permite aumentar la interacción y dar a todos los alumnos la oportunidad de expresar su opinión. Además, promueve el espíritu de competencia y hace que la clase sea más divertida.

   Dentro de las diversas herramientas que propone la aplicación señalada, el ***Muro Colaborativo*** me parece la más original y útil para estimular al público y atraer la atención de los alumnos en clase. Esta herramienta consiste en preparar una nube de palabras con alguna pregunta inicial. Cada una de las respuestas de los participantes (lo ideal es limitar a 3 palabras para cada uno), se van poniendo en pantalla y las palabras se van haciendo más grandes dependiendo del número de veces que se repitan. De ese modo, se percibe al instante y de una forma muy visual, las tendencias de respuesta de un grupo, puesto que la palabra que más se repita por los participantes, más grande se hará.

3. Por último, el último recurso tecnológico en el que nos apoyaremos será la aplicación "***Corubrics"***, y sus posibilidades de autoevaluación, heteroevaluación, coevaluación o evaluación entre iguales. Es una herramienta totalmente gratuita y bastante sencilla.

   Se elige una rúbrica de las muchas disponibles y se modifican las filas y las columnas a nuestro gusto. Después se accede desde cualquier navegador y se añaden los resultados. La gestión de los datos a posteriori ofrece todas las

posibilidades de una hoja de cálculo, de hecho usa plantillas de *Google Docs*, pues nos permite filtrar por los diversos campos de la tabla e incluso por los diferentes compañeros que han puntuado, si usamos la evaluación entre iguales.

Esta herramienta la usaremos para la evaluación de las exposiciones.

7. EVALUACIÓN.

7.1 Procedimientos e instrumentos de evaluación del aprendizaje del alumno.

Los instrumentos de evaluación que ayuden a llevar a cabo la valoración del alumnado serán variados, objetivos y transparentes.

Desde el punto de vista del profesor, es más difícil ser objetivo en una evaluación continua que en una evaluación con carácter calificador, pero esa desventaja tiene también la contraprestación de permitir una motivación constante del alumnado a lo largo del desarrollo del módulo y de proporcionar al profesor una visión más amplia del seguimiento que está realizando el alumnado de la materia que se transmite en clase.

Además, debemos ser exhaustivos pues, en una evaluación continua, también es más difícil demostrar al alumno las causas que han llevado a la obtención de una nota final. En este tipo de evaluación, los parámetros de valoración, cuando están escritos y detallados, que no es lo habitual, son en cierto modo subjetivos y fruto de la interpretación que se haga de ellos.

Incluso, en una evaluación con carácter calificador, también planea la sombra de la subjetividad cuando, por ejemplo, la prueba es de desarrollo o de preguntas cortas porque, sabiendo quién es el alumno que ha hecho el examen y su comportamiento en clase, su participación, sus aportaciones y su interés por la asignatura, el examinador se puede ver inducido a soslayar ciertos errores que pueden aparecer en la prueba porque; “en clase lo tenía claro” o “no ha escrito exactamente lo que pedía pero la idea que transmite se acerca a la definición correcta”.

Es fácil clasificar los resultados de una evaluación continua entre bueno, regular o malo, pero requiere un gran esfuerzo ser capaz de discernir entre lo bueno, lo muy bueno, lo sobresaliente, lo excelente o lo sublime.

Así, tal y como señala la **Orden Ministerial ECD/65/2015** “*El profesorado debe utilizar procedimientos de evaluación variados para facilitar la evaluación del alumnado como parte integral del proceso de enseñanza y aprendizaje, y como una herramienta esencial para mejorar la calidad de la educación”.*

Nada como el uso de varias herramientas de control para intentar que las conclusiones a las que se llegue en una evaluación sean concluyentes y aporten cierto grado de conocimiento sobre los factores que acompañen a una nota y que habrán sido determinantes en la construcción de un resultado final.

En este sentido, tanto las aportaciones en clase como la evaluación mediante rúbrica en hasta 6 apartados o rasgos distintos, nos ayuda en ese ideal de utilización de procedimientos de evaluación variados.

Esa misma Orden Ministerial señala, en su Artículo 7 que: *"Los niveles de desempeño de las competencias se podrán medir a través de indicadores de logro, tales como rúbricas o escalas de evaluación. Estos indicadores de logro deben incluir rangos dirigidos a la evaluación de desempeños".*

Así, la rúbrica nos ofrece una evaluación detallada de qué indicador o criterio ha superado cada alumno y en qué grado de desarrollo o perfección. Además, informado el alumno con anterioridad, le permite saber lo que se espera de él y no tiene que prepararse para lo que venga, evitando que dedique esfuerzos innecesarios en direcciones que no aporten valor a su nota y que, en consecuencia, impliquen cierto nivel de frustración y de injusticia por no ver la relación entre el esfuerzo realizado y los resultados obtenidos.

Además, la rúbrica puede ser uno de los instrumentos de evaluación más adecuados para una evaluación continua, en tanto que el alumno es consciente de lo que se le exige y se le puntúa, con bastante precisión. Es la mejor manera de que el alumno establezca un trabajo por objetivos, en el que cubra diferentes etapas y sea consciente de hasta donde ha llegado o donde se ha quedado, que tareas ha superado y cuales ha dejado sin completar.

Por último, dicha Orden Ministerial del Ministerio de Educación, Cultura y Deporte señala que: *"Asimismo, es necesario incorporar estrategias que permitan la participación del alumnado en la evaluación de sus logros, como la autoevaluación, la evaluación entre iguales o la coevaluación. Estos modelos de evaluación favorecen el aprendizaje desde la reflexión y valoración del alumnado sobre sus propias dificultades y fortalezas, sobre la participación de los compañeros en las actividades*

de tipo colaborativo y desde la colaboración con el profesorado en la regulación del proceso de enseñanza-aprendizaje".

En coherencia con estas aportaciones, entendemos que podríamos considerar las siguientes modalidades de evaluación:

- Evaluación por el personal docente o heteroevaluación: proceso mediante el cual docentes, tutores y otras figuras similares, de forma individual o en grupo, valoran las actuaciones y/o producciones del estudiante.
- Autoevaluación: proceso mediante el cual los estudiantes realizan un análisis y valoración de sus actuaciones y/o sus producciones.
- Evaluación entre iguales: Proceso mediante el cual los estudiantes realizan un análisis y valoración sobre las actuaciones y/o producciones desarrolladas por algún estudiante o grupo de estudiantes de su mismo estatus o nivel.
- **Coevaluación: proceso mediante el cual docentes y estudiantes realizan un análisis y valoración de forma colaborativa, conjunta y consensuada sobre las actuaciones y/o producciones de los estudiantes.**

Sobre la base de todas estas definiciones, podemos concluir que la diferencia fundamental entre la evaluación entre iguales y la coevaluación, reside en quiénes evalúan (estudiantes o estudiantes y profesores) y, más específicamente, si lo hacen con el mismo grado de responsabilidad y de participación en el proceso de evaluación.

En el caso de este módulo la evaluación se hará mediante el método de coevaluación, dando más peso a la valoración que haga el docente que a la que haga el alumnado, pero teniendo en cuenta ambas.

Ilustración 2. Modalidades de evaluación participación de los estudiantes.

Después de haber probado con éxito la herramienta ***"Corubrics"***, será ésta la que utilicemos por su originalidad y polivalencia, al permitir realizarlo todo desde el móvil y ser capaz de gestionar las diferentes modalidades de evaluación que consideremos utilizar, ya sea la autoevaluación, la heteroevaluación, la coevaluación o la evaluación entre iguales.

Además de todo lo anteriormente mencionado, respecto a la **evaluación mediante rúbrica** y **mediante estrategias que impliquen la participación del alumnado**, también llevaremos a cabo la **evaluación continua** durante las clases teóricas impartidas por el profesor, mediante la realización de preguntas de repaso orales y retos a los que se propondrán a los alumnos, siguiendo así lo indicado en la **Orden DEF/1434/2016, sobre evaluación y calificación en los centros docentes militares**:

"1. La evaluación, en el ámbito de la enseñanza militar de formación, para aquellas asignaturas no comprendidas en el título de grado, presenta los siguientes rasgos definitorios:

a) Tiene carácter continuo.

b) Contribuye al proceso de enseñanza y aprendizaje."

En conclusión, la calificación final del alumno vendrá dada en un **90% por la coevaluación**, que será llevada a cabo por compañeros y profesorado, los cuales evaluarán las exposiciones de los alumnos durante los tres últimos días y en un **10% mediante la evaluación de la participación del alumnado**, fruto de la respuesta que vayan dando los alumnos a las preguntas y problemas planteados por el profesor durante sus clases teóricas.

7.2 Criterios de calificación.

Las amenazas a las que nos enfrentamos en el mundo de la ciberseguridad son, a menudo, imprevisibles o inevitables, de modo que las únicas protecciones posibles son la **experiencia y el estudio de casos de interés**. Así, la forma de evaluar será mediante la participación en clase (10% de la nota final) y mediante la exposición de trabajos (90% de la nota final) que analicen casos reales, los cuales girarán en torno a la seguridad en las comunicaciones o en la informática.

Seguiremos la siguiente metodología de evaluación con los siguientes criterios específicos:

Evaluación de la participación del alumnado (10% de la nota final):

Se valorará mediante la comprobación fehaciente del grado de participación en clase del alumno, **durante las 11 clases teóricas impartidas por el profesor**. Al principio, durante y a la finalización de cada clase, se recogerán evidencias del aprendizaje de los estudiantes, lo cual permitirá sistematizar el nivel de logro. Se valorará mediante la estimulación al alumno con preguntas ora individuales ora grupales, con el objetivo de alcanzar una enseñanza participativa. Para esta evaluación se usarán las metodologías señaladas en el apartado 6.2 “Recursos de apoyo a la docencia”, como son la aplicación ***“Mentimeter”*****,** la cual permite aumentar la interacción y dar a todos los alumnos la oportunidad de expresar su opinión. Además, promueve el espíritu de competencia y hace que la clase sea más divertida y la indagación en la web que permite que un taller sea divertido, colaborativo e interactivo.

Coevaluación (90% de la nota final):

El trabajo de investigación, extracción de información y exposición, llevado a cabo en las últimas tres clases de exposición por parte de los alumnos, permitirá al alumno alcanzar las Competencias Generales 3 y 22; "*Potenciar adecuadamente la capacidad de aprendizaje, análisis y síntesis para construir conocimiento*" e "*Interpretar adecuadamente documentos profesionales operativos, para ordenar con claridad y precisión y ejecutar las órdenes que reciba con prontitud y habilidad*".

Las reglas de la exposición de los alumnos sobre temas de actualidad se detallan a continuación:

- Son 9 alumnos, luego se crearán 3 grupos de trabajo, cada uno compuesto por 3 personas.
- Durante las 3 últimas clases del módulo, se llevarán a efecto las exposiciones de los alumnos. Cada día expondrá uno de los grupos. Cuarenta y cinco minutos serán para exposición y cinco para preguntas del profesor. Estas exposiciones tendrán lugar durante las 3 últimas clases presenciales del módulo.
- El grupo realizará una única presentación, en formato "*ppt"*, que introducirá en el ordenador y que le servirá de apoyo para la exposición que hará cada uno de sus miembros.
- Cada uno de los miembros del grupo expondrá sobre una de las cuestiones en que he dividido cada caso y que se detallan a continuación.
- La extensión de la parte de cada uno en la presentación será cercana a las 10 transparencias y el tiempo de exposición será de aproximadamente 15 minutos por persona.
- Después, el grupo subirá la presentación al campus virtual.

El caso a desarrollar por cada grupo estará entre los señalados en el Anexo 2.

Con el objetivo de mejorar esa capacidad de análisis, para la evaluación de esta asignatura, un tercio de la nota será fruto de la *evaluación entre iguales* de sus compañeros de clase y dos tercios será la nota de heteroevaluación del profesor.

La evaluación se hará mediante la rúbrica que podemos ver en el Anexo I, en la cual se sumarán los puntos obtenidos en cada rasgo y se dividirá la suma entre el número de criterios contemplados. Los alumnos que no formen parte del equipo que está exponiendo, entrarán en su correo electrónico y abrirán el correo de ***CoRubrics*** que habrán recibido, rellenarán el campo con su nombre y, durante la presentación de sus compañeros, evaluará cada uno de los rasgos para los tres oradores.

Tras el análisis y ponderación de los datos obtenidos, el alumno recibirá la nota final en su dirección de correo electrónico.

7.3 Procedimientos e instrumentos de evaluación del profesorado.

Los objetivos de la evaluación de la práctica docente son:

a) Adecuar los apoyos del proceso enseñanza-aprendizaje a las singularidades de cada sección de clase y a las características de su alumnado. Ajustar, en caso necesario, la práctica docente a la respuesta del alumnado.
b) Comprobar los problemas y dificultades que van apareciendo asociados a la práctica docente, con el fin de corregirlos y mejorar el proceso.
c) Efectuar el seguimiento de las sesiones impartidas y revisar y modificar, si es necesario, la planificación hecha previamente sobre la unidad didáctica (temporalización, recursos, actividades…).
d) Analizar la motivación del alumnado desde el comienzo hasta la finalización de la unidad didáctica, adecuando las técnicas si es necesario.
e) Fomentar un buen clima de trabajo en las sesiones, aceptando propuestas de los alumnos, si es necesario, y solucionando las situaciones conflictivas.
f) Compartir la experiencia docente con otros compañeros, con el fin de mejorar conjuntamente nuestras destrezas y habilidades.

La metodología para la evaluación del profesorado consiste, acorde a lo señalado en las Normas del Director de Curso de la EMACOT, en la realización de 3 cuestionarios de satisfacción al finalizar el curso:

1. Cuestionario del Gabinete de Orientación Educativa sobre la calidad del profesorado.
2. Cuestionario del Director de Curso sobre las asignaturas, conferencias y prácticas, en cuanto a su duración, interés, calidad, contenido, etc.

3. Cuestionario del Área de Evaluación y Control para la Autoevaluación, con preguntas sobre el Plan de Estudios, la calidad de las aulas, de los alojamientos, de los servicios de la EMACOT, etc.

7.4 Revisión de calificaciones.

Según se indica en lo relativo a la **revisión de exámenes en la Orden DEF/368/2017**, de 4 de abril, por la que se aprueba el Régimen del Alumnado de la enseñanza de formación y se modifica la Orden DEF/1626/2015, de 29 de julio, por la que se aprueban las directrices generales para la elaboración de los currículos de la enseñanza de formación para el acceso a las diferentes escalas de suboficiales de los cuerpos de las Fuerzas Armadas:

"Todo alumno podrá solicitar revisión de exámenes, atendiendo a las normas de evaluación, progreso o promoción y permanencia o repetición que sean de aplicación y desarrollada por las normas de régimen interior del centro".

Acorde con esto, la EMACOT ha trasladado a sus Normas de Régimen Interior para Alumnos de Formación, lo indicado en la Orden DEF/1434/2016, de 31 de agosto, por la que se establecen las normas de evaluación, de progreso y de permanencia en los centros docentes militares de formación para la incorporación a las escalas de oficiales, quedando el procedimiento establecido de la siguiente manera:

1. Todo alumno podrá solicitar la revisión de examen, debiendo rellenar el Anexo H, Formato de solicitud de revisión de examen, de las Normas de Régimen Interior. Esta solicitud se dirigirá, en primera instancia, al profesor de la asignatura, que actuará de acuerdo con las normas establecidas por el departamento.

2. El profesor atenderá, durante los tres días hábiles siguientes a la notificación de las notas de cada materia o asignatura, y en el horario que se determine por el departamento, las solicitudes que haya por parte de los alumnos para la revisión de exámenes.

3. Cuando el examen sea el correspondiente a la última convocatoria, el alumno podrá solicitar la revisión por un tribunal constituido a tal efecto.

4. Si una vez realizada la revisión a que se refieren los dos párrafos anteriores, siguiera sin estar de acuerdo con la decisión adoptada, el alumno podrá formular recurso ante el director del centro correspondiente, en los plazos y condiciones que a tal efecto se establezcan.

8. PROCEDIMIENTOS Y ACTIVIDADES DE RECUPERACIÓN Y REFUERZO.

8.1 Actividades de Recuperación.

En caso de no superar la asignatura mediante evaluación continua, los alumnos tendrán opción de conseguirlo mediante la realización de un examen antes de la finalización del curso académico. Éste abarcará todo el contenido de los distintos temas que componen el módulo.

La prueba que se realice se considerará superada cuando el alumno obtenga una puntuación igual o superior a 5 sobre 10; siendo la nota obtenida la calificación definitiva de la asignatura. Si el resultado del examen fuera una nota inferior a 5, se considerará no superada la asignatura.

En la prueba que se diseñe para la recuperación de la asignatura, se emplearán como mínimos exigibles los mismos que se han definido para la evaluación continua del módulo.

8.2 Opciones de mejora.

Aquí también se aplicará lo indicado en la **Orden DEF/1434/2016 sobre Opciones de mejora**:

> 1. A la vista de la calificación obtenida por evaluación continua, en cualquier materia o asignatura excepto en instrucción y adiestramiento, todo alumno que la haya superado podrá solicitar ser sometido a una prueba, para la mejora de la calificación, sobre la totalidad de dicha materia o asignatura.
>
> 2. La prueba a realizar será la misma que la que hayan de superar los que, en la evaluación continua, no hayan obtenido al menos la calificación de cinco.
>
> 3. La calificación definitiva será la mejor de las obtenidas por evaluación continua o mediante la citada prueba de mejora.
>
> 4. Esta mejora no será aplicable en aquellas asignaturas que hayan obtenido reconocimiento de créditos.

9. PROPUESTA DE ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES.

Se adoptarán medidas, que se materializarán en clases de apoyo y tutorías, con el fin de permitir simultanear los estudios de la asignatura con las actividades de formación militar y aeronáutica.

Las clases de apoyo o refuerzo serán solicitadas por el alumno al Director de Curso y autorizadas por el Teniente Coronel Jefe de Estudios.

Las tutorías consistirán en una toma de contacto, mínimo una por trimestre, en la que el tutor del alumno realizará una entrevista individual con el estudiante, donde recogerá información de interés sobre él y abordará aquellas cuestiones que puedan resultar de interés para su actividad durante esta fase del curso; pudiendo concertar otro tipo de actividades y entrevistas a lo largo de éste.

El tutor, también desarrollará actividades de tutoría colectiva con todo el grupo en el que esté encuadrado el alumno con el fin de determinar su actitud y relaciones en el entorno social en el que se desenvuelve. Además, el profesor de la materia realizará una valoración de la evolución del alumno en función de su desempeño en clase, pudiendo recomendar al tutor la realización de entrevistas individuales para abordar cuestiones relativas a su rendimiento y problemática concreta.

El horario de tutorías y los datos de contacto de los profesores que imparten las distintas materias que componen la asignatura son los que figuran en la Guía Docente. En caso de que el alumno esté interesado en recibir una atención particularizada, deberá solicitar una cita con el profesor correspondiente, según los datos reflejados en la Guía.

Las actividades extraescolares que los centros docentes militares que imparten enseñanza de formación pueden establecer, orientadas a ampliar la oferta académica y cultural de los currículos, así como a enriquecer el bagaje de conocimientos y experiencias culturales de los alumnos que, estando o no relacionadas con las materias del currículo, no son objeto de evaluación y favorecen la formación integral del alumno, son propuestas y coordinadas por el Escuadrón de Alumnos.

Dichas actividades se denominan complementarias, cuando contribuyen de manera efectiva a la finalidad de los currículos y adicionales, cuando permiten extender la actividad a campos completamente distintos de los habituales y profundizan en ellos.

Las actividades optativas tendrán carácter voluntario y se realizarán en periodos de tiempo distintos a los programados para las actividades docentes.

El director de la EMACOT podrá limitar la participación de los alumnos de la enseñanza de formación en actividades adicionales en función de su progresión en los estudios, comportamiento, rendimiento académico y otras circunstancias personales, incluida la corrección a infracciones de carácter académico.

10. BIBLIOGRAFÍA.

- Centro Criptológico Nacional (2021). *"Guía de Seguridad de las TIC N.º CCN-STIC-201, Organización y gestión para la seguridad de las TIC".*
- Centro Criptológico Nacional (2009). *"Guía de Seguridad de las TIC N.º CCN-STIC-204, Estructura y contenido del documento abreviado CO/DRES/POS para estaciones de trabajo aisladas y pequeñas redes".*
- Oficina Nacional de Seguridad (2018). *"Normas de la Autoridad Nacional para la Protección de la Información Clasificada".*
- Gobierno de España (2010). *"Esquema Nacional de Seguridad".*
- JEMAD (2011). *"Visión del JEMAD de la Ciberdefensa Militar".*
- JEMAD (2018). *"Concepto de ciberdefensa. Resumen ejecutivo".*
- Presidencia Gobierno España (2020). *"Directiva Defensa Nacional".*
- Presidencia Gobierno España (2017). *"Estrategia de Seguridad Nacional".*
- Cortes Generales España (2015). *"Ley 36/2015 de Sistema de Seguridad Nacional".*
- Ministerio de Defensa (2013). *"Orden DEF 10/2013 de creación del Mando Conjunto de Ciberdefensa de las FAS".*
- Consejo Europeo (2008). *"Directiva 2008/114/CE de Identificación y designación de infraestructuras críticas europeas".*
- Cortes Generales España (2011). *"Ley 8/2011 de medidas para la protección de las infraestructuras críticas ".*
- Gobierno de España (2011). *"R.D. 704/2011. Reglamento de protección de infraestructuras críticas".*
- Consejo Europeo (2013). *"Directiva 2013/40/CE de ataques a los sistemas informáticos".*
- Cortes Generales España (2010). *"Instrumento de Ratificación del Convenio de Budapest sobre Ciberdelincuencia".*
- Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (2009). *"Manual de Tallin".*

- Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (2013). *"Peacetime Regime for State Activities in Cyberspace".*
- Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (2017). *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched".*
- Departamento de Defensa EEUU (2018). *"Cyber Operations Joint Publication 3-12".*
- Stone, O. (2016). *"Snowden"* (Película).
- Ronald M. Hernández (2017). *"Impacto de las TIC en la educación: Retos y Perspectivas".*
- Rodríguez Gómez G., Ibarra Saiz Mª. y García Jiménez (2013). *"Autoevaluación, evaluación entre iguales y coevaluación: conceptualización y práctica en las universidades españolas".*
- Orden DEF/1434/2016, de 31 de agosto, *por la que se establecen las normas de evaluación, de progreso y de permanencia en los centros docentes militares de formación para la incorporación a las escalas de oficiales.*
- Orden Ministerial ECD/65/2015, de 21 de enero, *por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato.*
- Resolución 452/38141/2020, de 2 de junio, de la Subsecretaría, *por la que se convocan los procesos de selección para el ingreso en los centros docentes militares de formación, mediante la forma de ingreso directo, con y sin exigencia de Titulación de Técnico Superior, para la incorporación como militar de carrera a las Escalas de Suboficiales de los Cuerpos Generales y del Cuerpo de Infantería de Marina.*
- Orden DEF/368/2017, de 4 de abril, *por la que se aprueba el Régimen del Alumnado de la enseñanza de formación.*
- Orden DEF/1626/2015, de 29 de julio, *por la que se aprueban las directrices generales para la elaboración de los currículos de la enseñanza de formación para el acceso a las diferentes escalas de suboficiales de los cuerpos de las Fuerzas Armadas.*

- Orden Ministerial ECD/65/2015, de 21 de enero, *por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato*.

DESARROLLO DE LA UNIDAD DIDÁCTICA 1

11. DESCRIPCIÓN DE LA UNIDAD DIDÁCTICA

11.1 Alumnos a los que se dirige.

Esta Unidad Didáctica se encuentra dentro del módulo de Ciberdefensa (ESFCYB13), desarrollado durante el tercer trimestre del primer curso, el cual es un módulo formativo de especialidad fundamental, se desarrolla durante 15 horas y **se dirige a Sargentos Alumnos de formación de primer curso** para el acceso a la Escala de Suboficiales del Cuerpo General del Ejército del Aire de la especialidad de Sistemas de Información, Comunicaciones y Ciberdefensa, mediante la forma de ingreso con exigencia de titulación previa.

La titulación exigida para acceder con estas condiciones y a esta especialidad es estar en posesión de uno de los siguientes tres Títulos de Técnico Superior (TTS):

- Sistemas de Telecomunicaciones e Informáticos.
- Administración de Sistemas Informáticos en Red.
- Desarrollo de Aplicaciones Multiplataforma.

Así, mediante esta forma de ingreso, solo se requerirá la superación del plan de estudios de la formación militar general, específica y para la adquisición de la especialidad fundamental, que se desarrollará en un curso académico.

Son 9 los Sargentos Alumnos que reciben este módulo.

11.2 Número y duración de las sesiones.

Esta Unidad Didáctica está repartida en 4 sesiones de 50 minutos cada una.

11.3 Lugar de desarrollo

Todas las sesiones teóricas y de exposición se desarrollarán en la Escuela de Técnicas de Mando, Control y Telecomunicaciones (EMACOT).

La ubicación dentro de ésta será en el Aula 1 del Edificio 23.

12. OBJETIVOS DIDÁCTICOS.

Al final de la unidad didáctica el alumno será capaz de alcanzar los siguientes objetivos:

- Identificar los aspectos generales de Ciberdefensa y Ciberseguridad y su relación con la Tecnología de la Información.
- Describir los ataques más dañinos.
- Distinguir los diferentes tipos de malware y los aspectos generales de Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Crimen y Ciber Conflictos entre estados naciones.
- Comprender los diferentes organismos oficiales de ciberseguridad y las actividades que en ellos se desarrollan.
- Integrar la legislación relativa, la normativa de ciberdefensa y la Estrategia Nacional de Ciberseguridad.
- Aplicar correctamente el desempeño necesario en posiciones de liderazgo, en diversos tipos de emprendimientos en el campo de la ciberdefensa y de la ciberseguridad.
- Manejar la metodología y rutinas a seguir en la aplicación de salvaguardas y procesos de seguridad lógica.
- Juzgar las responsabilidades en lo que concierne a los aspectos jurídicos a ser tenidos en cuenta por quienes actúen enfrentándose al Ciber Terrorismo, al Ciber Espionaje, al Activismo Hacker y al Ciber Crimen.
- Apreciar la importancia de los denominados equipos CERT (Computer Emergency Response Team) dentro del ámbito nacional y del Ministerio de Defensa en particular.

13. COMPETENCIAS

- CG.10. Aplicar de manera razonada la informática para su utilización como herramienta básica de trabajo.
- CG.12 Identificar las misiones y organización de las Fuerzas Armadas, en general, y del Ejército del Aire en particular.
- CG.15 Adquirir los fundamentos técnico-científicos necesarios para el ejercicio profesional.
- CE.6 Comprender los principios básicos de seguridad en sistemas informáticos y redes de datos, en función de las amenazas y vulnerabilidades de estos, de acuerdo a la normativa de Ciberdefensa.

14. CONTENIDOS DE APRENDIZAJE

14.1 Epígrafe de los contenidos.

- Análisis de la situación actual, los ataques más dañinos y donde informarnos. Importancia de los *fake videos* y *fake audios.*
- Vulnerabilidades, amenazas y ataques. Tipos de malware (código dañino) y las posibles salvaguardas.
- Organismos oficiales de seguridad: INCIBE, CCN, CNPIC, MCCD, EC3, NSA.
- Legislación relativa y estrategia nacional en ciberdefensa. Los mapas de las Ciberleyes.

14.2 Justificación de los contenidos.

Moverse en el ciberespacio es el desafío más agobiante de la modernidad, su gestión, conocimiento procesos y procedimientos, resultan esenciales al hombre moderno, ya que en este ambiente se desarrollan desde actividades lúdicas y recetas de cocina hasta el diseño de los más sofisticado sistemas, pasando por las estrategias nacionales, el desarrollo de sofisticadas formas criminales y de alta rentabilidad, tales como el lavado transnacional de activos, financiamiento del terrorismo, activismo hacker y ciberespionaje militar, científico e industrial.

Todo está en la nube, va por las redes o lo que es peor, sobre los sistemas de control y gestión a distancia de procesos, todo se desarrolla en lo que llamamos ciberespacio.

Conocer el ciberespacio y las actividades que en él se desarrollan es, probablemente, el desafío más importante al que se enfrenta el hombre moderno, llamado a gestionar organizaciones, empresas, sociedades o casi cualquier actividad humana. Incluso en el nivel del “Internet de las Cosas”, el conocimiento de este nuevo ambiente se torna imprescindible.

En una clara comprensión de esta problemática, el Estado Mayor de la Defensa inició en 2018, la carta de promulgación del *“Concepto de Ciberdefensa”,* con el objetivo de proporcionar el **marco conceptual** que sirviera de orientación para el proceso de implementación de las capacidades de Ciberdefensa dentro del ciclo de *Planeamiento de la Defensa*, así como para establecer los **principios fundamentales** que deben guiar el posterior **desarrollo doctrinal** para este nuevo ámbito de las operaciones militares.

Siendo este nuevo ambiente del conflicto quien envuelve a todos los otros ámbitos del desarrollo humano, la tierra, el agua, el aire y el espacio, nos vemos en la necesidad de su conocimiento tanto desde la perspectiva del más alto nivel de gerencia del estado o de la empresa privada, hasta los sectores más recónditos y desprotegidos, dado que el solo encendido de un celular de los denominados Smartphone, ya nos introduce en el ambiente ciberespacial.

14.3 Contenidos intelectivos, procedimentales y actitudinales.

- Aspectos generales de Ciberdefensa y Ciberseguridad y su relación con la Tecnología de la Información a través de un análisis de la situación actual, de la observación de los ataques más dañinos y de los repositorios web donde informarnos.
- Importancia de las fake news y estudiar el caso de Cambridge Analytica y su posible efecto en las elecciones de Estados Unidos.
- Tipos de malware y la forma de mantener nuestra organización protegida.
- Descripción del ciberespacio y de las actividades que en él se desarrollan, de forma que podamos aplicar directrices de seguridad y mantenerlas actualizadas gracias al acceso a las fuentes de conocimiento adecuadas generadas por los Organismos Oficiales de Seguridad.
- Descripción de los diferentes organismos oficiales de ciberseguridad y el ámbito de sus competencias.
- Conceptos legislativos relativos a Ciber Terrorismo, Ciber Espionaje, Activismo Hacker, Ciber Crimen y Ciber Conflictos entre estados y la estrategia nacional en ciberdefensa.
- Obtención de los repositorios web adecuados y de las fuentes de conocimiento de nuestra organización de la información sobre los principales activos a proteger y la forma de evitar el software dañino.
- Implementación la metodología descrita en las normas de nuestra organización y en los repositorios de acceso público, de forma que consigamos la correcta implantación de sistemas de defensa en profundidad, así como de rutinas procedimentales a seguir, tanto en la aplicación de salvaguardas como en la protección de procesos de seguridad lógica.
- Concienciación de la necesidad de seguir los requerimientos de seguridad tanto procedimentales como de configuración para proteger nuestra organización de ser vulnerable a un ataque de malware.

- Importancia en la respuesta ante ciberataques, de ponerse con contacto inmediatamente con los denominados equipos CERT (Computer Emergency Response Team) dentro del ámbito nacional y del Ministerio de Defensa en particular.
- Concepto emergente llamado ciberespacio, de vital importancia en el Ejército del Aire y ser conscientes de las actividades que en él se desarrollan.
- Responsabilidades en lo que concierne a los aspectos jurídicos a ser tenidos en cuenta por quienes actúen enfrentándose al Ciber Terrorismo, al Ciber Espionaje, al Activismo Hacker y al Ciber Crimen.

15. SECUENCIA DE ACTIVIDADES DE ENSEÑANZA APRENDIZAJE.

15.1 Sesión 1.

15.1.1 Actividades de inicio.

Breve explicación sobre la necesidad de estudiar los vectores de ataque exitosos y las vulnerabilidades ya explotadas, como forma de llegar a conocer el estado del arte actual en el ámbito de la ciberdefensa.

15.1.2 Actividades de desarrollo.

Continuaremos describiendo los ataques más famosos, uno por uno, empezando por el gusano Wannacry que asoló la red informática de Telefónica en España y de otras empresas en todo el mundo., el robo masivo de criptomonedas, el caso de Cambridge Analytica en las elecciones estadounidenses de 2016, el gusano Stuxnet que retrasó durante años el programa nuclear iraní, el caso del ataque de denegación de servicio contra Estonia en 2007 o el caso del software antivirus de Kaspersky que, según los gobiernos de Estados Unidos e Israel ha estado escaneando los ordenadores de la Administración americana en busca de programas clasificados del gobierno.

15.1.3 Actividades de acabado.

Durante el desarrollo de las actividades de acabado se realizará un resumen de lo más importante de cada sesión, se resolverán las dudas que pudieran existir, se obtendrán conclusiones y se realizará un ejercicio para que el alumno averigüe si su cuenta de correo ha sido *hackeada*.

15.2 Sesión 2.

15.2.1 Actividades de inicio.

Breve explicación sobre la importancia de clasificar bien el código dañino por su función, por su originador o por su finalidad, su evolución a lo largo de la historia y las buenas prácticas para evitar una infección por malware.

15.2.2 Actividades de desarrollo.

Continuaremos describiendo el tipo de malware según su clasificación y pasando a definir los conceptos de virus, gusanos, troyanos, puertas traseras, bombas lógicas, hoaxes, phising, rogue software y adware.

Además, se describirán otros tipos de software dañino como son: sniffer de red, rootkit, spam, spyware, cookies, keyloggers, ransomware y jokes.

Describiremos muchas de las buenas prácticas a realizar tanto para los usuarios como para los administradores de sistemas y redes, así como las estrategias de respuesta y recuperación.

15.2.3 Actividades de acabado.

Durante el desarrollo de las actividades de acabado se realizará un resumen de lo más importante de la sesión, se resolverán las dudas que pudieran existir, se obtendrán conclusiones y se realizará un ejercicio sobre cómo actuar ante un ataque de ransomware a nuestra organización.

15.3 Sesión 3.

15.3.1 Actividades de inicio.

Concienciación de los alumnos comenzando con las palabras del responsable del Mando Europeo de los Estados Unidos para asuntos de ciberseguridad en las que afirmaba que *"La próxima guerra puede desencadenarse desde un Starbucks*". Puede ser una exageración, pero lo cierto es que los estados han tomado conciencia de que la ciberseguridad es uno de los grandes retos de este siglo y requiere de Instituciones fuertes que lideren la defensa de un ciberespacio libre, seguro y predecible.

15.3.2 Actividades de desarrollo.

Continuaremos describiendo las entidades nacionales e internacionales de referencia encargadas del desarrollo de la ciberseguridad:

- **Instituto Nacional de Ciberseguridad (INCIBE)**. Dependiente del Ministerio de Economía y Empresa.
- **CCN-CERT**. Es el CERT dependiente del Centro Criptológico Nacional.
- **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC).** Dependiente del Ministerio del Interior.
- **Mando Conjunto de Ciberdefensa (MCCD)**, dependiente del Jefe de Estado Mayor de Defensa.
- **Centro de Excelencia de la OTAN para la Ciberdefensa (NATO CCD COE)**, con sede en Tallin, Estonia.
- **Centro Europeo de Ciberdelincuencia (EC3)**.
- **National Security Agency (NSA).**

15.3.3 Actividades de acabado.

Durante el desarrollo de las actividades de acabado se realizará un resumen de lo más importante de la sesión, se resolverán las dudas que pudieran existir, se obtendrán conclusiones y se realizará una puesta en común en la que los alumnos propondrán bajo la responsabilidad de qué autoridad estarían varios casos propuestos por el profesor.

15.4 Sesión 4.

15.4.1 Actividades de inicio.

Breve explicación sobre la importancia de conocer el mapa de las ciberleyes y la legislación sobre el cibercrimen en todo el mundo.

15.4.2 Actividades de desarrollo.

Continuaremos describiendo los organismos generadores de normativa sobre ciberdefensa en el ámbito nacional y de la OTAN. Veremos en detalle el Tallin Manual y la Carta de las naciones Unidas.

15.4.3 Actividades de acabado.

Durante el desarrollo de las actividades de acabado se realizará un resumen de lo más importante de la sesión, se resolverán las dudas que pudieran existir, se obtendrán conclusiones y se realizará un ejercicio en el que se analizará cuál es la normativa nacional, dentro de la variada panoplia de elementos, que nos afecta como Ejército del Aire.

16. RECURSOS DIDÁCTICOS.

16.1 Recursos metodológicos.

16.1.1 Estrategia expositiva

En las sesiones de teoría se fomentará el aprendizaje significativo utilizando para ello la técnica de la exposición oral, intentando motivar al alumno para despertar su interés por la materia. Durante las mismas se podrán hacer preguntas o incluso el profesor expondrá casos o ejemplos de casos reales ocurridos en los últimos años para despertar la curiosidad de los alumnos.

En la primera sesión se expondrán los ataques más dañinos ocurridos tanto en el mundo como en España.

Las siguientes sesiones se dedicarán a explicar los tipos de malware, los consejos de seguridad para protegernos de ataques y la legislación relativa al respecto.

Antes de la finalización de cada sesión se hará una recapitulación de los conceptos más importantes de la materia expuesta resolviendo las dudas que pudiera haber y que no hubiesen sido resueltas durante el transcurso de ésta.

16.1.2 Estrategia indagatoria

Este tipo de estrategia fomentará la participación de los alumnos ya que se utilizarán técnicas de aprendizaje basado en problemas, estudio de casos y simulaciones.

Para ello se propondrá a los alumnos distintas situaciones reales en el campo de la ciberseguridad, debiendo tomar una decisión acertada, razonando el proceso y justificando el mismo.

Además, según avanza la clase, se añaden preguntas de repaso que el docente pregunta individualmente, con el objetivo de apreciar el seguimiento que todos los alumnos van haciendo de la materia.

16.2 Recursos personales.

- Profesores titulares del Departamento de Tecnologías de la Información y las Comunicaciones Militares, de la EMACOT.
- Sargentos Alumnos que estén en su periodo de Formación Militar para alcanzar el empleo de Sargento y, que sean designados por la Dirección de Enseñanza.
- Personal de apoyo de la Secretaría de Estudios de la EMACOT encargado de temas administrativos.

16.3 Recursos materiales

- Pizarra blanca, rotuladores de colores y borrador.
- Pizarra electrónica.
- Ordenador con video proyector con las aplicaciones *PowerPoint* y *pdf reader.*
- Listas de control (cheklist).
- Documento base de la asignatura y apuntes recopilados por el Departamento TICM.

17. EVALUACIÓN

17.1 Evaluación inicial.

Se realizarán preguntas orales sobre los conocimientos previos de los alumnos sobre la materia a tratar, los estudios académicos que poseen, así como los cargos que ha desempeñado anteriormente y en qué Unidades del Ministerio de Defensa o empresas privadas civiles han ejercido sus cometidos.

Dos son los objetivos de esta evaluación inicial, por un lado, le sirven al docente para establecer unas estrategias que le sirvan para llegar a un determinado resultado y, por otro lado, también es útil para que el alumno tome conciencia de sus conocimientos previos.

17.2 Evaluación formativa.

Durante el desarrollo de los contenidos, se recogerá información a través de la observación a los alumnos en el aula, se realizarán preguntas de repaso y se obtendrá información sobre la resolución de los casos prácticos que se les proponga.

Se observará si el alumno es capaz de aplicar en cada caso las salvaguardas y consejos de seguridad que las adecuadas fuentes de conocimiento recomiendan, para los diversos tipos de ataque cibernético a los que puede estar sometida la organización.

Tal y como se señaló en el punto 6, tenemos dos recursos basados en las tecnologías para esta evaluación:

1. Por un lado, durante el transcurso de la clase se intentará que los alumnos encuentren la respuesta a ciertas preguntas propuestas por el profesor. Esto requerirá de cierta “indagación en la web”. Para ello se les permitirá usar los móviles o cualquier otro dispositivo que permita realizar búsquedas en la web.

2. La segunda opción se trata de la aplicación *Mentimeter* y, dentro de las diversas herramientas que propone la aplicación, el *Muro Colaborativo* me parece la más original y útil para estimular al público y atraer la atención de los alumnos en clase. Esta herramienta consiste en preparar una nube de palabras

con alguna pregunta inicial. Cada una de las respuestas de los participantes (lo ideal es limitar a 3 palabras para cada uno), se van poniendo en pantalla y las palabras se van haciendo más grandes dependiendo del número de veces que se repitan. De ese modo, se percibe al instante y de una forma muy visual, el grado de implicación y de comprensión de las materias tratadas por parte de los alumnos.

Esta evaluación está orientada a valorar el avance en los aprendizajes y a mejorar la enseñanza, regulando el proceso de aprendizaje, adaptándolo y modificando lo planeado si fuera necesario.

17.3 Evaluación sumativa.

Se realizará para determinar el nivel de aprendizaje alcanzado por el alumno, así como para obtener información sobre el nivel de logro en un contenido de aprendizaje concreto.

Esta evaluación sumativa se transformará en una calificación que resultará un punto de referencia para el alumno y no se realizará únicamente sobre esta Unidad Didáctica, sino que abarcará todos los conocimientos adquiridos en el conjunto de las Unidades Didácticas que componen el módulo.

Tal y como se señaló en el punto 7.1, la calificación final del alumno abarcará el total del módulo y vendrá dada en un 90% por la **coevaluación**, que será llevada a cabo por compañeros (*evaluación entre iguales*) y profesorado (*heteroevaluación*), los cuales evaluarán las exposiciones de los alumnos durante los tres últimos días y en un 10% mediante la medición de la participación en clase, fruto de la respuesta que vayan dando los alumnos a las preguntas y problemas planteados por el profesor durante sus 11 clases teóricas.

Las amenazas a las que nos enfrentamos en el mundo de la ciberseguridad son, a menudo, imprevisibles o inevitables, de modo que las únicas protecciones posibles son la experiencia y el estudio de casos de interés. Así, en las exposiciones de los alumnos, éstos deberán relacionar lo aprendido en clase, con la información disponible en repositorios oficiales, con la señalada en la bibliografía y con cualquiera otra que les permita relacionar conceptos y establecer conexiones entre los distintos agentes implicados en la seguridad del ciberespacio.

Podemos ver la rúbrica de evaluación en el Anexo I.

Además, el trabajo de investigación, extracción de información y exposición, permitirá al alumno alcanzar las Competencias Generales 3 y 22; "*Potenciar adecuadamente la capacidad de aprendizaje, análisis y síntesis para construir conocimiento"* e *"Interpretar adecuadamente documentos profesionales operativos, para ordenar con claridad y precisión y ejecutar las órdenes que reciba con prontitud y habilidad"*.

17.4 Autoevaluación del profesor.

La evaluación continua mediante preguntas y ejercicios en el aula es un tema importante para informar de los aprendizajes de los estudiantes, pero es el eje fundamental para que el docente pueda recapacitar respecto de su propuesta de enseñanza.

Esa tarea inquisitoria diaria es un método privilegiado para crear consideraciones de valor respecto a la metodología y los procesos de enseñanza-aprendizaje del docente.

Además, si consideramos la tarea del aula como un proyecto, este requerirá ser evaluado y, en su caso, retroalimentado y modificado.

La metodología para la evaluación del profesorado consiste, acorde a lo señalado en las Normas del Director de Curso de la EMACOT, en la realización de 2 cuestionarios de satisfacción al finalizar el curso:

1. Cuestionario del Gabinete de Orientación Educativa sobre la calidad del profesorado.

2. Cuestionario del Director de Curso sobre las asignaturas, conferencias y prácticas, en cuanto a su duración, interés, calidad, contenido, etc.

Finalmente, antes de los 15 días posteriores a la finalización del curso, se reunirá la Junta de Evaluación del mismo, en la que se discutirán y se harán públicos los resultados de las encuestas. Posteriormente, se levantará un Acta de la misma y se comunicará el resultado a los implicados.

17.5 Autoevaluación del alumno.

La observación y el diálogo entre el profesor y los alumnos serán las técnicas más usadas y comunes para llevar a cabo la autoevaluación del alumno.

Este diálogo y las preguntas diarias y constantes que se realizan en el aula, pondrán de manifiesto el nivel alcanzado por los alumnos y llevará a éstos a ser conscientes de lo que se les exige, animándolos a reflexionar sobre su grado de asimilación de la materia y tomar acción sobre ello, solicitando algún tipo de refuerzo o la aclaración de conceptos que ellos mismos han visto que deberían haber alcanzado y no lo han hecho.

ANEXO 1

Tabla 1. Rúbrica de la coevaluación.

	Excelente (10)	Bien (7)	Regular (4)	Mal (1)	Peso
Tamaño de la presentación Nº de transparencias	10	9 ó 11	8 ó 12	7 ó 13	10%
Duración de la presentación Minutos	15	14 ó 16	13 ó 17	12 ó 18	10%
Dominio del tema El alumno ha buscado información, la conoce y la ha procesado	Demuestra un excelente conocimiento del tema.	Demuestra un buen conocimiento del tema.	No parece conocer muy bien el tema.	No conoce el tema.	20%
Enfoque pedagógico Capacidad comunicativa	El discurso está muy bien preparado y estructurado. Las ideas que expone son precisas y están bien fundamentadas. Se expresa con corrección, naturalidad y seguridad. El registro se adapta completamente a la situación comunicativa.	El discurso está bien estructurado. Expone las ideas de forma clara y ordenada. Se expresa con de forma tranquila y correcta. El grado de formalidad es el adecuado.	La estructura del discurso no es adecuada a la situación comunicativa. Algunas ideas no acaban de quedar claras. A pesar de un cierto nerviosismo, su expresión es aceptable.	El discurso no está bien estructurado. Expone las ideas de forma confusa. Se expresa con nerviosismo y se bloquea.	20%

Gestión del conocimiento Uso de palabras clave	Utiliza palabras clave que resumen de forma clara y directa la información. La composición de palabras clave en la presentación permite con claridad realizar asociaciones.	Utiliza palabras clave, destacando algunos conceptos e ideas relevantes, pero en el contexto de la presentación no se asocian con claridad a ciertos contenidos significativos.	Utiliza de forma poco significativa palabras clave, asociando algunas ideas secundarias y poco significativas. No están contextualizadas en la infografía.	No utiliza palabras clave de forma idónea.	20%
Diseño Uso de imágenes y elección de formato	Utiliza como estímulo visual imágenes para representar los conceptos. El uso de colores contribuye a asociar y poner énfasis en los conceptos	Utiliza como estímulo visual imágenes para representar los conceptos, pero no se hace uso de colores para establecer asociaciones o enfatizar.	No se hace uso de colores y el número de imágenes es reducido.	No se utilizan imágenes ni colores para representar y asociar los conceptos.	20%

ANEXO 2

- **Caso 1: Análisis del caso Snowden**
    1. Recopilación y análisis de antecedentes.
    2. Estimación de los daños causados a los EEUU por el “Caso Snowden”
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas por el “Caso Snowden? PRISM.
    4. Situación actual y estimación de la evolución probable del “Caso Snowden”.
- **Caso 2: Análisis del caso Assange**
    1. Recopilación y análisis de antecedentes de Julián Assange y de Wikileaks
    2. Estimación de los daños causados por Wikileaks ¿Afectados por Wikileaks?
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo que evidenció Wikileaks?
    4. Situación actual y estimación de la evolución probable de la situación de Julián Assange
- **Caso 3: Análisis de los ciberataques a la infraestructura crítica tecno informacional en Estonia (2007)**
    1. Recopilación y análisis de antecedentes.
    2. Estimación de los daños causados.
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas?
    4. Situación actual y estimación de la evolución probable de la situación.
- **Caso 4: Evaluación de la viabilidad de adaptación del Tallin Manual a España**

1. Recopilación de antecedentes del Tallin Manual (versión actual).
2. Análisis de los puntos de vista del líder del equipo que elaboró el Tallin Manual (versión actual), Profesor Michael N. Schmitt (análisis de los videos generados por el CCDCOE al respecto)
3. Coincidencias y divergencias entre el Tallin Manual (versión actual) y la letra y el espíritu del Artículo 51 de la Carta de las Naciones Unidas.
4. Coincidencias y divergencias entre el Tallin Manual y la doctrina vigente en la Región en los aspectos correspondientes del Derecho Internacional Público.

- **Caso 5: Análisis de los ciberataques en Georgia (2008), conocidos por ser el primer caso en el que las operaciones cibernéticas fueron iniciadas dos meses antes y luego conducidas conjuntamente con operaciones militares armadas**
    1. Recopilación y análisis de antecedentes.
    2. Estimación de los daños causados.
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas?
    4. Situación actual y estimación de la evolución probable de la guerra cibernética llevada a cabo por gobiernos.
- **Caso 6: Análisis del virus Stuxnet (2010) que afectó al programa nuclear iraní**
    1. Recopilación y análisis de antecedentes.
    2. Estimación de los daños causados.
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas?
    4. Situación actual y estimación de la evolución probable de la guerra cibernética llevada a cabo por gobiernos.
- **Caso 7: Análisis del ransomware Wannacry.**
    1. Recopilación y análisis de antecedentes.

2. Estimación de los daños causados.
3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas?
4. ¿Cómo se infecta un ordenador y como se extiende el malware? ¿Todavía persiste la amenaza?

- **Caso 8: Análisis del ataque masivo a Yahoo, que afectó a 3.000 millones de cuentas**
    1. Recopilación y análisis de antecedentes.
    2. Estimación de los daños causados.
    3. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas?
- **Caso 9: VPN**
    1. ¿Qué es y para qué sirve?
    2. Oferta y ejemplos.
    3. Ventajas e inconvenientes.
        a. ¿Qué información es monitoreada o registrada por la VPN?
        b. ¿Puedo elegir la ubicación del servidor?
        c. ¿Puedo usar la VPN para compartir de punto a punto?
- **Caso 10: PGP**
    1. Recopilación y análisis de antecedentes.
    2. Que es PGP:
        a. ¿Cómo funciona PGP?
        b. ¿Cómo obtengo una clave PGP?
        c. ¿Por qué se usa PGP?
    3. Interfaces
- **Caso 11: Máquina enigma**
    1. Recopilación y análisis de antecedentes.

2. Las matemáticas detrás de la máquina enigma.
3. El descifrado de la máquina enigma.

- **Caso 12: Cifrado simétrico DES.**
    1. Recopilación y análisis de antecedentes.
    2. Las matemáticas detrás del cifrado simétrico DES.
    3. Ataques.
- **Caso 13: Cifrado simétrico AES.**
    1. Recopilación y análisis de antecedentes.
    2. Las matemáticas detrás del cifrado simétrico AES.
    3. Ataques.
- **Caso 14: Cifrado asimétrico RSA.**
    1. Recopilación y análisis de antecedentes.
    2. Las matemáticas detrás del cifrado simétrico RSA.
    3. Ataques.